Mieux adapter le droit aux défis posés à l'Etat de droit par le numérique – Analyse du cas particulier de la France

Auteur : **Patrice Cardot**

Ayant à faire face à des démocraties qui agonisent, à des administrations qui se délitent, à des gouvernances qui se détériorent, à une méfiance qui s'installe parmi les citoyens et à un pouvoir qui perd du sens, les Etats, à l'instar de la France, cherchent à tirer parti du numérique et de l'intelligence artificielle pour proposer des pistes nouvelles pour un projet de gouvernance doté de nouvelles légitimités et de nouveaux outils d'efficience porteurs d'une autre culture de service public, d'intérêt général et de gestion du bien public.

Des initiatives de gouvernement ouvert, souvent désigné comme l'e-gouvernement, l'administration numérique ou la démocratie 2.0[1], visent à rétablir le lien entre les citoyens, les élus et les fonctionnaires en augmentant la transparence des projets et des initiatives en même temps que les possibilités de collaboration *'top-down'* et *'bottom-up'* avec le plus grand nombre lors de leur concrétisation, les citoyens 'connectés' se trouvant dès lors en capacité de partager à titre individuel ou collectif leur vision de la société et de débattre des choix politiques dans des fora électroniques en ligne ou encore de surveiller l'intégrité des institutions démocratiques et la qualité des services publics.

Prenant appui sur les développements d'une étude plus ancienne portant sur le même thème[2], et mise à jour continuellement, la présente contribution propose une exploration des processus de transformation numérique qui opèrent aujourd'hui en France, une analyse des inquiétudes qu'ils soulèvent et un questionnement sur la nature démocratique de l'Etat de droit 2.0.

Y sont également formulées de nombreuses recommandations quant aux opportunités à saisir et aux initiatives à entreprendre aux niveaux international, européen et national, pour redonner force et crédibilité à cet Etat de droit 2.0.

[1] *Vers une démocratie 2.0 ? :* https://digital-society-forum.orange.com/fr/les-forums/901-vers-une-democratie-20

[2] *De l'adaptation de l'Etat de droit aux défis du numérique – Analyse du cas particulier de la France* – Patrice Cardot (Collection Carte blanche - Entremises Editions - ISBN 978-2-38255-023-6)

La transformation numérique à l'œuvre en France

La France, qui souffre de difficultés considérables sur le registre de la médiation entre citoyens et administration [3] est devenue en 2014 la première nation européenne en matière d'administration numérique. Elle entend accélérer sa transformation pour simplifier encore davantage les démarches des particuliers et des entreprises grâce à Internet, et rendre les services publics plus efficaces et plus réactifs.

Pas à pas, l'administration avance vers un service public 100 % dématérialisé, comme le veut le programme Action publique 2022 (*cf.* les différentes initiatives publiques développées au niveau de l'Etat central[4,5,6], et celles développées autour du numérique au service des territoires[7] ou autour de *l'open data*[8]).

Aux quatre coins du territoire, le recours à la dématérialisation numérique est devenu l'alpha et l'oméga de tout projet de modernisation au coeur de la puissance publique (bien au-delà de l'Etat central), des laboratoires d'innovation ou des démarches qui s'en approchent qui ambitionnent de repenser l'action publique fleurissent : ce que ceux-ci font vraiment, pour qui et comment reste parfois un mystère ... Des *Legal-tech*[9] apparaissent ... Les technologies et les services qui se développent autour du protocole novateur de la blockchain émergent à un rythme effréné.

Le Gouvernement s'est engagé, lors du 3e comité interministériel de la transformation publique (CITP) à ce que, en 2022, 250 démarches administratives « phares » soient accessibles en ligne pour les citoyens, avec un haut niveau de qualité[10].

Pour tenir cet objectif, la direction interministérielle du numérique (DINUM[11]) a lancé un observatoire de la qualité des services numériques[12], ainsi qu'un dispositif pour recueillir la satisfaction des usagers.

Ces deux outils permettront d'identifier les pistes d'amélioration prioritaires[13,14].

L'État est devenu, en France, le premier producteur de données et, progressivement, avec l'*open data*, d'immenses quantités de données de qualité vont être mises à disposition du public.

Les Français plébiscitent cette numérisation des services publics comme le montrent les chiffres d'accès à FranceConnect + : en quatre ans, le nombre d'usagers est passé de 500 000 à 28 millions. Trente millions de visiteurs étaient attendus pour la fin 2021.

---

[3] *Cf.* le rapport de France Stratégie intitulé *Médiation accomplie ? Discours et pratiques de la médiation entre citoyens et administrations* : https://www.strategie.gouv.fr/publications/mediation-accomplie-discours-pratiques-de-mediation-entre-citoyens-administrations

[4] *Le numérique : instrument de la transformation de l'État :* https://www.gouvernement.fr/action/le-numerique-instrument-de-la-transformation-de-l-etat

[5] *La direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) :* https://www.numerique.gouv.fr/dinum/

[6] *franceconnect.gouv.fr :* https://franceconnect.gouv.fr/

[7] *Administration numérique : un nouveau programme DCANT 2018-2020 :* https://www.lagazettedescommunes.com/541855/administration-numerique-un-nouveau-programme-dcant-2018-2020/

[8] www.lebigdata.fr/open-data-definition

[9] *Cf.* http://legal-tech.fr/legaltech

[10] *13e édition du panorama des grands projets numériques de l'État :* https://www.numerique.gouv.fr/actualites/decouvrez-la-13e-edition-du-panorama-des-grands-projets-numeriques-etat/

[11] *Direction interministérielle du numérique* : https://www.numerique.gouv.fr/dinum/

[12] *0bservatoire de la qualité des services numériques :* https://observatoire.numerique.gouv.fr/observatoire/

[13] *Qualité des services numériques : deux nouveaux outils pour suivre l'avancée de la dématérialisation et recueillir l'avis des usagers :* https://www.numerique.gouv.fr/actualites/qualite-des-services-numeriques-deux-nouveaux-outils-pour-suivre-lavancee-de-la-dematerialisation-et-recueillir-lavis-des-usagers/

[14] *Observatoire de la dématérialisation de qualité : tableau de bord des démarches phares de l'État :* https://www.data.gouv.fr/es/datasets/observatoire-de-la-dematerialisation-de-qualite-tableau-de-bord-des-demarches-phares-de-letat/

Il convient de ne pas succomber à un angélisme de mauvais aloi en se félicitant d'un tel dynamisme public sur un registre de cette nature, ne serait-ce que parce que, lorsqu'elles ont été engagées, les expérimentations, leur évaluation comme les études d'impact qui s'y rapportent semblent parfois entreprises dans la précipitation et avec une approche insuffisamment systémique. Car, selon France Stratégie, une part importante de la population française est concernée par l'*illectronisme* (parce qu'ils ne sont pas équipés de smartphone, tablette ou ordinateur, ne les maîtrisent pas, ou ne disposent pas d'accès Internet). Et un Français sur cinq a déjà abandonné avant la fin une démarche administrative entreprise en ligne.

Au début du quinquennat, *le président de la République annonçait un Plan 'France Très Haut Débit'* visant à couvrir l'intégralité du territoire en très haut débit, mais également à garantir un accès au bon haut débit pour tous dès 2022. Présentes dans les 15 réformes clés du mandat d'Emmanuel Macron, *« l'e-inclusion »* prévoyait d'empêcher le décrochage de certains territoires français, en formant plus de 3 millions de personnes au numérique. Selon les chiffres d'une enquête de UFC Que-Choisir, nous en sommes encore loin.

Cette situation est également relevée par la Commission européenne qui procède au suivi de l'état d'avancement de l'Europe numérique au sein de ses Etats-membres[15,16].

Pour agir contre l'incapacité à utiliser des appareils numériques, l'État privilégie la formation, à la fois des aidants numériques, et des citoyens.[17]

Si les efforts que l'Etat consacre à la réduction de la fracture numérique de premier niveau (l'accès) sont considérables et doivent être salués, il n'en demeure pas moins sa relative impuissance devant les fractures numériques de deuxième (les usages) et troisième (l'intelligence artificielle) niveaux.

Une sociologue du numérique, Eszter Hargittai, montra en 2020 qu'il existait aussi une fracture de 2ème niveau : celle des usages. En effet, à travers différentes expérimentations, elle observa que certaines parties de la population n'avaient pas ou trop peu de compétences pour utiliser Internet et remplir certaines tâches en ligne. C'est encore aujourd'hui le cas des populations les plus âgées qui n'ont pas acquis suffisamment de « culture numérique » pour être apte à utiliser correctement les services publics en ligne. Par ailleurs, une fracture plus sournoise est en train d'apparaître car elle touche une grande majorité de la population sans une réelle prise de conscience de sa part. À l'origine de cette fracture ; le « big data » (les grandes masses de données) accompagné des algorithmes qui traitent ces données permettant à une intelligence artificielle de les transformer en actions, en prise de décisions parfois à la place de l'utilisateur. Cette fracture de 3ème niveau est celle de l'intelligence artificielle (IA). Paradoxalement, dans un monde où l'information devient pléthorique, cette fracture est marquée par une méconnaissance du fonctionnement de cette IA, de ses algorithmes et de l'écosystème qui l'environne.[18]

D'après l'OCDE, 32 % des emplois sont amenés à être profondément transformés par l'automatisation. Rappelant la nécessité de sensibiliser les travailleurs à l'utilisation des algorithmes, Salima Benhamou, économiste à France Stratégie, souligne que le salarié « *a besoin de comprendre comment s'élabore une donnée et comment elle s'inscrit dans le processus ; sinon, la data ne sert à rien* ».

---

[15] *Cf.* https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/les-rapports-de-la-commission-europeenne-sur-letat-davancement-de-leurope-numerique.html

[16] *DESI country profile* : https://ec.europa.eu/digital-single-market/en/scoreboard/france

[17] *Comment agir contre l'illectronisme :* https://www.gouvernement.fr/comment-agir-contre-l-illectronisme

[18] *Cf.* Fabrice Le Guel *in accès, usages, intelligence artificielle, les trois fractures numériques :* https://theconversation.com/en-images-acces-usages-intelligence-artificielle-les-trois-fractures-numeriques-171191

La simplification administrative pour les entreprises franchira une nouvelle étape en 2022, avec la refonte de plusieurs services en ligne dédiés aux professionnels. Trois nouveaux sites seront mis en ligne par le gouvernement.

Entreprendre.service-public.fr sera le centre d'information et d'orientation pour les créateurs et les chefs d'entreprise. La nouvelle version de *formalites.entreprises.gouv.fr* fera office de guichet unique pour l'ensemble des formalités d'immatriculation, de modification ou de cessation d'activité, et pour déposer ses comptes. Elle regroupera les ressources d'une dizaine de sites différents, gérés notamment par les Centres de Formalités des Entreprises (CFE), auxquels le nouveau site se substituera dès le 1er janvier 2023.

Enfin, *portailpro.gouv.fr* permettra de déclarer et payer les sommes dues à l'Urssaf, aux impôts et à la Douane, et d'effectuer les démarches fiscales et sociales à l'aide d'un identifiant unique. Le site affichera une synthèse de la situation de l'entreprise sous forme de tableau de bord, et proposera également une messagerie sécurisée avec les services publics concernés.

Le gouvernement s'est fixé comme objectif de former au moins 3 700 étudiants spécialistes de l'IA d'ici à 2025.

Le ministère du travail s'est associé à l'Institut national de recherche en sciences et technologies du numérique (Inria) pour mettre au point un programme de recherche Le 19 novembre 2021 a été annoncé le lancement de « LaborIA », un laboratoire destiné à mesurer l'impact de l'intelligence artificielle sur l'emploi et les conditions de travail. Prévu sur cinq ans, le projet est mené par l'institut Matrice, un incubateur et un centre de formation autour des nouvelles technologies.

S'agissant de l'éducation, l'expérience du confinement lors de la crise pandémique de la Covid-19 a eu le mérite d'induire un changement d'échelle dans l'appropriation que les enseignants et leurs élèves ont réalisée du numérique. Pour autant, ce recours contraint aux techniques numériques a également fait apparaître à tous de nombreuses déficiences que les Etats généraux du numérique[19], organisés en novembre 2020 par la Direction du numérique pour l'Éducation (DNE), ont relevées. En particulier, les compétences numériques des jeunes, essentiellement acquises par l'expérience, ne correspondent pas toujours à celles requises pour une utilisation scolaire.

Deux problèmes de formation des jeunes au numérique sont ainsi mis en évidence, aussi importants l'un que l'autre. Le premier concerne l'éducation citoyenne au numérique et le deuxième, plus circonscrit, la formation aux compétences numériques mobilisées à l'École. Pour remédier à cette situation, le gouvernement a pris un certain nombre de mesures phares applicables dès la rentrée 2021.[20]

En particulier, la CNIL, le CSA, le Défenseur des droits et l'HADOPI ont créé un kit pédagogique, qui regroupe l'ensemble des ressources conçues pour l'éducation du citoyen numérique, à destination des formateurs et des parents qui accompagnent les jeunes en matière de numérique.[21]

Mais les choses bougent dans un sens favorable comme l'indiquent de manière très claire les résultats du sondage effectué en mai 2021 auprès d'un panel représentatif des seniors[22].

[19] *Etats généraux du numérique :* https://www.education.gouv.fr/les-etats-generaux-du-numerique-pour-l-education-304117

[20] *Vers une généralisation du numérique à l'École :* https://www.education.gouv.fr/l-utilisation-du-numerique-l-ecole-12074

[21] *Kit pédagogique sur le numérique :* https://www.defenseurdesdroits.fr/fr/guides/kit-pedagogique-du-citoyen-numerique

[22] *Cf.* https://www.actuia.com/actualite/silver-valley-a-realise-une-etude-autour-des-usages-du-numerique-chez-les-personnes-de-60-ans-et-plus/

Dans le détail de leurs compétences, ils sont 97% à déclarer savoir envoyer un mail, 94% savent faire une recherche avec un moteur et 88% indiquent suivre une visioconférence depuis son ordinateur ou son smartphone.

En revanche, seuls 40% des répondants disent savoir gérer un ou plusieurs réseaux sociaux. Côté matériel, les plus de 60 ans ont un taux d'équipement et d'usage assez élevé puisque 35% des répondants déclarent posséder le trio ordinateur, tablette et smartphone. Ils sont également 35% à déclarer avoir un ordinateur et un smartphone.

Selon Nicolas Menet, Directeur Général de Silver Valley : *« Les seniors de façon globale sont 74% en France à avoir accès à Internet depuis une box, ce qui ne veut pas dire qu'ils l'utilisent au quotidien mais il y a une très forte pénétration du numérique dans la population des personnes de plus de 60 ans. Aujourd'hui, il y a quatre millions d'exclus du numérique selon une étude de 2019 de l'Institut CSA et des Petits Frères des Pauvres, mais sur 16 millions de personnes de plus de 60 ans, il y a à peu près 12 millions de personnes qui sont plutôt connectées, plutôt à l'aise avec le numérique et friandes d'en apprendre plus. Plus on avance dans le temps, plus la fracture numérique qu'on disait être liée à l'âge, autour de 75 ans, devient sociale et territoriale »*

A la demande de la commission des finances du Sénat, trois ans après le début de sa mise en œuvre, la Cour des Comptes a établi un premier bilan de cette nouvelle approche de politique publique destinée à réduire la fracture numérique, ambition rendue plus essentielle encore par la crise sanitaire qui a confirmé le caractère crucial d'un accès de qualité sur tout le territoire au très haut débit mobile pour la vie économique, culturelle, éducative, sanitaire et sociale. Au terme de son enquête, la Cour formule neuf recommandations pour assurer la réussite du *« New Deal »* mobile et répondre plus largement aux défis de l'aménagement numérique mobile du territoire.[23]

[23] *Réduire la fracture numérique mobile : le pari du « New Deal » 4G :* https://www.vie-publique.fr/sites/default/files/rapport/pdf/281680.pdf

De nombreuses sources d'inquiétude nourrissent des réserves à l'égard de l'action de l'Etat sur le registre numérique

La crise du Covid-19 a été l'occasion pour l'Etat d'accélérer et d'amplifier le recours aux technologies numériques dans sa gestion des différents volets de son intervention au profit des populations[24], soulevant alors de nombreuses interrogations et craintes quant aux risques encourus par un usage aussi systématisé, dans un contexte d'état d'exception suspecté de favoriser l'émergence de comportements erratiques en regard des valeurs et principes démocratiques les plus fondamentaux.

S'agissant de l'adaptation du droit et de l'Etat de droit aux nouveaux défis posés à la démocratie par l'avènement tous azimuts de la donnée dans l'espace public comme dans l'espace privé, les initiatives ont longtemps été engagées à droit constant, l'Etat agissant fréquemment comme s'il partait du principe erroné que le numérique ne bouleversait pas les règles générales du droit.

En 2016, une loi pour une République numérique *(République 2.0)* a été élaborée puis promulguée, donnant à penser que l'Etat de droit s'était adapté par la loi aux défis posés à la République par sa transformation numérique.

Or, cela n'est pas le cas. Et les voies de recours se sont souvent révélées inadaptées.

Parmi les principales sources d'inquiétude qui émergent à l'égard de l'action de l'Etat figure la persistance de nombreuses défaillances et vulnérabilités au cœur même de ses propres institutions.

- *La République s'organise pour protéger la nation et le citoyen contre les dérives et les risques potentiels ou avérés du numérique.*

En 2017, faisant suite à deux précédentes études, la première en 1998 intitulée *'Internet et les réseaux numériques'* et la deuxième sur *'Le numérique et les droits fondamentaux'* en 2014[25], le Conseil d'État a décidé en 2017 de poursuivre sa réflexion sur l'évolution des politiques publiques du numérique, en s'attachant cette fois-ci à l'ébranlement des économies et des modèles sociaux traditionnels qui est en cours.[26]

Son étude annuelle de 2014, en proposant 50 propositions du Conseil d'État pour mettre le numérique au service des droits individuels et de l'intérêt général, apporta une analyse approfondie des principaux enjeux soulevés par la future loi sur le numérique : Comment repenser concrètement la protection des droits fondamentaux face à la révolution numérique ? Comment renforcer le pouvoir des individus face à l'utilisation de leurs données ? Comment repenser la place et le rôle des autorités publiques ? Comment, enfin, en matière de droit international, trouver le bon équilibre entre le principe du "pays de l'internaute" et le principe du "pays du site internet" ?

A - Repenser les principes fondant la protection des droits fondamentaux (propositions 1 à 3) :

[24] Pour équiper les agents publics, 160 000 ordinateurs portables ont ainsi été commandés depuis mars 2020 (contre 40 000 en moyenne chaque année), le gouvernement souhaitant que tous les agents ayant des fonctions télétravaillables soient équipés avant la fin de l'année 2021.

[25] *Etude annuelle 2014 – Le numérique et les droits fondamentaux :* https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux

[26] *Etude annuelle 2017 - Puissance publique et plateformes numériques : accompagner l'« ubérisation » :* https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2017-puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation

- Renforcer la place de l'individu dans le droit à la protection de ses données (*« autodétermination informationnelle »)* pour lui permettre de décider de la communication et de l'utilisation de ses données à caractère personnel ;
- Consacrer le principe de neutralité du net, garantie fondamentale des libertés d'expression, de la liberté d'entreprendre et de la liberté d'association (permettre à toute entreprise, toute association ou tout particulier de bénéficier d'un égal accès à tous les internautes) ;
- Créer une nouvelle catégorie juridique pour les « plateformes » (distincte à la fois des éditeurs et des hébergeurs) qui proposent des services de classement ou de référencement de contenus, biens ou services mis en ligne par des tiers ; les soumettre à une obligation de loyauté envers leurs utilisateurs (les non professionnels dans le cadre du droit de la consommation et les professionnels dans le cadre du droit de la concurrence.

B - Renforcer les pouvoirs des individus et de leurs groupements (propositions 4 à 11) :

- Donner à la CNIL et à l'ensemble des autorités de protection des données européennes une mission explicite de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation des données à caractère personnel ;
- Mettre en œuvre de manière efficace le droit au déréférencement (reconnu par la Cour de Justice de l'Union Européenne dans son arrêt *Google Spain* du 13 mai 2014) ;
- Définir les obligations des plateformes envers leurs utilisateurs qui découlent du principe de loyauté ;
- Créer une action collective destinée à faire cesser les violations de la législation sur les données personnelles.

C - Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques (proposition 12 à 30) :

- L'intervention publique doit assurer la sécurisation juridique des usages des données et un encadrement plus étroit des traitements présentant les risques les plus importants ;
- Afin de sécuriser le développement du Big Data en Europe, maintenir sans ambiguïté dans la proposition de règlement européen la liberté de réutilisation statistique des données personnelles, sous réserve que cette réutilisation soit entourée de garanties d'anonymat appropriées ;
- Définir un droit des algorithmes prédictifs ;
- Revoir les modalités du contrôle de la concentration dans les médias afin de mieux garantir le pluralisme au regard de l'ensemble des modes de diffusion contemporains ;
- Développer la médiation pour régler les litiges liés à l'utilisation des technologies numériques.

D - Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques (propositions 32 à 42) :

- Poursuivre l'ouverture des données publiques tout en prévenant les risques pour la vie privée ;
- Renforcer les garanties entourant l'usage des fichiers de police ;
- Conjuguer le plein respect des droits fondamentaux avec l'efficacité de la surveillance des communications électroniques à des fins de renseignement, notamment en transformant la Commission nationale de contrôle des interceptions de sécurité (CNCIS) en une Autorité de contrôle des services de renseignement ;

- En matière d'ouverture des données publiques, adopter une charte d'engagement et de bonnes pratiques signée par l'Etat, les associations de collectivités territoriales et les représentants des utilisateurs des données publiques, et définir des standards d'anonymisation afin de lutter contre les risques de réidentification.

E - Organiser la coopération européenne et internationale (propositions 43 à 50) :

- Définir un socle de règles pour lesquelles prévaut le « principe du pays de l'internaute », c'est-à-dire applicables à tous les services dirigés vers l'Union européenne ou la France, quel que soit leur lieu d'établissement. Il comprendrait notamment : - La législation européenne relative à la protection des données personnelles ; - L'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires ; - Le droit pénal, qui est déjà applicable à l'ensemble des sites destinés au public français.
- Réformer le « Safe Harbor » en développant les contrôles de son respect effectif par les autorités américaines et en donnant un droit de regard aux autorités européennes ;
- Promouvoir la démocratisation de l'ICANN (organisme de gestion des noms de domaine), notamment en rendant le conseil d'administration responsable devant une assemblée générale des parties prenantes ;
- Promouvoir l'adoption d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet. »

Une autre loi relative à la protection des données personnelles, qui adapte la loi 'informatique et libertés » du 6 janvier 1978 au 'paquet européen de protection des données'[27], a été promulguée le 20 juin 2018. Cette loi n'aménage que quelques points de la précédente dite « loi CNIL » de 1978, afin notamment de répondre aux évolutions technologiques et sociétales.

Depuis le droit d'accès aux documents administratifs (loi de 1978), les obligations légales et réglementaires en matière d'*open data* n'ont cessé de se renforcer. Mettre à disposition des données gratuites et fiables constitue l'objet d'une politique publique. Ne pas s'y plier est facteur de risques : détérioration ou perte de données, non valorisation de données (frein à leur réutilisation pour de nouveaux services), image négative vis-à-vis des citoyens ou usagers (manque de transparence…). En outre, cela entretient une crainte quant à la disponibilité des données personnelles, au respect de la confidentialité des données ou à leur anonymisation.

[27] Ce paquet européen comprend le RGPD, un règlement du 27 avril 2016 directement applicable dans tous les pays européens au 25 mai 2018 ainsi qu'une directive datée du même jour sur les fichiers en matière pénale, dite directive "police" *cf.* https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&from=FR.

Les missions de la CNIL évoluent afin de les adapter à la nouvelle logique de responsabilisation et d'accompagnement des acteurs traitant des données (entreprises, administrations, etc.) instaurée par le RGPD[28,29], tout en tirant parti des souplesses de ce dernier.

La loi du 20 juin 2018 vient la compléter en ajoutant d'autres dérogations à celles inscrites dans la loi précédente.

Les décisions fondées exclusivement sur un algorithme ne sont plus interdites.

Le 31 janvier 2019, la DGCCRF et la CNIL (Commission nationale de l'informatique et des libertés) ont signé un nouveau protocole de coopération dans l'objectif d'une meilleure protection des consommateurs. Les deux autorités ont décidé de mettre à jour la convention initialement signée en janvier 2011 afin de renforcer leur collaboration et de l'adapter aux nouveaux enjeux numériques.[30,31]

D'autres ministères se sont également engagés à développer leurs propres algorithmes, illustrant la volonté de l'État de mobiliser les données qu'ils recueillent, notamment dans le but de contribuer à la préservation d'emplois et à la pérennité d'entreprises.

Alors que fin 2017 seules 63% des démarches administratives étaient disponibles en ligne, 85% le sont en septembre 2021, soit 212 des 250 formalités « essentielles à la vie quotidienne ».

L'observatoire de la qualité des démarches administratives ressence ainsi les démarches qui ont été numérisées et sur lesquelles trois millions de Français ont déjà donné leur avis. Elles touchent des domaines aussi variés que la déclaration de la TVA, l'immatriculation des professions libérales, la demande d'une carte grise, l'achat du timbre fiscal, la demande d'aide aux ovins ou l'inscription au lycée.

La rubrique *« Dites-le nous une fois »* opèrera une simplification majeure puisque toutes les informations, une fois entrées, seront ensuite diffusées automatiquement auprès des autres administrations, ce qui évitera de les répéter à chaque nouvelle démarche.

Pour simplifier encore, la plupart de ces démarches seront ensuite disponibles directement sur le téléphone portable : changement d'adresse en ligne, demande d'extrait de casier judiciaire, attestation d'employeur, recensement citoyen obligatoire, notamment.

---

[28] Le RGPD – Règlement Général de Protection des Données – est entré en application le 25 mai 2018. Il vise à encadrer l'utilisation des données personnelles par les entreprises. Ces objectifs sont :

1. Limiter l'utilisation des données personnelles par les entreprises au strict minimum nécessaire et faire adopter le principe du *privacy by design* qui place le respect des données personnelles en amont de la conception.
2. Fournir une description précise des données collectées, des traitements appliqués, de la période de rétention de l'information, et demander un consentement explicite à la personne fournissant ses données personnelles.
3. Maintenir les données personnelles à jour.
4. Interdire les données dites sensibles : la religion, l'origine ethnique, les idées politiques, les orientations sexuelles.
5. Fournir sur demande d'un client une copie de l'ensemble des données le concernant, permettre la portabilité de ses données vers d'autres entités, permettre la rectification ou la suppression ses données personnelles (droit à l'oubli). Ces demandes de rectification et d'effacement doivent ensuite, par cascade, être transférées aux entités auxquelles les données ont été transmises, et ainsi permettre de propager ces instructions à chaque intermédiaire.
6. S'assurer que les entreprises mettent en œuvre les moyens nécessaires pour garantir un niveau de sécurité adapté au risque.
7. Prévoir des amendes en cas de non-respect de ces règles allant jusqu'à 4 % du chiffre d'affaires.

Et tout cela en respectant évidemment toutes les autres réglementations existantes qu'elles soient européennes ou nationales.
Le RGPD prévoit aussi que chaque entreprise se dote d'un DPO (*Data Protection Officer*) qui veillera à la bonne application de cette réglementation, et coordonnera toutes les demandes de copie, rectification ou effacement de données.
Il s'agit d'un règlement extraterritorial s'appliquant non seulement aux entités actives sur le territoire européen, mais également à toutes celles qui traitent des données concernant des citoyens européens où qu'elles se trouvent dans le monde.

[29] *Cf.* https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-etes-un-internaute.html

[30] *Cf.* le communiqué publié à cette occasion :
https://www.cnil.fr/fr/la-cnil-et-la-dgccrf-font-evoluer-leur-protocole-de-cooperation-pour-renforcer-la-protection-des

[31] Les obligations d'information des plateformes numériques :
https://www.economie.gouv.fr/dgccrf/les-obligations-dinformation-des-plateformes-numeriques

Plus de la moitié des formalités sont donc ainsi numérisées dans chaque ministère.

L'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse) a vu ses missions s'étendre aux enjeux de la révolution numérique à l'œuvre (messageries, régulation par la donnée), ce qui l'a conduit à faire évoluer sa culture et l'organisation de son travail pour devenir une « administration libérée », en même temps qu'à entreprendre de nouveaux travaux de mutualisation menés avec d'autres régulateurs : l'AMF, l'Autorité de la Concurrence, l'ARJEL, l'ART, la CNIL, la CRE, le CSA et la HADOPI.[32,33]

En mars 2021, le gouvernement a réaffirmé ses objectifs sur le pilotage des données, la digitalisation des services publics, et sa stratégie *cloud*.[34]

A la suite du rapport du député Eric Bothorel sur la politique publique de la donnée, des algorithmes et des codes sources, remis au Premier ministre en décembre 2020, le Premier ministre a publié une circulaire à destination des ministères et des préfets de régions sur ce sujet, en rappelant que la politique de la donnée doit être une priorité stratégique de l'Etat.[35]

Les ministères sont appelés à nommer un administrateur ministériel des données qui aura pour tâche d'élaborer la stratégie du ministère et d'être le point de contact des utilisateurs de données. La coordination de ces administrateurs est dévolue à la DINUM en sa qualité d'administrateur général des données, algorithmes et codes sources.

Sur le plan territorial, le Premier ministre demande la nomination de référents 'données, algorithmes et codes sources' auprès des préfets de région.

Le lien avec le secteur privé n'est pas oublié avec les acteurs détenant des données dites d'intérêt général (comme dans le cas de Doctolib pour la vaccination contre le Covid-19). Une fonction de médiateur de la donnée d'intérêt général est instituée.

L'Etat entend également accélérer sa politique d'ouverture des données publiques.

Sur le volet *'open source'*, la DINUM s'est vu confier une mission dédiée à l'animation et à la promotion interministérielle en matière de logiciel libre. Cette mission a eu comme tâche de créer le portail interministériel code.gouv.fr.

Dans le cadre de ses missions au sein de la DINUM, le département Etalab a réalisé un travail de recensement des bases et jeux de données publiques existantes dans plusieurs domaines et de publier ces inventaires en *open data*[36].

S'agissant par exemple du domaine de la santé, 172 bases de données de 79 gestionnaires ont été recensés[37]. Pour faciliter la découverte des données, cette page présente une sélection des principales bases qui sont disponibles en format ouvert sur le portail national data.gouv.fr. La liste n'est pas exhaustive et est ouverte aux contributions.[38]

10

[32] *Cf.* https://www.arcep.fr/larcep/nos-missions.html

[33] *Référentiel des usages numériques* (Arcep – CSA) : https://www.arcep.fr/fileadmin/cru-1611912788/user_upload/pole-numerique-arcep-csa/referentiel-arcep-csa-usages-numeriques_fev2021.pdf

[34] *Cf.* notamment *Le Monde informatique* : https://www.lemondeinformatique.fr/actualites/lire-le-gouvernement-reoriente-sa-strategie-sur-le-cloud-de-confiance-82937.html

[35] *Circulaire n°6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources :* https://www.legifrance.gouv.fr/download/pdf/circ?id=45162

[36] *Cf.* https://www.data.gouv.fr/fr/datasets/

[37] *Cf.* https://www.data.gouv.fr/fr/datasets/inventaire-des-bases-de-donnees-relatives-a-la-sante/

[38] Ces jeux de données sont présentés en 3 catégories :
Données de santé publique et épidémiologie : données sur les habitudes de vie, les inégalités de santé, l'épidémiologie, etc.
Données sur les offres de soins : informations sur les infrastructures, les services proposés, le personnel, les honoraires, etc.
Données sur les consommations de soins et dépenses **:** données sur les activités des établissements de santé, les consultations, les médicaments et dispositifs, etc.

L'APRIL, association qui s'est donnée comme objectifs la promotion et la défense du logiciel libre[39], avait pourtant exprimé le souhait *« qu'il s'agisse d'une véritable forge logicielle publique, accueillant les codes sources produits par les administrations et librement accessible, et non pas d'un simple portail listant les liens vers des codes hébergés sur des forges extérieures. »*

Dans une volonté de moderniser l'accès aux données, la Direction de l'information légale et administrative française (DILA) a annoncé en novembre 2021 l'ouverture de la 'data' de ses sites économiques ***via*** de nouvelles interfaces de programmation d'application (API).

Faisant suite à la circulaire du Premier ministre du 27 avril 2021 sur la politique publique de la donnée, des algorithmes et des codes sources, la DILA met ainsi en avant l'importance de ce type d'ouverture et de réutilisation des données publiques.

Pour moderniser la collecte, l'enrichissement, la publication et l'exploitation de données des divers supports d'annonces légales qu'elle édite, la DILA a encouragé la réutilisation de ses informations publiques par l'innovation collaborative dès 2014. En juin 2021, elle ajoute de nouveaux moyens pour accéder aux données publiques. Pour ce faire, elle s'appuie sur les interfaces de programmation d'application (API) qui permettent le libre accès aux données de masse et aux fonctionnalités à grande échelle.

L'ouverture annoncée concerne les annonces civiles et commerciales du BODDAC (33 millions d'annonces publiées), les annonces des associations et fondations d'entreprise et leurs dépôts de comptes annuels (4,9 millions d'annonces), les annonces de marchés publics du BOAMP (3,2 millions d'annonces) ainsi que les annonces légales et obligatoires du BALO (128 000 annonces).[40]

Ces données sont mises à disposition pour pouvoir être utiles tant aux décideurs publics comme qu'aux citoyens et acteurs privés, que ce soit pour le pilotage, l'efficacité de l'action publique mais aussi dans un souci de transparence et de débat démocratique. Par son action, la DILA facilite le pilotage des décideurs publics, la transparence auprès des citoyens, permet une exploitation des données à des fins économiques et fournit de nouvelles ressources pour l'innovation économique et sociale.

Données sur les performances et opérations **:** informations sur les performances financières, les performances opérationnelles, etc.

11

Chaque base listée ci-dessous fait l'objet d'une page dédiée sur data.gouv.fr, présentant de manière plus détaillée les données téléchargeables. Sont ensuite listés les noms des principales organisations gestionnaires des données relatives à la santé. La plupart de ces gestionnaires proposent sur leurs portails ou sites web des informations ou publications construites sur la base des jeux de données listés ci-dessous.

[39] *Cf.* https://www.april.org/

[40] Les données BOAMP / Le BOAMP diffuse les avis d'appel public à la concurrence et les résultats de marchés de l'État, de l'armée, des collectivités territoriales et de leurs établissements publics ; il publie également des contrats de partenariat public-privé et des avis de concession.

Les données BALO / Depuis 1907, le BALO recense l'ensemble des informations relatives aux sociétés faisant appel public **à** l'épargne et aux établissements bancaires et financiers, telles que les opérations financières, les avis de convocations aux assemblées générales, les comptes annuels.

Les données BODACC / Le BODACC assure la publicité des actes enregistrés au registre du commerce et des sociétés. Il publie les avis prévus par le code du commerce et les textes législatifs et réglementaires (ventes et cessions, immatriculations, créations d'établissements, les modifications et radiations de personnes physiques ou morales inscrites au registre du commerce et des sociétés, avis de dépôts de comptes…).

Les données Associations / Le jeu de données Associations (JOAFE, *Journal officiel associations et fondations d'entreprise*) publie les déclarations de création, modification ou dissolution des associations régies par la loi de 1901 depuis l'origine et des extraits de décisions de justice afférentes au domaine associatif.

Les données comptes associations / Le jeu de données Comptes associations publie les comptes annuels des associations, fondations d'entreprise, fondations partenariales, associations professionnelles nationales de militaires fonds de dotation.

Chacun peut désormais interroger les données économiques rapidement, par le biais de filtres et critères spécifiques, croiser ces données pour des rapports ou analyses sur les marchés publics ou la vie des entreprises et associations.

Ces données sont téléchargeables sous différents formats tels que Excel, CSV ou encore JSON.

Pour toutes les structures souhaitant industrialiser et automatiser les recherches récurrentes, il leur est possible de mettre en place un programme qui intègre ces APIs. Il y a quatre APIs DILA (les données des associations sont sur la même interface que les comptes des associations).

Il est important de relever que, conformément au document *« Avertissement sur les données personnelles »*, la mise à disposition par la DILA de jeux de données pouvant contenir des données personnelles n'affranchit pas le réutilisateur du respect de la loi *« informatique et libertés »*.

Sur le registre éthique, un "comité pilote d'éthique du numérique", qui agit sous l'égide du CCNE pour les sciences de la vie et de la santé, est chargé depuis sa création en décembre 2019 d'aborder de manière globale les enjeux éthiques du numérique et de l'intelligence artificielle.

Outre la publication de son *« Manifeste pour une éthique du numérique »*[41], ce comité procède régulièrement à des consultations publiques, et publie régulièrement des bulletins de veille autour de ces questions.

De son côté France Stratégie a publié en mai 2021 un document formulant 56 recommandations pour des entreprises numériquement responsables tout au long de la chaîne de valeur des produits, sur les plans règlementaire, éthique, sociétal et environnemental.[42] Ce document consacre notamment la notion de responsabilité numérique des entreprises (RNE)[43]

Mais est-ce véritablement suffisant en regard de l'ampleur des enjeux éthiques ?

- *Au sein de l'exécutif, la dématérialisation des services publics interroge par son caractère impératif.*

« À travers les concepts d'« État plateforme » ou de « start-up d'État[44] », les nouveaux réformateurs comptent sur les « corporate hackers » et l'innovation disruptive pour transformer de l'intérieur les bureaucraties publiques, laisser libre cours à la créativité, renouer avec la transparence, déployer des méthodes « agiles » et s'adapter à un environnement en perpétuelle transformation, le tout à moindre coût. L'« État digital » – un concept vanté en juin 2017 par Emmanuel Macron lors d'une ode à la « startup nation » *restée célèbre – est aussi et surtout un État en voie d'automatisation : pour accompagner l'horizon du non-remplacement de près de 50 000 fonctionnaires d'ici à 2022, le plan Action Publique 2022 lancé en octobre 2018 misait sur des « technologies telles que l'intelligence artificielle et les RPA* (« *robotic process automation* »)*, ce afin « d'automatiser les tâches répétitives et à faible valeur ajoutée ». »*[45]

[41] *Manifeste pour une éthique du numérique :* https://www.ccne-ethique.fr/fr/actualites/manifeste-pour-une-ethique-du-numerique

[42] *Responsabilité numérique des entreprises : enjeux des données, environnementaux et sociaux :* https://www.strategie.gouv.fr/infographies/responsabilite-numerique-entreprises-enjeux-donnees-environnementaux-sociaux

[43] *"La Responsabilité numérique des entreprises est un déploiement nouveau et incontournable de la RSE, qui se fonde sur les mêmes principes de redevabilité, d'éthique et d'échanges avec les parties prenantes des entreprises. À savoir : la responsabilité environnementale ; la responsabilité réglementaire liée à la protection des données ; la responsabilité éthique liée aux logiciels relatifs à l'intelligence artificielle ; la responsabilité sociétale relative à la gestion et au partage des données, à la transformation des modes de travail, et à l'inclusion de toutes et tous."*

[44] Voir par exemple : Algan, Yann et Cazenave, Thomas, 2016. *L'Etat en mode start-up*. Paris : Eyrolles. Bertholet, Clément et Létourneau, Laura, 2017. *Ubérisons l'État ! Avant que d'autres ne s'en chargent*. Malakoff : Armand Colin. Pezziardi, Pierre et Verdier, Henri, 2017. *Des startups d'État à l'État plateforme*. CreateSpace Independent Publishing Platform.

[45] *Cf.* Félix Tréguer *in IA et réforme de l'État : vers des bureaucraties sans humains ?*

En mai 2021, le Premier ministre a présenté sa stratégie nationale pour un *cloud* souverain[46]. L'enjeu : garantir la protection et la maîtrise des données hébergées en France pour s'opposer à des lois extraterritoriales, comme le *Cloud Act* américain.

La doctrine sur l'usage du cloud par l'État pour ses propres services a été officialisée par une circulaire du Premier Ministre en date du 5 juillet 2021 (en lieu et place de la précédente datant du 8 novembre 2018).[47]

Cette stratégie de l'Etat repose sur un *« équilibre entre les différents publics »* à savoir les usagers, les agents publics et les acteurs de la démocratie, ainsi que sur trois axes prioritaires que sont la qualité des services publics, l'ouverture et la transparence, et la souveraineté et la sécurité. Mais le marché étant dominé par Amazon, Microsoft et Google, la réalité économique impose à l'Etat de miser sur des accords de licence des technologies américaines.

Désormais, la loi ouvre plus largement la possibilité pour l'administration de recourir à des décisions individuelles automatisées … et ce alors même que la sécurité du *cloud* est mise en cause par une série d'imprudences et de mauvaises pratiques comme le démontre une étude de Varonis.[48,49,*50*]

Néanmoins, de nouvelles garanties sont données aux administrés : droits à l'information et à l'explication (déjà consacrés par la loi pour une République numérique de 2016), droit à recours avec une intervention humaine *a posteriori*, obligation pour l'administration de maîtriser l'algorithme et ses évolutions (prohibition des algorithmes auto-apprenants) afin d'éviter le recul de l'Etat de droit qu'occasionnerait l'incapacité des administrés à contester les décisions les concernant, interdiction d'utiliser des données sensibles[51].

Le respect de ces garanties est fondamental car, comme le souligne Félix Tréguer : *« dans une bureaucratie automatisée, aucune marge de manœuvre n'est plus possible pour l'application des règles inscrites dans les dispositifs, aucun lanceur d'alerte ne pourra plus avertir d'éventuelles dérives : l'automatisation bureaucratique a le potentiel de faire advenir un gouvernement totalement déshumanisé. »*

Or, bien qu'en vigueur depuis plusieurs années, les nouvelles obligations de transparence nées de la loi Numérique demeurent assez largement ignorées des acteurs publics.

C'est ce que révèle un rapport rédigé par des élèves de l'ENA consacré aux difficultés rencontrées par les administrations[52].

Ce nouveau cadre juridique est perçu par les administrations « *comme une contrainte et une tâche d'une ampleur incompatible avec les moyens disponibles* », notent les élèves de l'ENA à la suite de multiples auditions.

---

https://aoc.media/analyse/2021/11/11/ia-et-reforme-de-letat-vers-des-bureaucraties-sans-humains/

[46] https://www.economie.gouv.fr/files/files/Thematiques/numerique/Transcript_presentation_strategie_nationale_cloud.pdf

[47] *Circulaire 6282/SG : Doctrine d'utilisation de l'informatique en nuage au sein de l'Etat :* https://www.transformation.gouv.fr/files/presse/Circulaire-n6282-SG-5072021-doctrineuutilisation-informatique-en-nuage-Etat.pdf

[48] *Cf.* https://www.cio-online.com/actualites/lire-le-cloud-mis-en-danger-par-les-mauvaises-pratiques-13471.html

[49] Voir également Philippe Van Hove *in L'accélération de la migration vers le cloud ne doit pas faire oublier les questions de sécurité :* https://solutions.lesechos.fr/tech/c/lacceleration-de-la-migration-vers-le-cloud-ne-doit-pas-faire-oublier-les-questions-de-securite-28999/

[50] Le remarquable Blog de Jean-Paul Pinte offre une très large visibilité sur toutes ces questions et les solutions qui peuvent y être apportées : https://cybercriminalite.blog/

[51] *Le rôle du juge face aux décisions administratives algorithmiques :* https://news.predictice.com/le-r%C3%B4le-du-juge-face-aux-d%C3%A9cisions-administratives-algorithmiques-d3b263e8eedb

[52] *Ethique et responsabilité des algorithmes publics* (Rapport établi à la demande de la mission Etalab - direction interministérielle du numérique et du système d'information et de communication de l'Etat) : https://www.etalab.gouv.fr/wp-content/uploads/2020/01/Rapport-ENA-Ethique-et-responsabilit%C3%A9-des-algorithmes-publics.pdf

De « *nombreux interlocuteurs rencontrés* » ont ainsi indiqué que les moyens humains et financiers dont ils disposaient n'étaient « *pas suffisants* » pour mettre en œuvre les obligations introduites par la loi pour une République numérique. Ce qui explique probablement pourquoi (très) rares sont les acteurs publics à s'être pliés à ce nouveau cadre légal.

La réglementation *a priori* classique peut se trouver dépassée par la difficulté à appréhender un environnement en évolution continue et à l'horizon inconnu.

L'action de l'Etat (et *de facto* des régulateurs) peut en complément s'inscrire dans le cadre évolutif que permet la régulation par la donnée, qui vient compléter les outils traditionnels du régulateur. Celle-ci combine responsabilisation des acteurs, capacité renforcée d'analyse du régulateur, et information des utilisateurs[53] et de la société civile. Au lieu de prescrire aux acteurs économiques un certain comportement, il s'agit de créer un réseau d'informations et d'incitations pour réduire les asymétries d'information et démultiplier l'impact de l'action du régulateur en mobilisant les utilisateurs et leurs relais.

Cette approche appelle une nouvelle culture et de nouvelles compétences au sein de l'Etat de manière à lui permettre à la fois d'amplifier sa capacité d'action en tant que régulateur, notamment dans une logique de supervision, d'éclairer les choix des utilisateurs et de mieux orienter le marché. En pratique, cela passe non seulement par la collecte d'informations auprès des acteurs régulés mais aussi par un élargissement des données, par des outils de *crowdsourcing,* par des démarches de simulation, par l'animation d'un écosystème d'acteurs de la mesure, de comparateurs ...

Un autre point fondamental mérite toute notre attention. Il est apparu en novembre 2019 que contraindre les usagers des services publics à passer par Internet pour leurs démarches pourrait bien être illégal. Le Conseil d'Etat estime cependant inutile de modifier le décret du 27 mai 2016, qui autorise la prise de rendez-vous par Internet, car ce décret ne rend pas obligatoire, mais seulement optionnelle, la dématérialisation.

Le recours de plus en plus systématique aux algorithmes par l'administration soulève également de très nombreuses interrogations (comme il en pose aussi de manière beaucoup plus globale[54]).

Le rapport évoqué *supra* s'arrête également sur les problématiques liées à l'explicitation du fonctionnement des algorithmes publics : « *Les informations fournies à la demande de l'intéressé dans le cadre d'une décision individuelle prise sur le fondement d'un algorithme (article R.311-3-1-2 du CRPA) sont mal appréhendées par les administrations. Celles-ci sont nombreuses à faire état de leur difficulté à traduire de manière opérationnelle les obligations prévues et à identifier le degré d'information devant être apporté aux administrés afin d'être conforme au cadre juridique.* »

Un tableau détaillant les éléments d'explication à fournir a ainsi été élaboré, et agrémenté d'exemples. On peut notamment y lire que les administrations doivent « *retracer – sous une forme littérale – les calculs réalisés par l'algorithme. La combinaison de ces différentes informations doit permettre de vérifier si, par rapport à la situation et aux données, les résultats obtenus sont conformes.* » Une consigne malheureusement pas toujours bien appliquée ….

Pourtant, les auteurs du rapport disent avoir constaté « *que certaines administrations avaient pris des mesures d'organisation pour répondre aux obligations propres à l'usage des algorithmes* ».

[53] Entendu comme l'ensemble des utilisateurs finals des services sur le marché de détail (consommateurs, usagers, professionnels, etc.)

[54] *À quoi rêvent les algorithmes* : https://journals.openedition.org/lectures/20554

Si la mise en œuvre de ces réformes nécessite un « *investissement supplémentaire* », celui-ci « *reste modeste par rapport à l'ampleur des réorganisations nécessaires pour se conformer au RGPD* ».

« *Plus qu'une réelle incapacité matérielle à remplir ces obligations* », nuance ainsi le rapport, « *ce sentiment semble nourri par une forme d'incompréhension du cadre juridique récent* ».

L'ampleur des obligations prévues par la loi Lemaire fait en effet « *l'objet d'interprétations diverses* ».

En oubliant parfois, comme l'ancien président du Conseil Pierre Mendès-France l'affirma jadis, que : *« La démocratie est d'abord un état d'esprit. »*

Loin de jeter la pierre aux pouvoirs publics, le rapport souligne malgré tout que la loi pour une République numérique a été adoptée « *sans réelle contribution de la part des administrations* », alors que « *le processus d'écriture de cette loi fait figure de modèle en ce qu'il a, pour la première fois, autorisé des contributions ouvertes afin d'informer le travail législatif* ».

Les auteurs voient ainsi dans cette « *rencontre manquée* » un signe de « *l'insuffisante acculturation des administrations aux enjeux du numérique* », d'où résulte aujourd'hui « *une certaine frustration de leur part au moment où elles se trouvent confrontées aux difficultés de mise en œuvre de ces nouvelles obligations* ».

Les yeux rivés vers l'avenir, le rapport préconise un « *accompagnement renforcé* » des administrations, qui passerait notamment par une consolidation des moyens dévolus au département Etalab. Le récent guide sur les algorithmes publics gagnerait à être enrichi, estiment les élèves de l'ENA, « *afin de répondre aux interrogations des administrations et assurer une application homogène des dispositions relatives aux algorithmes* ».

Pour les auteurs du rapport, la mise en conformité avec les nouvelles obligations nées notamment de la loi Lemaire doit aussi « *être l'occasion de sensibiliser plus largement les administrations aux questions de responsabilité et d'éthique liées à l'usage des algorithmes* ».

Les jeunes énarques s'inquiètent ainsi du « *caractère encore embryonnaire de la réflexion éthique autour des algorithmes au sein des administrations – qu'il s'agisse de l'État ou des collectivités* ».

Garde-fou « *nécessaire mais non suffisant* », les obligations de transparence en vigueur ne peuvent pourtant garantir la loyauté des algorithmes, soulignent-ils. « *Intervenant après la conception ou la prise de décision, la transparence fonctionne avant tout comme une corde de rappel pour les administrations qui doivent intégrer cette exigence de loyauté dès la conception des traitements auxquels elles ont recours.* »

Et surtout, de nombreuses dérogations existent (pour les algorithmes qui n'aboutissent pas à des décisions individuelles, pour ceux protégés par le 'secret défense'[55], etc.).

[55] Le secret défense vise à protéger certains documents dont l'accès pourrait représenter un danger pour la sécurité nationale face à des services de renseignement étrangers, des groupes terroristes ou criminels. En général, au-delà d'un certain délai, ces documents classifiés peuvent être consultés. Toutefois, des exceptions perdurent.
L'encadrement juridique du secret défense a été révisé avec l'instruction générale interministérielle (IGI n°1300) sur la protection du secret de la défense nationale publiée au *Journal officiel* le 11 août 2021 en annexe d'un arrêté du 9 août 2021. Par ailleurs, son usage est encadré par le code de la défense qui définit la chaîne de responsabilité au sein du pouvoir exécutif, du Premier ministre au haut fonctionnaire de défense et de sécurité (HFDS).
Pour sa part, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) assure l'interface entre le Premier ministre et les ministres dans leur champ d'attribution respectif. Il est aussi l'autorité référente pour les services de l'État, indépendants des ministères, habilités au secret défense. Il est enfin l'interlocuteur des pays étrangers dans le cadre d'accords bilatéraux ou multilatéraux sur des questions de sécurité et de protection du secret défense.
Pour en savoir plus : https://www.vie-publique.fr/eclairage/281595-protection-du-secret-defense-un-acces-revu-aux-archives

Le rapport soutient que « *la nécessité de réguler les algorithmes se pose avec une acuité particulière dans le secteur public* », et ce pour trois raisons :

« *Premièrement, là où des algorithmes privés sont au service d'intérêts particuliers, les algorithmes publics sont régulièrement utilisés afin de faire appliquer une loi, prévoyant des dispositions au service de l'intérêt général.*

Deuxièmement, contrairement à des algorithmes privés dont l'utilisation est rarement obligatoire (ex : un utilisateur de Facebook peut choisir de ne plus recourir au réseau social s'il n'est pas satisfait de l'algorithme à l'origine de la présentation des publications sur sa page d'accueil), les algorithmes publics s'imposent aux administrés (ex : le calcul des impôts).

Troisièmement, les algorithmes pouvant renforcer le sentiment d'éloignement de l'administration et d'isolement du citoyen, les collectivités publiques qui les déploient se doivent d'y recourir de manière exemplaire. »

Pour autant, « *nul besoin de prévoir de nouvelles obligations législatives ou réglementaires : l'enjeu est avant tout organisationnel* », affirment les élèves de l'ENA.

« *Identifier au mieux les responsabilités avant tout déploiement, faire travailler ensemble les services juridiques, informatiques et métiers (ainsi que les prestataires lorsque l'algorithme est développé en externe), former l'ensemble des acteurs de la chaîne algorithmes apparaissent en effet comme autant de bonnes pratiques à favoriser.* »

Le rapport plaide tout particulièrement pour la mise en oeuvre « *d'un véritable management des algorithmes publics* », qui passerait notamment par la constitution d'un réseau de « *référents éthiques* », dotés d'une certaine indépendance.

En juin 2020, à l'issue du premier confinement imposé lors de la crise pandémique de la Covid 19, une enquête post-confinement a été réalisée en ligne auprès des usagers et des agents du service public, qui distingue leurs attentes respectives avant, pendant et après le confinement[56]. Il s'en dégage les constats suivants :

Du côté des usagers, si les pratiques digitales sont déjà bien installées dans les relations usagers-administrations (60 % du total des contacts), trois administrations émergent de ce point de vue : les impôts, les allocations familiales/assurance maladie, les caisses de retraite, pour lesquelles le digital est largement prépondérant. *A contrario,* le face-à-face et le téléphone restent majoritaires pour les mairies/préfectures, l'éducation nationale et la police/justice/ gendarmerie. Si la crise a profité à un canal, c'est d'abord au téléphone (en augmentation plus nette que le numérique depuis le confinement), ce qui prouve que le besoin de contact avec un agent reste réel. Les projections d'usage restent néanmoins en faveur du digital (+ 4 points d'intentions). Les motifs de satisfaction le concernant sont logiquement l'accessibilité, l'immédiateté et la simplicité... Il semble, pour les usagers, que les principaux points d'achoppement liés au contact direct (temps d'attente, manque d'accessibilité, de compétence, d'amabilité…) soient directement compensables par les bénéfices du digital. Ainsi, sur la posture à l'égard de l'administration et du digital, on retient que :
• 90 % de l'échantillon attendent la digitalisation de l'ensemble des services publics ;
• 66 % pensent que les démarches à effectuer auprès des administrations sont trop complexes ;
• 61 % jugent que la transmission des données personnelles est acceptable si c'est à visée de simplification de démarche.

Du côté des agents de la fonction publique, avant la crise, moins de 10 % des agents pratiquaient le télétravail (en majorité dans la fonction publique de l'État et la catégorie A). Le confinement

[56] *Covid : les attentes des agents et des usagers des services publics*
https://www.acteurspublics.fr/articles/covid-les-attentes-des-agents-et-des-usagers-des-services-publics

a eu un réel effet déclencheur sur cet aspect, puisqu'on observe une augmentation de 35 % des pratiques (45 % de télétravail, au moins partiel pendant le confinement) … avec toujours cette prédominance de la fonction publique de l'État et de la catégorie A.

L'expérience s'avère positive puisque près de 70 % des agents ayant télétravaillé s'en déclarent satisfaits. Les agents se montrent donc prêts à une évolution sur ce versant : 76 % souhaitent que le télétravail se développe, au moins partiellement.

Ce sont les structures de l'administration publique qui semblent inadaptées aujourd'hui car majoritairement jugées comme manquant de modernité, de souplesse, d'agilité…

Cette tension explique que la question du maintien de la qualité du service public est polarisante : 50 % des agents estimant qu'elle peut être identique à distance, contre 50 % estimant qu'elle est susceptible d'être dégradée.

Force est de constater que, ayant été réalisée en ligne, cette enquête occulte nécessairement les inquiétudes, les difficultés et les réticences des millions de personnes victimes d'illectronisme.

Or, comme le souligne Charles de Laubier dans un article publié dans le quotidien *Le Monde* en mai 2021[57], en accentuant la dépendance aux démarches en ligne, et en retardant encore le déploiement de la couverture très haut débit du territoire, le confinement imposé par l'Etat lors de la première phase de la gestion de la crise pandémique du Covid-19 a renforcé les inégalités d'accès au numérique en France**.**

Dans son rapport rendu public le 1er octobre 2021, la Défenseure des Droits souligne : *« Près d'un quart des personnes âgées de plus 65 ans déclarent être confrontées à des difficultés dans la réalisation de leurs démarches administratives. Ces difficultés sont davantage rapportées par les personnes en situation de dépendance, de précarité financière ou en situation d'illectronisme. Ce dernier résultat souligne l'impact de la dématérialisation sur l'accès aux services publics par cette catégorie de population, dont 30 % indiquent ne pas disposer d'un accès à Internet à leur domicile. Les personnes âgées évoquent la déshumanisation des relations avec les services publics et la perte du lien social. Comme le souligne l'un des aidants ayant participé à l'enquête, la difficulté à dialoguer directement avec une personne et à obtenir des informations sur leur situation renforce leur sentiment d'exclusion : « Je pense qu'ils souffrent de ne pas avoir d'interlocuteur en face d'eux qui les aide, les rassure ou valide ce qu'ils font. Il y a le côté 'Oh si je fais une bêtise' ». Ces difficultés peuvent être à l'origine d'un renoncement aux droits : face à des problèmes administratifs 15 % des personnes âgées déclarent avoir abandonné leurs démarches. »*[58]

Par ailleurs, la généralisation de la dématérialisation des démarches administratives présuppose que toute la population française soit en capacité de détenir une adresse électronique ; ce qui implique soit que tous les individus disposent des ressources financières pour supporter les coûts financiers importants liés à la possession des ressources technologiques correspondantes (coûts d'acquisition et de maintenance des matériels informatiques, coûts d'accès à des prestations donnant accès à Internet, …), soit qu'ils puissent avoir accès à ces ressources de manière permanente et sur tout le territoire à des coûts réellement supportables.

[57] *La fracture numérique au révélateur du Covid 19* : https://europagora.eu/fracture-numerique-inegalites/

[58] *Etudes et résultats – Difficultés d'accès aux droits et discriminations liées à l'âge avancé :* https://www.defenseurdesdroits.fr/fr/communique-de-presse/2021/10/difficultes-dacces-aux-droits-et-discriminations-des-plus-de-65-ans-une

Nous en sommes encore très loin et, pourtant, rien ne semble indiquer que cette exigence républicaine fasse l'objet d'une attention particulière de la part des pouvoirs publics et des institutions parlementaires.

- *Le système judiciaire français se trouve confronté à de nouveaux défis démocratiques*

Parmi les 15 secteurs de l'économie française identifiés en 2019 comme étant les plus impactés par l'IA figure celui des *'LegalTech'*.[59]

Dans sa décision du 12 juin 2018, le Conseil constitutionnel a jugé conforme à la Constitution les nouvelles règles régissant l'emploi des algorithmes par l'administration, considérant que "*le législateur a défini des garanties appropriées pour la sauvegarde des droits et libertés des personnes soumises aux décisions administratives individuelles prises sur le fondement exclusif d'un algorithme*". Sans véritablement avoir pris la mesure de tous les enjeux attachés à ces questions ! En pratique, plusieurs points doivent encore être tranchés[60].

Selon Renaud Vedel, Coordonnateur de la stratégie nationale pour l'intelligence artificielle (IA) au ministère de l'Economie, des finances et de la relance, les dernières évolutions grâce à de nouvelles technologies telles que les *« transformers »* permettent des progrès importants dans le traitement automatique du langage.

Ainsi, beaucoup d'avancées dans l'aide à l'analyse de documents pourraient être utilisées dans le domaine du droit. Par exemple, l'IA pourrait être utilisée pour des outils à la lecture de productions sémantiques du droit mais de manière générale pour aider les professionnels du droit.

Pierre-Antoine Chevalier, Responsable du pôle données à Etalab (DINUM), évoque trois cas d'usage pour lesquels Etalab a accompagné les administrations.

L'open data des décisions de justice est la première réalisation concrète du ministère de la Justice pour ouvrir les données du ministère. Avec la nécessité de pseudonymiser les décisions de justice, ce qui requiert d'utiliser des algorithmes et des codes-source. L'objectif visé est d'atteindre 20.000 à 2 millions décisions de justice annuelles d'ici 2025. Il faudra ensuite étudier comment réutiliser ces données.[61]

Le Conseil d'Etat expérimente un algorithme qui détecte les contentieux avec les mêmes questions de droit. Cet algorithme permet d'extraire les moyens ainsi que les conclusions et identifient les similarités, ce qui pourrait permettre de mieux affecter les contentieux.

La Cour de Cassation expérimente, en collaboration avec l'INRIA, un algorithme destiné à détecter les divergences dans les décisions de justice, ainsi qu'à donner des titres aux décisions à partir des résumés ou des sommaires, et ce afin de pouvoir regrouper les décisions qui traitent des mêmes questions.

---

[59] *Cf.* le rapport de la Direction général des entreprises : https://www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/Intelligence_artificielle/2019-02-intelligence-artificielle-etat-de-l-art-et-perspectives.pdf

[60] Le lecteur trouvera dans ma publication citée *supra* des développements plus substantiels sur ces questions.

[61] Le *big data* juridique ne se limite pas à la législation et la jurisprudence françaises. Depuis plusieurs années déjà, certains acteurs de la *legaltech* s'intéressent et s'efforcent de récupérer d'autres corpus de données qui présentent un intérêt pour les professionnels du droit, de l'assurance, de la conformité ou de la gestion des risques. Documents parlementaires (comptes-rendus des débats, rapport d'information, études d'impact, avis du Conseil d'État, questions écrites au gouvernement, etc.), lignes directrices et commentaires émis par les régulateurs, conventions collectives et accords d'entreprise, avis et travaux préparatoires établis par des instances locales, nationales ou internationales, actions de plaidoyer portées par des ONG… La liste des sources d'informations susceptibles d'intéresser les juristes est longue et varie selon les secteurs d'activité. Et pour répondre aux attentes de leurs clients, les start-ups du droit s'attachent à développer des solutions technologiques sur mesure. (Source : Miren Lartigue, journaliste / https://www.dalloz-actualite.fr/taxonomy/term/16265)

Lors d'une conférence prononcée au Collège France au cours de laquelle il examina l'impact croissant du droit de la numérisation et de l'IA[62], le professeur Simon Deakin interrogea la capacité du droit à canaliser la technologie, tout en s'interrogeant sur la capacité du droit à maintenir l'autonomie de ses opérations face à un changement technologique global, résultat qui est loin d'être garanti : « *Qu'il s'agisse d'une simple automatisation des tâches, d'une aide à la décision, ou de prédiction, l'utilisation d'algorithmes et de l'intelligence artificielle dans le domaine de la justice pose des questions d'ordre technique et éthique. Si l'introduction des outils numériques dans ce champ régalien offre des perspectives d'amélioration (rapidité, impartialité…), les risques de dérives éthiques sont néanmoins nombreux (perte d'humanité et de dialogue, renforcement des stéréotypes…). Afin d'en tirer le maximum de bénéfices pour la société sans risquer de mettre en péril les principes fondamentaux de la justice et de la démocratie, il conviendrait de mettre en place un cadre, piloté par la puissance publique et impliquant à la fois des professionnels du droit et des experts en intelligence artificielle. En effet, toutes les étapes de la mise en œuvre progressive de ces outils, de la conception à l'utilisation (collecte et traitement des données, contrôle des acteurs privés comme les Legal Tech …) nécessitent précautions et garde-fous institutionnels. C'est à ce prix que l'assurance de l'éthique et la préservation de l'équité pourront être respectés*. »[63]

Un avocat en droit numérique, une docteure en science numérique, et un ingénieur en IA dans l'industrie : Adrien Basdevant, Aurélie Jean et Victor Storchan, se sont associés pour analyser, sous un angle scientifique et juridique, les grands principes de la justice algorithmisée et ses mécanismes sous-jacents. [64]

Dans son ouvrage intitulé *'Les algorithmes font-ils la loi ?'*, Aurélie Jean apporte des réponses pertinentes aux grandes questions suivantes : Comment la loi est-elle pensée et appliquée au temps des algorithmes ? Comment les algorithmes sont-ils utilisés au sein du système judiciaire ? Et est-il vraiment possible de les réguler ?

Elle explique pourquoi il est primordial de *« comprendre les défis actuels et les solutions recherchées pour anticiper les lois* […] *et éviter que les algorithmes imposent des règles »* que l'on ne comprend pas. *« Il faut encadrer les pratiques de développement, de tests et d'usages des algorithmes. En d'autres termes, il faut encourager, pour ne pas dire imposer, aux acteurs de construire une gouvernance algorithmique pertinente et efficace pour assurer le bon fonctionnement de leurs outils. Cela passe entre autres par les méthodes de calcul d'explicabilité (des calculs numériques pour extraire une partie de la logique de l'algorithme) qui permettent de mieux comprendre les outils afin d'en souligner des biais ou des dysfonctionnements, et donc les réparer rapidement avant que le mal ne soit fait sur les utilisateurs. »*

Pour Aurélie Jean, c'est un fait : les algorithmes rythment nos vies. Ils nous aident à nous déplacer, à travailler, à nous soigner, et même à légiférer. Certains, alarmistes, diraient qu'ils sont de partout... Or, peu d'entre nous les comprennent, sans parler d'en maîtriser les subtilités. Nos dirigeants, parlementaires et nos juristes n'y font pas exception, et participent pour certains à augmenter la confusion autour de leur utilisation et de leur supposé danger... Pourtant, il est aujourd'hui nécessaire, voire capital, de comprendre le fonctionnement des algorithmes développés, mais aussi d'anticiper leur développement, de l'encadrer et de l'accompagner aussi

[62] *Droit et technologie : influence du droit sur la technologie, et capacité du droit de canaliser la technologie :* https://www.college-de-france.fr/site/alain-supiot/guestlecturer-2019-05-22-17h00.htm?fbclid=IwAR3iMXmjYReCYBgTGLGC1-OIv5TrDk1IEbGQBIrHb243_kxTeGahlFzZOw0

[63] *Justice algorithmique : s'assurer de l'éthique et préserver l'équité ?:* https://www.ihest.fr/les-formations/le-cycle-national/cycles-nationaux-precedents/cycle-national-2018-2019-l-inconnaissance-vecteur-d-inventivite/productions/justice-algorithmique-s-assurer-de-l-ethique-et-preserver-l-equite

[64] *Cf. Mécanisme d'une justice algorithmisée : https://jean-jaures.org/sites/default/files/justice.pdf*

judicieusement que justement. Une chose demeure cependant certaine : les algorithmes ne disposent d'aucune personnalité juridique face à un tribunal. En revanche, s'ils ne peuvent réellement faire la loi, ils l'influencent et en orientent désormais la pratique. Mal employés, ils deviennent une menace pour ses principes de transparence et d'équité. Bien maîtrisés, ils peuvent, au contraire, guider ceux qui la font et l'exercent afin de garantir le traitement égalitaire de chacun face à la justice.

Aurélie Jean nous appelle à agir et propose de dompter (plutôt que de réguler) les algorithmes à travers des lois souples et anticipatrices, afin de ne rien sacrifier au progrès tout en les pensant dans la plus grande objectivité scientifique, sociale et économique. Car c'est cette même transparence intrinsèque à l'exercice de la justice qui doit s'appliquer dans le champ des algorithmes afin de permettre à chacun - du citoyen au législateur - de garantir l'harmonie, la justice et l'essor intellectuel au sein de nos sociétés.

Le 30 décembre 2021, le Conseil d'Etat a validé le projet d'algorithme DataJust – qui devait servir à établir un référentiel fiable et officiel de l'indemnisation des victimes de préjudices corporels - créé par décret le 27 mars 2020, après avis de la CNIL, en statuant à l'égard d'une requête formulée par des cabinets d'avocats ainsi que par les associations APF, France handicap et la Quadrature du Net.

« Le traitement autorisé par ce décret vise à développer un algorithme, chargé d'extraire de manière automatique et d'exploiter les données contenues dans les décisions de justice portant sur l'indemnisation des préjudices corporels » précise le ministère de la justice sur son site.

Les décisions rendues en appel par les juridictions administratives et les formations civiles des juridictions judiciaires entre les années 2017 et 2019, recensées respectivement dans les bases de données de la Cour de Cassation et du Conseil d'Etat, devaient alimenter ce traitement par extraction automatique des données, indique Odile Jami-Caston, directrice du pôle Data et RGPD Compliance au sein du cabinet ITLaw Avocats dans une tribune publiée par le Monde du Droit, en ajoutant que *« malgré leur pseudonymisation avant leur transmission au ministère de la justice (occultation des noms et prénoms des personnes physiques parties aux instances concernées), le maintien d'autres éléments d'identification (date de naissance, lien de parenté), soumet le traitement DataJust au dispositif européen de protection des données personnelles (RGPD) et à la loi Informatique et libertés ».*

Dans le cadre de la procédure pénale numérique, l'objectif était de fournir le maximum d'outils aux magistrats pendant l'audience pour présenter les données d'une affaire de *« manière la plus aidante ».*[65]

Mais, au cours du mois de janvier 2022, alors que cet algorithme était en phase d'expérimentation jusqu'au 27 mars 2022, le ministère de la Justice a mis un terme au développement de son algorithme DataJust,

Comme le souligne Emile Marlzof sur le site *Acteurs Publics*[66], « *de tels référentiels et simulateurs circulent déjà de manière officieuse, fondés sur des analyses partielles. Tout l'enjeu était donc de s'appuyer sur la puissance supposée de l'intelligence artificielle pour en construire un officiel et fiable – mais uniquement indicatif – à partir des décisions de justice, dont l'accès, malgré la politique d'open data, est encore très limité pour les chercheurs et les entreprises spécialisées. Le ministère de la Justice poursuivait aussi, avec ce référentiel, un objectif de désengorgement des tribunaux en espérant qu'il favoriserait le règlement à*

[65] *Cf.* Arnaud Dumourier *in Le potentiel de la donnée appliqué aux domaines du droit et de la justice :* https://www.lemondedudroit.fr/decryptages/78511-le-potentiel-de-la-donnee-applique-aux-domaines-du-droit-et-de-la-justice.html

[66] *Cf.* https://www.acteurspublics.fr/articles/exclusif-le-ministere-de-la-justice-renonce-a-son-algorithme-datajust

l'amiable des litiges. […] Toute la question, désormais, pour le ministère, est de trouver une voie de sortie honorable, ou à tout le moins d'offrir une seconde vie aux travaux initiés en 2019 par la direction des affaires civiles et du sceau avec le programme "Entrepreneurs d'intérêt général", pour tester l'approche et commencer à structurer les données issues des décisions de justice. Le ministère réfléchit donc à un moyen légal de sauver les données collectées dans le cadre de l'expérimentation – plutôt que de les supprimer, comme l'exige le décret de création – et d'en ouvrir l'accès sous conditions à des chercheurs pour qu'ils poursuivent ou mènent leurs propres travaux. La "justice prédictive" n'est pas encore pour demain … »

Concours de circonstance, le décret validant l'usage de DataJust avait été publié quelques jours avant la publication de la recommandation du Conseil de l'Europe sur les impacts des systèmes algorithmiques sur les droits de l'Homme[67] qui met en garde les Etats sur la nécessité d'avoir un système algorithmique qui intègre les droits fondamentaux de l'individu, notamment le droit au procès équitable et à l'égalité des traitements.

Le contexte exceptionnel créé par la pandémie de Covid-19 n'a pas permis la concrétisation des appels lancés en France par les professionnels du droit à leur égard, et ce alors même que nombre des mesures prises au sein de l'UE en réponse à cette pandémie ont eu une incidence sur les systèmes judiciaires au point de conduire les instances compétences de l'UE et du Conseil de l'Europe à mettre en ligne des sites dédiés à ces différents impacts.[68,69]

En particulier, alors que les articles 20 et 21 de la loi pour une République numérique prévoyaient la mise à disposition du public des jugements rendus par la justice française, le dossier est resté en suspens cinq ans après l'adoption de ce texte. Le décret d'application a finalement été publié au mois de juin 2020, en renvoyant certaines des dispositions à la publication d'arrêtés. Dans une décision rendue en janvier 2021, le Conseil d'Etat, saisi par l'association 'Ouvre-boîte', une association dont l'objet est d'obtenir l'accès et la publication effective des documents administratifs et qui avait entamé la procédure en fin d'année 2018, en demandant au garde des Sceaux la publication des décrets d'application relatifs à la publication des données de justice, a sommé le gouvernement de publier l'arrêté en question[70].

Au début de l'automne 2021, la justice administrative a fait un pas de plus dans la diffusion et l'accessibilité de ses décisions. Avec l'ouverture de la plateforme *open data*, toutes les décisions de justice du Conseil d'Etat sont désormais accessibles en format ouvert, suivies par celles des cours administratives d'appel et des tribunaux administratifs au printemps 2022.[71,72]

Lors du Conseil des ministres du 14 avril 2021, Éric Dupond-Moretti, garde des sceaux, ministre de la Justice a présenté un projet de loi pour la confiance dans l'institution judiciaire. Le gouvernement a engagé la procédure accélérée sur ce texte. Le 18 novembre 2021, le Sénat a définitivement adopté le projet de loi, modifié par six amendements du gouvernement, lequel avait été adopté en première lecture, avec modifications, par l'Assemblée nationale le 25 mai

---

[67] *Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme* : https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016809e1124

[68] *Incidences de la pandémie de COVID-19 sur la justice* (site de l'Union européenne) : https://e-justice.europa.eu/content_impact_of_covid19_on_the_justice_field-37147-fr.do?fbclid=IwAR0yuRmP7uUuaY4cCVINw7XuU0VezP0CFp6Zq3o2umHo3ZwTdJ8y7DlAeGU

[69] *Management of the judiciary - compilation of comments and comments by country* (Council of Europe) : https://www.coe.int/en/web/cepej/compilation-comments

[70] *Cf.* https://www.zdnet.fr/actualites/donnees-de-justice-le-conseil-d-tat-rappelle-le-gouvernement-a-l-ordre-39916885.htm

[71] *Qu'est-ce que l'open data du Conseil d'État ?* https://opendata.conseil-etat.fr/

[72] Cette plateforme vient compléter l'offre proposée par la base de jurisprudence *Ariane Web* qui met déjà disposition plus de 270 000 décisions sélectionnées et publiées en raison de leur intérêt jurisprudentiel.
Ariane Web : https://www.conseil-etat.fr/ressources/decisions-contentieuses/arianeweb2

2021, puis par le Sénat le 29 septembre 2021. Le 16 novembre 2021, l'Assemblée nationale avait adopté le texte de compromis, tel qu'élaboré par la commission mixte paritaire le 21 octobre 2021. Avant sa promulgation par le Président de la République, le Premier ministre a fait le choix de procéder à deux saisines du Conseil constitutionnel.

Dans sa décision en date du 17 décembre 2021[73], le Conseil constitutionnel a déclaré l'article 4 de la loi organique pour la confiance dans l'institution judiciaire contraire à la Constitution, et sous les réserves énoncées aux paragraphes 10, 12 et 16, l'article 1er de la loi organique déférée conforme à la Constitution. Les autres dispositions de la loi organique déférée sont conformes à la Constitution. Quant à la question de la conformité à la Constitution de la procédure d'adoption de ladite loi, le Conseil constitutionnel a statué positivement dans une seconde décision en date du même jour[74].

Alors que la justice, grâce aux actions collectives sur la protection des données et de la vie privée, apparaît comme le dernier rempart à l'hégémonie des GAFAM, le système judiciaire national se trouve confronté aux défaillances introduites par une dématérialisation numérique aussi imprudente que précipitée, qui soulève des questions d'ordre technique et éthique.

Or cette loi pour la confiance dans l'institution judiciaire ne comporte aucune disposition relative aux points en suspens ayant trait aux défis posés au système judiciaire par le numérique.

La justice algorithmique comme cette nouvelle loi apporteront-elles réellement les réponses appropriées à l'appel lancé par 3000 magistrats qui dénoncent ouvertement les nombreuses défaillances du système judiciaire : *« […] nous, magistrats judiciaires, qui ne prenons que très rarement la parole publiquement, avons décidé aujourd'hui de sonner l'alarme. Autour de nous, les arrêts maladie se multiplient, tant chez les nouveaux magistrats que chez les magistrats plus expérimentés. L'importante discordance entre notre volonté de rendre une justice de qualité et la réalité de notre quotidien fait perdre le sens à notre métier et crée une grande souffrance. […] Aujourd'hui, nous témoignons car nous ne voulons plus d'une justice qui n'écoute pas, qui raisonne uniquement en chiffres, qui chronomètre tout et comptabilise tout. Nous, magistrats, faisons le même constat que les justiciables. Nous comprenons que les personnes n'aient plus confiance aujourd'hui en la justice que nous rendons, car nous sommes finalement confrontés à un dilemme intenable : juger vite mais mal, ou juger bien mais dans des délais inacceptables. Les attentes fortes des justiciables à l'égard de la justice sont légitimes, les critiques doivent être entendues et vues comme une chance de progresser pour notre institution. Nous devons rester à l'écoute. Mais ce dialogue entre la justice et la société est aujourd'hui rendu impossible par une vision gestionnaire de notre métier à laquelle nous sommes chaque jour un peu plus soumis.*

Affaiblissement de l'Etat de droit : Nous constatons chez nos partenaires du quotidien (services publics de la santé, de l'éducation, de la police…) la même souffrance éthique, le même sentiment de perte de sens. Alors que se sont ouverts les états généraux de la justice [cent vingt jours de consultation citoyenne et de débats qui ont démarré le 18 octobre] avec pour objectif annoncé de renouer les liens entre les citoyens et leur justice, nous, juges du quotidien des tribunaux judiciaires, souhaitons témoigner de nos expériences et de nos inquiétudes sur les conditions dans lesquelles la justice est rendue en France et sur l'affaiblissement de l'Etat de droit qui en découle.

[73] Décision n° 2021-829 DC du 17 décembre 2021 relative à la Loi organique pour la confiance dans l'institution judiciaire : https://www.conseil-constitutionnel.fr/decision/2021/2021829DC.htm

[74] Décision n° 2021-830 DC du 17 décembre 2021 relative à la Loi organique pour la confiance dans l'institution judiciaire : https://www.conseil-constitutionnel.fr/decision/2021/2021830DC.htm .

Nous souhaitons dire haut et fort que malgré notre indéfectible conscience professionnelle, notre justice souffre de cette logique de rationalisation qui déshumanise et tend à faire des magistrats des exécutants statistiques, là où, plus que nulle part ailleurs, il doit être question avant tout d'humanité. Nous souhaitons ainsi rappeler avec force que notre volonté est de rendre la justice avec indépendance, impartialité et attention portée à autrui, telle que l'exige toute société démocratique. »[75]

Il est à noter que cette loi intervient avant même la tenue des Etats généraux de la Justice qui se déroulent sous la supervision d'un comité indépendant présidé par Jean-Marc Sauvé, qui est chargé de garantir l'impartialité et la transparence de la démarche, d'analyser les propositions et de réaliser une synthèse qui sera remise au président de la République.[76]

Or ces Etats généraux constituent une occasion exceptionnelle d'associer les citoyens, les acteurs et les partenaires de la Justice invités à utiliser la plate-forme parlonsjustice.fr pour témoigner de leur expérience et à formuler des propositions concrètes pour bâtir la Justice de demain autour des grandes interrogations suivantes : *Quelle place pour la Justice au sein de notre société ? Comment garantir un meilleur fonctionnement de l'institution pour une Justice plus rapide et plus efficace ?*

- *L'avènement en cours d'une régulation par la donnée modifie profondément le rapport à la norme et interroge la manière dont la société conçoit l'identité comme l'échange social à l'ère numérique.*

Dans un article publié sur le site du Conseil constitutionnel[77], le secrétaire général de la CNIL relève : « *À l'instar des précédentes révolutions industrielles, la révolution numérique bouscule l'ensemble des modèles économiques, technologiques et sociaux habituels. Mais elle modifie aussi profondément le rapport à la norme, qu'il s'agisse de sa substance, de son élaboration […] ou de son application. L'accompagnement de l'innovation implique en effet de passer d'une logique de réglementation à une logique de régulation, c'est-à-dire à un type d'encadrement et d'accompagnement qui combine la fidélité à des principes fondamentaux et à une règle de droit claire, et des nouveaux modes d'intervention du régulateur, fondés sur le droit souple. Or, l'univers numérique repose entièrement sur les données, et notamment sur les données personnelles. […] L'enjeu est dès lors de concilier l'innovation et la protection de ces droits fondamentaux qui sont garantis par la Constitution ou la Charte des droits fondamentaux de l'UE. Cette conciliation n'est ni impossible, comme on le lit parfois, ni un « mal nécessaire ». Elle est la condition sine qua non pour la création d'un environnement éthique et juridique de confiance.* » [78,79]

En vertu du droit à l'information, toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.

---

[75] *Cf.* https://www.lemonde.fr/idees/article/2021/11/23/l-appel-de-3-000-magistrats-et-d-une-centaine-de-greffiers-nous-ne-voulons-plus-d-une-justice-qui-n-ecoute-pas-et-qui-chronometre-tout_6103309_3232.html

[76] *Les États généraux de la Justice :* http://www.justice.gouv.fr/etats-generaux-de-la-justice-13010/

[77] *Droits fondamentaux et innovation : quelle régulation à l'ère numérique ?* : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/droits-fondamentaux-et-innovation-quelle-regulation-a-l-ere-numerique

[78] *A l'heure de la dématérialisation et des services numériques, comment garantir la confiance ? :* https://www.haas-avocats.com/actualite-juridique/a-lheure-de-la-dematerialisation-et-des-services-numeriques-comment-garantir-la-confiance/

[79] *Les outils numériques et la réinvention du fonctionnement de l'Etat :* https://journals.openedition.org/pyramides/988

L'Académie des Technologies, dans son avis rendu public en avril 2020[80], considère que l'amplification de la circulation des données numériques peut assurer une résilience accrue de la société française et européenne en renforçant son indépendance et sa souveraineté, tout en respectant ses valeurs fondamentales et ses lois.

Mais elle ne doit obérer ni la protection de la vie privée, ni le respect des libertés individuelles, ni les droits de propriété.

Plus généralement, cette circulation peut et doit être guidée par l'intérêt général et ne pas remettre en cause les valeurs fondamentales de notre société. Elle déplore que cette circulation existe sous des formes variées et largement sous-contrôlées, que ces données sont thésaurisées le plus souvent dans des entrepôts numériques de quelques grands groupes mondiaux, et que le *Cloud Act* américain permet au gouvernement américain d'avoir accès à toutes les données numériques situées sur son sol[81].

Les professionnels évoluant quotidiennement dans cet univers numérique sont conscients de l'existence d'inquiétudes fortes à l'égard de la montée en puissance des algorithmes dans de nombreux registres de la société.

En témoigne notamment Frédéric Cavazza lorsqu'il affirme : *« La question des algorithmes est clairement devenue un débat de société, car elle touche quasiment tous les aspects de notre quotidien. Certains militent pour un « CSA des algorithmes », un organisme chargé de contrôler et encadrer leur utilisation ; d'autres pour un « serment d'Hippocrate des algorithmes », prononcé par les personnes chargées de les concevoir et les mettre en oeuvre. Je ne saurais pas vous dire si ces solutions pourraient être efficaces, mais s'il la question se pose, c'est qu'il y a un problème, a minima un problème de conscience ou d'acceptation. […] La quatrième révolution industrielle est en marche et personne ne peut l'arrêter. À partir de ce constat, il est de la responsabilité de chacun de comprendre ces changements (leur origine, nature et finalité), de les accepter (s'adapter, changer ses habitudes) et d'y contribuer pour pouvoir en bénéficier. Ce dernier point est très certainement le plus important, car s'il y a bien une leçon que nous ont enseignée les précédentes révolutions industrielles, c'est que ce sont des périodes critiques où s'accélère le déclin des anciens modèles et où les nouveaux sont capables de générer une croissance exponentielle de la valeur. Pour s'en convaincre, il suffit de constater la valorisation des géants numériques et la concentration des capitaux. »*[82]

Dans un article intitulé '*Gouvernance des données et algorithmes publics : quelle stratégie pour l'État* ?'[83], Gaëlle Marraud des Grottes propose un focus particulièrement éclairant sur deux problématiques ayant trait à ces questions : quelle gouvernance pour les données mises à disposition ? L'État doit-il développer ses propres algorithmes ?

Au-delà, la question de l'élaboration d'un véritable *'droit des data'* est plus que jamais pregnante.

[80] *Pour une circulation vertueuse des données numériques :* https://www.academie-technologies.fr/blog/categories/publications-de-l-academie/posts/pour-une-circulation-vertueuse-des-donnees-numeriques

[81] Voir notamment à cet égard : *US Defense Intelligence Agency admits to buying citizens' location data* https://www-theverge-com.cdn.ampproject.org/c/s/www.theverge.com/platform/amp/2021/1/22/22244848/us-intelligence-memo-admits-buying-smartphone-location-data?fbclid=IwAR35myx0Pa1QDX2r20qNur7Q2XuX8xHHsH15J8ZXPkCFbuUiX39O941OOSQ

[82] *Sommes-nous et souhaitons-nous être contrôlés par des algorithmes ?* https://fredcavazza.net/2021/10/21/sommes-nous-et-souhaitons-nous-etre-controles-par-des-algorithmes

[83] *Gouvernance des données et algorithmes publics : quelle stratégie pour l'État ?* https://www.actualitesdudroit.fr/browse/tech-droit/intelligence-artificielle/21517/gouvernance-des-donnees-et-algorithmes-publics-quelle-strategie-pour-l-etat

- *Les objets connectés interrogent*

Après l'Internet, le web puis les *social networks*, nous assistons désormais à l'apparition d'un quatrième réseau, celui des objets connectés. Rendu possible par le développement de la 5G, cette nouvelle connectivité demeure largement impensée.

Bernard Benhamou, alors qu'il était Délégué aux Usages de l'Internet au sein du Secrétariat d'Etat au développement de l'économie numérique : *« L'irruption de l'Internet dans la « vie de tous les jours » soulève cependant de nombreuses questions sur les mesures que les créateurs de ces nouveaux services prendront pour éviter que la vie privée ne soit progressivement remise en question. À mesure que l'Internet épouse l'ensemble des activités quotidiennes des citoyens, la protection des libertés et de la vie privée devient plus essentielle encore. En effet, la convergence des technologies de mobilité, de géolocalisation et d'identification des objets pourrait installer auprès des citoyens des systèmes de plus en plus intrusifs. En effaçant progressivement les frontières entre individus connectés et non connectés, et en devenant « invisibles » pour leurs utilisateurs, ces réseaux ubiquitaires ou encore cet Everyware, pour reprendre le néologisme d'Adam Greenfield, pourraient aussi remettre en cause la notion même de vie privée. L'objectif d'une « connectivité généralisée » évoqué par l'ensemble des acteurs industriels de ce secteur, s'il est porteur d'espoirs économiques pourrait aussi se transformer en perspective « orwellienne » si des précautions n'étaient pas prises pour s'assurer que les citoyens en gardent la maîtrise. »* tout en soulignant le rôle crucial joué par l'Union européenne pour l'émergence d'une gouvernance européenne de ces objets.[84]

Dans son essai *The Computer for the 21st Century* de 1991, dans lequel il imagina les ordinateurs et le monde des ordinateurs au milieu ou à la fin du 21e siècle, Mark Weiser alertait déjà près de 20 années plus tôt sur les risques soulevés par l'invisibilité de ces technologies : *« Les technologies les plus profondément enracinées sont les technologies invisibles. Elles s'intègrent dans la trame de la vie quotidienne jusqu'à ne plus pouvoir en être distinguées. »*

Dès 2008, l'OCDE alertait également sur les enjeux de sécurité attachés au développement des objets connectés : *« La création d'un "Internet des Objets", le développement et la diffusion ubiquitaire des technologies basées sur les capteurs, vont à terme brouiller les frontières entre monde virtuel et monde physique et pourraient modifier la nature même de la vie privée. Les enjeux de sécurité sur le long terme restent encore à analyser et à résoudre. »*[85]

Aujourd'hui, le sociologue Dominique Boulier appelle à un grand débat public : *« L'affaire semble entendue, l'Internet des objets est non seulement annoncé comme inéluctable mais il est déjà là. Et tous les objets connectés que nous utilisons sans nous en rendre compte, de même que les capteurs qui équipent nos villes nous le démontrent, même s'ils ne sont pas connectés à Internet et utilisent des technologies WiFi ou Bluetooth ou des RFID en local : nous ne pouvons pas nous en passer. Pourtant, le saut que constitue cette nouvelle connectivité (des adresses IP pour tous les objets) mérite examen, et même plus, débat public. Car c'est d'un nouveau réseau qu'il s'agit, qu'il faut penser et discuter stratégiquement pour l'orienter selon des visées de bien commun et non seulement parce que le code court et que l'innovation n'attend pas. Trois questions (au moins) méritent d'être soulevées avant ce déploiement déjà bien avancé : l'architecture de réseau, la sécurité et notre couplage aux objets. »*[86]

[84] *L'Internet des objets. Défis technologiques, économiques et politiques :* https://esprit.presse.fr/article/benhamou-bernard/l-Internet-des-objets-defis-technologiques-economiques-et-politiques-14799

[85] *Radio Frequency Identification (RFID) : A Focus on Information Security and Privacy* (Working Party on Information Security & Privacy- OCDE, 14 janvier 2008 http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/$FILE/JT03238682.PDF

[86] *Internet des objets : pour une stratégie médiologique* https://aoc.media/analyse/2021/11/17/Internet-des-objets-pour-une-strategie-mediologique/

- *Les craintes associées à l'émergence du Web 3.0 et du métavers*[87]

« *Le Web 2.0 nous a dépossédés de tout : nous ne sommes rien en ligne, nous ne sommes qu'un produit de Google ou de Facebook… Nous donnons tout à ces sociétés qui contrôlent notre être numérique* », dénonce Pascal Gauthier, le directeur général de l'entreprise technologique française *Ledger*, qui conçoit, fabrique et commercialise des clefs sécurisées pour conserver cryptomonnaies et *NFT* (objets numériques certifiés).

Dans le *Web 3.0*, « *je possède tout, je peux avoir par exemple mon argent et mes données de santé sur un portefeuille sécurisé* », explique-t-il. « *Quand je suis chez le médecin, je lui ouvre l'accès à mes données de santé avec le portefeuille sécurisé, et quand il n'en a plus besoin, je lui coupe l'accès* ».

Qu'est-ce que l'on appelle *Web 3.0* qui succède au *Web 2.0*[88] : *« Le Web 2.0 est l'Internet tel que nous le connaissons aujourd'hui, à commencer par les prototypes de pages Facebook et le commerce électronique. C'est une période où la connectivité est largement mise en avant ; vous pouvez discuter avec des amis, recevoir des réponses instantanées à n'importe quelle question dans le monde et acheter presque tout ce que vous voulez en ligne. Bien que le Web 2.0 ait apporté de vastes changements, il pose également de nombreux problèmes pour les utilisateurs finaux. La plupart des critiques formulées contre le Web 2.0 concernaient ceux qui détenaient le pouvoir sur Internet. Bien sûr, l'avènement d'entreprises comme Méta-plateformes (NASDAQ : FB) et Alphabet (NASDAQ : GOOG, NASDAQ : GOOGL) ont apporté d'énormes commodités, mais ils ont également créé une perturbation quant à savoir qui contrôle l'espace numérique. Les récents scandales de Meta ont été l'exemple le plus brillant de ce déplacement de pouvoir. Les lanceurs d'alerte ont exposé les manières dont l'entreprise a manipulé ses utilisateurs, les consommateurs finaux d'Internet. De plus, il existe une grande controverse sur la manière dont les entreprises extraient les données personnelles et les utilisent pour cibler des utilisateurs spécifiques.*

Le Web 3.0 est la réponse directe à ce déséquilibre de pouvoir. Il cherche à résoudre ce problème en remettant le pouvoir entre les mains des utilisateurs grâce à la décentralisation. Les données et le pouvoir sont actuellement centralisés parmi les géants de la technologie comme Meta et Alphabet. Avec le Web 3.0, ces données peuvent rester aussi privées que l'utilisateur le souhaite. Il libère également les utilisateurs des indiscrétions des règles de ces sociétés sur les utilisateurs. Internet est considéré comme une frontière pour la liberté d'expression, en grande partie grâce à la connectivité favorisée par les médias sociaux. Et pourtant, les utilisateurs sont toujours soumis à des règles établies au gré des sociétés au pouvoir.

Grâce aux progrès de la technologie blockchain, la voie à suivre pour le Web 3.0 est relativement claire. Vous entendez tout le temps des crypto bulls parler de décentralisation sur les réseaux blockchain. Il existe des applications décentralisées, des finances décentralisées, des organisations autonomes décentralisées (DAO) et ainsi de suite. L'Internet tel que nous le connaissons évolue lentement vers la blockchain, car c'est là que les utilisateurs peuvent conserver leur propre indépendance. Comme le démontre la crypto-monnaie, il existe une forte demande pour un endroit où les gens peuvent investir leur argent comme ils le souhaitent et pour des rendements supérieurs à ceux que les banques peuvent offrir ; cela ressort clairement

[87] Un « métavers » est un monde virtuel fictif. Le terme est régulièrement utilisé pour décrire une future version d'Internet où des espaces virtuels, persistants et partagés sont accessibles via interaction 3D
Qu'est-ce que le métavers ? https://www.francetvinfo.fr/economie/bitcoin/on-vous-explique-ce-qu-est-le-metavers-l-Internet-du-futur-qui-fait-rever-la-tech_4757523.html

[88] *FAQ Web3 : qu'est-ce que le Web 3.0 ? Et pourquoi Elon Musk l'appelle-t-il « BS » ?*
https://www.marseillenews.net/faq-web3-quest-ce-que-le-web-3-0-et-pourquoi-elon-musk-lappelle-t-il-bs.html

du succès des protocoles DeFi, qui permettent de faire des choses comme mettre des actifs en jeu pour un revenu passif.

Il existe également une forte demande pour un Internet décentralisé. Avec le Web 3.0, on pourra utiliser des choses comme les applications de médias sociaux, où les développeurs ont renoncé au pouvoir et les utilisateurs établissent des règles sur le type de contenu qui peut et ne peut pas être publié via les efforts de vote de la communauté. Ils pourraient ensuite passer à un protocole DeFi et effectuer un échange de jetons, ou utiliser leurs jetons dans le métaverse. Plus important encore, ils pouvaient faire tout cela sur un seul compte personnel, en se connectant gratuitement. Les possibilités sont aussi infinies qu'Internet tel que nous le connaissons aujourd'hui, mais sans sacrifier la puissance ou les données.

[…] À l'heure actuelle, il existe une poignée de projets de cryptographie Web 3.0. Les développeurs créent des protocoles pour partager Internet sans fil, partager un espace de stockage de données sécurisé et créer les bases d'un Internet décentralisé plus large. Des projets comme Pois (CCC : DOT-USD) mènent la charge comme certains des premiers efforts du Web 3.0 ; en effet, Polkadot a le soutien total de la Fondation Web3, qui cherche à accélérer le développement de la prochaine itération d'Internet. »

À l'image de la technologie du *Cloud*, le *Web 3.0* a révolutionné le fonctionnement d'Internet, mais de façon beaucoup plus importante. La décentralisation est une caractéristique indissociable du *Web 3.0*. La gestion des données n'étant pas centralisée, le *Web 3.0* offre une meilleure socialisation des utilisateurs pour le travail et les loisirs. Ces différentes interactions peuvent se réaliser dans un espace virtuel innovant appelé métavers (ou métaverse). Outre son aspect ludique, la capacité de cet espace à développer une économie parallèle a conduit de nombreuses entreprises à accélérer leurs plans de transformation numérique.

Le métavers a connu une adoption massive en un rien de temps. En effet, depuis janvier 2020 le nombre d'utilisateurs actifs de *wallets* en lien avec le métavers a été multiplié par 10. Cette donnée est un bon indicateur pour jauger l'adhésion du public à moyen terme. Si pour l'heure les principaux cas d'usage du Métavers et des NFT se trouvent dans la sphère du *gaming*, les opportunités offertes sont bien plus nombreuses.

Les possibilités étant nombreuses, chaque entreprise de l'industrie numérique définit sa propre vision du rôle que doit jouer le métavers dans le *Web 3.0*.

Leaders du secteur, Microsoft, Facebook et Apple ont donc décidé de développer des métavers propres à leurs communautés respectives. Ces géants de la technologie tentent de se challenger eux-mêmes grâce à l'évolution de la façon dont les utilisateurs passent leur temps libre.

Cette course cache malheureusement un désir de contrôler les données qui seront générées dans le *Web 3.0*. On s'aperçoit alors très vite que le fait de laisser le développement des métavers à ces sociétés remettra en cause la décentralisation du *Web 3.0.*

Pour James Muldoon, auteur de *'Platform Socialism : How to Reclaim Our Digital Future From Big Tech'* : *« Le virage de Mark Zuckerberg vers le « métavers » a pour but d'ajouter une strate numérique supplémentaire à notre réalité. Mais la nouvelle marque Meta de Facebook n'augmente pas votre réalité – elle veut tout simplement en tirer plus d'argent. »*[89]

Dans un article publié par la revue en ligne *The Conversation* et dans lequel il liste les différentes initiatives et entreprises engagées dans cette nouvelle compétition technologique, le professeur Oihab Allal-Chérif soulève d'autres questions : *« Doit-on laisser une entreprise aussi dominante que Meta, qui a fait l'objet de plusieurs polémiques en 2021 et de nombreuses*

[89] *Facebook Is Now Meta. And It Wants to Monetize Your Whole Existence :* https://jacobinmag.com/2021/10/mark-zuckerberg-meta-facebook-rebrand-metaverse

autres controverses depuis sa création, créer une plate-forme tellement puissante qu'elle permettra de contrôler tous les aspects de notre vie ? Quelles sont les garanties données aux utilisateurs des métavers que ces espaces virtuels seront sécurisés et éthiques ? Comment éviter une hypercentralisation de l'activité numérique où une seule entité privée gérera toutes nos interactions sociales et nos transactions pour en tirer profit ?

Ces inquiétudes sont d'autant plus légitimes que le projet de Meta conduit par nature à une situation monopolistique en voulant remplacer tout Internet. D'une part il n'est rentabilisé et ne fonctionne de manière optimale qu'au-delà d'une taille critique très grande. D'autre part les utilisateurs, qui ont un temps limité et cherchent à optimiser leurs activités numériques, vont choisir de manière quasi exclusive d'être présents dans un seul métavers.

La démarche de Meta semblerait donc aboutir à une propriété et un contrôle total du métavers à travers le matériel et le système d'exploitation. Cependant, Meta affirme déjà que son métavers sera ouvert, collaboratif, et interopérable avec des standards universels. Comme Internet, il ne serait la propriété de personne et serait régulé par toutes les parties prenantes, dont les pouvoirs publics. Plusieurs métavers pourraient coexister et être connectés les uns aux autres, ce qui limiterait la captivité et les dérives.

Cependant, à défaut d'une régulation par les gouvernements qui sont toujours très en retard sur la technologie, il semble essentiel que les entreprises s'accordent sur de bonnes pratiques en matière de respect de la vie privée, de cybersécurité, de lutte contre la désinformation, et de consentement éclairé des consommateurs vis-à-vis des technologies utilisées dans les métavers. »[90]

Les interrogations que soulèvent cette nouvelle évolution sont suffisamment fondamentales pour que *The Conversation* y consacre un numéro spécial dans lequel David Crête alerte sur les risques que pourraient générer l'apparition du métavers, et notamment les addictions qui pourraient en découler[91].

Andreas Kaplan s'attache dans ce dossier à remettre les choses en perspective quant à l'agenda technologique dédié au déploiement du métavers pour conclure son propos par les questions suivantes : *« que signifierait un tel développement pour notre société, et si cela est souhaitable pour l'humanité ? Comment se préparer au mieux à une telle évolution éventuelle ? »*[92].

Dans un dossier publié sur le portail de l'intelligence économique sous l'intitulé *'Le metaverse, enjeu de souveraineté'*, Matthias Hauser appelle les Etats à agir pour ne pas subir : *« Bien sûr, les sociétés humaines semblent encore très loin d'une telle situation. Mais en 2000, qui aurait pu imaginer que 10 ans plus tard la quasi-totalité des rapports humains passeraient via des réseaux sociaux ? Les échelles de temps sur lesquelles s'opèrent les changements sociétaux se sont accélérées. En 2021, quiconque se demande si le monde s'achemine vers le « metaverse » a déjà 5 ans de retard. La question ne se pose pas, ou plutôt elle ne se pose plus. Ce monde est déjà là, il est en construction. Notre seule marge de manœuvre se trouve dans notre capacité à orienter ce modèle qui se construit : normes, lois, incitations, protection de la vie privée, place laissée aux GAFAM, centralisation, émergence de nouvelles entreprises, régulation de ces dernières, etc. Or, la réponse à apporter à cette métaversisation du monde commence maintenant, en ne réduisant pas ce sujet à sa seule dimension technique et numérique mais en saisissant les profondes ramifications des changements que cela entraînera.*

[90] *Univers parallèles et mondes virtuels : la guerre des métavers est commencée :* https://theconversation.com/univers-paralleles-et-mondes-virtuels-la-guerre-des-metavers-est-commencee-169695

[91] *Le métavers de Facebook : prison ou révolution ?* https://theconversation.com/le-metavers-de-facebook-prison-ou-revolution-171997

[92] *Facebook et son « métavers » : le cauchemar devient-il réalité ?* https://theconversation.com/facebook-et-son-metavers-le-cauchemar-devient-il-realite-172455

Sauf cygne noir, nos enfants passeront le plus clair de leur temps dans des mondes virtuels, c'est-à-dire qu'ils accorderont probablement plus de valeur à leur vie virtuelle qu'à leur vie physique. Cela est déjà acté, même si on peut le regretter.

La seule question qui se pose encore aujourd'hui est donc de savoir si les mondes virtuels où vivront nos enfants seront encore sous le contrôle des États… ou bien sous le contrôle de quelques entreprises qui émettront leur monnaie virtuelle, choisiront leurs taux d'intérêt virtuels, les loyers de vos appartements ou bureaux virtuels, qui feront de leurs Terms of Service le nouveau Code Civil de ces lieux virtuels, qui nommeront une police virtuelle pour exclure de ce monde (et donc du monde) les utilisateurs problématiques.

C'est parce que les États restent à genoux que les entreprises privées sont grandes. Cela restait vrai jusqu'à aujourd'hui, avec en filigrane l'espoir d'une riposte étatique pour reconquérir la sphère numérique et la réguler. Mais cet espoir diminue à mesure que l'idée du Metaverse fait son chemin : le retard des États sur ces sujets pourrait rapidement s'avérer irréversible. Sans action puissante des décideurs politiques, sans prise de conscience immédiate de l'opinion publique, les États risquent donc d'être davantage phagocytés par les intérêts privés qui se substituent déjà à certaines fonctions (privatisation de l'éducation et de la santé ou autres services sociaux). C'est aujourd'hui que les États doivent choisir s'ils seront encore ce qu'ils sont dans le monde de demain. »[93]

Dont acte.

- *La protection des droits numériques appelle à repenser le modèle actuel*

Nitin Gaur**,** le fondateur et directeur d'*IBM Digital Asset Labs*, où il élabore des normes de l'industrie et des cas d'utilisation et travaille à faire de la blockchain pour l'entreprise une réalité, appelle à repenser le modèle actuel des droits numériques pour l'adapter au nouveau contexte du *Web 3.0* tout en proposant des préconisations techniques opérationnelles : *« Pour comprendre la complexité de la gestion des droits numériques, ou DRM, il faut d'abord comprendre les défis DRM des systèmes actuels, puis les défis (et les opportunités) présentés par la technologie blockchain qui se targue de la transparence, la liaison de données et l'immuabilité comme certaines des principales caractéristiques qui se prête aux systèmes de confiance.*

Avec le Web 2.0, la création et la diffusion de contenus se font via une plateforme qui fait office d'intermédiaire et, comme tout intermédiaire, a développé des modèles économiques qui monétisent les voies de diffusion des contenus, les données et métadonnées qui en résultent. Le contenu numérique (films, images, musique, etc.) peut être facilement répliqué et les plates-formes créent des fossés économiques et des mécanismes de contrôle pour accéder au contenu avec la conception compliquée à n-tiers des mots de passe, de l'authentification, de l'autorisation et de la mesure de l'utilisation.

Au fil du temps, cela a été exploité en raison des vulnérabilités de la technologie Web 2.0 conçue pour la diffusion de l'information. Le Web 3.0 basé sur les systèmes de blockchain remet en question ce modèle en modifiant fondamentalement les caractéristiques de la plate-forme des plates-formes compatibles Web 2.0, car toutes les constructions du Web 3.0 tournent autour de modèles décentralisés (ou dans certains cas quasi-décentralisés), axés sur la conception et appliquent des principes fondamentaux du commerce (des actifs numériques), de la confiance (appliquée par le protocole, c'est-à-dire des modèles de consensus) et de la propriété (revendication sur l'actif).

[93] *Le metaverse, enjeu de souveraineté :* https://portail-ie.fr/analysis/3022/le-metaverse-enjeu-de-souverainete-12

L'avènement du Web 3.0 modifie les modèles informatiques fondamentaux en les décentralisant : stockage et interconnexion enveloppés d'une structure économique incitative qui favorise la participation et l'engagement et donne naissance à une toute nouvelle plateforme de structure économique. Dans un véritable marché axé sur le numérique, le réseau alimenté par la blockchain garantit que les relations et les interactions dynamiques du marché se reflètent de manière systémique et intelligente.

Alors que nous concevons des réseaux de blockchain pour les industries, nous voyons émerger de nouveaux modèles commerciaux intéressants, amenant de nombreuses organisations à repenser leurs modèles commerciaux actuels, la concurrence et le paysage global du marché. Cette co-création implique l'ouverture et la possibilité pour les participants d'échanger des données à travers les nœuds qui prennent en charge la nouvelle vague d'infrastructure Web 3.0. Cela implique le stockage de données, de contenu et d'autres mèmes précieux qui reflètent la communauté numérique et la culture peer-to-peer si intrinsèque aux écosystèmes basés sur la blockchain.

Avec ces principes de conception et de distribution, comment les « droits numériques » sont-ils gérés sur la blockchain sans normes claires concernant l'identité, l'accès et les défis liés à l'interopérabilité ? Le système de blockchain est fondamentalement un système de transaction, sécurisé par un ordinateur distribué pour plus de résilience et d'efficacité, et les constructions de portefeuille (structure de clé privée-publique) fournissent un cadre de réclamation pour les actifs numériques sécurisés par le système de transaction. Les DRM ne peuvent tout simplement pas s'intégrer dans la conservation des clés privées avec des portefeuilles ou des réclamations sur les actifs. Bien que ERC-721 et ERC-1155 fournissent un cadre de jeton non fongible (NFT), il ne fournit certainement pas un soutien systémique et des mesures de protection technologique centrées sur une plate-forme unique.

La révision de DRM nécessite de repenser au-delà de l'accès aux données et au contenu qui peuvent être copiés et répliqués. Nous devons commencer à inclure les notions de valeur, de propriété et de revendications comme impératifs de conception. Ces impératifs de conception peuvent faire partie de la première couche, qui serait systémique, ou construits en tant qu'application de couche deux ou organisation autonome décentralisée (DAO).

Les NFT ont révolutionné le paysage créatif de l'art, de la culture, de la musique, du sport et plus encore, mais la nature du contenu numérique et les dangers de celui-ci demeurent, et envelopper cette représentation tokenisée avec une vérification chiffrée et un processus de validation garanti par la blockchain n'est pas suffisant. C'est parce que ceux-ci sont confinés à un seul réseau et peuvent avoir besoin d'utiliser des ponts pour déplacer les représentations tokenisées avec une vérification supplémentaire, et cela ne concerne que la propriété ou la revendication. Il ne garantit pas des « droits ».

Nous devons nous lancer dans un modèle qui s'appuie sur la technologie et les systèmes de registre numérique qui traitent les droits numériques comme une revendication irréfutable et incluent la licence et l'attribution dans l'accès et les revendications à une représentation symbolique. Cela peut être réalisé en développant une identité en tant que jeton NFT et en utilisant ensuite le jeton avec une licence et une attribution qui fournit une revendication et un accès irréfutables, déléguant ainsi l'attribution à la représentation tokenisée. Une telle conception comprendra un modèle multi-tokens qui devra être joint pour les revendications et l'accès – comme un jeton d'identité pour lequel la licence et l'attribution sont soit des classes d'actifs soit des métadonnées – et les NFT seraient les actifs qui auraient alors besoin d'une preuve de propriété ou licence et un méta-modèle d'attribution. Le modèle utiliserait la structure économique du Web 3.0 pour stocker, vérifier et diffuser du contenu. »

- *La monétisation des données suscite bon nombre d'interrogations.*

La monétisation des données est devenue un enjeu capitalistique considérable.

Le site *Privacy Affairs* a mis à jour son indice des prix pratiqués sur le *Dark web* pour l'année 2021.

Et comme chaque année, les chiffres donnés peuvent laisser sans voix. De fait, le coût relativement faible de certains éléments, comme des codes de cartes bleues, nous montre à quel point l'offre est grande.

On apprend aussi que certaines informations ou accès numériques, comme à un compte Gmail, valent plus que des données bancaires.

Et cela en dit long sur la santé du monde de la cybercriminalité, plus florissant que jamais avec des cibles géantes comme *FireEye*, *SolarWinds*, *Visa*, *Mastercard*, *Microsoft*, *Lockheed Martin* et bien d'autres, tous touchés par des vol de données l'an dernier.[94]

Pour l'avocat Philippe Mösching : *« Le principe de monétisation des données personnelles se fonde sur un principe individualiste de propriété appliqué aux données alors que l'économie de la connaissance par les données se fonde sur la collecte de données la plus large possible et leur libre partage. Ces deux approches sont incompatibles. Monétiser ses données, c'est tuer la connaissance par les données, c'est priver la société de l'extraordinaire pouvoir que l'exploitation de ces données peut nous offrir. C'est aussi faire le deuil de projets nécessaires et qui dépassent la société humaine, comme la mesure de l'impact environnemental par les comportements humains : déplacements, consommation, habitudes alimentaires, besoin en énergie, dont l'objectif est de mieux connaître pour mieux servir à moindre impact. »*[95]

- *La technologie 'Blockchain' est en mesure de bouleverser le droit en profondeur*

Une blockchain est une base de données décentralisée et sans intermédiaire qui permet d'automatiser une transaction, de l'authentifier et de l'horodater, tout en garantissant son immuabilité et son inviolabilité[96]. Pour le moment (voir *infra*), cette technologie permet également d'assurer la confidentialité des données grâce au cryptage.

---

[94] *Sur le dark web, votre compte Gmail coûte plus cher qu'une carte bleue volée :* https://www.clubic.com/antivirus-securite-informatique/actualite-372998-sur-le-dark-web-votre-compte-gmail-coute-plus-cher-qu-une-carte-bleue-volee.html

[95] *Tirer profit du Big Data sans compromettre nos libertés :* *https://www.contrepoints.org/2020/06/01/372580-tirer-profit-du-big-data-sans-compromettre-nos-libertes-4-5*

[96] *« Une blockchain associe de manière originale deux technologies déjà connues. La première consiste en la sécurisation de blocs de données par cryptages successifs rendant impossible la falsification de l'un de ces blocs, tous étant comme « encastrés », avec leurs dates, dans une série d'autres blocs. La seconde est l'exploitation d'un réseau distribué pour exécuter une application informatique. En d'autres termes, une blockchain est une base de données, un registre qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Et cette base de données est distribuée, transparente, décentralisée et sécurisée. En informatique, une base de données distribuée est traitée par un réseau d'ordinateurs interconnectés dont chacun stocke les données en cause. Ensuite, on enchaîne les blocs d'informations les uns aux autres grâce à des hashs, des empreintes numériques uniques pour chacun. L'intérêt du hashage est de ne s'appliquer que dans un 2 sens : il n'est pas possible, à partir d'un hash donné, de remonter au contenu d'origine ; en revanche, il suffit de hasher à nouveau ce contenu pour vérifier que les hashs sont identiques et donc qu'aucune modification du contenu en question n'a été opérée. La blockchain est ainsi protégée contre les risques de falsification par les nœuds de stockage, tout le monde pouvant vérifier la validité d'une information en consultant la base de données. Et sa grande caractéristique est bien de fonctionner sans organe central de contrôle, sans intermédiaire, sans serveur principal. L'inaltérabilité est garantie par un réseau de pairs indépendants. Chaque ordinateur possédant une copie de la blockchain constitue un « nœud » s'assurant en permanence de son intégrité. C'est pourquoi la technologie blockchain est extrêmement solide : ce n'est pas un tiers de confiance éventuellement corruptible ou partial qui valide les opérations. Chaque bloc comporte une marque numérique qui l'associe au bloc précédent et le certifie ; et cette opération de marquage est assurée par des utilisateurs volontaires, appelés « mineurs ». Ces derniers mettent à disposition la puissance de calcul de leurs ordinateurs pour administrer la blockchain contre rémunération — ce qui a donné naissance au phénomène du « cryptojacking », consistant à introduire un script qui, lors de*

Dans une publication intitulée *'Les blockchains et le droit'*[97], Boris Barraud, enseignant-chercheur en droit et en sciences de l'information et de la communication, spécialiste de la communication numérique et de l'intelligence artificielle, tire la sonnette d'alarme sur les grands bouleversements qu'est en train d'occasionner cette technologie de rupture : *« Cette technologie pourrait engendrer des conséquences importantes à l'égard du système juridique et des habitudes des juristes. Les enjeux liés à la relation entre blockchains et droit sont majeurs, en termes de blockchains saisies par le droit, mais aussi et surtout en termes de droit saisi par les blockchains. En particulier, la gouvernance des blockchains et la force juridique des opérations réalisées au moyen de cette technologie posent question ; et les réponses commencent seulement à se stabiliser. Les blockchains obligent à réinventer les métiers de légiste et de juriste, tandis que les codeurs sont appelés à faire du droit — plus ou moins consciemment. Dans un futur qu'il n'est pas nécessaire d'imaginer lointain, les legal start-up [ou legaltech) spécialisées dans la technologie blockchain pourraient produire et/ou appliquer beaucoup de normes, complétant ou concurrençant le droit « classique ». Les professionnels du droit devraient alors collaborer avec les développeurs afin de créer les outils juridiques de demain. Profitant de l'essor des nouvelles technologies numériques, les blockchains seraient à l'origine d'un phénomène de remplacement rapide d'un modèle par un autre ; et cela impacterait jusqu'au droit et à l'État. Elles pourraient être l'élément déterminant dans le processus menant du droit moderne au droit postmoderne et de l'État moderne à l'État postmoderne — à moins qu'il faille davantage y voir la source d'un paradroit, une forme de régulation sans droit et sans État. Au-delà, l'économie, la finance et la structure et le fonctionnement de la société dans son ensemble pourraient être profondément changés, avec la grande mutation des mécanismes de transaction et de certification. Serait notamment remise en cause l'utilité des plateformes jouant un rôle d'intermédiation. Ces promesses s'accompagnent forcément de défis et de menaces, qui touchent y compris le droit et qui l'obligent à réagir. Les États pourraient être lourdement impactés, interrogés dans nombre de leurs missions dites « régaliennes », qu'ils ne seraient plus seuls en mesure d'accomplir. Le rêve libertarien et crypto-anarchiste serait proche de devenir réalité : en profitant des opportunités offertes par les nouvelles technologies de communication, se passer d'État — si ce n'est pour assurer par la force le respect des conventions privées. »*

---

l'utilisation d'un service en ligne, déclenche des calculs de « minage », monopolisant ainsi le processeur de l'utilisateur sans son consentement.

[…] Par ailleurs, doivent être distinguées les blockchains publiques et les blockchains privées. Les blockchains publiques sont ouvertes à tous ; n'importe quel utilisateur peut enregistrer des opérations sur les chaînes de blocs ou participer à la validation des opérations. À l'inverse, l'accès aux blockchains privées et leur utilisation sont restreints à certains acteurs précisément identifiés et sont sous le contrôle d'un organisme particulier qui maîtrise le processus d'approbation. Avec la chaîne de blocs privée, une seule et même organisation peut limiter les autorisations d'entrée, de lecture et d'écriture, de telle sorte qu'un tiers de confiance apparaît et que la décentralisation est très imparfaite, ce qui, pour beaucoup de spécialistes, va à l'encontre de l'esprit originel de la technologie blockchain — « blockchain privée » serait un oxymore. Une blockchain privée peut aussi reposer sur des procédés de cooptation ou de consortium, les contrôles étant alors effectués par un ensemble présélectionné de nœuds.

[…] Pour l'heure, la technologie blockchain souffre toutefois de la complexité de son protocole, qui la rend peu accessible. Elle en serait au même niveau que le protocole TCP/IP avant l'invention du World Wide Web, au temps d'Arpanet, ancêtre de l'internet actuel. À bien des égards, la situation actuelle ressemble à celle de l'internet dans les années 1980 — les attentes, parfois exagérées, côtoient le scepticisme, parfois également exagéré, mais le potentiel de la technologie est certain.

[…] Pour l'instant, il n'existe pas encore de véritable écosystème des blockchains. Très peu de start-up s'y intéressant dégagent des bénéfices. L'heure est toujours à l'exploration. Pour autant, des sociétés multinationales commencent à investir dans cette technologie, conscientes que leurs secteurs d'activité pourraient être bientôt « blockchainisés ». L'engouement suscité par les blockchains et par leurs promesses a un effet d'entraînement et un cercle vertueux s'enclenche, laissant supposer que les blockchains seraient en mesure de conquérir le monde comme l'internet l'a fait. » (Boris Barraud)

[97] *'Les blockchains et le droit'*, Revue Lamy droit de l'immatériel (Wolters Kluwer), n° 147, avr. 2018, p. 48-62 https://www.academia.edu/36141168/_Les_blockchains_et_le_droit_Revue_Lamy_droit_de_l_immat%C3%A9riel_Wolters_Kluwer_n_147_avr_2018_p_48_62

- *La disparition progressive des liquidités monétaires au profit des transactions numériques, en participant à l'avènement du monde post-moderne, interroge*

L'engouement dans le monde pour les monnaies digitales (ou cryptomonnaies) de banques centrales, qui accompagnent l'accélération de la digitalisation de la société en répondant aux projets de monnaies digitales privées comme *Bitcoin* ou *Libra*, et en ouvrant de nouvelles voies de soutien monétaire plus directes – entre les banques centrales et les agents économiques - et plus efficaces – y compris sur le registre de la sobriété énergétique[98] -, tout en accroissant la stabilité financière, témoigne d'une volonté générale de rupture avec les monnaies traditionnelles et les sources d'instabilité et de crises systémiques qu'elles induisent de manière cyclique.

Ces monnaies digitales reposent nécessairement sur l'emploi de la technologie *'blockchain'*.

Pourtant, comme le relève Floriant Renault : *« À ce jour, la blockchain est clivante : elle peut tout aussi bien être considérée comme fascinante ou dangereuse. Les grandes institutions internationales critiquent son utilisation, jusqu'à réfuter sa définition de monnaie. « Les cryptomonnaies ne sont pas des monnaies. Point final. » a déclaré Christine Lagarde. Or l'intérêt des banques centrales pour la technologie blockchain est bien réel. Chacune à leur tour, elles annoncent des projets définissant leurs monnaies numériques, comme le e-Yuan en Chine, le MNBC en Europe ou le CBDC aux États-Unis. Créer leur propre monnaie leur permettrait une traçabilité absolue de chaque unité monétaire numérique. Ce contrôle total aurait pour effet de taxer chaque individu et de prévenir toute possibilité d'évasion fiscale. Les échanges monétaires jusqu'aux échanges intercontinentaux seraient instantanés, et de surcroît à un coût négligeable. Par nature, une cryptomonnaie est définie par deux paramètres principaux : la masse monétaire totale et son volume d'émission dans le temps. Néanmoins, ce n'est pas encore le cas des projets des cryptos made in banques centrales. En effet, la cryptomonnaie des institutions est assimilable au « fiat », c'est-à-dire qu'elle représente une monnaie fiduciaire, comme le dollar ou l'euro. Tout le système en est donc dénaturé : il s'agirait alors d'un simple tour de passe-passe intégrant une nouvelle technologie tout en omettant certains de ces paramètres pour prolonger une politique monétaire toujours plus accommodante. L'injection de monnaie dans l'économie depuis 2008, et d'autant plus depuis la pandémie, interroge en termes d'impact sur l'inflation. Une monnaie dont le nombre d'unités est connu à l'avance semble devenir, pour une part des crypto connaisseurs, un autre moyen de se couvrir contre l'inflation, en plus d'un pari sur la technologie, face à des marchés financiers allant de sommets en sommets. Certaines banques, fonds d'investissements ou même entreprises tels que GP Morgan, Deutsche Bank, Grayscale ou MicroStrategy proposent déjà cette nouvelle exposition. […] 2 milliards de personnes n'ont aujourd'hui pas accès à des services bancaires, mais ont un smartphone. C'est un nouveau monde qui s'offre à eux en simplifiant les échanges entre les personnes, les entreprises et leurs gouvernements. Le Salvador a d'ailleurs instauré le Bitcoin comme monnaie officielle, devenant pionnier en la matière. D'autres pays émergents d'Amérique du sud ou d'Afrique suivent le pas. Dans des pays où la monnaie est parfois dollarisée ou face à une dominance d'une autre monnaie, il leur est vital de gagner en autonomie. […] Avant tout, il faut comprendre cette technologie dans ses grandes visions et solutions. Il est essentiel de regarder l'utilité qu'annonce le projet et s'il tient ces promesses de développement. Il ne faut pas oublier qu'un grand nombre de projets échouent à prouver leurs capacités à concevoir ou même leurs utilités concrètes. Mais conservons à l'esprit que certains projets seront les nouveaux GAFAM de la cryptomonnaie. Il y a déjà 300 millions de personnes dans le monde, dont la majorité depuis moins d'un an, ont*

[98] Par exemple, en utilisant l'énergie renouvelable non utilisée par d'autres usages, les cryptomonnaies apporteront à l'égard des défis de la transition énergétique une réponse numérique que les monnaies classiques ne peuvent offrir alors même que leur empreinte carbone est bien plus grande.

fait le pari d'adopter la crypto. Cette technologie va bouleverser durablement notre monde. Tant en termes de facilité dans nos échanges de tous les jours, que de la confiance qu'apporte la décentralisation de la monnaie face à la nationalisation des monnaies utilisées comme arme économique. »[99]

Selon Eric Vergaeghe, fondateur du média numérique *'Le Courrier des Stratèges'* : *« Pour éviter la pagaille d'une bataille locale perdue face aux pirates, les banques centrales se proposent de supprimer le cash et les mouvements émiettés entre banques pour constituer une sorte de grand livre des opérations monétaires. Concrètement, l'euro numérique, par exemple, sera suivi de A à Z par un big data niché dans les serveurs de la Banque Centrale Européenne, et aucun compte bancaire n'échappera à ce contrôle. Les banques ne seront, plus en réalité, que des succursales d'une seule institution publique appelée banque centrale. Facialement, la concurrence continuera à jouer. Facialement, nous continuerons à ouvrir un compte dans une banque, mais l'argent que nous y placerons sera une sorte de "jeton" numéroté que la banque centrale pourra désactiver quand elle le souhaitera. On connaît déjà tous les motifs de désactivation, ce sont ceux des systèmes totalitaires ordinaires : lutte contre la criminalité, le terrorisme, et autres prétextes invoqués pour, tôt ou tard, faire taire les opposants. Christine Lagarde les a déjà annoncés, énoncés et justifiés. La croyance naïve selon laquelle la réponse à une faiblesse consiste à toujours plus centraliser le pouvoir est au coeur même de la logique de Davos. On n'y peut pas grand-chose. Elle donnera l'occasion d'une très belle confiscation du pouvoir si elle se réalise, dans l'indifférence générale ou presque des populations. Précisons que la BCE a reçu 8.000 réponses à sa consultation sur l'euro numérique, ce qui est un record historique. Et que très majoritairement, les participants ont insisté sur leur crainte de voir leur vie privée anéantie par la monnaie numérique. Les termes du débat sont d'ores et déjà posés. »*

Des initiatives anticipent ce grand bouleversement dont les impacts sur le droit et sur les libertés individuelles sont encore sous-estimés, quand bien même la Banque centrale européenne y porte un intérêt réel dans ses travaux relatifs à la mise en place d'un euro digital[100].

Une nouvelle monnaie numérique, provisoirement nommée DCJPY, va faire son apparition en 2022 au Japon. Le projet implique 70 organisations et les banques les plus importantes du pays, regroupées sous le nom de *Digital Currency Forum*. En introduction d'un livre blanc sur le projet, le groupe explique la nécessité de s'adapter au monde d'aujourd'hui, qui se digitalise de plus en plus. « *La propagation de la maladie Covid-19 a incité les efforts de numérisation du point de vue du développement et de l'infrastructure pour soutenir les activités économiques et sociales, tout en évitant le contact physique* », est-il indiqué.

La pandémie semble donc avoir accéléré le développement de ce type de projet, qui apparaît comme une nécessité dans un monde où les contacts physiques se réduisent. Pour utiliser cette monnaie, les participants devront transférer de l'argent d'un compte bancaire classique vers un compte en devise numérique. Cette devise sera stockée sur une plateforme conçue spécialement pour la DCJPY. Cette sorte de digi-yen pourra être transférée à d'autres utilisateurs, via cette plateforme. Il sera aussi possible de choisir de transférer cette monnaie sur un compte bancaire classique. Toutefois, la conversion en monnaie fiduciaire ne sera pas possible dans un premier temps. La DCJPY utilisera la technologie de la blockchain.

[99] *La guerre des nouvelles monnaies numériques : l'heure de vérité des crypto-monnaies* : https://www.lerevenu.com/bourse/devises/la-guerre-des-nouvelles-monnaies-numeriques-lheure-de-verite-des-crypto-monnaies

[100] *Cf.* le chapitre consacré aux "exigences de confidentialité" qui doivent être établies et respectées pour protéger les libertés individuelles dans le rapport relatif à la mise en place d'un euro digital où figure notamment ce passage : *« Users' privacy can be protected to various degrees, depending on the preferred balance between individual rights and public interest ... » Report on a digital euro* : https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html

Le livre blanc expose les trois principales raisons qui justifient la création de ce groupe et de cette monnaie : « *La première justification est l'interopérabilité. Ce terme désigne la capacité d'un produit à fonctionner avec d'autres produits ou systèmes, sans restriction. La East Japan Railway, membre de ce projet et plus grande entreprise ferroviaire du Japon, propose par exemple déjà aux détenteurs de ses cartes à puces* « *Suica* » *de les utiliser pour effectuer des paiements dans les gares et quelques magasins. Cependant, ce système n'est pas interopérable, comme l'explique le livre blanc. Beaucoup de monnaies numériques ne peuvent pas être converties en monnaies physiques une fois mises sur une carte. Les monnaies virtuelles permettraient de résoudre de tels problèmes, et amèneraient probablement de nouvelles innovations en termes de solutions de paiements. La seconde justification est d'éviter la concurrence entre une monnaie numérique et les comptes bancaires, en faisant en sorte que la monnaie virtuelle soit émise directement par les banques. Surtout, et c'est là l'un des principaux atouts des monnaies numériques, elles permettent de réduire le temps de règlement des transactions commerciales et transfrontalière, ainsi que leurs coûts. Des économies de temps et d'argent possibles car ce type de monnaie supprime bon nombre d'intermédiaires lors d'une transaction. La troisième justification mise en avant est le fait que les monnaies virtuelles sont plus appropriées que les physiques pour l'exécution de smart contracts. Elles facilitent également le règlement d'actifs numériques comme des NFT. »*[101]

Lors d'une audition devant le Parlement européen en novembre 2021, la Banque centrale européenne, par l'intermédiaire de Fabio Benetta, membre de son directoire, a marqué son intention d'aller vite en mettant en place un prototype d'euro numérique dès 2023 afin de répondre à la dématérialisation croissante des paiements et à la multiplication des cryptomonnaies.

En décembre 2021, en réponse à une question sur la capacité de l'agence de renseignement à limiter les attaques de *ransomware*[102] émanant de l'étranger[103], William Burns, le directeur de la *Central Intelligence Agency* (*CIA*), a déclaré que son prédécesseur « *avait mis en place un certain nombre de projets différents axés sur les crypto-monnaies et essayant d'examiner les conséquences de deuxième et troisième ordre ainsi que d'aider nos collègues dans d'autres parties du gouvernement américain à fournir des renseignements solides sur ce que nous voyons.* ». William Burns est resté vague sur ce que fait exactement la CIA. Par exemple, étudie-t-elle les réseaux ou tente-t-elle de les perturber ? Mais il a ajouté : « *L'une des façons de s'attaquer aux attaques de rançongiciels et de les dissuader est de pouvoir s'attaquer aux réseaux financiers qu'un grand nombre de ces réseaux criminels utilisent et cela touche également à la question des monnaies numériques.*

Plus tôt dans l'année, l'un des prédécesseurs de William Burns à la tête de la CIA lors des présidences Obama, Michael Morell, a qualifié la technologie blockchain d' « *atout pour la surveillance* » dans un rapport publié par le *Crypto Council for Innovation*, dirigé par Coinbase et Square.

L'une des armes couramment utilisées par les États-Unis pour faire plier certaines nations est le spectre des sanctions financières. Plus de 9.000 sanctions de ce type sont actuellement en

[101] *Cf. Le Japon va lancer une monnaie digitale* : https://siecledigital.fr/2021/11/25/le-japon-va-lancer-une-monnaie-numerique-avec-le-soutien-des-banques/

[102] Un ransomware est un type de logiciel malveillant conçu pour éteindre un ordinateur ou un réseau jusqu'à ce qu'un paiement soit reçu, souvent en bitcoin ou une autre crypto-monnaie. En 2021, des attaques ont entraîné la fermeture d'un important oléoduc, d'usines et d'infrastructures informatiques d'entreprises.

[103] Prenant appui sur un document officiel de 37 pages intitulé '*La stratégie des États-Unis pour contrer la corruption'*, l'administration Biden a qualifié la lutte contre les ransomwares de « *priorité* » au même titre que la limitation des possibilités de nations étrangères d'échapper aux sanctions américaines.
United States Strategy on Countering Corruption :
https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf

vigueur, notamment vis-à-vis de pays comme la Corée du Nord ou l'Iran. Depuis septembre 2021, le Salvador a adopté le Bitcoin comme monnaie nationale. Le Costa Rica, le Laos, le Zimbabwe, le Liban, la Jamaïque, le Pérou et d'autres contrées envisagent sérieusement de faire de même. Or un rapport publié en octobre 2021 par l'administration Biden a fait ressortir que les actifs numériques représentaient un risque pour son système de sanctions.

« *Ces technologies offrent des opportunités à des acteurs malveillants de détenir et transférer des fonds en dehors du système financier fondé sur le dollar. Ils donnent à nos adversaires des moyens de bâtir des systèmes de paiement ayant pour but de diminuer le rôle global du dollar.* »

Dès le début de l'été 2021, le Congrès s'était saisi de la question. Une première *task force* a été mise en place afin de lutter officiellement contre le recours à des cryptomonnaies dans des activités financières illicites.

Or, devant la multiplication des évènements cybercriminels à travers le monde, les principales banques centrales comme les protagonistes du Forum économique mondial envisagent comme probable l'éventualité d'une gigantesque cyberattaque susceptible de provoquer des ralentissements, voire des neutralisations des systèmes de paiement bancaire, et une paralysie de l'économie mondiale.

Un vaste exercice de simulation a même été entrepris à l'été 2021.[104]

Selon un document du *Global Legal Research Directorate* de la *Law Library of Congress*[105], le nombre de pays ayant émis des interdictions relatives aux cryptomonnaies est en hausse et s'élève maintenant à 51. Ce document intitulé "*Regulation of cryptocurrency around the world*" a été publié pour la première fois en 2018 et présente un récapitulatif de l'évolution du cadre réglementaire national relatif à l'industrie crypto de l'ensemble des pays du monde.

Pour déterminer la position d'un pays à l'égard des cryptomonnaies, l'étude se concentre sur les deux points suivants : le statut juridique des crypto-actifs, c'est-à-dire le fait qu'un pays interdise explicitement ou implicitement les cryptomonnaies ; le cadre réglementaire entourant ces actifs, en particulier concernant l'application des lois fiscales et des lois sur la lutte contre le blanchiment d'argent et le financement du terrorisme.

Interdire aux banques et autres institutions financières d'effectuer des transactions relatives aux cryptomonnaies ou d'offrir des services aux particuliers/entreprises qui se livrent au trading de cryptomonnaies sont des exemples d'interdictions implicites. L'interdiction placée sur les exchanges cryptos de mener des activités dans une juridiction donnée fait également partie des interdictions implicites. Les interdictions absolues font référence à celles qui rendent les cryptomonnaies illégales.

En 2018, les auteurs avaient alors identifié 8 juridictions avec une interdiction absolue et 15 juridictions avec une interdiction implicite alors que la mise à jour de novembre 2021 identifie 9 juridictions avec une interdiction absolue et 42 avec une interdiction implicite. Les 9 pays ayant opté pour une interdiction absolue sont l'Algérie, le Bangladesh, la Chine, l'Égypte, l'Irak, le Maroc, le Népal, le Qatar et la Tunisie. Parmi ceux ayant choisi une interdiction implicite, on trouve Bahrein, plusieurs pays d'Afrique tels que le Congo, la Côte d'Ivoire, le Gabon, le Lesotho, le Nigeria ou encore le Kenya, mais aussi la Géorgie, l'Indonésie, le Kazakhstan, le Liban et la Turquie.

De même, l'application des lois fiscales, des lois LAB/CFT ou des deux types de lois aux cryptomonnaies a augmenté de manière exponentielle : 103 juridictions ont été identifiées comme appliquant ces lois aux cryptomonnaies et la majorité d'entre elles appliquent les deux.

[104] https://cyberpolygon.com/about/

[105] *Regulation of cryptocurrency around the world :* https://www.loc.gov/item/2021687419/

Ces juridictions comprennent les États membres de l'Union européenne, à l'exception de la Bulgarie.

Auparavant, en 2018, seules 33 juridictions disposaient d'une réglementation relative aux cryptomonnaies dans ces domaines, parmi lesquelles cinq seulement appliquant à la fois des lois fiscales et des lois de lutte contre le blanchiment et le financement du terrorisme.

Par ailleurs, le document note également que 21 pays n'appliquent pas les réglementations relatives à la lutte contre le blanchiment d'argent et au financement du terrorisme à l'industrie crypto. Parmi ces derniers, se trouvent plusieurs pays d'Afrique, dont l'Afrique du Sud, au sein desquels la situation sur ce point est relativement floue, plusieurs d'entre eux ne disposant pas de textes réglementaires clairs définissant les procédures requises. On retrouve également dans ces 21 pays le Brésil, le Guernesey, la Jordanie, le Pakistan et le Kazakhstan, qui est pourtant actuellement un des principaux centres de minage du monde.[106]

En juin 2021, le comité de Bâle sur le contrôle bancaire, sorte d'ONU des banques centrales, a publié une proposition sur la régulation des cryptomonnaies[107]. Un texte important qui pourrait inspirer les obligations prudentielles en la matière à l'échelle mondiale.

Ces obligations définissent la manière dont les banques couvriront les risques des cryptomonnaies qu'elles intégreraient dans leur offre. Les banques devront aussi surveiller les risques purement technologiques des cryptomonnaies comme la stabilité du réseau et du blockchain qui le sous-tend, la fiabilité des nœuds du blockchain pour éviter leur manipulation, la protection adéquate des clés de celui qui possède la cryptomonnaie. Si la banque n'arrive pas à évaluer correctement les risques des cryptomonnaies, les autorités prudentielles devront durcir les stress tests exigés des banques, demander des provisions supplémentaires ou tout simplement limiter l'activité crypto des banques.

Les monnaies digitales des banques centrales comme l'Euro digital ne sont pas soumises aux obligations formulées dans cette proposition du comité de Bâle. [108]

Toutes ces initiatives participent à consacrer la disparition d'un droit fondamental : la propriété de ce qui a été légitimement acquis et matérialisé par la monnaie sous sa forme matérielle, en contravention avec l'article 17 de la Déclaration universelle des Droits de l'homme de 1948 qui stipule : *« 1. Toute personne, aussi bien seule qu'en collectivité, a droit à la propriété. 2. Nul ne peut être arbitrairement privé de sa propriété. »*

Pour l'économiste Simone Wapler : *« La disparition des espèces comme option de paiement parmi d'autres menace les libertés fondamentales. En premier lieu, elle nous soumet au lobby bancaire. Rappelons que des liquidités sur notre compte en banque ne sont plus « notre » argent mais une créance qu'une banque reconnaît nous devoir. En cas de crise financière, que vaut cette créance ? En second lieu, elle institue un droit de regard de l'Etat sur toutes nos transactions, heures et lieux compris. Bien entendu, le réflexe normal de l'individu normal en temps normal consiste à dire : « je suis honnête, je n'ai rien à cacher ». Mais parfois, les temps deviennent moins « normaux », politiquement ou même techniquement. Que se passe-t-il lorsqu'une grande panne de réseau interdit toute transaction comme cela s'est produit au Royaume-Uni et au nord de l'Europe continentale en juin 2018 ? Qui n'a jamais eu à subir les effets d'un bug informatique ? Qui n'a jamais été victime d'une erreur de l'administration ?*

[106] *Cf. Réglementation : les pays ayant interdit les cryptomonnaies sur leurs territoires :* https://fr.cryptonews.com/exclusives/les-pays-qui-ont-interdit-les-cryptomonnaies-sur-leurs-territoires.htm

[107] *Prudential treatment of cryptoasset exposures*, June 21, Basel Committee on Banking supervision : https://www.bis.org/bcbs/publ/d519.pdf

[108] Pour en savoir plus sur les principes et les modalités de cette régulation, voir par exemple Comment les banques devront courir les risques des cryptomonnaies pour leurs clients : https://www.latribune.fr/opinions/tribunes/comment-les-banques-devront-couvrir-les-risques-des-cryptomonnaies-pour-leurs-clients-890132.html

Dans l'hypothèse où le cash deviendrait hors-la-loi, la mise au ban de la société d'un individu devient instantanément possible. Sans aucune procédure contradictoire, avec seulement le bon vouloir d'un fonctionnaire de Tracfin ou d'un agent de la nouvelle police fiscale (entité habilitée à pratiquer des écoutes téléphoniques, des perquisitions, des géolocalisations, des filatures ou des gardes à vue), chacun risquera de se voir « coupé de son argent » et même de la charité puisqu'il sera impossible de lui donner autrement qu'en nature. »

Patrice Baubeau[109] se montre moins pessimiste à l'égard des monnaies digitales des banques centrales : *« Dans un monde où l'émission d'actifs monétaires, la création d'identités et la gestion des profils correspondants ne sont plus du seul ressort des États, il devient urgent de réfléchir à l'articulation de ces différentes dimensions afin de conserver les bénéfices des innovations suscitées par l'essor d'Internet sans y perdre nos droits, nos biens et nos êtres. Et donc de prendre en compte la quatrième fonction de la monnaie : l'identification [qui renverse la perspective usuelle sur l'anonymat. L'anonymat n'apparaît plus comme une propriété du cash, mais devient l'une des modalités de l'identification par la monnaie. […] [Les monnaies digitales des Banques centrales] limitent le risque d'entraîner la substitution d'une forme lucrative d'identité à la forme civique dont nos droits dépendent, en soumettant le paiement à l'identification plutôt que l'inverse. […] Dans un État de droit, non seulement les individus ont un droit à l'identité que l'État ne peut leur dénier, mais les modalités de l'identification relèvent du domaine de la loi, avec les garanties juridiques qui l'entourent. »*

André Peters prolonge ce propos en élargissant le spectre des questionnements posées par ces monnaies digitales à la question fondamentale de la démocratie monétaire : *« Le développement des monnaies digitales est en plein bouillonnement. De nombreux acteurs (banques, fintechs, réseaux sociaux, Banques centrales, banques commerciales, citoyens, associations, etc.) sont en présence et essaient tous de défendre leur solution. On a vu que ce bouillonnement est révélateur de nombreux enjeux sociétaux et démocratiques de première importance qui, bien souvent, restent enfouis sous des considérations techniques ou restent masqués. Selon moi, la question monétaire est un enjeu politique tellement fondamental que je le reprends systématiquement sous le vocable « démocratie monétaire ». La digitalisation de la monnaie constitue un momentum particulier pendant lequel les citoyens ont la possibilité de réinterroger l'institution monétaire et de vérifier si elle est bien adaptée aux besoins contemporains en se rappelant que les acteurs en scène défendent leurs intérêts particuliers et que personne ne représente l'intérêt général. »*[110]

« *Avec la réserve fédérale, vous avez quelque chose qui n'est pas contrôlable, n'est-ce pas ? C'est un système monétaire qui est complètement opaque pour tout le monde*« , explique Jimmy Song, un auteur, podcasteur et programmeur informatique qui organise des séminaires de deux jours dans le monde entier pour former des codeurs à travailler dans l'industrie du bitcoin.

« *Avec le bitcoin, vous avez la possibilité de procéder vous-même à des vérifications, […].* » Tout le monde peut participer au processus de soumission et de révision du nouveau code, quels que soient son identité, son lieu de résidence ou ses diplômes. Le bitcoin étant un logiciel libre, les règles qui régissent son fonctionnement sont également totalement transparentes.[111]

Au-delà des perspectives d'essor considérable de l'impact des monnaies digitales sur l'économie, celles attachées aux Fintechs utilisant Internet et les infrastructures associées

[109] *L'identification, la quatrième fonction de la monnaie :* https://theconversation.com/lidentification-la-quatrieme-fonction-de-la-monnaie-166351

[110] *Monnaies digitales et démocratie monétaire ?* https://econologiste.org/2021/03/18/monnaies-digitales-et-democratie-monetaire/

[111] https://reason.com/video/2022/01/06/bitcoin-doesnt-care-about-your-college-degree/

interrogent l'économie mondiale, quelques années après la grande crise financière systémique qui a secoué la planète entière.

Eric Benhamou relève à leur égard dans *La Tribune* : *« En moins de trois ans, la société britannique spécialisée dans les solutions de paiement en ligne Checkout.com, fondée il y a dix ans, a levé auprès d'investisseurs près de 1,8 milliard de dollars et a vu sa valorisation multipliée par vingt. La dernière levée de fonds (en série D), d'un montant d'un milliard de dollars, réalisée en janvier 2022, valorise en effet la fintech à 40 milliards de dollars ! Soit deux fois et demie la valorisation atteinte tout juste un an avant. Pendant cette période, en 2021, le volume de paiement traité a été multiplié par trois, à 100 milliards de d'euros, et ce pour la troisième année consécutive. La croissance du chiffre d'affaires est logiquement dans le même ordre de grandeur. 40 milliards de dollars, c'est beaucoup mais cela reste encore inférieur à certains concurrents, comme l'Américain Stripe (95 milliards de dollars en mars 2021) ou le néerlandais Adyen qui pèse 61 milliards de dollars en Bourse. Sur un registre un peu différent (le paiement fractionné), le suédois Klarna frôle les 46 milliards de dollars. Enfin, l'acteur historique des paiements en ligne, PayPal, avoisine les 210 milliards de dollars sur le Nasdaq. Ces sommes peuvent paraître extravagantes pour des sociétés qui n'existaient pas, ou à peine, il y a dix ans et qui compte quelques milliers de salariés. Le jeu des comparaisons avec le secteur bancaire est encore plus frappant : BNP Paribas, première banque européenne, 118 milliards de dollars de fonds propres et 190.000 salariés, est actuellement valorisée 93 milliards de dollars. Pour certains, ces folles valorisations sont bien la preuve de l'existence d'une bulle sur la fintech, alimentée par des liquidités excessives. »*

Une chose est sûre, les valorisations démentes de ces entreprises de technologie dans le digital traduisent avant tout un changement radical du monde dans lequel nous vivons

Mais c'est sans compter sur l'extrême vulnérabilité des navigateurs et clouds disponibles comme en témoignent les difficultés rencontrées par Google, la majorité des instances (serveurs) *Google Cloud* piratées étant utilisées pour miner des cryptomonnaies, selon les équipes de cybersécurité de Google.[112]

Dans un tel contexte où rien n'est jamais stabilisé de manière pérenne, la Chine est le premier pays à avoir pris des initiatives claires quant à l'usage des cryptomonnaies, des blockchains et des NFT.

Les blockchains publiques ne peuvent pas y fonctionner légalement, les NFT ne posent aucun problème juridique en Chine tant qu'ils ne sont pas utilisés en conjonction avec Bitcoin ou autres cryptomonnaies, en l'absence d'une infrastructure nationale dédiée aux NFT, celles-ci ne peuvent être organisées sur des chaînes privées.

La Chine, qui est particulièrement innovante dans tous ces différents segments de la compétition technologique, a pris la décision de soutenir un projet (son nom officiel est *BSN-Distributed Digital Certificate (BSN-DDC)*) qui vise à soutenir la mise en œuvre de NFT non cryptographiques en fournissant des interfaces de programmation d'applications pour le développement de portails où la monnaie traditionnelle est la seule méthode de paiement. Yifan He, le PDG de *Red Date Technology*, la société qui fournit la technologie pour BSN, a déclaré que l'infrastructure qu'ils construisent utilise une blockchain ouverte, qui facilite la gouvernance sur la chaîne. En permettant à une entité centralisée de gouverner l'infrastructure et d'intervenir dans les activités illégales, Red Date prévoit de créer une plateforme NFT totalement distincte du profil des crypto-monnaies.

[112] *Comment Google Cloud est piraté pour miner des crypto-monnaies :* https://www.cnetfrance.fr/news/comment-google-cloud-est-pirate-pour-miner-des-crypto-monnaies-39933759.htm

Cette initiative ouvre la voie à d'autres et laisse espérer une transition moins brutale vers le monde numérique de demain.

- *L'identité numérique et la biométrie comportementale*

A l'ère du numérique, la dématérialisation des démarches administratives et la multiplication des services en ligne et des outils numériques de démocratie participative posent la question d'une redéfinition de l'identité.[113]

« *L'identité numérique est perçue comme un catalyseur essentiel des transactions numériques que ce soit pour des individus ou des personnes morales ou des objets connectés. Aujourd'hui, la fourniture d'identité numérique subit une profonde révolution, car de nombreuses entités telles que les banques, les fournisseurs de services de communications électroniques ou les principales plateformes en ligne agissent de plus en plus en tant que fournisseurs d'identité, sans pour autant s'appuyer sur une quelconque réglementation. Enfin, la crise de la COVID-19 a mis en évidence l'urgence de fournir rapidement à tous les citoyens et entreprises européens une identité numérique universellement acceptée et fiable pour permettre une continuité d'activité dans le cadre du Marché Unique Numérique*[114]*, l'accès à des services publics en ligne cruciaux et sensibles tels que l'e-Santé, l'administration en ligne ou encore l'e-justice et atténuer la fraude à l'identité. […] L'usage de tels moyens d'identification est particulièrement hétérogène d'un Etat à l'autre, certains ne permettant pas leur recours dans le secteur privé (ex : domaine bancaire). Des solutions sûres et fiables connaissent un certain succès national mais ne peuvent prospérer dans l'ensemble de l'UE, en absence d'une réglementation commune. De même, les solutions d'identification des Twitter, Linkedin, Facebook ou autre plate-forme sociale permettent de s'authentifier auprès de sites Web tiers en utilisant les profils utilisateurs de leurs abonnés en contrepartie de la perte de contrôle sur les données personnelles ainsi divulguées. De plus, ces solutions sont fréquemment déconnectées d'une identité physique vérifiée, ce qui rend la fraude (comme le vol ou l'usurpation d'identité) et les menaces de cybersécurité en augmentation constantes. En outre, cette pratique met en exergue l'intrusion des GAFAM dans les domaines régaliens et leur impact sur les conditions de concurrence équitables dans le cadre d'un marché européen concurrentiel des services d'identité numérique. En conséquence, il n'est pas possible aujourd'hui de s'identifier en ligne avec une identité numérique unique, sécurisée, pratique et digne de confiance et de protéger les données personnelles autant qu'avec une carte d'identité ou un passeport dans le monde physique.* » (Eric A. Caprioli et Pascal Agosti, avocats associés, docteurs en droit)

La France dispose depuis 2016 d'un premier dispositif d'identité numérique, *'France Connect'*, qui permet aux internautes de s'authentifier sur un service en ligne par l'intermédiaire d'un compte existant sur un service public. En juillet 2021, la DINUM a été mandatée pour accélérer le déploiement de *FranceConnect* en l'étendant à titre expérimental aux services en ligne proposés par des entreprises privées, au-delà des centaines de démarches qui peuvent déjà être réalisées auprès des administrations.

Mais pour passer à un niveau de sécurité supérieur, le ministère de l'Intérieur et l'agence nationale des titres sécurisés (ANTS) développent l'outil Alicem (Authentification en ligne certifiée sur mobile) qui utilise notamment un logiciel de comparaison faciale.

[113] Voir notamment à cet égard Olivier Desouches *in L'identité numérique entre secret, visibilité… et régulation :* http://ses.ens-lyon.fr/articles/lidentite-numerique-entre-secret-visibilite-et-regulation

[114] Voir notamment à son sujet : *Un plan en 16 actions pour construire un marché numérique unique en Europe* https://www.usine-digitale.fr/editorial/un-plan-en-16-actions-pour-construire-un-marche-numerique-unique-en-europe.N328454

Le 14 octobre 2021, le sénateur Alain Cadec a déposé une proposition de loi *« instituant une Autorité de contrôle de l'identité numérique »*. Le texte visait à imposer, pour toute inscription sur un réseau social, la transmission à cette nouvelle autorité de documents attestant de l'identité de l'utilisateur. Cette autorité, composée de huit personnes, enregistrerait alors cette pièce d'identité dans un espace sécurisé. Puis elle pourrait transmettre au réseau social « *un identifiant non nominatif »* , attestant que l'identité de l'utilisateur est vérifiée, mais sans la révéler pour préserver sa vie privée. La nouvelle autorité ne pourrait ensuite révéler l'identité d'un internaute que sur demande d'une juridiction responsable, et uniquement pour sanctionner un message tombant sous le coup de la loi (haineux, raciste, homophobe, sexiste…).[115] En l'état, cette loi n'a aucune chance d'être adoptée, car cette *« autorité »* aurait toutes les compétences d'un service d'identité numérique. Or, si le gouvernement avance sur la mise en place d'une identité numérique robuste pour tous les Français, son déploiement n'est pas prévu avant 2022 ou 2023 au mieux. Qui plus est, pour être applicable, cette loi imposerait une refonte de la politique de confidentialité et des modalités d'inscription de l'ensemble des réseaux sociaux opérant en France. Un chantier techniquement possible, mais de très grande ampleur, et qui devrait, pour être réaliste, s'insérer dans une loi plus vaste sur l'identité dans l'espace numérique.

Dans un article intitulé *'Les défis éthiques de l'identité numérique',* Armen Khatchatourov, enseignant-chercheur et membre de Chaire Valeurs et politiques des informations personnelles de l'IMT, et Pierre-Antoine Chardel, Professeur de sciences sociales et d'éthique, interrogent les enjeux soulevés par les identités numériques : *« Si le RGPD est entré en application récemment, en plaçant l'Europe à l'avant-garde de la protection des données à caractère personnel, il ne doit pas nous dissuader de nous interroger en profondeur sur la question des identités, dont les contours se sont redéfinis à l'ère numérique. Il s'agit bel et bien de porter une réflexion critique sur des enjeux éthiques et philosophiques majeurs, au-delà de la seule question de la protection des informations personnelles et de la privacy.*

Les politiques actuelles sur la protection des données mettent l'accent sur les droits de la personne. Mais elles ne prennent pas la mesure de la manière dont l'exercice de notre libre arbitre se voit de plus en plus empêché au sein d'environnements technologiques complexes, et encore moins des effets de la métamorphose numérique sur les processus de subjectivation, le devenir-soi de l'individu. On considère le plus souvent, dans ces textes, un sujet déjà constitué, capable d'exercer ses droits, sa propre volonté et ses principes. Or, le propre des technologies numériques – telle est la thèse ici défendue – est de participer à la formation des subjectivités selon un mode nouveau : en redistribuant sans cesse le jeu des contraintes et des incitations, elles créent les conditions d'une plus grande malléabilité des individus. Nous détaillons ces processus dans l'ouvrage 'Les identités numériques en tension'[116]*, réalisé dans le cadre de la Chaire Valeurs et politiques des informations personnelles de l'IMT.*

Si les moyens mis en place par le RGPD sont clairement nécessaires pour soutenir l'initiative et l'autonomie de l'individu dans la gestion de sa vie numérique, il faut cependant souligner que les notions mêmes de consentement et de contrôle par l'utilisateur vis-à-vis de ses données, et sur lesquels le mouvement actuel repose, restent problématiques. Et cela parce que deux logiques, distinctes mais concordantes, sont aujourd'hui à l'œuvre. Si une certaine sensibilité des utilisateurs aux traces laissées volontairement ou involontairement au cours de leurs activités en ligne, et dont il peut avoir connaissance (comme, par exemple, des métadonnées de connexion), semble s'accroître, et peut servir de support à l'approche basée sur le consentement, cette dynamique rencontre assez vite ses limites.

[115] Source : https://incyber.fr/un-senateur-veut-controler-lidentite-numerique/
[116] *Les identités numériques en tension – Entre autonomie et contrôle :* https://www.istegroup.com/fr/produit/les-identites-numeriques-en-tension/

Tout d'abord, la multiplication des informations récoltées rend irréaliste l'exercice systématique du consentement et le contrôle par l'utilisateur, ne serait-ce qu'en raison de la surcharge cognitive que cet exercice effectif exigerait de sa part. Ensuite, le changement de nature des moyens techniques de collecte, exemplifiée par l'avènement des objets connectés, conduit à la démultiplication des capteurs qui collectent les données sans même que l'utilisateur puisse s'en rendre compte, comme le montre l'exemple, de moins en moins hypothétique, de la vidéo-surveillance couplée à la reconnaissance faciale et, plus amplement, le cas de toutes les connaissances que les opérateurs acquièrent sur la base de ces données. Il s'agit ici d'une couche de l'identité numérique dont le contenu et de nombreuses exploitations possibles sont absolument inconnus de la personne qui en est la source. Qui plus est, une forte tendance des acteurs, étatiques et privés, consiste à vouloir décrire l'individu de manière exhaustive et totale, en créant le risque de le réduire à un ensemble de plus en plus complet d'attributs. Dans ce nouveau régime de pouvoir, le visible se réduit à ce qui peut être saisi en données, à ce qui relève de la mise à disposition immédiate des êtres, comme s'il s'agissait en fin de compte de simples objets.

La deuxième logique à l'œuvre dans nos sociétés hypermodernes touche à l'inscription de ce paradigme basé sur la protection et le consentement dans les mécanismes de la société néolibérale. La société contemporaine conjugue en effet deux aspects en matière de 'privacy' : il s'agit de considérer l'individu comme étant visible de manière permanente, et comme étant responsable individuellement pour ce qui est vu de lui. Un tel ensemble de normes sociales se consolide à chaque fois que l'utilisateur exerce le consentement – ou l'opposition – à l'utilisation de ses données. En effet, à chaque itération, l'utilisateur renforce sa compréhension de soi-même comme l'auteur et le responsable de la circulation des données. Il endosse aussi l'injonction à la maîtrise des données alors même que cette dernière est le plus souvent illusoire. Surtout, il endosse l'injonction à calculer les bénéfices que le partage des informations peut lui apporter. En ce sens, l'application stricte et croissante du paradigme de consentement peut être considérée comme étant corrélative d'une conception de l'individu qui devient non seulement l'objet d'une visibilité quasi-totale, mais aussi – et surtout – un agent économique rationnel, à même d'analyser son agir en termes de coûts et de bénéfices.

Cette difficulté fondamentale fait que les enjeux futurs des identités numériques ne se réduisent pas à donner plus de contrôle explicite, ou plus de consentement éclairé. Il convient bel et bien de trouver d'autres voies complémentaires, qui se situent sans doute du côté des pratiques (et non simplement des « usages ») des utilisateurs, à condition que de telles pratiques mettent en place des stratégies de résistance pour contourner l'impératif de visibilité absolue et de définition de l'individu comme agent économique rationnel.

De telles pratiques digitales doivent en outre nous inciter à dépasser la compréhension de l'échange social – numérique ou non – sous le régime du calcul des bénéfices que l'on en retire ou des externalités. Ainsi, les enjeux soulevés par les identités numériques dépassent largement les enjeux de protection de l'individu ou les enjeux des « modèles d'affaires », et touchent à la manière même dont la société dans son ensemble conçoit la signification de l'échange social.

Dans un tel horizon, il est primordial d'affronter les ambivalences et les jeux de tension qui sont intrinsèques aux technologies numériques, en examinant les nouveaux modes de subjectivation qui sont induits dans ces opérations. C'est à partir d'un tel exercice de discernement que pourra advenir un mode de gouvernance des données plus responsable. »[117]

[117] *Les défis éthiques de l'identité numérique :* https://theconversation.com/les-defis-ethiques-de-lidentite-numerique-111881

Nous nous trouvons là dans un registre complexe qui touche aux libertés et aux droits fondamentaux dans un contexte où le droit est indubitablement en retard par rapport à l'offre technologique.

Cette question est d'autant plus importante que la gestion de l'identité en France est une prérogative de l'Etat depuis la création de l'état civil et que l'UE a donné son feu vert pour la mise en place dès 2021 d'une carte d'identité numérique conforme au droit européen.

Ce sujet épineux de l'identité numérique est un véritable serpent de mer auquel l'Etat a déjà consacré quatre projets de réglementation et entrepris en 2020 une cinquième démarche, législative. Afin d'éviter de nouveaux blocages, une consultation publique a été engagée sur le sujet en mars 2020[118].

L'usurpation de l'identité constitue la principale menace qui pèse sur les entreprises comme sur les particuliers. Elle nourrit de très grandes inquiétudes dans un contexte où la cybersécurité semble constituer un leurre. *« Personne n'est à l'abri d'une usurpation d'identité. »*[119]

Cette question de l'avenir de notre identité trouve également des motifs d'inquiétude et d'interrogation dans la disparition de la signature comme moyen d'authentification d'un acte écrit, et au-delà, dans la lente disparition de la preuve écrite fiable, au profit d'écrits sous forme électronique (mails, documents bureautiques) qui n'accèdent pourtant pas au même niveau de fiabilité probatoire que ceux qu'ils remplacent.

« Un arrêt de la Cour de Cassation du 12 mai 2021[120] *illustre parfaitement la mutation en cours de l'écrit juridique fiable vers un écrit aux qualités probatoires beaucoup plus incertaines. La Haute juridiction est confrontée à cette mutation non-maîtrisée de l'écrit et à l'évidente nécessité de ne pouvoir disqualifier une pratique à l'aune de l'efficacité juridique. D'où une étonnante pirouette pour faire coïncider le droit avec le fait.*

La deuxième chambre civile a estimé que, dans le cadre d'une contrainte délivrée conformément à l'article L161-1-5 du Code de la sécurité sociale, « l'apposition sur la contrainte d'une image numérisée d'une signature manuscrite ne permet pas, à elle seule, de retenir que son signataire était dépourvu de la qualité requise pour décerner cet acte ».

Etrange formulation dans laquelle la Cour de Cassation semble refuser de se saisir de la proie pour lui préférer son ombre. Car une image numérisée d'une signature manuscrite n'a jamais été et ne peut pas être une signature. Elle ne répond ni aux conditions de l'article 1367 du Code civil ni même à celles de l'article 1379 si l'on voulait considérer qu'il puisse s'agir d'une copie d'une signature originale.

Nous pensons que la Cour de Cassation aurait dû le constater et s'arrêter là : pas de signature donc pas de contrainte.

Pour sauver l'efficacité juridique de la contrainte, la Cour de Cassation élude la question de la signature pour ne s'intéresser qu'à la qualité du signataire. La Cour de Cassation, pour sauver l'ersatz de signature, et avec elle la contrainte, prend un chemin étrange en constatant que rien ne prouve que le signataire était dépourvu de qualité pour émettre la contrainte. Or, précisément veut-on lui répondre : comme il n'y a pas de signature, il n'y a pas de signataire ! Alors pourquoi s'intéresser à la qualité du signataire s'il n'y a pas de signature ?

Imaginez toutes ces contraintes produites par la sécurité sociale qui, du jour au lendemain, ne vaudraient plus rien car non revêtues de la signature manuscrite du directeur de l'organisme habilité à les faire délivrer ? La Cour de Cassation ne veut l'imaginer. On aurait pu lui objecter

[118] *Cf.* https://consultation.democratie-numerique.assemblee-nationale.fr/identitenumerique
[119] *Cf.* https://idverif.com/
[120] Arrêt n° 20-10.584, n° 20-10.826.

que les greffiers des Tribunaux arrivent à produire chaque jour, dans les juridictions, des copies exécutoires signées des jugements prononcés. Mais elle préfère, aux motifs non-dits que le processus d'édition automatisé des contraintes a l'apparence de la fiabilité, ne plus s'embarrasser d'une formalité en passe de devenir obsolète : la signature manuscrite. » (Etienne Papin, Avocat[121])

La boussole numérique de la Commission européenne pour 2030[122] définit un certain nombre d'étapes et d'objectifs que l'identité numérique européenne contribuera à atteindre. D'ici à 2030, tous les services publics clés devraient être disponibles en ligne, tous les citoyens auront accès à leurs dossiers médicaux électroniques et 80 % des citoyens devraient utiliser une solution d'identification électronique.

Le 4 juin 2021, la Commission européenne a proposé un cadre européen relatif à une identité numérique qui sera accessible à tous les citoyens, résidents et entreprises de l'UE[123].

Pour cette initiative, la Commission s'appuie sur le cadre juridique transfrontière existant pour les identités numériques de confiance, l'initiative européenne sur l'identification électronique et les services de confiance (règlement eIDAS). Adopté en 2014, ce règlement fournit la base des procédures électroniques transfrontières pour l'identification, l'authentification et la certification de site web au sein de l'UE. Quelque 60 % des Européens peuvent déjà bénéficier du système actuel.

L'article 6 du Règlement eIDAS organise les modalités de la reconnaissance mutuelle et de l'interopérabilité dans l'UE des identités (régaliennes) notifiées par les Etats membres à la Commission et publiées au Journal officiel de l'Union européenne, sans pour autant régir les systèmes d'identification (identité numérique) relevant du pouvoir souverain de chaque État membre.

Trois niveaux de schémas d'identification sont prévus par le Règlement eIDAS : faible, substantiel et élevé : seuls les deux derniers niveaux peuvent être notifiés à la Commission. Divers actes d'exécution disponibles sur le site de l'ANSSI[124] sont venus préciser les modalités propres à l'identification électronique régalienne comme les modalités de collaboration entre Etats membres en matière d'identification électronique (art. 12-7 Règlement eIDAS), les Spécifications techniques minimums et procédures pour les niveaux d'assurance pour l'identification électronique (art. 8-3 Règlement eIDAS) ou le cadre d'interopérabilité (art. 12-8 Règlement eIDAS).

Dans le cadre du nouveau règlement, les États membres offriront aux citoyens et aux entreprises des portefeuilles numériques qui seront en mesure d'établir un lien entre leur identité numérique nationale et la preuve d'autres attributs personnels (tels que permis de conduire, diplômes, compte bancaire). Ces portefeuilles pourront être fournis par des autorités publiques ou par des entités privées, à condition d'être reconnus par les États membres.

---

[121] *De la disparition de la signature et des mutations de la preuve écrite :* https://www.village-justice.com/articles/disparation-signature-des-mutations-preuve-ecrite,39265.html

44

[122] *Décennie numérique de l'Europe : objectifs numériques pour 2030* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

[123] *Règlement concernant un cadre européen relatif à une identité numérique :* https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation
Recommandation concernant un cadre européen relatif à une identité numérique : *https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-recommendation*

[124] *Référentiel documentaire lié au Règlement eIDAS* : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/

Les nouveaux portefeuilles européens d'identité numérique permettront à tous les Européens d'accéder à des services en ligne sans devoir recourir à des méthodes d'identification privées ni à partager inutilement des données à caractère personnel. Grâce à cette solution, ils auront la pleine maîtrise des données qu'ils partagent.

Le cadre européen relatif à une identité numérique aura les caractéristiques suivantes :

- Il sera accessible à toute personne souhaitant l'utiliser **:** Tout citoyen, résident ou entreprise de l'UE qui désire utiliser l'identité numérique européenne pourra le faire.
- Il offrira de multiples possibilités d'utilisation **:** Le portefeuille européen d'identité numérique pourra être employé largement, comme moyen soit d'identifier un utilisateur, soit de prouver certains attributs personnels, aux fins d'accès à des services numériques publics et privés dans l'ensemble de l'Union.
- Les utilisateurs auront la maîtrise de leurs données **:** Les portefeuilles européens d'identité numérique permettront aux citoyens de déterminer quels éléments de leur d'identité, de leurs données et de leurs certificats ils partagent avec des tiers, et de garder la trace de ce partage. La maîtrise laissée à l'utilisateur garantit que seules les informations dont le partage est indispensable seront partagées.

Afin que cette initiative se concrétise dans les meilleurs délais, la proposition est accompagnée d'une recommandation. La Commission invite les États membres à mettre en place une boîte à outils commune d'ici à septembre 2022 et à entamer immédiatement les travaux préparatoires nécessaires. Cette boîte à outils devrait comprendre l'architecture technique, des normes et des lignes directrices relatives aux bonnes pratiques.

Parallèlement au processus législatif, la Commission collaborera avec les États membres et le secteur privé sur les aspects techniques de l'identité numérique européenne. À travers le programme pour une Europe numérique, la Commission soutiendra la mise en œuvre du cadre européen relatif à une identité numérique, et de nombreux États membres ont prévu des projets pour la mise en œuvre des solutions d'administration en ligne, y compris l'identité numérique européenne, dans leurs plans nationaux au titre de la facilité pour la reprise et la résilience[125].

Dans sa stratégie « *Shaping Europe's digital future*[126] », la Commission européenne s'est engagée à réviser le règlement eIDAS afin d'en améliorer l'efficacité, d'étendre son application au secteur privé et de promouvoir des identités numériques fiables pour tous les Européens. Si le règlement eIDAS a introduit un premier cadre transfrontalier pour les identités numériques de confiance et les services de confiance dès 2014, seuls 15 des 27 États membres représentant environ 58 % de la population européenne offrent à leurs citoyens des services d'identité électronique transfrontaliers.

Dans un article qu'ils consacrent à la révision de ce règlement, Eric A. Caprioli et Pascal Agosti, relèvent : *« Le Règlement eIDAS, dans son chapitre consacré à l'identification électronique, se caractérise par un système fédéré fondé sur la neutralité technologique et la reconnaissance mutuelle liant diverses solutions d'identité numérique déployées par les États membres pour une utilisation transfrontière. Or, les mécanismes de coordination volontaire existants entre les États membres ne sont pas susceptibles d'apporter des améliorations suffisantes pour une généralisation de l'identité numérique dans l'UE. La nécessité d'assurer la reconnaissance transfrontière d'un système d'identité numérique dans tous les États membres ne peut être atteinte par des initiatives propres des États membres, dont la portée, l'ambition, l'architecture*

[125] *Facilité pour la reprise et la résilience :* https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_fr
[126] *Shaping Europe's digital future* : https://digital-strategy.ec.europa.eu/en

technique, les solutions retenues et les dispositions juridiques varient, y compris les questions de responsabilité et la disponibilité de l'utilisation par le secteur privé. Les solutions individuelles conduiraient à la fragmentation du marché unique et encourageraient le forum shopping pour les prestataires de services, conduisant à une offre inégale au détriment des opportunités commerciales, de l'offre de services et de l'expérience utilisateur. […]

La révision du Règlement eIDAS vient remplacer les dispositions actuelles du chapitre II relatif à l'identité régalienne en définissant "l'European Digital Identity Wallet" comme "*a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a ; and to create qualified electronic signatures and seal*". *Dès lors, l'identité numérique est pensée dans sa multiplicité de supports et de sources (privées ou publiques). En outre, le lien existant entre moyen d'identification et services de confiance qualifiés (signature ou cachet) est désormais express dès la définition du portefeuille d'identité. En effet, un tel moyen répondant aux exigences du Règlement eIDAS et figurant dans le portefeuille d'une personne facilitera la création d'une signature électronique qualifiée, une aubaine pour certains secteurs d'activité comme les banques. L'entrée en relation serait ainsi simplifiée. Enfin, tout comme pour les services de confiance, les portefeuilles d'identité pourraient bénéficier d'un label de confiance (Trust Mark) s'ils répondent aux exigences formulées dans la Proposition de Règlement eIDAS. […]*

Il conviendra d'être vigilant sur les évolutions à venir dans la Proposition de Règlement, étant précisé ici que cette révision devrait produire ses effets à compter de 2022. Le texte à ce stade de proposition demeure relativement complexe et gagnera à être simplifié et clarifié. »[127]

Une équipe de spécialistes de l'identité numérique composée de Philippe Morel, Bernard Hauzeur, Dinesh Ujoodah, Anthony Sitbon et Alain Bensoussan constatent unanimement que les études sur la question abondent… et piétinent.

« Au-delà d'améliorations ponctuelles, elles reformulent les mêmes conseils et inventaires sans jamais trancher les questions de souveraineté, de délégation, de preuve, ni de statut des entités autonomes comme les robots et les intelligences artificielles (IA). Une répétition qui nous conduit insensiblement à accepter comme un état de fait la prédominance du commerce et de la technologie sur le droit et la vie privée.

C'est une convergence fortuite de rencontres et d'évènements qui a amené une équipe de spécialiste de l'identité numérique à entrevoir la possibilité de se poser la question autrement. A la base, le souci de ne pas – une fois de plus – tenter de légaliser de la technologie pour créer une identité, mais de partir du droit « strict » et de l'évidence d'un monde numérique qui crée une forme d'existence où le « doute » est roi. Que le monde soit physique ou virtuel, il y a des personnes (humaines, morales, et désormais aussi des robots et entités intelligentes), et des communautés, avec un édifice central à tout système de droit : la souveraineté ; et un mécanisme essentiel à l'action : le mandat. »

Ces spécialistes se sont donné comme mission *« de structurer et de pousser ces travaux pour soit confirmer définitivement les limites du droit dans le monde virtuel, soit aboutir – comme c'est le cas – à une nouvelle proposition d'identité – numérique : une identité 5.0, souveraine, capable de replacer la personne (morale, humaine, et robot/ IA) au centre d'un système porteur de tous les effets du droit nécessaires à la protection et la confiance dans les activités humaines, commerciales, et industrielles, tant dans le monde physique que virtuel. »*

[127] *Révision du Règlement eIDAS et identité numérique :* https://www.usine-digitale.fr/article/revision-du-reglement-eidas-et-identite-numerique.N1116709

L'objectif de leur livre blanc '*Identité numérique 5.0*'[128] est d'*« apporter une contribution au projet global d'émergence d'une identité universelle et irrévocable, supranationale, et opposable aux tiers. »* Un livre blanc qui *« pose les bases nécessaires à la mise en œuvre d'identités numériques interopérables et interopposables dans un écosystème de communautés souveraines dont les opérateurs ne sont plus émetteurs d'identités mais seulement garants des procédures. »*

Sujet connexe à celui de l'identité numérique, la biométrie comportementale[129] est aujourd'hui la forme la plus poussée de la *'datazerisation'* des êtres humains.

Selon la CNIL : *« La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel, car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.). »*

Pour les États elle constitue un outil de contrôle social à part entière, quand bien même ses protagonistes arguent qu'elle contribue à une meilleure sécurité des individus. Ce que les faits ne cessent de démentir.

Depuis le 2 août 2021 la nouvelle carte d'identité biométrique est entrée en vigueur en France afin de respecter la législation européenne. Les données personnelles contenues dans cette nouvelle carte d'identité sont stockées dans le fichier des titres électroniques sécurités (TES), géré par le ministère de l'Intérieur.

Le Conseil constitutionnel avait pourtant retoqué en 2012 le projet du gouvernement - traduit dans la loi - de créer une base de données centralisée devant servir à la délivrance des cartes d'identité et la prévention des usurpations d'identité[130].

- *Autres sujets fondamentaux qui interrogent, ceux du droit à l'oubli, de l'anonymat, du droit à l'image et au respect de la vie privée sur Internet.*

Un autre sujet crucial connexe à celui de l'identité numérique est celui de la *'mort numérique'*.

Alors que « *chaque jour, près de 8 000 personnes inscrites sur Facebook décèdent dans le monde* », la CNIL rappelle dans un billet en date du 28 octobre 2020[131] que, par principe, « *le profil de la personne décédée continue d'exister* », puisque la plateforme n'est pas informée de la situation.

Mais, en vertu des dispositions de l'article 85 de la loi Informatique et Libertés : « *les héritiers d'une personne décédée justifiant de leur identité peuvent demander au responsable d'un fichier de tenir compte du décès de celle-ci, et de procéder à l'actualisation de ses données* », rappelle la CNIL. « *Dans la même logique, les réseaux sociaux organisent des fonctionnalités permettant de prendre en compte le décès d'une personne. Par exemple, Facebook propose aux proches du défunt de transformer le compte d'une personne décédée en "Mémorial" afin de permettre à sa famille et à ses amis de se recueillir et d'échanger entre eux, et d'offrir au défunt une sorte d'éternité numérique* ».

Le billet de la CNIL fournit plusieurs liens vers les pages dédiées sur chaque réseau social pour lancer cette alerte.

---

[128] Livre blanc '*Identité numérique 5.0' : https://www.alain-bensoussan.com/download/livre-blanc-identite-numerique-5-0/*

[129] *La biologie comportementale, c'est quoi ?* https://justaskthales.com/fr/la-biometrie-comportementale-cest-quoi/

[130] *Cf.* https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2012-652-dc-du-22-mars-2012-communique-de-presse

[131] *Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ?* https://www.cnil.fr/fr/mort-numerique-effacement-informations-personne-decedee

Ces dispositions sont nées en 2016, à l'initiative de la loi Lemaire pour une République numérique, qui prévoit la mise en place d'un registre d'enregistrement des directives générales relatives à la conservation, à l'effacement et à la communication des données d'un utilisateur, après son décès, ainsi que la désignation d'un tiers de confiance.

Mais, cinq ans plus tard, son décret d'application n'a toutefois pas encore été publié.

Cependant, les arrêts du Conseil d'Etat en date du 6 décembre 2019 - pris à la lumière de l'arrêt de la CJUE rendu le 24 septembre 2019 qui établit que Google n'était pas tenue de respecter la politique européenne du droit à l'oubli à l'échelle mondiale[132] – définissent les conditions dans lesquelles doit être respecté le droit au référencement sur Internet prévu par le RGPD.

Dans une décision rendue le 27 mars 2020, le Conseil d'Etat estime que le droit de déréférencement doit s'appliquer au sein de l'UE. Il donne ainsi raison à Google face à la CNIL, qui obtient l'annulation d'une sanction prononcée par la CNIL en 2016.

Avec ces arrêts, le Conseil d'Etat est ainsi devenu la première juridiction française à livrer à Google et à la CNIL un mode d'emploi du droit à l'oubli[133].

Le 'droit à l'anonymat' est à considérer sous l'angle du consentement ou du refus à être identifié. Il y a traitement de données à caractère personnel dès l'instant que la personne est identifiée ou identifiable.

Le RGPD a renforcé la notion de consentement des personnes concernées pour qu'un traitement de données soit réalisé, ce qui est le cas de la publication en ligne d'un prénom et d'un nom. Toutes les fois où le traitement n'est pas rendu obligatoire (pouvoirs publics) ou encore nécessaire par des impératifs particuliers, la personne concernée doit avoir donné son consentement (article 7 du RGPD). L'un de ces impératifs, accordé aux activités journalistiques professionnelles, est l'information du public. Un organe de presse peut donc nommer une personne dès lors qu'elle est présente dans l'actualité. Mais en revanche, un simple blogueur ne peut se le permettre puisqu'il n'est pas journaliste professionnel. L'article 7, point 3 spécifie également que la personne « a le droit de retirer son consentement à tout moment ».

Le décret relatif aux catégories de documents administratifs pouvant être rendus publics (notamment diffusés en *open data*) sans faire l'objet d'un processus d'anonymisation préalable publié 12 décembre 2018, fait suite à la loi pour une République numérique d'octobre 2016 et pour l'application de l'article L. 312-1-2 du Code des relations entre le public et l'administration (CRPA). Celui-ci prévoyait que sauf dispositions législatives ou réglementaires contraires ou accord des intéressés, les documents administratifs comportant des données personnelles ne peuvent être rendus publics qu'après avoir été anonymisées. Mais des exceptions à cette obligation d'anonymisation étaient prévues par cet article, que ce décret a fixées.[134]

Saisie par la direction interministérielle du numérique et du système d'information de l'Etat d'une demande d'avis sur le projet de décret, la CNIL avait rendu son avis le 15 mars 2018 sur le projet de décret. C'est à sa demande que le décret publié le 12 décembre comporte de façon explicite la typologie des documents concernés ainsi que les modalités techniques encadrant la diffusion de ces documents. *« Ces documents pourraient également intégrer des recommandations de bonnes pratiques pour éviter les administrations à opérer, préalablement à chaque publication de*

[132] *The operator of a search engine is not required to carry out a de-referencing on all versions of its search engine* : https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf

[133] *Droit à l'oubli : le Conseil d'État donne le mode d'emploi* : http://www.globalsecuritymag.fr/Droit-a-l-oubli-le-Conseil-d-Etat,20191206,93567.html?fbclid=IwAR0XLscBxcF_6a5kxofYfDsDDZ7eDmb7aGCKSx2KtgjJS_mRCTCugJEKQmE

[134] *Décret n° 2018-1117 du 10 décembre 2018 relatif aux catégories de documents administratifs pouvant être rendus publics sans faire l'objet d'un processus d'anonymisation : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037797147/*

documents, un équilibre entre l'intérêt de l'information du public et les atteintes potentielles à la vie privée », indiquait alors la présidente de la CNIL, Isabelle Falque-Pierrotin.

Parmi ses différentes recommandations, la commission rappelait également que *« toute réutilisation des données à caractère personnel, notamment à des fins commerciales, devra être conciliée avec le droit d'opposition des personnes concernées. La réutilisation des données devra ainsi respecter la volonté des personnes concernées telle qu'exprimée lors de la collecte ».* Elle recommandait donc aux administrations de mettre en œuvre des dispositifs permettant aux réutilisateurs d'identifier précisément les documents pour lesquels des droits d'opposition à certaines réutilisations avaient été enregistrés par le responsable du traitement initial. La commission rappelait également, à titre général, que *« la publication de documents administratifs sans anonymisation préalable doit avoir lieu sans préjudice des obligations imposées aux ré-utilisateurs par le cadre juridique relatif à la protection des données personnelles. »*

Le ‘droit à l'image‘ permet d'autoriser ou de refuser la reproduction et la diffusion publique de votre image. Il est possible de demander le retrait d'une image au responsable de sa diffusion. En cas de refus, une action en justice peut être engagée en cas d'atteinte à la vie privée. Toutefois le ‘droit à l'image’ est limité par le droit à l'information.[135]

- *La manipulation de l’information, des opinions et des comportements*

Dans le numéro de novembre 2021 que la *Revue Esprit* consacre aux bouleversements politiques portés par le numérique sous l’intitulé « *Internet en mal de démocratie*, Romain Badouard et Charles Girard écrivent : *« Une conviction guide cette démarche : la régulation d’Internet ne peut pas faire l’économie d’une réinterprétation des exigences associées au débat public. Ce dernier ne saurait en effet prendre la même forme en ligne et hors ligne. Il ne suffit donc pas de transposer les catégories d’analyses et les cadres régulateurs forgés pour d’autres formes de communication aux technologies numériques. Cette nouvelle transformation de l’espace public nous oblige, au contraire, à reconsidérer les conditions sociales et les dispositions légales susceptibles de le préserver. Les textes réunis dans ce dossier examinent ainsi certains des défis majeurs soulevés par la numérisation du débat public : la propagation de fausses informations, la mobilisation de nouveaux publics, l’émergence de pouvoirs de régulation privés ou la déstabilisation des cadres légaux traditionnels. L’ambition des contributeurs n’est pas de formuler des propositions de réforme, mais de contribuer au diagnostic qui en constitue le préalable nécessaire : comprendre ce qu’Internet, sous sa forme actuelle, fait à l’espace public. »*[136]

« Séduction et manipulation cognitives constituent l'une des faces sombres du cyberespace. Le monde ouvert du partage de l’information s’avère être également, voire surtout, le monde cynique de la fabrique artificielle du sens et du consentement, attisant la défiance individuelle, approfondissant « l’archipélisation » sociale, menaçant la stabilité étatique. » (Général Paul Cesari – CSFRS)

« De la haine en ligne à la manipulation des opinions publiques, en passant par la censure d'un président en exercice, les enjeux démocratiques du numérique sont considérables. L'année 2020 marque un tournant, avec l'infodémie liée au Covid, caractérisée par une

[135] *Droit à l'image et respect de la vie privée :* https://www.service-public.fr/particuliers/vosdroits/F32103?fbclid=IwAR3BrqtZH2ZH0ES9ibAf5UxH7UwoLgn9-p4lxJd8UzsseZty7Ztf-yyAevY

[136] *Cf.* https://esprit.presse.fr/article/romain-badouard-et-charles-girard/internet-en-mal-de-democratie-43625

amplification sans précédent de la désinformation. » (Brunessen Bertrand, Professeure agrégée de droit public[137])

Jean-Louis Missika, spécialiste en analyse des stratégies politiques et de la relation aux médias, et Henri Verdier, Ambassadeur pour les affaires numériques au sein du ministère français de l'Europe et des Affaires étrangères, posent un terrible constat sur les impacts de cette évolution technologique brutale sur la démocratie et la Nation : *« La liberté d'expression, comme nous l'entendions jusqu'à présent, reposait sur l'idée que des humains parlaient à d'autres humains. Il y a toujours eu une asymétrie entre ceux qui parlent et ceux qui écoutent, mais cette asymétrie demeurait dans le cadre de l'humanité. Qu'en est-il de cette asymétrie quand ce sont des machines et des algorithmes qui s'adressent aux humains ? Quand les humains qui reçoivent les messages n'ont aucune idée de ce que les machines savent sur eux et de la raison pour laquelle ils les reçoivent [...]*

C'est ainsi que la vie politique change de nature. L'agenda de la campagne électorale compte beaucoup moins. La bataille pour le contrôler perd de son importance. Il y a encore des débats ou des échanges d'arguments entre responsables politiques, mais l'important se passe en-deçà ou au-delà de l'espace public. Comme le souligne Lessig : « L'économie moderne de la liberté d'expression n'est pas pilotée par des éditeurs qui cherchent à publier ce que leurs lecteurs pourraient comprendre, mais par des machines qui fabriquent un discours fondé sur le comportement que l'on désire obtenir. Dans la plupart des cas, ce comportement est simplement commercial : cliquer sur une publicité. De façon plus préoccupante, ce comportement va parfois au-delà du commercial : prendre d'assaut le Capitole » [...]

Que devient la démocratie si une campagne électorale cesse d'être ce moment où la communauté nationale, par le débat public et la controverse, décide collectivement de son destin ? Si elle devient la résultante de stratégies d'investissements publicitaires fondées sur un micro-découpage de l'opinion et des micromanipulations quotidiennes ? Que devient, même, la Nation ? La fragmentation de la communauté nationale en de multiples cibles, l'envoi de messages spécifiques à ces micro-segments, dans le secret et sans contradiction, interdisent une réelle délibération politique, préalable au vote. La démocratie est née dans l'agora. Elle a besoin d'un espace public qui soit réellement public. Le microciblage et la publicité politique personnalisée désintègrent l'espace public [...]

Créer de fausses identités pour infiltrer des communautés, créer de faux médias pour donner au mensonge l'apparence d'une information vérifiée, produire de fausses informations, fondées sur de fausses preuves quasiment indétectables, le "faire paraître vrai" a changé de nature avec les réseaux sociaux et l'intelligence artificielle. Il s'est sophistiqué et éloigné des techniques rudimentaires de la propagande. Ce qu'on appelle à tort "post-vérité" n'est rien d'autre que ce changement de registre du "vraisemblable" et de sa mise en forme. » [138]

Pour Jan-Werner Müller, professeur de sciences politiques à l'université de Princeton[139] : *« La liberté de la presse n'a jamais été aussi mal en point qu'aujourd'hui. Les régimes autoritaires mettent leurs appareils législatifs au service d'une répression de la société civile et exploitent le manque de transparence et de régulation des plateformes numériques. »*

[137] *Comment l'UE lutte contre la désinformation en ligne :* https://theconversation.com/comment-lue-lutte-contre-la-desinformation-en-ligne-171230

[138] *La démocratie, otage des algorithmes - Une désintégration de l'espace public* : https://www.telos-eu.com/fr/politique-francaise-et-internationale/la-democratie-otage-des-algorithmes.html

[139] *Qu'est-ce qui menace la liberté de la presse aujourd'hui ?:* *https://esprit.presse.fr/article/jan-werner-muller/qu-est-ce-qui-menace-la-liberte-de-la-presse-aujourd-hui-43444*

Selon le Dr Pierre-Nicolas Schwab, expert en "Big Data", "*le design des sites Web est conçu de manière à orienter le comportement de l'internaute vers le consentement. Boutons d'acceptation plus gros, mieux placés, plus colorés, politiques de confidentialité kilométriques... toutes les stratégies sont bonnes pour éviter que l'utilisateur ne s'interroge trop*".[140]

Lorsque Tim Cook, le successeur de Steve Jobs à la tête d'Appel, affirme que lorsque le service est gratuit cela veut dire que le client final est le produit, il pointe un des véritables enjeux.

Bernard E. Harcourt, professeur de philosophie politique et de droit, affirme que nous avons tort de comparer les sociétés de surveillance à *1984* : *« Nous ne sommes pas face à une dictature cherchant à atténuer nos désirs, au contraire. C'est pour cela que nous n'allons pas résister en limitant notre accès aux écrans, ceux de nos proches ou de nos enfants. Ça ne va pas marcher et ça ne peut pas marcher car nous éprouvons tellement de jouissance dans ce nouveau monde, tellement de plaisir dans le numérique, qu'on ne peut l'arrêter en remontant le temps et décélérant… Chez Orwell, les résistances sont rendues possibles car les habitants avaient envie d'autre chose : ils voulaient du café, du thé, du rouge à lèvres, une chambre à eux pour voir leurs amants, tous nos petits plaisirs qui leur étaient défendus. Aujourd'hui, c'est non seulement autorisé, mais même encouragé ! C'est comme ça que ça marche : en nous séduisant et en nous incitant à exposer nos désirs […] c'est effrayant que la résistance doit dépendre de vouloir, et non devoir, changer le monde. Or, c'est le plus grand défi puisque nous sommes face à un système reposant sur le désir. »* [141]

La défense des citoyens en matière de protection des données personnelles se fait en grande partie contre leur gré. La fatale attraction de la gratuité, les biais cognitifs dont celui qui consiste à penser que *« je n'ai rien à cacher »* ont raison de tout discours d'alerte considéré comme catastrophiste et rétrograde. La majorité des internautes cliquent de façon automatique sur les boutons "j'accepte" des sites qu'ils visitent. Peu savent ou essaie de savoir ce que le règlement en question comporte. Paresseux ou pressé, l'internaute ne semble pas vouloir s'informer et encore moins agir pour reprendre la main sur ses données privées alors qu'il semble bien conscient de l'importance et de la valeur de leurs données. Une enquête menée en 2018 par Axios-Survey Monkey rapportait que 56 % des internautes européens acceptaient les conditions d'utilisation des sites sans réfléchir, seuls 13 % déclarent les lire "toujours".[142]

Or cette situation est générale.

« Les innovations numériques telles que la 'deepfake reality' instaurent une ère de 'post-vérité intégrale'. Le business-modèle attractif des GAFAM se fonde sur un "encerclement cognitif" qui expose les internautes à la désinformation, la division et la manipulation

[140] En octobre 2020, la CNIL a présenté de nouvelles règles que doivent respecter tous les sites dès le 1er avril 2021. « Refuser les traceurs doit être aussi aisé que de les accepter », affirme l'autorité. Tout site ne proposant pas un bouton de refus aussi accessible – en un clic – que le bouton de consentement sera donc hors la loi dès ce jour.
L'affichage d'un bouton "Tout refuser" aux côtés du bouton "Tout accepter" est donc préconisé. En outre, par une décision du Conseil d'Etat de juin 2020 (https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-lignes-directrices-de-la-cnil-relatives-aux-cookies-et-autres-traceurs-de-connexion), les éditeurs sont libres de bloquer l'accès à leur site (ou de le rendre payant) en cas de refus.
Par ailleurs, l'information qui doit éclairer le consentement est désormais plus encadrée. Les éditeurs de site Internet doivent désormais clairement indiquer la nature et l'objectif des cookies qui seront soumis aux internautes. Tout comme l'identité des acteurs qui recueillent des informations personnelles. Les seuls cookies qui ne sont pas soumis à ces règles, selon la CNIL, sont ceux destinés à améliorer le confort de l'internaute. Soit des cookies qui servent à conserver un article en panier pour un site marchand, ou ceux qui permettent de rester authentifié à un service.

[141] *La société d'exposition, désir et désobéissance à l'ère numérique* :
https://usbeketrica.com/article/le-numerique-est-beaucoup-plus-fute-et-tenace-que-l-humain?fbclid=IwAR3pUKHqaQktdBQ9D9Btk0RKeX2t0oc02QTSh4PTFfucg0ITlysdtNjDNoQ

[142] Il est intéressant de relever que le 2 septembre 2021, la Cour de Justice de l'UE (CJUE) a rendu un arrêt sur deux affaires allemandes concernant des offres « tarif nul » de Fournisseurs d'Accès Internet (FAI). Pour la deuxième fois en l'espace d'un an la Cour a estimé cette pratique contraire au règlement européen sur l'accès à un Internet ouvert.
Cf. https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-09/cp210145fr.pdf

psychologique. […] Le manque à la fois de volonté politique et de capacités techniques adaptées pour contrer la diffusion de trolls et fausses nouvelles rendent les démocraties occidentales vulnérables aux interférences d'acteurs hostiles. » [143]

Une véritable guerre de l'influence par l'information, la désinformation et le déni d'accès s'est installée opposant des protagonistes aux motivations les plus diverses, dans laquelle les Etats interviennent à la fois comme 'influenceur' et comme 'cible.

La question fondamentale est la crédibilité des informations que nous percevrons demain à travers le cyberespace.

Avec l'espionnage industriel qu'a largement favorisé l'encouragement par les pouvoirs publics à recourir au télétravail pendant la crise pandémique de la Covid19, le *phishing*, la manipulation de l'information est devenue un autre grand fléau de la pandémie virale, puisant notamment sa raison d'être dans la méconnaissance scientifique du virus comme dans la volonté de certains 'influenceurs' de profiter de la crise pour miner la confiance des populations envers leurs gouvernements.

La loi française du 22 décembre 2018 relative à la lutte contre la manipulation de l'information[144] définit une fausse information comme toute allégation ou imputation d'un fait dépourvu d'éléments vérifiables de nature à la rendre vraisemblable.

Le Conseil constitutionnel a précisé qu'il ne pouvait s'agir que d'allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir. Cela ne couvre ni les opinions, ni les parodies, ni les inexactitudes partielles ou les simples exagérations.

Au niveau européen, la désinformation est définie dans le plan d'action pour la démocratie européenne de 2020[145] comme des contenus faux ou trompeurs diffusés avec l'intention de tromper dans un but lucratif ou politique et susceptibles de causer un préjudice public. La désinformation se différencie ainsi de la mésinformation par le critère de l'intention.

La diffusion de la haine sur les réseaux sociaux pose une triple responsabilité : celle des auteurs de contenus, qui doivent assumer leurs propos ; celle des réseaux sociaux, qui doivent en toute transparence mettre en oeuvre une organisation susceptible de bannir la haine en ligne ; et celle des Etats qui doivent fixer les règles et s'assurer qu'auteurs et plateformes les respectent.

En mai 2019, la mission de régulation des réseaux sociaux a remis au secrétaire d'État en charge du numérique son rapport "*Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne*".[146]

Le rapport propose des pistes de réflexion et d'action qui sont venus nourrir les travaux parlementaires qui ont débouché sur l'adoption en janvier 2020 de la '*loi Avia'* qui impose aux plateformes en ligne (plateformes ayant plusieurs millions de visiteurs par mois - Facebook, Twitter, You Tube… - mais également, désormais, forum de n'importe quel site de presse, d'une plateforme militante, d'un petit hébergeur associatif ou de tout nœud d'un réseau social

[143] *"La deepfake reality : vers la fin de la vérité dans le cyberespace ?", Questions à Franck DeCloquement.* https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-articles-de-la-revue-de-la-gendarmerie-nationale/la-deepfake-reality-vers-la-fin-de-la-verite-dans-le-cyberespace-rgn-268

[144] *LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information :* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559

[145] *Plan d'action pour la démocratie européenne : renforcer les démocraties de l'UE :* https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0790&from=FR

[146] *Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne :* https://www.numerique.gouv.fr/uploads/rapport-mission-regulation-reseaux-sociaux.pdf

décentralisé…) de supprimer dans l'heure tout contenu terroriste ou pédopornographique sur simple injonction de la police, en dehors de tout contrôle par un juge.

Si l'initiative peut sembler louable et rassurante, des effets pervers sont à craindre.

Pour la rédaction du site *La Quadrature du Net*, avec cette loi « *ces plateformes n'auront d'autres choix que de fermer boutique ou de déléguer leur modération aux outils de censure automatisée fournis par Google et Facebook. Dans tous les cas, les grands vainqueurs seront ces deux dernières entreprises, dont la concurrence sera anéantie ou mise sous leur joug.* »

Dès son adoption par le Parlement, le Conseil constitutionnel a été saisi par la voie d'une question prioritaire de constitutionnalité pour qu'en soit vérifiée sa conformité à la Constitution. Le 18 juin 2020, il a statué en concluant à une non-conformité partielle de ladite loi[147].

Brunessen Bertrand rappelle que *« le droit français, notamment la loi de 1881 sur la presse et le code électoral, encadre et sanctionne la diffusion de fausse information de longue date. Ce cadre juridique s'est révélé inadapté au regard des nouveaux usages induits par le numérique en ce qu'il ne s'intéressait qu'à l'émetteur originel d'une fausse information et non aux personnes participant ensuite à la diffusion d'une information ayant perdu son caractère nouveau. La loi de 2018 cherche à réguler le comportement de ceux qui, de bonne foi, diffusent des informations fausses et participent à les rendre virales. Pendant les trois mois précédant une élection nationale, les opérateurs de plates-formes en ligne dont le nombre de connexions sur le territoire français dépasse les 5 millions de visiteurs par mois doivent fournir aux utilisateurs une information « loyale, claire et transparente » sur l'identité des annonceurs de « contenus d'information se rattachant à un débat d'intérêt général ».*

Les plates-formes doivent aussi prévoir un dispositif de signalement des fake news, mettre en œuvre des mesures sur la transparence de leurs algorithmes, être transparentes sur la promotion des contenus issus d'entreprises de communication audiovisuelle, lutter contre les comptes propageant massivement de fausses informations, informer les utilisateurs sur l'identité de la personne leur versant des rémunérations en contrepartie de la promotion de contenus d'information.

Au niveau européen, les éléments de régulation sont fragmentés et insuffisants. Le RGPD protège les données personnelles même s'il est parfois difficile à faire respecter en pratique, surtout à l'égard de plates-formes qui opèrent à une échelle internationale et déterritorialisée.

Pour lutter contre la désinformation, l'UE ne dispose que d'un instrument non contraignant, le code de bonnes pratiques contre la désinformation[148] auquel les plates-formes sont invitées à adhérer de façon spontanée depuis 2018, qui prévoit des mesures pour la transparence de la publicité à caractère politique, la fermeture des faux comptes ou la limitation de la monétisation des fausses informations.

Certaines obligations envisagées dans le Digital Services Act (voir *infra*) *pourraient renforcer son action. Cette proposition de règlement envisage des formes de corégulation par des codes de conduite pour limiter les risques systémiques liés à la désinformation, en particulier des mesures de transparence pour la modération de contenus et la publicité.*

[147] *Décision n° 2020-801 DC du 18 juin 2020 relative à la Loi visant à lutter contre les contenus haineux sur Internet :* https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm

[148] *Lutte contre la désinformation en ligne : publication du rapport sur la mise en œuvre du code européen de bonnes pratiques :* https://www.csa.fr/Informer/Espace-presse/Communiques-de-presse/Lutte-contre-la-desinformation-en-ligne-publication-du-rapport-sur-la-mise-en-oeuvre-du-code-europeen-de-bonnes-pratiques

Ce texte prévoit aussi l'obligation pour les très grandes plates-formes en ligne d'évaluer les risques systémiques liés à la manipulation intentionnelle de leurs algorithmes. La Commission européenne souhaite aussi proposer une législation sur la transparence du contenu politique sponsorisé.

Les enjeux sont vastes tant la lutte contre la désinformation est déséquilibrée pour les démocraties libérales. La voie la plus prometteuse, mais de long terme, reste une éducation au numérique pour éclairer les citoyens sur ces questions fondamentales. »

Franck DeCloquement, expert de l'intelligence stratégique, et membre de la cybertaskorce, nous alerte sur les risques de manipulation des opinions et des informations par les principaux réseaux sociaux en ligne : *« Les géants de la Big Tech représentent une réelle menace pour nos nations occidentales. Car le vrai danger des GAFA n'est pas tant qu'ils trustent le marché de l'information traditionnel, mais qu'ils ébranlent par ce biais le fonctionnement même de nos démocraties. […] Ne l'oublions pas, ces « mediums 2.0 » (au sens de Marshall McLuhan) que sont en réalité ces plateformes de mise en contact « universelle », ne sont pas neutre : bien au contraire. Alors que les GAFA se présentent encore comme de simples « hébergeurs » (comme l'affirme la loi française) pour s'exonérer visiblement de toutes responsabilités pénales (ce que permet leur statut de droit privé américain), de plus en plus de voix s'élèvent dans l'hexagone pour les assujettir aux principes de la loi de 1881 sur la presse. Ces opérateurs exercent en réalité par cette entremise labile généralisée d'une multitude d'acteurs – via leurs différentes interfaces – un magistère intellectuel et une emprise stratégique certaine, peu ou prou formateur d'opinions. Ce ne sont naturellement pas des acteurs passifs, bien au contraire, comme l'a révélé en outre l'affaire « Cambridge Analytica » et ses divers accès négociés aux données utilisateurs massives détenues par Facebook.*[149] *Pour preuve également de ce que nous avançons, les différents « contrats » passés par certains gouvernements pour réguler ce qui se passe en ligne sur leurs différents réseaux, en prévision de la tenue des prochaines élections présidentielles. L'exécutif français au premier chef. Facebook avait été d'ailleurs pris la main dans le sac par les autorités américaines, suite à une « expérience de sociologie active » à grande échelle, en lien avec la « contagion des émotions ». La plateforme sociale avait en effet conduit une expérience très secrète sur les internautes en manipulant le flux d'actualité de 700.000 utilisateurs, mais sans que ces derniers n'aient donné leur accord explicite. Cette découverte inopinée avait suscité une très forte vague d'indignation aux Etats-Unis. Le réseau social s'était alors abrité derrière une clause de sa « Politique d'utilisation des données » : « nous pouvons utiliser les informations que nous recevons à votre sujet pour des opérations internes, dont le dépannage, l'analyse des données, les tests, la recherche et l'amélioration des services ». Mais peut-on dignement assimiler les « toutes petites lignes » d'un document que peu d'internautes lisent, à un consentement éclairé ? »*[150]

Dans un article publié sur le site *portail-ie.fr*, Juliette Biau aborde le rôle majeur joué par les GAFAM dans ce registre : *« Dans son livre paru en mars dernier, Jillian C. York démontre qu'aujourd'hui, « les entreprises et les plateformes exercent un contrôle plus important sur notre capacité à accéder à l'information et à partager les connaissances que n'importe quel État ». En effet, au-delà du débat sur le pouvoir qu'ont les acteurs de la Silicon Valley sur la liberté d'expression, raisonnent également des problématiques quant à la possibilité pour les utilisateurs d'accéder à une information neutre et exempte de tout biais idéologique. Les algorithmes des plateformes numériques sont conçus de manière à déréférencer ou, au*

[149] *Comment la communication a façonné l'empire hégémonique de Facebook* : https://theconversation.com/comment-la-communication-a-faconne-lempire-hegemonique-de-facebook-157079

[150] *Pourquoi il devient urgent de sauver nos démocraties de la technologie* : https://www.atlantico.fr/decryptage/3594226/pourquoi-il-devient-urgent-de-sauver-nos-democraties-de-la-technologie-franck-decloquement?fbclid=IwAR0dccA1rmIXUKlVmAiOQszt_ssz_i1aOKN0ULGnZOCOj_tfCf5ncnPa6NA

contraire, améliorer la visibilité de certains contenus selon des techniques mathématiques et d'intelligence artificielle dont la logique est de moins en moins lisible et compréhensible par l'utilisateur. Deux tendances semblent émerger dans la gestion des contenus par les plateformes de réseaux sociaux.

D'une part, certaines mesures mises en œuvre depuis le début de la crise sanitaire visent à offrir aux utilisateurs uniquement des informations considérées comme « fiables » par les plateformes. A titre d'exemple, la politique de Youtube relative aux contenus sur « la désinformation liée au Covid 19 » indique que l'entreprise n'autorise pas la publication d'« allégations concernant la vaccination qui contredisent le consensus des experts des autorités sanitaires locales ou de l'OMS ». De même, tout contenu relatif à des sujets sensibles dans l'opinion publique (politique, élections, Covid 19, etc.) est fréquemment accompagné de messages d'avertissement donnant des indications sur la provenance ou la fiabilité des informations qu'il véhicule. « Faux », « information partiellement fausse », « cette publication manque de contexte » sont des bannières que Facebook affiche sous des contenus considérés comme peu fiables par les vérificateurs du réseau social, et renvoyant vers des sources officielles. Twitter affiche également des libellés relatifs aux comptes de médias gouvernementaux ou affiliés à un État. La chaîne de télévision russe RT France est qualifiée de « Média affilié à un État, Russie » alors qu'en parallèle, les chaînes publiques France Culture, France Inter ou encore la BBC sont des « organisations de médias financées par un État mais dotées d'une indépendance éditoriale » selon la politique de Twitter. Le fait de montrer ou non certaines informations n'est pas neutre : cela correspond à une certaine vision du monde que les plateformes tentent de diffuser massivement. Cette stratégie contribue également à l'encerclement cognitif des utilisateurs, en créant une dépendance à leurs services via *l'utilisation des algorithmes pour les enfermer dans une bulle informationnelle.*

D'autre part, les réseaux sociaux apparaissent de plus en plus comme un outil de gouvernance susceptible d'être utilisé par les élites politiques pour servir leurs intérêts. En effet, certaines injonctions étatiques peuvent aller à l'encontre des intérêts économiques des plateformes et vont pousser ces dernières à collaborer. Ainsi, suite à une demande formulée en avril par le Premier ministre indien Narendra Modi, Facebook, Instagram et Twitter ont accepté de supprimer certains messages critiquant la gestion de la crise sanitaire par le gouvernement indien. Enfin, la limitation de la diffusion d'un article paru en octobre 2020 dans le New York Post susceptible d'impacter la campagne présidentielle de Joe Biden est un exemple parlant de la capacité des plateformes à moduler l'importance d'une information et d'en réguler la viralité. […].

Loin de promouvoir le lien social entre les individus et une réelle entente entre les différentes communautés qu'ils constituent, les médias sociaux sont des entreprises privées dont l'objectif premier est la recherche du profit. Ainsi, le choix des contenus qui seront massivement vus ou non par les utilisateurs se fait en fonction du rendement que ceux-ci peuvent apporter aux plateformes. Certes, les mesures adoptées par les GAFA pendant la crise sanitaire et lors des périodes électorales illustrent leur volonté de limiter la diffusion de fausses informations et de ne pas apparaître comme vecteurs de leur propagation. Néanmoins, le risque associé à la suppression de contenus non conformes au « consensus » général ou en opposition avec la politique d'un État est celui de voir apparaître une information formatée ne pouvant faire l'objet d'aucune remise en question. Alors même que les débats et affrontements d'idées est ce qui a permis aux plateformes de prospérer et de s'enrichir, les mesures mises en œuvre aboutissent à un contrôle du débat public et à une restriction de ce qui peut être discuté ou non au sein de l'opinion. Or, comme l'a indiqué la Cour européenne des droits de l'homme en 1998, « peu importe que l'opinion [soit] minoritaire et qu'elle [puisse] sembler dénuée de fondement

: dans un domaine où la certitude est improbable, il serait particulièrement excessif de limiter la liberté d'expression à l'exposé des seules idées généralement admises ». »[151]

Cette manipulation de l'information a des formes et origines diverses que *l'Observatoire (dés)information et géopolitique au temps du Covid* de l'IRIS décrypte à travers une série d'analyses constitutives d'un dossier intitulé : '*le virus du faux'*.[152,153,154]

De leurs côtés, les Académies des Sciences, de Médecine, de Pharmacie et des Technologies mettent en garde collectivement, avec insistance et gravité, les citoyens contre la fausseté des informations propagées à propos de la gestion de la crise pandémique : *« Leur diffusion au sein de notre société, notamment auprès des plus jeunes, est de nature à compromettre le fondement rationnel des actions de santé publique nécessaires pour le contrôle de la pandémie en cours, qu'il s'agisse des mesures de distanciation, de confinement, de traçage des cas contacts ou de la mise en place espérée proche d'une vaccination. Au-delà de la santé, les attaques contre la science affectent aujourd'hui de nombreux aspects de la vie de nos sociétés. Ces attaques invitent scientifiques, éducateurs, professionnels des médias et citoyens à la plus grande vigilance. Il faut poursuivre auprès de tous la recherche des réponses appropriées et les efforts de pédagogie et de transparence sur l'état des connaissances scientifiques et technologiques, qui évoluent rapidement. »*[155]

Un rapport de l'Institut de Recherche Stratégique de l'École Militaire (IRSEM) révèle les nouvelles armes d'influence de la Chine dans le monde entier[156] un changement de doctrine, plus agressive, destinée à convaincre voire contraindre et imposer le récit de Pékin à tous les étages des sociétés dans le monde.[157]

Dans cette nouvelle fabrique du sens qu'est devenu l'Internet, une vigilance accrue des pouvoirs publics se fait jour face aux nouvelles *« menaces à la vérité »*.

Face à la nouvelle menace contre la démocratie que constitue la diffusion de fausses nouvelles, l'UE a incité, dès le début de la crise sanitaire, les plateformes à lutter contre les fausses informations en leur demandant de supprimer les contenus illicites. C'est ainsi que Twitter a été amené à fermer plusieurs millions de comptes. Elle a également demandé aux Etats de mettre fin aux fausses informations relatives à la circulation du virus.

---

[151] *Nouveaux censeurs : les GAFA et l'accès à l'information :*
https://portail-ie.fr/analysis/2941/nouveaux-censeurs-les-gafa-et-lacces-a-linformation

56

[152] *Cf.* notamment le glossaire proposé par cet observatoire :
https://www.iris-france.org/wp-content/uploads/2020/10/Glossaire_FR-EN_Covid.pdf

[153] Voir également *Comment lutter contre l'infodémie ? Dossier #6 :*
https://www.iris-france.org/wp-content/uploads/2021/03/Dossier-6-Le-virus-du-faux.pdf

[154] Voir également : *Comment les français s'informent-ils sur Internet ?*
https://www.fondationdescartes.org/2021/03/comment-les-francais-sinforment-ils-sur-Internet/

[155] Communiqué tétra-académique de l'Académie des sciences, l'Académie nationale de médecine, l'Académie nationale de Pharmacie et l'Académie des technologies - Paris, le 26 novembre 2020 :
https://www.academie-sciences.fr/fr/Rapports-ouvrages-avis-et-recommandations-de-l-Academie/hold-up-sur-la-science.html

[156] *Cf. Les opérations d'influence chinoise – Un moment machiavélien* (Paul Charon & Jean-Baptiste Jeangène Vilmer :
https://drive.google.com/file/d/1qxUvLrLG4SSg8ANZnqvBfDOxUrtPmaB5/edit

[157] L'Armée Populaire de Libération (APL) tient à sa disposition une constellation de pigistes prêts à diffuser cette désinformation et à assurer la publicité de la Chine. Ces petites mains sont pilotées par l'unité 61070 chargée de la propagande réseaux au sein de la base 311, le cœur opérationnel de l'influence chinoise. Elles sont chargées des opérations informationnelles, tactique directement inspirée de la méthode russe, et se divisent en deux catégories. Des trolls, en chair et en os, sont notamment sollicités pour pratiquer l'Astroturf dont l'objectif est d'inonder les réseaux ciblés d'un maximum de messages de désinformation en donnant l'illusion d'un soutien spontané ou d'une dénonciation populaire authentique pour contre attaquer les discours hostiles au régime. Mais le chiffre annoncé par les auteurs de l'enquête concerne ceux que l'on appelle couramment "l'armée des 50 centimes". Leur travail d'occupation s'applique moins à intervenir sur les sujets de discorde qu'à allumer des contre-feux en distrayant le public et en assurant la promotion de la Chine..

Le Parlement britannique a mis en place une commission d'enquête ; le Parlement allemand a légiféré ; les autorités italiennes ont mis en place une plateforme de signalement de fausses nouvelles. La France ne pouvait rester immobile.

Une loi contre la manipulation de l'information a donc été adoptée en novembre 2018 puis validée par le Conseil constitutionnel en décembre 2018. Le texte s'attaque à la diffusion massive et extrêmement rapide des fausses nouvelles *via* les outils numériques, notamment les tuyaux de propagation que sont les réseaux sociaux et les médias sous influence d'un État étranger. Si l'attention est particulièrement portée sur les périodes de campagne électorale, juste avant et durant les élections, pour concentrer les outils sur le vrai danger, c'est-à-dire les tentatives d'influencer les résultats d'élections, elle s'est également penchée sur la déontologie de la presse, en invitant à instaurer une instance de déontologie de la presse associant journalistes, éditeurs et société civile – cette proposition pouvant se traduire par un texte législatif ou réglementaire.[158,159]

Mais force est de déplorer l'absence de dispositions à l'égard du risque de diffusion massive et extrêmement rapide de fausses nouvelles au travers des principaux médias nationaux dont les actionnaires entretiennent simultanément des rapports d'actionnariat étroits avec les grands opérateurs de communication numérique, au point d'apparaître comme des oligarques de fait.[160]

Le gouvernement français a pris la décision le 12 janvier 2021, lors d'une réunion du Conseil de Défense, de faire la guerre aux *« fake news »* pilotées de l'étranger. Marqué par les MacronLeaks, ces milliers de mails privés et professionnels de responsables d'En Marche publiés au dernier jour de la campagne présidentielle de 2017, puis par les *« campagnes antifrançaises »* sur les réseaux sociaux après les attentats de Conflans-Sainte-Honorine et de Nice à l'automne 2020, l'exécutif a décidé de s'armer.

À l'instar des États-Unis ou encore du Royaume-Uni, la France a décidé de créer une agence destinée à lutter contre la désinformation en provenance de l'étranger, sous l'égide du SGDSN. Cette agence est baptisée Viginum, pour *« Service de vigilance et de protection contre les ingérences numériques étrangères »*

D'autres pays ou groupes d'Etats se sont d'ores et déjà dotés de telles structures. L'Union européenne par exemple a créé en 2015 *'East Strat Comm'*, spécifiquement consacrée à lutter contre les manipulations en provenance de Russie. Aux Etats-Unis, un organisme rattaché au département d'Etat, le GES, a la mission de *« diriger, synchroniser, intégrer et coordonner les efforts du gouvernement fédéral pour détecter, comprendre, exposer et contrer la propagande étatique et non-étatique, les manœuvres de désinformations visant à saper ou influer sur la politique, la sécurité ou la stabilité des Etats-Unis, de leurs alliés et de leurs partenaires »*.

Conscient du risque que cette nouvelle agence passe pour un outil d'influence en ligne au service de l'exécutif français à un an de la présidentielle, le SGDSN promet la "transparence totale" sur ses actions. Un comité d'éthique et scientifique a été institué, composé d'un membre du Conseil d'Etat, d'un membre du Conseil supérieur de l'audiovisuel (CSA), d'un magistrat, d'un ambassadeur, de journalistes et de chercheurs pour veiller sur les activités de cette agence, qui ambitionne de devenir un 'Graphika d'Etat', le spécialiste américain de l'étude des nouveaux médias. Si la nécessité d'une telle initiative semble incontestable, des questions demeurent sur

[158] *Cf.* https://www.gouvernement.fr/action/lutte-contre-la-manipulation-de-l-information

[159] NB : Aujourd'hui, aucun texte ne s'attaque à la diffusion massive et extrêmement rapide des fausses nouvelles *via* les outils numériques, notamment les tuyaux de propagation que sont les réseaux sociaux et les médias sous influence d'un acteur politique national entretenant des relations particulières avec les principaux actionnaires des grands opérateurs numériques nationaux ou étrangers et les propriétaires des médias mainstream intervenant au sein du paysage audiovisuel national.

[160] Les oligarchies de fait sont les sociétés dont le gouvernement est constitutionnellement et démocratiquement ouvert à tous les citoyens mais où en fait ce pouvoir est confisqué par une petite partie de ceux-ci

les usages réels et les cibles potentielles comme sur les finalités politiques des actions opérées à partir d'une telle agence, l'histoire recélant d'expériences dramatiques où les vérités d'Etat résistaient mal à des analyses 'indépendantes' et/ou 'scientifiques', aucun Etat ne pouvant prétendre être paré des attributs d'un parangon de vertu, pas même l'Etat français …

Dès lors que faut-il penser de cette association de l'Agence France Presse (AFP) avec Google pour la conduite de leur programme *« Objectif Désinfox »* de lutte contre la désinformation à destination des rédactions françaises à l'approche des élections nationales de 2022 ?

Faut-il voir une explication dans le fait que les Etats-Unis aient rejoint en décembre 2021 l'appel de Paris lancé le 12 novembre 2018 lors du Forum de Paris sur la Paix pour assurer la confiance et la sécurité dans le cyberespace, appel qui rassemble aujourd'hui 80 États, 36 organismes publics et administrations territoriales, et surtout 391 organisations et membres de la société civile, sans oublier 706 entreprises comme Microsoft et Google ?

- *Les échanges culturels sur Internet font l'objet de dispositions du droit qui inquiètent*

De nombreux débats éthiques et juridiques sont survenus depuis le début des années 2010 à propos de la mise en place d'une Haute autorité (HADOPI) pour identifier les personnes qui partagent des œuvres sur Internet.

Saisi en février 2020 par la Quadrature du Net, FDN, DDDN et Franciliens.net au travers une QPC à propos des pouvoirs que la loi sur l'audiovisuelle en vigueur donne à la HADOPI (par exemple en identifiant les adresses IP connectées à divers flux BitTorrent), le Conseil Constitutionnel a rendu sa décision d'inconstitutionnalité des dispositions en cause le 20 mai 2020.[161] Ces pouvoirs ont pris fin le 31 décembre 2020. Cette décision s'inscrit dans la continuité d'une jurisprudence déployée depuis cinq ans par le Conseil constitutionnel, en parallèle de la CJUE, qui tend à replacer l'autorité judiciaire dans son rôle de contrôle préalable de l'administration, notamment quand il s'agit de lever l'anonymat des internautes.

Or, la raison d'être de la HADOPI était précisément de contourner la justice afin de surveiller le plus grand nombre d'internautes et de les dissuader de partager des œuvres en ligne. Puisqu'il lui est enfin imposé de passer par la justice, la raison d'être de la HADOPI disparait. Or, si le projet de nouvelle loi audiovisuelle prévoyait déjà de supprimer la HADOPI, il prévoyait néanmoins de transmettre ses missions au CSA. La décision du Conseil constitutionnel ne le permettra pas, car il est désormais illégal de perpétuer des missions dont l'incompatibilité à la Constitution a été désormais reconnue.

Ces deux derniers organismes ont fusionné au 1er janvier 2022 pour donner naissance à l'ARCOM, l'Autorité de régulation de la communication audiovisuel et numérique, dont le fonctionnement est collégial et indépendant.

C'est la loi relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique du 25 octobre 2021[162] qui a entériné sa création, en lui assignant 3 missions **:** la protection des oeuvres et des objets auxquels sont attachés un droit d'auteur, un droit voisin ou d'un droit d'exploitation audiovisuelle ; l'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite des oeuvres et des objets protégés par un droit d'auteur, un droit voisin ou un droit d'exploitation audiovisuelle ; réguler et veiller dans le domaine des mesures techniques de protection et d'identification des oeuvres et des objets protégés.

[161] *Décision n° 2020-841 QPC du 20 mai 2020 :* https://www.conseil-constitutionnel.fr/decision/2020/2020841QPC.htm

[162] LOI n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (1) : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044245615

Le champ d'application des pouvoirs de l'ARCOM ne se limite pas à une juxtaposition des compétences du CSA et de l'HADOPI. En effet, elle voit son champ de compétences élargi à des acteurs du secteur numérique, notamment les services de vidéo à la demande par abonnement (Netflix, Disney +...) ainsi que les plateformes en ligne dans la lutte contre la manipulation de l'information et la haine en ligne. L'ARCOM est ainsi par exemple chargée de contrôler les moyens mis en oeuvre par le réseau social Facebook, TikTok ou encore YouTube pour lutter contre les fausses informations et la diffusion de contenus haineux.

La loi renforce également ses pouvoirs en matière de lutte contre le piratage.

L'ARCOM conserve le fameux mécanisme dit de "*réponse graduée"* qui vise à assurer le respect du droit d'auteur sur Internet, d'abord par l'envoi d'avertissement au titulaire d'une connexion à Internet et, en cas d'échec, par la transmission à l'autorité judiciaire du dossier révélant les faits de nature à caractériser une infraction.

Trois nouveaux dispositifs s'ajoutent à cette mesure visant cette fois-ci non pas l'utilisateur final mais les services intermédiaires.

En vertu du mécanisme des "*listes noires*"**,** l'ARCOM sera chargée d'établir une liste publique des plateformes de partage de contenus audiovisuels et numériques portant atteinte "*de manière grave et répétée au droit d'auteur et aux droits voisins*". L'un des objectifs est de pouvoir couper les flux transitant par les boîtiers IPTV (mode de consommation de la télévision qui est illégale lorsqu'elle donne accès à des contenus diffusés par des acteurs qui ne sont pas titulaires des droits).

La loi prévoit aussi un dispositif de blocage ou de déréférencement des "*sites miroirs*". Ces dernières reprennent en grande partie ou en totalité les contenus d'un site condamné en justice. Le gendarme pourra demander leur blocage aux fournisseurs d'accès Internet (FAI) et aux opérateurs de noms de domaines. Le déréférencement pourra lui être exigé auprès des moteurs de recherche.

- *La surveillance généralisée des réseaux interroge*

En 2014, les institutions européennes ont adopté une directive exigeant des fournisseurs de services de télécommunication et d'Internet qu'ils conservent toutes les données de communication pendant 2 ans et les mettent à la disposition des services répressifs sur demande.

Dans un arrêt pris le 6 octobre 2020[163], la CJUE a considéré que la directive constituait *« une ingérence étendue et particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, sans que cette ingérence soit limitée au strict nécessaire »*.

Le Parlement européen était censé modifier la directive mais ne l'a pas fait et celle-ci reste aujourd'hui en vigueur.

Devant cette situation équivoque et faisant valoir des impératifs de sécurité nationale, l'exécutif français a considéré que l'Etat pouvait légitimement demander aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée pendant un an les données de toutes nos communications personnelles ou professionnelles : numéro de téléphone appelé ou appelant, date, heure et durée de la communication, géolocalisation, identification du matériel utilisé, nom et adresse de l'utilisateur du matériel, adresse IP utilisée pour les services Internet, etc. De quoi permettre aux services de renseignement, à la justice et à la police de puiser, sous conditions, dans cette masse d'informations au gré de leurs besoins préventifs ou probatoires.

[163] *Cf.* https://curia.europa.eu/juris/document/document.jsf?mode=req&doclang=fr&docid=232084

Amené à devoir trancher entre l'exigence de respect du droit européen et celle d'accorder à l'Etat français le bénéfice du caractère dérogatoire au droit général européen des mesures ayant trait à la sécurité nationale[164], le Conseil d'Etat, par sa décision du 20 avril 2021, refuse d'appliquer l'arrêt de la CJUE estimant que tant le droit français du renseignement que l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion (IP, localisation, etc.) sont contraires aux droits fondamentaux.[165]

Or cette dernière notion de 'sécurité nationale' constitue un élément nouveau dans le droit français qui soulève toujours de nombreux questionnements.

Pour le professeur Bertrand Warusfel : *« Si l'on veut donner à ce nouveau concept une portée juridique opérationnelle et non simplement en rester à une affirmation symbolique, il convient non seulement d'en préciser le contenu mais aussi d'en délimiter et d'en contrôler la portée. A notre sens, le respect des principes essentiels de l'Etat de droit impose de satisfaire à trois conditions cumulatives : déterminer précisément les menaces dont le traitement relève du champ de la sécurité nationale, définir légalement les moyens juridiques dérogatoires que la puissance publique peut employer pour y faire face et mettre en place un contrôle indépendant chargé de garantir la bonne adéquation des fins et des moyens de la sécurité nationale. La définition du champ est en soi un exercice difficile comme nous venons de l'évoquer précédemment. En effet, la lecture des seules dispositions de la loi du 29 juillet 2009 ne nous permet pas d'identifier avec précision la frontière entre les menaces majeures justifiant le recours aux moyens spéciaux de sécurité nationale et celles qui – malgré leur importance intrinsèque – doivent relever des pratiques normales de sécurité publique et de maintien de l'ordre ou de toute autre politique publique classique.*

Le risque en cette matière est d'entrer dans un processus que certains politistes anglo-saxons dénomment "sécuritisation" ("securitization") et qui consiste pour un acteur politique à désigner comme une menace existentielle un enjeu – même non vital - qui va lui permettre de légitimer dans ce domaine des interventions allant au-delà des actions publiques classiques. Or, l'indétermination originelle du concept en France peut porter en elle le germe d'une telle dérive. Lorsque le Président de la République parle de la stratégie de sécurité nationale "qui associe, sans les confondre, la politique de défense, la politique de sécurité intérieure, la politique étrangère et la politique économique", on sent bien derrière ses mots le risque d'amalgamer certaines priorités politiques autour d'un concept volontairement large et aux contours indéfinis. Il n'est d'ailleurs pas indifférent que, dans les milieux de la sécurité (et notamment de la sécurité intérieure) l'on utilise fréquemment les termes de "sécurité globale" pour désigner cette imbrication des différents champs d'action et moyens d'intervention. […] A la globalisation indifférenciée de toutes les problématiques de sécurité dans un dispositif unique qui irait de la prévention de la petite délinquance à la protection de la Nation contre un conflit armé, en passant par la lutte contre la grande criminalité, le terrorisme ou l'espionnage économique (ce que certains appelaient parfois aussi le "continuum défense-sécurité"), les exigences juridiques opposent au contraire le maintien d'une distinction fondamentale entre l'exercice quotidien du droit commun de la sécurité publique et la mise en oeuvre d'un droit dérogatoire qu'autorisent seules certaines circonstances ou menaces exceptionnelles. »[166]

---

[164] Plusieurs options s'opposent sur l'interprétation des dispositions du traité de Lisbonne relatives à la sécurité nationale. Voir ma position sur ce sujet complexe : *De la sécurité nationale dans le traité de Lisbonne*

- *http://regards-citoyens.over-blog.com/article-de-la-securite-nationale-dans-le-traite-de-lisbonne-deuxieme-partie-nouvelle-edition-82372181.html*
- *http://regards-citoyens.over-blog.com/article-de-la-securite-nationale-dans-le-traite-de-lisbonne-troisieme-partie-nouvelle-edition-58649050.html*

[165] *Le Conseil d'État valide durablement la surveillance de masse :* *https://www.laquadrature.net/2021/04/21/le-conseil-detat-valide-durablement-la-surveillance-de-masse/*

[166] *La sécurité nationale, nouveau concept du droit français*

La surveillance généralisée des réseaux mobilise nombre d'associations internationales qui dénoncent les pratiques de certaines officines spécialisées.

Le scandale autour de la surveillance exercée par certains Etats s'étant doté de technologies de cybersécurité offensives auprès de la société technologique israélienne NSO - au travers du programme Pegasus - participe à alimenter les craintes des opinions publiques à cet égard.[167]

Meta a annoncé jeudi 16 décembre 2021 avoir fermé 1.500 comptes Facebook et Instagram liés à des cyber-mercenaires qui les ont utilisés pour espionner jusqu'à 50.000 militants, dissidents et journalistes pour le compte de clients dans le monde entier.

Les comptes en question étaient connectés à sept sociétés offrant des services allant de la collecte d'informations publiques en ligne à l'utilisation de fausses identités pour entrer en relation avec les cibles en passant par de l'espionnage numérique via du piratage.

Quatre des sociétés concernées sont basées en Israël (*Cobwebs Technologies, Cognyte, Black Cube* and *Bluehawk CI*). Les trois autres sont *BellTroX*, basée en Inde, *Cytrox*, basée en Macédoine du Nord et une société non identifiée basée en Chine.

Ces entreprises semblent prêtes à cibler n'importe qui pour le compte du plus offrant. Elles se présentent comme des "services d'intelligence sur internet", spécialisés dans la collecte et l'analyse d'informations récupérées sur des sites, des blogs, des forums de discussion, des pages de médias, etc.

Les cyber-mercenaires créent parfois des faux comptes sur les réseaux sociaux pour glaner encore plus d'éléments personnels, rejoignant même les groupes ou conversations auxquels ces personnes participent. Ils tentent également de gagner la confiance de leur cible avant de les duper en leur envoyant des liens ou des pièces jointes piégés et ainsi accéder, frauduleusement, à leurs téléphones ou ordinateurs. Ils peuvent alors récupérer des données sensibles comme des mots de passe, des numéros de téléphones, des photos, vidéos et messages, indique le rapport. Elles peuvent aussi activer les micros, caméras ou les fonctions de géolocalisation pour mieux espionner.

Pour le philosophe Michel Lhomme : « *la post-démocratie est en train d'opérer une synthèse encore plus radicale, celle de l'autoritarisme numérique et de la démocratie libérale utilisant l'intelligence artificielle et les données recueillies pour surveiller et prévenir tout dérapage oppositionnel à la vision mondialiste car le numérique ne promet pas seulement une nouvelle économie pour réformer le monde, il promet aussi au gouvernement de lui permettre de mieux comprendre le comportement de ses citoyens pour les surveiller et les contrôler en permanence. Cette nouvelle réalité citoyenne offrirait ainsi aux gouvernants une alternative possible à la démocratie libérale d'hier restée trop gênante parce que source d'oppositions argumentatives. Il ne s'agirait plus d'éduquer mais de formater, à la lettre une éducation non plus critique à la Condorcet mais de la confiance […] en l'autorité immuable de l'administration des choses […], par suivi informatique des déplacements et des pensées.* »[168].

---

http://www2.droit.parisdescartes.fr/warusfel/articles/Securite%CC%81Nationale_Warusfel2011

[167] Un consortium de médias international coordonné par l'organisation *Forbidden Stories* a eu accès à plus de 50 000 numéros de téléphone potentiellement ciblés et espionnés par une dizaine d'États, via le logiciel israélien Pegasus développé par l'entreprise de sécurité israélienne NSO. Sont concernés des journalistes, des chefs d'entreprise, et autres opposants politiques. Ce logiciel espion est extrêmement performant et discret : le propriétaire du téléphone ne peut pas le détecter. Il peut être installé à distance sans aucune intervention du propriétaire du téléphone, la machine n'est pas ralentie, la transmission des données est quasi-indétectable puis le logiciel s'autodétruit une fois la mission terminée. Près d'un millier de Français auraient été espionnés depuis 2014 par ce logiciel. Amnesty international précise comment savoir si on a été contaminé ou non : https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[168] *La Post-démocratie, une démocratie sans liberté ? :* https://www.polemia.com/post-democratie-liberte/

Autre illustration des débats houleux qui ont marqué l'année 2019 sur le registre du droit, celui qui s'est développé autour du projet très contesté de surveillance généralisée des réseaux sociaux pour y dénicher des indices relatifs à de la fraude fiscale. Ce débat est désormais clos, le Conseil constitutionnel ayant *in fine* validé en décembre 2019 le dispositif (seul un point secondaire a été rejeté)[169], les membres de l'institution faisant observer que la lutte contre la fraude et l'évasion fiscale est un « *objectif de valeur constitutionnelle* ». En conséquence, désormais, au cours de la période d'expérimentation de trois années, le Parlement aura tout loisir de légiférer pour combattre cette fraude et cette évasion fiscale sur les réseaux sociaux.

- *La protection des données au sein du cyberespace interroge*

La sécurité des données personnelles est, au-delà d'une obligation légale, un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. La CNIL reçoit, chaque année, de nombreuses notifications de violations de données qui peuvent avoir de lourdes conséquences.

La CNIL occupe une place centrale, avec l'ANSSI[170], dans le dispositif gouvernemental dédié à la protection des données conformément au RGPD[171] et à la lutte contre la cybercriminalité. Elle a produit et met en ligne des 'droits numériques'[172] qui peuvent être exercé auprès des organismes qui utilisent les données. Elle pilote l'analyse d'impact relatives à la protection des données (AIPD)[173] qui est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, et qui concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et les libertés des personnes concernées. La CNIL gère la mise à disposition de son logiciel *'open source'* PIA qui facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des données telles que prévues par le RGPD.

La CNIL s'intéresse depuis longtemps à la protection des données des mineurs et a notamment participé à l'émergence d'un « droit à l'oubli » renforcé. Pour faire face à ce défi, des mécanismes de protection des mineurs existent et se renforcent sous l'effet de certaines législations européennes et nationales. La protection des données personnelles peut utilement y contribuer, notamment grâce aux voies de recours qu'offre l'exercice des droits numériques. Afin d'accompagner les jeunes, les parents et les professionnels dans la mise en place d'un environnement numérique plus respectueux de l'intérêt de l'enfant, la CNIL a publié 8 recommandations issues d'une réflexion menée avec l'ensemble des acteurs concernés.[174]

L'UE poursuit activement une stratégie globale visant à réduire les risques sur la sécurité des personnes et la sauvegarde des droits humains induits par des usages intrusifs abusifs - sortant du cadre du droit - des technologies de surveillance.

---

[169] *Décision n° 2019-796 DC du 27 décembre 2019 - Loi de finances pour 2020 :* https://www.conseil-constitutionnel.fr/decision/2019/2019796DC.htm

62

[170] Pour sensibiliser aux bonnes pratiques de sécurité numérique et accompagner les entreprises et administrations dans la mise en œuvre de ces mesures de sécurité, l'ANSSI produit de nombreux documents destinés à des publics variés. Des guides techniques aux recueils de bonnes pratiques élémentaires en passant par les infographies, l'agence autorise et encourage le téléchargement, le partage et la réutilisation de ces informations dans le respect des conditions de réutilisation de l'information publique ou de la Licence ETALAB (https://www.etalab.gouv.fr/wp-content/uploads/2014/05/Licence_Ouverte.pdf), qui prévoient la mention explicite de l'auteur, de la source et de la version de l'information.
https://www.ssi.gouv.fr/administration/bonnes-pratiques/

[171] *Le rôle de la CNIL en matière de cybersécurité :*
https://www.cnil.fr/sites/default/files/atoms/files/cybersecurite_-_chiffres_2020_et_informations.pdf

[172] *Les droits pour maîtriser vos données personnelles !*
https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

[173] *L'analyse d'impact relative à la protection des données (AIPD) :*
https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

[174] *La CNIL publie 8 recommandations pour renforcer la protection des mineurs en ligne :*
https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne

L'Europe a une avance indéniable en matière de protection des consommateurs et des entreprises vis-à-vis des plates-formes du numérique.

En 2018, l'entrée en application du RGPD a largement modifié le paysage juridique en introduisant pour la première fois, dans le droit européen de la protection des données, des dispositions spécifiques aux mineurs. Elles prévoient, en particulier, l'exigence d'une information adaptée, le renforcement de leur droit à l'oubli et une capacité **à** consentir, sous certaines conditions, au traitement de leurs données (seuls au-delà de 15 ans ou avec leurs parents avant cet âge). Elles appellent également à une vigilance particulière à l'égard du profilage des mineurs**.** Ces textes ont toutefois suscité certaines interrogations et un besoin de clarification, notamment pour préciser leurs implications pratiques et leur articulation avec le droit national, en particulier le droit des contrats et de la famille.[175]

Dans une résolution adoptée le 10 juin 2021, les députés européens ont appelé à un renforcement des normes européennes pour les dispositifs connectés, applications et systèmes d'exploitation, tout en se félicitant de l'intention de la Commission européenne de proposer une législation horizontale sur les exigences en matière de cybersécurité applicables aux objets connectés et produits associés, cette dernière ayant présenté en décembre 2020 une nouvelle stratégie visant à accroître la résilience des entités critiques physiques et numériques.[176] Cependant, ils s'inquiètent d'une fragmentation du marché intérieur car chaque Etat membre de l'UE possède actuellement ses propres règles.

« Les capacités en matière de cybersécurité sont hétérogènes entre les États membres et que le signalement des incidents et le partage d'informations entre eux n'ont rien de systématique ou de complet, tandis que le recours aux centres d'échange et d'analyse (ISAC) pour l'échange d'informations entre les secteurs public et privé n'a pas atteint son plein potentiel », peut-on lire dans la résolution.

Le RGPD a 'théoriquement' accru la protection des personnes physiques.

Le nouveau règlement P2B renforce la protection des entreprises qui vendent via des plates-formes Internet.

Le futur règlement '*Digital Service Act'* (voir *infra*) va inclure des mesures pour assurer la sécurité des utilisateurs en ligne des plates-formes et imposer le partage de données avec les entreprises concurrentes. Car la structuration actuelle du Web est, à de très nombreux égards, non optimale. Les alternatives à Facebook, WhatsApp, Uber, Airbnb, Amazon existent, mais sont limitées par le faible nombre d'utilisateurs.

Les cyberattaques sont de plus en plus fréquentes.

« Le piratage des données est devenu une problématique majeure, dont les exemples sont quotidiens. Rien que sur l'année 2020, 3 950 fuites de données ont été détectées, selon une vaste enquête[177] menée récemment par la société Verizon. Le plus souvent, elles touchent de grandes plates-formes numériques (Facebook, LinkedIn, etc.) ou des acteurs socio-économiques importants – c'est le cas dans 72 % des cas recensés – et elles engendrent une fuite de données

[175] Parallèlement, des initiatives se multiplient à l'international, comme en témoignent la récente *« Observation générale sur les droits de l'enfant dans l'environnement numérique »* de l'ONU ou encore les actions de l'UNICEF, de l'OCDE, du Conseil de l'Europe ou encore de l'Union internationale des télécommunications (UIT). Le Comité européen de la protection des données (CEPD) et le réseau européen des défenseurs des enfants (ENOC) ont aussi engagé des travaux sur le sujet. En parallèle, plusieurs autorités nationales de protection des données, ont fait de ce sujet une priorité, comme le « Code de l'âge » de l'ICO britannique, les « 14 principes fondamentaux pour une approche du traitement des données centrée sur l'enfant » de la DPC irlandaise.

[176] *Résolution du Parlement européen du 10 juin 2021 sur la stratégie de cybersécurité de l'Union pour la décennie numérique (2021/2568(RSP))* : https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_FR.html

[177] https://www.verizon.com/business/resources/executivebriefs/2020-dbir-executive-brief.pdfx

personnelles dans 58 % de l'ensemble des cas. Les données personnelles sont en effet une cible de choix et cette fuite affecte aussi bien l'opérateur de services que les utilisateurs eux-mêmes. Une fuite de données peut donc concerner des données personnelles, qui sont en réalité des données de clients ou d'utilisateurs d'un service, mais également des données liées à l'organisation elle-même. Citons par exemple les informations de transactions d'une entreprise, les résultats de tests ou d'expérimentation de nouveaux produits ou services, etc. »[178]

Dans son rapport d'activité 2021, la direction générale des entreprises du ministère en charge de l'Economie a indiqué avoir détecté, grâce aux outils de prévention mis en place par le SISSE (Service de l'information stratégique et de la sécurité économiques), *"30 à 50 nouvelles alertes de sécurité économique chaque mois depuis la crise sanitaire"*. Soit plus de 700 alertes répertoriées depuis le 1er janvier 2020, dont des tentatives de rachat d'entreprises sensibles. *"La menace s'est intensifiée en 2021"*, a d'ailleurs expliqué la DGE, dont une de ces missions est de veiller à doter la France d'une économie souveraine et résiliente.

Le *Global Risks Report 2022* établi dans la perspective de l'édition 2022 du Forum économique de Davos consacre un chapitre entier aux risques cyber qui menacent les grands équilibres mondiaux et sociétaux.[179]

L' 'échec de la cybersécurité ' se classe parmi les cinq premiers risques en Asie de l'Est, dans le Pacifique et en Europe, tandis que quatre pays – l'Australie, la Grande-Bretagne, l'Irlande et la Nouvelle-Zélande – l'ont classé en pole position. De nombreuses « petites » économies hautement numérisées, à l'instar du Danemark, d'Israël, du Japon, de Taïwan (Chine), de Singapour et des Émirats arabes unis— ont également classé le risque parmi leurs cinq principales préoccupations.

Le métavers va étendre la surface d'attaque.

Dans un contexte de dépendance généralisée à des systèmes numériques de plus en plus complexes, les cybermenaces croissantes dépassent les capacités des sociétés à les prévenir efficacement et à les gérer, analyse le rapport.

Mais au-delà des événements cyber de 2021, et de ceux de ce début d'année, qui se voient notamment amplifiés par le télétravail, l'étude s'inquiète de l'émergence du métaverse qui « *pourrait également étendre la surface d'attaque pour les acteurs malveillants en créant davantage de points d'entrées pour les logiciels malveillants et les violations de données.* » Comme la valeur du commerce numérique dans le métaverse grandit « *en portée et en échelle* » – selon certaines estimations, il représentera plus de 800 milliards de dollars d'ici à 2024 -, « *ces types d'attaques augmenteront en fréquence et agressions*« , prédit le rapport.

Les cyberpompiers de l'ANSSI ont traité en 2020 128 incidents informatiques au sein des ministères. Si les ministères en charge de l'éducation nationale et de la transition écologique sont le plus souvent visés, deux attaques d'envergure ont touché Bercy et le Quai d'Orsay, nécessitant la mise en place d'opérations de cyberdéfense.

La parution le 24 octobre 2019 d'un rapport sénatorial démontrant la persistance d'importantes failles de sécurité numériques au sein de l'Assemblée nationale et du Sénat rappelle l'importance critique de ce sujet pour les pouvoirs publics[180].

[178] *Cf.* Benoit Loeillet *in Que font les hackers de vos données volées ?* https://theconversation.com/que-font-les-hackers-de-vos-donnees-volees-171032

[179] *Global Risks Report 2022 : https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf*

[180] *Cf.* https://www.senat.fr/rap/r19-082/r19-082_mono.html#toc0

Toutes les informations sensibles et confidentielles des parlementaires et des sénateurs sont vulnérables, et cette vulnérabilité s'est accrue avec le *Cloud Act* voté aux Etats-Unis en mars 2018, qui concède le droit au gouvernement américain d'obliger les entreprises américaines et leurs filiales à l'étranger à fournir les données de leurs utilisateurs, y compris lorsqu'elles sont stockées hors des Etats-Unis, en cas de demandes émanant de la justice américaine dans le cadre d'une enquête, ou encore avec la loi 'sur l'accès légal aux données chiffrées' qui met fin au chiffrement à l'épreuve des garanties dans les appareils, les plateformes *Cloud* et les systèmes informatiques, donnant notamment alors au gouvernement américain la possibilité d'exiger des backdoors (portes informatiques dérobées) dans le cadre d'un large éventail d'ordonnances de surveillance, dans les affaires pénales et de sécurité nationale, y compris l'article 215 de *l'USA Patriot Act.*

Le sujet est suffisamment sensible pour que la CJUE s'en saisisse et décide d'invalider un texte important dans l'écosystème numérique : le '*EU-US Privacy Shield'*[181] censé simplifier les échanges de données entre Europe et États-Unis - en remplacement de l'accord '*Safe Harbor'* (lui-même retoqué par la CJUE) -, considérant que ce texte ne garantit pas des protections suffisantes[182].

Aurélie Luttrin et Franck DeCloquement précisent à cet égard : *« La méconnaissance et une certaine forme d'aveuglement dans lequel reste plongé – peu ou prou – un grand nombre de personnes, mettent en péril nos institutions et nos sous-bassements démocratiques. Et à ce titre l'intelligence collective commune et notre détermination éclairée doivent devenir nos voies de Salut privilégiées. L'Etat doit se donner les moyens humains de fédérer les énergies communes autour de cette stratégie de protection des intérêts prioritaires de la Nation. Pour ce faire, l'Union européenne peut être un moyen – tant politique que financier – pour y parvenir. Mais il ne peut être le seul ! Car notre responsabilité à cet égard ne peut être déléguée. »*[183]

Le télétravail et la mobilité permanente des collaborateurs sont devenus incontournables et exposent les entreprises à de nouveaux défis en termes de sécurité mobile.

Dans ce contexte, 80 % des entreprises ont déjà subi des cyberattaques contre leurs systèmes. Une étude menée en 2021 fait apparaître que 50% des PME françaises ont déjà subi une intrusion sur leur site web et 40% sont attaquées chaque mois.[184] Et pourtant, moins de 25 % des téléphones mobiles d'entreprise sont sécurisés alors que les terminaux mobiles font partie des principales causes de fuites de données informatiques d'entreprise.

Marc Bothorel, référent cybersécurité national de la Confédération des petites et moyennes entreprises (CPME), relevant que le revenu du cybercrime est évalué à 6 000 milliards de dollars en 2021, estime que ce revenu devrait très probablement correspondre à la troisième économie mondiale derrière les États-Unis et la Chine en 2025.

Lors d'une audition qui s'est tenue le 27 mai 2020 devant la Commission de la défense nationale et des forces armées de l'Assemblée nationale1, le directeur général de l'ANSSI, Guillaume Poupard, rappelait qu'une des recommandations était « *d'éviter l'usage trop répandu d'équipements personnels »*, moins sécurisés que les outils professionnels et plus faciles à pirater. Il ajoutait que *« le développement du télétravail par des outils non maîtrisés a par ailleurs généré de nouveaux risques majeurs. Les outils de visioconférence non européens tels que Zoom, par exemple, peu sécurisés et régis par des réglementations non-européennes comme le Cloud Act, sont inadaptés aux échanges sensibles ».*

[181] *Cf.* https://www.cnil.fr/fr/le-privacy-shield
[182] *Cf.* https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf
[183] *Traitement de nos données en France : l'atteinte à nos intérêts fondamentaux :* https://cercle-k2.fr/etudes/traitement-de-nos-donnees-en-france-l-atteinte-a-nos-interets-fondamentaux
[184] *Cf.* https://www.globalsecuritymag.fr/Etude-cybersecurite-50-des-PME-ont,20210224,108618.html

Les auteurs d'une note de l'Institut Sapiens relevaient que *« l'un des aspects les plus inquiétants de la massification du télétravail non préparé […] est celui de la sécurisation des données et des échanges »*. Reprenant la classification de la direction générale de la sécurité intérieure (DGSI), cette note énonce un certain nombre de problèmes potentiels : le vol de données par des applications tierces (vol de données personnelles, mais aussi espionnage industriel) ; le ralentissement voire la paralysie des systèmes d'information du fait de connexions à travers des canaux non prévus ; l'usurpation d'identité, à travers des procédés plus ou moins subtils, comme l'hameçonnage.

Si ces risques informatiques ne sont pas spécifiques au télétravail, et si les attaques informatiques peuvent intervenir à tout moment (y compris la nuit ou les jours de fermeture des entreprises), il est clair que l'environnement plus ouvert rendu nécessaire par le télétravail constitue un terrain propice au piratage informatique.

La réponse à une telle menace passe par la fourniture aux employés de matériels sécurisés, plutôt que de permettre l'utilisation d'outils informatiques personnels. Elle passe aussi par une sensibilisation accrue des personnels en télétravail aux problématiques de sécurité informatique, tout le monde n'étant pas conscient des risques encourus ou même informés des astuces utilisées par les pirates informatiques. Elle passe enfin par le développement des métiers de la cybersécurité ou encore le souci d'installer des data center sur le territoire national, pour ne pas dépendre d'outils extérieurs, notamment américains.[185]

Pour Bernard Barbier, patron de la société BBCyber, membre de l'Académie Française des Technologies, membre du Conseil d'Administration de l'ARCSI, et ancien directeur technique de la DGSE, *« actuellement le réflexe classique des directions informatiques c'est d'empiler des outils de protection en ayant la fausse illusion d'être protégé. »*[186]

Selon Thibaut Heckmann, Officier de Gendarmerie, Chercheur Associé au Centre de Recherche de l'EOGN (CREOGN) et à l'ENS-Ulm : *« Les réseaux criminels n'utilisent pas les systèmes d'exploitation normaux car ils sont potentiellement reconfigurables par les utilisateurs à la différence des darkphones qui sont distribués par la tête du réseau et dont les paramètres ne sont pas modifiables (pas de consultation sur Internet, pas de message types SMS MMS, pas de communication téléphonique, pas de photographie ou vidéo possible). Pour contrer ces mesures de dissimulation criminelle, les forces de l'ordre ont dû développer des techniques de pointes pour faire face et s'unir. En 2015, grâce à une forte coopération policière internationale, la Gendarmerie royale canadienne a fait tomber le réseau de drakphones blackberry PGP, suivie par la Police néerlandaise qui a fait tomber successivement Ennetcom en 2016, puis PGP Safe en 2018. Le FBI a démantelé le réseau Phantom Secure en 2018. Notons enfin que le réseau Encrochat a été neutralisé en 2020 par la Gendarmerie française, en collaboration avec la Police néerlandaise et sous l'égide d'Eurojust, mettant un coup d'arrêt à plusieurs milliers de criminels dans le monde. … Ainsi, le renforcement de la coopération internationale du point de vue technique permet à la Gendarmerie française et à ses partenaires internationaux de développer et de rechercher des failles de sécurités logicielles et matérielles et d'acquérir du matériel de pointe pour lire les données à très bas niveaux et contourner les mécanismes de sécurité utilisés à des fins criminelles. Malheureusement, même si les réseaux Encrochat, Phantom Secure, PGP Safe, Ennetcom ont été démantelés, d'autres réseaux*

[185] *Cf.* Céline Boulay-Espéronnier, Cécile Cukierman et Stéphane Sautarel, sénateurs, *in* Rapport d'information fait au nom de la Délégation à la prospective, et intitulé '8 questions sur l'avenir du télétravail - vers une révolution du travail à distance ?' : https://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2021/2021-Documents_PDF/20211021_Rapport_Avenir_Teletravail.pdf

[186] *Cf. Vers une nouvelle gouvernance de la cybersécurité : une approche systémique de la maîtrise du risque numérique – La sécurité 360° de l'entreprise* : https://www.arcsi.fr/doc/B-Barbier-vers-une-nouvelle-ORGANISATION-CYBERSECURITE-en-entreprises.pdf

émergent déjà, en utilisant des technologies différentes (Omerta, SkyECC). Le jeu du chat et de la souris perdure encore et toujours. Les réseaux criminels s'efforcent d'utiliser des technologies permettant l'échange sécurisé dans leur réseau, les forces de l'ordre tentant d'anticiper les difficultés techniques d'accès aux données en développant leurs propres outils afin de mettre fin aux agissements criminels. »[187]

Si la durée de vie des plateformes du *Dark web* dépasse rarement une année puisque les activités illégales qu'elles hébergent se font en général rattraper par les polices, il n'en demeure pas moins que leurs activités illicites sont de plus en plus nombreuses et toutes ne sont pas anéanties. Un site comme la plateforme russophone Hydra vit bien et même très bien : le site compte désormais 2,5 millions de comptes et a reçu, depuis sa création en 2015, l'équivalent de 3,4 milliards de dollars en bitcoins.

Or, comme le souligne Eloise Tremblay : *« démanteler un site dans le Dark web est très complexe : l'IP n'est pas forcément connue – donc la localisation géographique exacte du serveur non plus – et dans l'éventualité où on trouverait le serveur, celui-ci pourrait être dans un endroit inaccessible juridiquement, comme par exemple un pays peu enclin à une coopération judiciaire internationale. De plus, d'un point de vue technique, si l'on identifie un des relais Tor par lequel il est possible d'accéder à Hydra, il en existe bien d'autres non listés ! Quant à les lister tous, ce serait remettre en cause la liberté du web, principe fondateur d'Internet. »*[188]

L'Etat français est préoccupé par cette situation[189] et développe régulièrement des initiatives visant à améliorer son dispositif dédié à la cybermalveillance[190].

Le ministère de l'Intérieur a publié un rapport[191] tentant d'évaluer l'évolution des attaques de rançongiciels visant les institutions et grandes entreprises.

Les difficultés rencontrées par la CNIL dans la mise en œuvre opérationnelle de décisions de la Cour européenne de Justice[192,193] ou du Comité européen à la protection des données[194] ayant trait à certains aspects clés de ces enjeux ont probablement joué un rôle incitatif dans cette mobilisation soudaine.

Et c'est dans un domaine aussi régalien que la lutte contre la cybercriminalité que l'engagement collectif s'avère d'abord primordial. Ainsi, le plan de renforcement de la cybersécurité se veut-il une incitation à la coopération, avec notamment la création d'un campus Cyber ouvert à une

---

[187] *Téléphones sécurisés, darkphones : quand le chiffrement devient la norme :* https://www.cercle-k2.fr/etudes/telephones-securises-darkphones-quand-le-chiffrement-devient-la-norme-526?fbclid=IwAR15u9p1P30KLKpk54h6V0umcyxgZR0ZRpoYLwEoZg4q_Ipoon5oTRMw33M

67

[188] *Le Dark Web, une nouvelle arme géopolitique :* https://atlantico.fr/article/decryptage/le-dark-web-une-nouvelle-arme-geopolitique-eloise-tremblay

[189] *Cf.* https://www.ssi.gouv.fr/uploads/2021/02/ANSSI-guide-tpe_pme.pdf

[190] Voir notamment : https://www.economie.gouv.fr/files/files/2021/20210720_dispositif_alterte_cybersecurite.pdf

[191] *Attaques par rançongiciel envers les entreprises et les institutions - Interstats Analyse N°37* : https://www.interieur.gouv.fr/Interstats/Actualites/Attaques-par-rancongiciel-envers-les-entreprises-et-les-institutions-Interstats-Analyse-N-37

[192] *Invalidation du Privacy Shield par la Cour de justice de l'Union européenne* : https://www.nextinpact.com/article/30416/109182-retour-sur-invalidation-privacy-shield-par-justice-europeenne
Avec cet arrêt, la CJUE a considéré que les États-Unis n'offraient pas le niveau de protection adéquat pour traiter les données des personnes physiques installées en Europe.

[193] *Invalidation du Privacy Shield : les organisations professionnelles réclament des mesures contre l'insécurité juridique :* https://www.nextinpact.com/lebrief/43893/invalidation-privacy-shield-organisations-professionnelles-reclament-mesures-contre-linsecurite-juridique

[194] *La Cnil européenne exhorte les institutions à ne plus transférer de données vers les Etats-Unis :* https://www-usine--digitale-fr.cdn.ampproject.org/c/s/www.usine-digitale.fr/amp/article/la-cnil-europeenne-exhorte-les-institutions-a-ne-plus-transferer-de-donnees-vers-les-etats-unis.N1023029?fbclid=IwAR0_7PuwIBWpRgLE31xsd4pP5p976Twb3QG5qIrLX92mgRB13ebcR3XzxJw

pluralité d'acteurs – parmi lesquels la Gendarmerie -, et dont l'une des tâches sera de former les personnels et favoriser la montée en compétences dans le numérique.

Guillaume Poupard se montre optimiste : si toutes les entreprises et les organisations prennent conscience que tout le monde est attaqué et investissent dans leur cybersécurité en considérant qu'il s'agit désormais d'une 'dépense vitale', alors il est possible de stopper dans les cinq prochaines années l'explosion actuelle des cyberattaques, qui ont déjà augmenté de 60% en 2021 après avoir quadruplé en 2020.

La Gendarmerie nationale ayant su développer un socle de compétences scientifiques et techniques de premier plan sur le registre numérique[195] qui la place en position de leader étatique incontestable dans la recherche de solutions techniques permettant de s'affranchir des vicissitudes inhérentes à une trop forte dépendance stratégique, technologique et opérative aux GAFAM et à leurs satellites anglo-saxons qui ont leurs propres objectifs et leur propre agenda[196], c'est sur elle et sur l'ANSSI que l'Etat s'est appuyé pour la mise en place du dispositif gouvernemental d'assistance et de prévention du risque numérique au service des publics.[197,198]

Face à la recrudescente des cyberattaques ciblant les administrations, l'État a décidé d'agir, en incluant un dispositif dédié à travers le plan France Relance, piloté par l'ANSSI.

L'une des priorités : les établissements de santé, cibles de 27 attaques informatiques en 2020. Une vulnérabilité des systèmes qui met en danger la santé des patients. Les Groupements hospitaliers de territoire (GHT) sont les principaux bénéficiaires de ce dispositif, car ils sont plus vulnérables que les CHU et les grands hôpitaux. Une offre de "Parcours de cybersécurité", qui comprend un diagnostic, une mise à niveau, ou encore des mesures organisationnelles et techniques de cybersécurité, leur est proposée. Par ailleurs, le gouvernement a décidé d'intégrer les hôpitaux au régime des Opérateurs de services essentiels, soumis à des obligations en matière de sécurité informatique.

Dans le cadre de France Relance et du 4ème Programme d'investissements d'avenir (PIA 4), le Gouvernement a lancé en 2021 une stratégie permettant d'accélérer le développement d'une filière économique française en cybersécurité. L'appel à manifestation d'intérêt (AMI) *« Sécuriser les territoires »* s'inscrit dans cette stratégie au niveau régional et dans la stratégie nationale de cybersécurité lancée fin février pour laquelle 1 milliard d'euros a été mobilisé, dont 720 millions de financements publics. Cet AMI, opéré par la Banque des territoires pour le compte de l'Etat dans le cadre du PIA 4, a pour objectif d'identifier les collectivités territoriales, ports et établissements de santé, qui présentaient des besoins en solutions cyber et souhaitaient héberger des prototypes appelés *« démonstrateurs de cybersécurité »*. Six

[195] *Comment les gendarmes s'organisent sans le cyberespace :* https://lessor.org/societe/comment-les-gendarmes-sorganisent-dans-le-cyberespace?fbclid=IwAR116CCOceHPWxYqrAaRU0dknMWmargrHOvs25avMwc0NHSdCNUATWm2DPw

[196] *L'effet GAFAM : stratégies et logiques de l'oligopole de l'Internet* : https://www.cairn.info/article.php?ID_ARTICLE=COMLA_188_0061

[197] Cybermalveillance.gouv.fr a pour missions d'aider les entreprises, les particuliers et les collectivités victimes de cybermalveillance, de les informer sur les menaces numériques et de leur donner les moyens de se défendre. https://www.cybermalveillance.gouv.fr/?fbclid=IwAR0jLdMTFFsy5jZi2NEN4HWXpA8D8thkZBsdRdd7f6HnVFnwx_X5L-i57Hs

Voir également *le guide de bonnes pratiques sur la gestion des attaques de ransomware élaboré par l'ANSSI, en partenariat avec la direction des Affaires criminelles et des grâces* : https://www.ssi.gouv.fr/uploads/2020/09/ANSSI-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

[198] Ses initiatives remarquables, notamment grâce au développement en son sein d'un malware pour compromettre les conversations de la messagerie cryptée Encrochat, une technologie utilisée par des milliers de criminels, ont permis aux polices européennes de démanteler des réseaux de grande envergure, avec des arrestations et des saisies records à la clé.
Cf. https://www.numerama.com/cyberguerre/634963-encrochat-comprendre-le-hack-des-smartphones-de-criminels-par-les-gendarmes-francais-en-5-questions.html

structures ont été sélectionnées pour accueillir des démonstrateurs de cybersécurité. Les 6 lauréats couvrent l'ensemble des structures identifiées comme prioritaires : une infrastructure portuaire, une collectivité locale et quatre établissements.[199]

La seconde étape consistera en un appel à projets, co-construit par l'État et les lauréats. Il permettra de sélectionner les entreprises qui réaliseront ces démonstrateurs et d'en co-financer le développement. Les lauréats seront ainsi les premiers à bénéficier du surcroît de protection induit par les démonstrateurs. A l'issue de l'expérimentation, puis de leur validation, le déploiement à plus large échelle de ces solutions adaptées aux besoins spécifiques des acteurs territoriaux sera engagé.

Par ailleurs, six sociétés françaises ont décidé d'unir leur expertise et leur force commerciale. Ensemble, ils proposent aux entreprises une offre complète de sécurité couvrant toute la surface d'exposition aux menaces, au sein d'une seule et même interface. Cette plateforme rassemble la technologie propriétaire spécifique de chacun : Sekoia (détection des menaces), Vade (filtrage des emails), Harfanglab (protection des postes de travail), Gatewatcher (sondes réseaux), Glimps (analyse des malwares), et Pradeo (protection des mobiles).

Le 11 janvier 2022, l'ANSSI a procédé au lancement d'un « *programme d'incubation pour accompagner un développement accéléré* » de création de 7 centres régionaux de réponse aux incidents cyber (CSIRT), censés « *soutenir le tissu économique et social de chaque territoire face aux cybermenaces* ».

Dès février 2022, les CSIRT de Bourgogne Franche-Comté, du Centre Val de Loire, de Corse, du Grand Est, de Normandie, de Nouvelle Aquitaine et du Sud-Provence Alpes Côte d'Azur participeront à ce programme d'incubation mis en place par l'ANSSI, qui leur alloue une subvention « *à hauteur d'un million d'euros à chaque région volontaire* ». Ils « *travailleront au service des entreprises, collectivités et associations locales pour les sensibiliser et les former aux bonnes pratiques cyber, réceptionner leurs signalements d'incident et les qualifier, mettre en relation les victimes avec les structures adaptées pour les accompagner dans la résolution de l'incident* ». Une deuxième session sera organisée de septembre à décembre 2022. L'objectif est que toutes les régions volontaires puissent disposer dès 2022 d'un tel centre, « *dont les capacités opérationnelles seront pleinement atteintes à l'horizon 2024* ». À terme, l'objectif est la mise en réseau des CSIRT régionaux au sein de l'InterCERT France – le réseau français des CSIRT – afin de créer en son sein un groupe de coopération et de partage dédié à leurs enjeux territoriaux.[200]

La coopération franco-allemande est elle aussi mobilisée dans cette lutte.

---

[199] GCS e-santé Bretagne **:** le démonstrateur portera sur les fuites de données de santé. Il visera le développement d'une solution de marquage des données aux différents stades de leurs traitements.
CHU de Caen **:** le démonstrateur portera sur la sécurisation des objets connectés servant aux soins à domicile. Il visera la conception d'une couche de sécurité entre des objets connectés de santé et un centre hospitalier.
CHRU de Nancy **:** le démonstrateur proposera une réponse aux failles présentes dans les nombreux équipements biomédicaux présents dans les hôpitaux. Il sera un système auto-apprenant basé sur de l'intelligence artificielle qui automatisera l'analyse des données et le traitement des incidents.
GCS Ametis **:** le démonstrateur centralisera les outils de sécurisation des établissements de santé. Il rassemblera dans un même dispositif la gestion des identités, de la surveillance cyber ainsi que des services supplémentaires tels que des audits de sécurité.
Haropa Port **:** le démonstrateur proposera un outil centralisant la sécurisation des multiples systèmes informatiques présents dans les ports de commerce. Le développement du démonstrateur comprendra une cartographie exhaustive des flux et des interconnexions ainsi que la mise en place d'un SOC maritime (*Security Operation Center*).
La Région Bretagne **:** le démonstrateur proposera un outil rassemblant les commandes et instruments nécessaires au pilotage de la cybersécurité pour les collectivités territoriales. Le démonstrateur centralisera la supervision, les simulations d'attaques et la sécurisation des accès critiques.

[200] Voir son communiqué de presse : https://www.ssi.gouv.fr/uploads/2022/01/anssi-communique_presse-csirt_regions.pdf

En novembre 2021, l'ANSSI et son équivalent allemand, le BSI, ont publié leur quatrième rapport commun[201], centré sur les rançongiciels. Entre 2019 et 2020, les deux organismes ont remarqué que le nombre d'attaques impliquant un rançongiciel a augmenté de 255 %. Le rapport indique que *« certaines attaques par rançongiciel ne peuvent plus être reléguées au rang de simples attaques à but lucratif »*. Même si les groupes derrières ces attaques n'hésitent pas à revendre les données qu'ils ont réussi à récupérer, *« la sophistication des attaques, leur impact sur les données sensibles de la victime et la perte de continuité des activités les élèvent au niveau des attaques traditionnellement associées à des groupes d'attaquants étatiques »*.

« *Ce qui fait notre force, c'est notre capacité à travailler ensemble. C'est notre seule chance de gagner contre les attaquants »*, explique Guillaume Poupard qui appelle la France à ne pas oublier les acteurs européens du *cloud* au profit des GAFAM, et à profiter de la présidence française du Conseil de l'UE, au premier semestre 2022, pour définir *« l'Europe de la cyber »*, étendre la portée de la directive NIS et créer des *« pompiers cyber européens »* capables d'intervenir partout.

La cybercriminalité se jouant des frontières, la coopération internationale est un impératif absolu pour s'y attaquer.

Habituellement, Moscou refusait de collaborer avec les pouvoirs étrangers, et la Russie était perçue comme un refuge pour certains réseaux cybercriminels. Le 14 janvier 2022, le renseignement russe a organisé l'arrestation sur son territoire de 14 cybercriminels soupçonnés de faire partie du célèbre gang cybercriminel REvil. Fait rarissime, cette opération policière fait suite à un appel des autorités américaines. Si ce genre de collaboration se reproduisait, ce serait un changement de fond dans la lutte contre la cybercriminalité.

Ces dernières années, les Etats ont renforcé de manière totalement transparente leurs capacités de cyberdéfense et de cyberguerre, indiquant par là-mêmes aux autres puissances, voisines ou non, qu'ils ont les moyens de riposter, si besoin en était. La France s'est, par exemple, dotée en 2019 d'une doctrine militaire offensive dans le cyberespace (LIO) tout en renforçant sa politique de Lutte informatique défensive (LID).

- *L'assurabilité des entreprises face au risque cyber constitue un dossier complexe*

Mais il demeure un registre laissé vierge dans ce paysage : celui de l'assurabilité des entreprises face au risque cyber, sujet que la délégation sénatoriale aux entreprises (DES) prend très au sérieux, comme le confirme Serge Babary, son président, qui a déclaré lors de la table ronde de la DSE du 25 novembre 2021 que : « *Le cyber risque et son assurabilité constituent un sujet majeur pour les entreprises mais aussi les collectivités territoriales. Nous devons réagir rapidement ! Le Sénat attend du groupe de travail lancé par le ministère des finances sur la cybersécurité des propositions structurelles concertées, y compris sur la question des rançons* ».

Stéphane Blanc, président fondateur d'Antemeta, déplore le désengagement des milieux de l'assurance : « *Face à un risque systémique, les assureurs se désengagent des cyber-risques. Et quand ils s'y engagent, c'est sans assurer les rançongiciels. Or, depuis 4-5 ans, nous assistons à une évolution multifactorielle des cyber-risques et à des attaques non plus individuelles, mais organisées parfois par des états dans le cadre d'une guerre économique mondiale. Nous ne sommes donc pas organisés pour mener une défense, voir une contre-attaque* ».

Christophe Delcamp, directeur adjoint au pôle Assurances de dommages et responsabilité de la Fédération Française de l'Assurance (FFA) partage ce constat **:** « *La FFA est bien consciente*

[201] *Fourth edition of the Franco-German Common Situational Picture :* https://www.ssi.gouv.fr/uploads/2021/11/anssi_bsi_csp_2021.pdf

des risques liés à la digitalisation de l'économie et des processus des entreprises. Ces cyber-risques peuvent d'ailleurs générer des dommages sans commune mesure avec ce que nous avons pu connaître par le passé lors des précédentes révolutions industrielles. C'est là que réside l'une des difficultés pour les assureurs qui veulent accompagner correctement les entreprises ». Il remarque également que le marché de la cyber assurance est insuffisamment mature, tant du côté des offres des assureurs, que des entreprises dans ce domaine.

Selon la FFA, le poids du marché de la cyber assurance n'est que 135 M€ en primes, soit seulement 0,225 % des 60 Md€ de l'assurance non-vie en France. « *Aux Etats-Unis, le même ratio est lui de 0,56% pour 4 Md$ de primes. C'est faible certes, mais je constate une véritable dynamique car ce marché progresse de 29 % tant en France qu'aux Etats-Unis* ».

Mais il rassure en assurant que les membres de la FFA clarifient leurs offres de cyber assurance, « *démarche qui est en cours depuis 2020 et qui sera finalisée en 2022* ».

- *Le chiffrement des communications ne constitue plus la panacée*

Le chiffrement des communications posant un problème dans la collecte de preuves pour démanteler des réseaux terroristes, le Conseil des ministres de l'UE justifie le recours au chiffrement en ces termes : *« L'Union européenne soutient pleinement le développement, la mise en œuvre et l'utilisation d'un cryptage fort. Le cryptage est un moyen nécessaire pour protéger les droits fondamentaux et la sécurité numérique des gouvernements, des industries et des sociétés. Dans le même temps, l'Union européenne doit garantir la capacité des autorités compétentes dans le domaine de la sécurité et de la justice pénale, par exemple le droit des autorités répressives et judiciaires à exercer leurs pouvoirs légaux, en ligne et hors ligne. »* Tout en précisant que si les autorités sont légalement en mesure de récupérer des données, ces dernières ne sont pas lisibles.

L'informatique quantique pourrait venir bouleverser la physionomie de la sécurisation des communications et des informations sur des canaux comme Internet[202]. L'utilisation des mécanismes de sécurité y est permanente, qu'il s'agisse d'opérations bancaires, de communications cellulaires ou d'objets connectés. Or l'informatique quantique pourrait être capable de réduire à néant les outils de sécurité actuellement en place, comme l'utilisation de clés RSA fonctionnant sur la base d'algorithmes de cryptographie asymétrique.

Selon le magazine *Business Insider*, Divesh Aggarwal, chercheur à l'Université nationale de Singapour, a prédit en 2017 que les ordinateurs quantiques seraient sur le point de casser la cryptographie des crypto-monnaies, *« dans une décennie »*. Un autre scientifique, Jian-Wei Pan, créateur d'un ordinateur quantique de 66 qubits, a déclaré dans *El Confidencial* qu'il reste à peine 3 ou 4 ans pour que cette prédiction se réalise. L'une des premières applications militaires serait *« de casser le chiffrement des communications »*, note le département américain du Commerce.

À l'heure actuelle, aucune machine n'est capable de casser les clés de chiffrement les plus sophistiquées, mais un ordinateur quantique pourrait le faire en quelques minutes. Et c'est un danger qui est déjà d'actualité.

Selon un spécialiste tchèque de ces questions, Michal Křelina : *« Certaines communications secrètes concernent des informations qui seront encore valables dans 10 à 15 ans. Il suffit donc*

[202] Capable d'effectuer des calculs irréalisables avec les machines d'aujourd'hui, l'ordinateur quantique pourrait révolutionner toutes les industries. Mais cette machine n'existe aujourd'hui qu'à l'état embryonnaire, et ses capacités potentielles restent théoriques. A l'heure actuelle, les scientifiques ne s'accordent même pas sur la méthode d'ingénierie pour produire le phénomène nécessaire au fonctionnement de l'ordinateur quantique, le fameux qubit. IBM et Google misent par exemple sur les circuits supraconducteurs, Microsoft sur les fermions de Majorana, IonQ et Honeywell sur les ions piégés, tandis que le CEA tente sa chance avec des spins d'électrons dans le silicium. Autrement dit, plusieurs ordinateurs quantiques, bâtis différemment, pourraient voir le jour, tout comme ils ne pourraient jamais atteindre le potentiel espéré.

que des espions les volent aujourd'hui et attendent que la technologie quantique soit mature pour découvrir ces secrets ».

D'où l'importance de trouver des contre-mesures. La plus avancée est l'envoi de clés de déchiffrement quantique. Autrement dit, le message secret est transmis en utilisant les voies traditionnelles de communication, mais la clé qui permettra de le rendre lisible est envoyée via un réseau quantique qui – sans entrer dans les détails techniques – est censé être impossible à pirater. La Chine a déjà prouvé que c'était faisable, en 2016, en *« sécurisant ainsi les transmissions lors d'une conférence réunissant des personnes à Pékin et à Vienne »,* rappelle l'Otan, dans un billet de blog consacré aux technologies quantiques.

La cryptographie et la cryptanalyse n'ont donc pas le choix et ce n'est qu'une question de temps : elles doivent d'ores et déjà se préparer à l'avenir.[203]

- *La « compliance » est perçue comme un cheval de Troie juridique*

Dans la guerre du droit, la *« compliance »* (en français : la conformité juridique) est parfois perçue comme un nouveau cheval de Troie qui menace les entreprises.

Catherine Delhaye, qui préside le Cercle de la compliance, offre une définition très complète de cette démarche, tout en en explicitant les différents enjeux : *« A partir des années 2000, dans la mouvance du Global compact des Nations Unies et des pratiques anglosaxonnes, nombre d'entreprises françaises se sont emparées de l'éthique des affaires. Elles ont établi des principes, décliné de grandes valeurs, vanté leur intégrité, pris des engagements sociaux et sociétaux très forts. Elles les ont souvent matérialisés dans des codes, des chartes exprimant leur vision d'un monde des affaires vertueux et constituant au bout du compte, une forme de constitution de l'entreprise, de socle commun auquel les collaborateurs et les partenaires, prestataires et autres fournisseurs doivent adhérer comme on adhère à un contrat, à défaut d'y croire. Mais à la différence d'un contrat, un code d'éthique est le plus souvent générique, conceptuel ; il permet de comprendre la direction ou l'orientation de l'entreprise en terme d'intégrité. En revanche, faute d'instructions précises, d'indications spécifiques, il est rarement suffisamment détaillé pour permettre en pratique aux collaborateurs de se conformer à des réglementations strictes, avec le niveau d'orthodoxie attendu par les régulateurs.*

La prévention de la corruption, le respect des règles antitrust, le contrôle à l'exportation et maintenant la protection des données personnelles peuvent certainement s'inspirer de telles lignes directrices ; mais au-delà des principes, ils ont besoin de règles, d'explications, de contrôles, de sanctions, en d'autres termes : de conformité ou compliance, c'est-à-dire de cette méthodologie qui permet de transformer des valeurs éthiques, des principes d'intégrité et une volonté de bien faire, en règles explicites, en actions de prévention tangibles et en résultats.

Qu'elle que soit son origine - américaine, anglaise, brésilienne ou désormais française -, cette démarche met en effet en œuvre les mêmes étapes, les mêmes leviers, les mêmes exigences et

[203] Selon la Quadrature du Net : *« Si les clés RSA sont réputées actuellement pour leur robustesse, elles vont être largement remises en cause par l'informatique quantique. Ces clés RSA ont un rôle essentiel dans la sécurisation des systèmes d'information. Avec les ordinateurs quantiques, une cyberattaque viendrait compromettre l'ensemble de l'infrastructure et rendre de nombreuses informations confidentielles visibles, telles que des données bancaires, des dossiers médicaux ou encore des éléments de propriété intellectuelle. Même constat au niveau des solutions de signatures électroniques, de plus en plus utilisées dans notre vie quotidienne, des actions d'authentification de courriels et de documents .... Les gros émetteurs de clés via des certificats devront donc disposer des outils nécessaires pour lutter contre les attaques quantiques. Dans ce contexte, il est nécessaire de mettre au point une approche de la cryptographie post-quantique, capable de résister aux attaques de ces ordinateurs dont le fonctionnement est fondamentalement différent de celui des ordinateurs actuels. Il faut pour cela créer un prototype de certificat "quantique résistant. … Pour faire face à la menace que représente l'ordinateur quantique, l'ANSSI invite à assurer la transition vers la cryptographique post-quantique à l'aide de mécanismes hybrides et à des certificats hybrides post-quantiques sécurisés. L'ANSSI préconise ainsi de conjuguer des algorithmes cryptographiques pré et post-quantiques dans ce type de mécanismes hybrides, conçus pour être résistants non seulement aux ordinateurs classiques, mais aussi aux ordinateurs ayant atteint la suprématie quantique. Ces mécanismes pourront ainsi être déployés sans changement dans une infrastructure de réseaux numériques, indépendamment du canal de communication. »*

contraintes : Un engagement formel, affirmé de la direction générale à faire des affaires de manière intègre ; un code d'éthique bien sûr mais aussi des politiques précises, des instructions claires, des formations, l'implication du management, des systèmes d'alertes et de prévention, des contrôles internes, des audits et une démarche continue de progrès.

[…] Mettre en place un dispositif de conformité ou Compliance, c'est bien sûr répondre à des obligations légales, en particulier pour les entreprises qui opèrent à l'étranger :

• en vertu de lois qui imposent la mise en oeuvre de programmes de prévention du risque (la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite Loi Sapin II, le UK Bribery Act, les lois canadienne, brésilienne… contre la corruption, au niveau européen, le Règlement Général de Protection des Données, etc) et sanctionnent l'absence de programmes ou l'insuffisance des dispositifs mis en place ou des moyens alloués par l'entreprise,

• en vertu de lois sur la protection des droits de l'homme telles que la loi française sur le devoir de vigilance, le UK Slavery act, la loi californienne qui là encore exigent la mise en place de mesures particulières de prévention,

• en vertu de réglementation qui imposent aux commissaires aux comptes une obligation de vérification des politiques anti-corruption ou environnementales de leurs clients,

• en vertu de directives récentes qui imposent un reporting détaillé et mesuré sur le domaine extra financier dans les documents de référence.

S'engager dans la compliance, c'est une démarche de gestion de risques :

• c'est identifier les risques juridiques et règlementaires de l'entreprise au moyen d'une cartographie destinée à les détecter, évaluer et réduire par des programmes et plans d'action adaptés,

• c'est prévenir et combattre certains risques, (Anticorruption, antitrust, export contrôle, protection des données personnelles) au moyen de programmes précis, ciblés, évalués,

• c'est mettre à jour cette cartographie en fonction des risques effectivement rencontrés, faire évoluer les plans d'action correspondants et mettre à jour les programmes de compliance pour qu'ils soient toujours adaptés à la réalité opérationnelle de l'entreprise,

• c'est porter une attention particulière aux entreprises nouvellement acquises, à leur culture et aux pratiques de leurs collaborateurs.

[…] C'est aussi un défi managérial, en particulier pour les multinationales qui emploient des milliers de personnes réunissant des dizaines nationalités, de multiples culture et religions, avec des convictions, des sensibilités, des pratiques et des niveaux de maîtrise de ces risques très différents :

• compte tenu des traditions tenaces dans certaines régions du monde ou dans certains secteurs d'activité,

• compte tenu des pratiques de concurrents moins scrupuleux,

• compte tenu de l'écart entre la véritable corruption (avantages accordés en contrepartie et dans l'attente d'une décision ou d'un bénéfice) et ce que les collaborateurs et en particulier les commerciaux perçoivent encore comme un simple geste de convivialité, traditionnel et nécessaire dans les relations d'affaires,

• compte tenu des difficultés desdits commerciaux à comprendre ou admettre qu'un dîner soigné ou un événement festif dont l'opportunité et la licéité sont désormais contestables, sont à bannir quand bien même elles ne seraient pas illicites,

• compte tenu de la créativité et de l'imagination des corrompus ou corrupteurs jamais à court d'idées, qui obligent à une vigilance de tous les instants pour un management de risque efficace. »[204]

La loi Sapin 2 a en outre créé l'Agence française anticorruption (AFA) placée sous l'autorité du ministère de la Justice et du ministère du Budget. Elle a pour rôle d'accompagner les entreprises dans la mise en place d'un plan de prévention contre la corruption, notamment par le développement de la cartographie des risques et du contrôle des liens que l'entreprise peut avoir avec les fournisseurs, les sous-traitants et les clients.

En visant à développer l'un des meilleurs standards européens et internationaux en matière de lutte contre la corruption, cette loi constitue aussi une réponse au problème de l'extraterritorialité des normes anticorruption, en particulier américaines (établies par le *Foreign Corrupt Pratices Act* ou *FCPA*, de 1977), qui s'appliquent au-delà de la compétence territoriale de l'État français.

Or force est de déplorer que la *« compliance »* peut aussi concourir à ouvrir des perspectives bien moins positives.

Comme le souligne Brigitte Pereira, professeur de droit du travail, droit pénal des affaires et droit des contrats, la loi Sapin n'a pas écarté tous les risques.[205]

La possibilité d'un espionnage légal *via* les règles de conformité juridique imposées aux entreprises du secteur de la défense par les dispositions de la loi Sapin II inquiète les services de renseignement et le ministère français des Armées, qui met en garde contre le risque d'un *« désarmement par le droit ».*

Dans une note relative aux difficultés que rencontrent aujourd'hui les entreprises de défense françaises dans leur recherche de financements bancaires, un des groupements professionnels de ce secteur, le GICAT *(Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres),* dénonce : « *Depuis maintenant deux ans, notre industrie de défense est confrontée à un problème croissant : le système bancaire et financier français est de plus en plus réticent à accompagner nos entreprises du secteur de la défense tant pour leur développement qu'en soutien à l'exportation ».*

Les refus de financement des banques françaises se multiplient, les témoignages désespérés, notamment des PME ou start-up de la filière défense, aussi. Clairement les banques, dont BNP Paribas et Société Générale (deux organismes bancaires qui furent condamnés par la Justice américaine en vertu de l'extraterritorialité du droit américain), jouent de moins en moins le jeu pour financer et/ou accompagner une industrie souveraine qui reste pourtant soutenue par l'État français. Les refus de financement se décident principalement dans les bureaux discrets des équipes de juristes et d'avocats (compliance et éthique) devenues très puissantes au sein des directions des banques françaises.

"Les organismes bancaires décident de manière discrétionnaire de critères de compliance très poussés, se basant sur les analyses et recommandations de prestataires privés dont il n'est pas précisé le nom ou la nationalité", regrette l'organisation professionnelle.

Au-delà de ces difficultés financières, le respect scrupuleux des règles attachées à la compliance fait courir un autre risque à ces entreprises. Des algorithmes dédiés apparaissent

[204] *La compliance, plus qu'une défense - De l'éthique à la compliance :* *https://www.lecercledelacompliance.com/wp-content/uploads/2019/05/JMJ-69-compliance.pdf*
[205] *L'Agence française anticorruption, une réponse aux normes extraterritoriales américaines :* https://theconversation.com/lagence-francaise-anticorruption-une-reponse-aux-normes-extraterritoriales-americaines-166059

pour explorer les contenus des systèmes informatiques et y détecter d'éventuels codes sous licence utilisés de manière illicite. L'enjeu n'est pas mince : les règles de propriété intellectuelle pourraient conduire les entreprises « négligentes » à devoir dévoiler à un concurrent « floué » l'ensemble de leur programme informatique et donc certaines données potentiellement stratégiques.

Il y a bien un là un sujet suffisamment préoccupant pour que le Parlement s'en soit saisi.

- *Le monopole de fait que l'Etat – comme l'UE – a décidé de réserver à la dématérialisation des relations que les administrés devront entretenir avec ses services introduit une source supplémentaire de vulnérabilité de nature stratégique auquel il n'est pas en mesure de faire face.*

La panne géante qui a touché le 4 octobre 2021 Facebook et ses services associés (Instagram, WhatsApp et Messenger) [206, 207], met en évidence la dépendance de la France, et plus globalement, de l'UE, à ces plateformes numériques qui transforment entièrement notre quotidien.

Héberger toutes les applications sur Google, Apple, Amazon, Facebook ou Microsoft s'avère être problématique quant à l'accès et la protection des informations.

« *Le développement de l'Internet a souvent été étudié comme un phénomène déstabilisant les modes d'organisation bureaucratique et d'intervention des États : l'infrastructure décentrée du net permet en effet le contournement des législations nationales et la régulation technique opérée par le code informatique favorise l'intervention d'experts pour la gouvernance du réseau*. » (Anne Bellon[208,209])

Tom Burt, Vice-président chargé de la sécurité au sein de Microsoft, déclarait le 30 juin 2021 devant la commission judiciaire de la Chambre des représentants, qu'un tiers des demandes d'accès aux données sollicitées par le gouvernement des Etats-Unis sont accompagnées d'une ordonnance de confidentialité et que, par conséquent, le client final ainsi visé par ces consultation « discrétionnaires » des données n'est évidemment pas informé.

« Notre siècle est celui de tous les dangers comme celui de toutes les opportunités. La France est à un carrefour de son existence où ses choix stratégiques conditionneront son avenir, sa place dans l'échiquier mondial et la survie de notre modèle d'existence collective […] Jusqu'à présent, notre Nation, oscillant entre ignorance, compromission délibérée et naïveté confondante, a été la mère nourricière de puissances étrangères en matière de captation et de traitement de nos données stratégiques et souveraines. La circulaire du Directeur interministériel du numérique, en date du 15 septembre 2021, demandant aux administrations françaises de ne plus migrer vers la suite bureautique de Microsoft hébergée dans le cloud Microsoft 365, est-elle le marqueur tardif d'une prise de conscience réelle sur l'impérieuse nécessité de construire une politique de protection des données stratégiques de la Nation, ce fameux « or noir » du XXIème siècle ? » (Aurélie Luttrin et Franck DeCloquement)

[206] *Cf.* Tim Green *in Panne de Facebook : une succession d'événements malheureux* : https://www.lemondeinformatique.fr/actualites/lire-panne-de-facebook-une-succession-d-evenements-malheureux-84396.html

[207] *Cf.* François Jolain *in Facebook : un bug révélateur des fragilités d'Internet :* https://www.contrepoints.org/2021/10/08/407962-facebook-un-bug-revelateur-des-fragilites-dInternet

[208] *Des utopies du net aux startups administratives, la place des acteurs publics dans la révolution numérique :* http://regards-citoyens.over-blog.com/2019/09/des-utopies-du-net-aux-startups-administratives-la-place-des-acteurs-publics-dans-la-revolution-numerique.html

[209] *Des outils numériques pour améliorer le fonctionnement de l'Etat : solutions ou problèmes ?* : https://journals.openedition.org/pyramides/989

Un collectif d'acteurs européens du numérique, de l'entreprise, du syndicalisme et des collectivités locales plaide en faveur de l'interopérabilité des données, afin de briser le monopole des géants du numérique : « *Les solutions existent pour construire un Web décentralisé et démocratique dans le monde de l'après-Covid-19* ».

Or, le choix pris délibérément tant en Europe que plus spécifiquement en France de s'en remettre aux principaux acteurs américains du numérique (à l'exception de quelques rares niches où Bull a paru un temps en capacité d'offrir les garanties nécessaires) pour disposer des ressources numériques requises en pareilles domaines participent à rendre totalement illusoire une telle ambition tant que la question de la souveraineté numérique - désormais largement abordée en France comme dans certains autres milieux européens - ne trouvera pas de réponses effectives appropriées.

A l'été 2021, après une enquête de 16 mois et la collecte de plus de 1,2 millions de documents, les 13 députés de la commission antitrust de la Chambre des représentants des Etats-Unis ont préconisé une condamnation sans précédent des GAFAM dans un rapport sur leurs pratiques anticoncurrentielles (démantèlement, interdiction de donner la préférence à leurs propres produits, présomption de refus pour les futurs rachats de start-up, non-respect des lois anti-trust[210]…).

En France, un rapport sénatorial établi au nom de la commission d'enquête sur la souveraineté numérique, a également appelé formellement la France et, plus généralement l'UE, à faire ces mêmes pratiques anticoncurrentielles des GAFAM, tout en soulignant que la solution de leur démantèlement était insuffisante et qu'une modification appropriée du droit de la concurrence s'imposait. [211] Le non-respect par Google d'injonctions prononcées à son encontre par l'Autorité de la Concurrence illustre l'impuissance de l'Etat à faire prévaloir le droit.[212]

Ce qui pourrait valoir pour les Big Tech américaines vaudrait nécessairement aussi pour les BATX, leurs équivalents chinois.

Mais ces préconisations interrogent elles-aussi dans la mesure où elles battent en brèche un certain nombre de principes fondamentaux de la vie démocratique en même temps qu'elles mettent quelque peu à mal les principes mêmes d'une économie de marché qui constitue elle-aussi un élément fondamental de nos démocraties libérales.

« Ce n'est pas à dire que le marché n'a besoin d'aucune institution, aucun mécanisme de régulation ou aucune surveillance. C'est précisément parce que le droit est si nécessaire au fonctionnement sain de la vie économique qu'il doit être utilisé avec la plus grande prudence. Friedrich A. Hayek identifiait trois critères pour juger du bien-fondé des lois encadrant la concurrence. Elles devraient être abstraites (c'est-à-dire qu'elles posent des principes sur ce qui est interdit plutôt que d'établir une liste de ce qui demeure autorisé), générales (ne viser aucune entreprise en particulier), et certaines (soit relativement stables dans le temps, afin de ne pas changer les règles du jeu en cours de route et perturber les plans des entrepreneurs). Les appels incessants à l'adoption de lois toujours plus nombreuses, toujours plus larges, pour s'en prendre à quelques entreprises identifiées sur des critères arbitraires et à qui l'on reproche de faire plutôt que de chercher systématiquement dans le maquis règlementaire une bonne

[210] Dans le cadre de leur accord 'secret' Jedi Blue, *Google & Facebook* ont travaillé ensemble pour améliorer la capacité de Facebook à reconnaître les internautes sur des navigateurs bloquant les cookies, sur des terminaux Apple et sur le navigateur Safari. En cela, elles ont miné les efforts d'une société Big Tech *[Apple]* pour se démarquer en protégeant mieux la vie privée.

[211] *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique :* http://www.senat.fr/rap/r19-007-1/r19-007-11.pdf

[212] Voir notamment à cet égard les termes du contentieux qui oppose en France l'Autorité de la Concurrence à Google à propos de la rémunération des droits voisins des éditeurs et agences de presse : https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/remuneration-des-droits-voisins-lautorite-sanctionne-google-hauteur-de-500

raison de ne pas faire va à l'encontre de ces trois principes et risque fort, sous couvert de bonnes intentions et même avec une relative bonne foi, de nous emmener toujours plus loin sur la route de la servitude. » (Pierre Schweitzer[213])

Pour le sociologue Patrick Singolani, *« l'une des tâches politiques qui s'ouvre à nous consiste à réfléchir à leur possible collectivisation, car, si elles participent d'un capitalisme avide de données, elles ont aussi ouvert des espaces de sociabilité et de créativité inimaginables jusque-là. »*[214]

Mais comme l'affirme Eric Sadin : *« la seule dénonciation des géants du numérique nous défausse de notre part de responsabilité ».*

Choisir l'option d'un non-alignement stratégique sur des tiers non européens en matière d'appropriation, de gestion et de protection des données numériques sensibles – comme celles évoquées ici - impose de disposer en pleine souveraineté des capacités technologiques et opérationnelles appropriées.

Encore faudrait-il que l'Etat français ne joue pas un double jeu en poursuivant ses initiatives permettant aux acteurs technologiques américains, et partant aux agences étatiques américaines intervenant dans le dispositif stratégique des Etats-Unis, de garder les clés de notre souveraineté.

Est-il cohérent de la part de l'Etat, alors que le gouvernement soutient l'idée de reconquête de la souveraineté numérique européenne[215], d'imposer à ses administrations de recourir à Qwant, le moteur de recherche censé concurrencer Google, alors qu'il fonctionne grâce à l'américain Microsoft et qu'il est mis en cause dans un rapport de la DINUM ? Est-il cohérent qu'il permette à In-Q-Tel, le fonds d'investissement de l'Agence centrale de renseignement, la CIA, de prendre une participation au capital d'une start-up française, Prophesee[216] ? Est-il cohérent qu'il permette à la Commission européenne de mettre sur pied la signature d'un accord commercial hors Traités de l'Union sur la brevetabilité des logiciels, une manoeuvre qui interdit aux Parlements européen et national un droit de regard et d'avis sur le texte et va mettre à mal, si ce n'est anéantir, nos pépites nationales[217] ?

Est-il cohérent de la part de l'Etat de favoriser la pénétration des sociétés américaines dans l'univers national de l'enseignement supérieur et la recherche ?

A la suite de l'arrêt *Schrems II*, la CNIL a été saisie par la Conférence des présidents d'université et la Conférence des grandes écoles sur l'utilisation des *« suites collaboratives pour l'éducation »* proposées par des sociétés américaines.

Compte tenu du risque d'accès illégal aux données, la CNIL appelle à des évolutions dans l'emploi de ces outils et accompagnera les organismes concernés pour identifier les alternatives possibles[218].

---

[213] *Faut-il réguler les grandes plateformes numériques ?* https://www.libinst.ch/publications/IL-Schweitzer-GAFA.pdf

[214] *Cf. Critique du quotidien numérique :* https://aoc.media/analyse/2021/10/06/critique-du-quotidien-numerique/

[215] *Cf.* https://www.zdnet.fr/actualites/penser-la-souverainete-numerique-pour-une-autonomie-strategique-39912845.htm

[216] *Cf.* Romain Mielcarek *in Défense et sécurité : faut-il s'inquiéter des appétits américains pour les start-up stratégiques françaises ?* https://major.com/media/760-defense-securite-appetits-americains-startup-strategiques-francaises?fbclid=IwAR1tzsbS8AHk7DQb9NiPGlFDGkFOvtp5FtdOn8YeMIpT8osYKnMrFk0gWI0

[217] Voir par exemple à ce sujet *By-pass » par les GAFAM de la législation européenne sur les brevets logiciels - Question écrite de M. Philippe Latombe :* https://philippe-latombe.smartrezo.com/article-by-pass-par-les-gafam-de-la-legislation-europeenne-s.html?id=25770&fbclid=IwAR3ZQuPFoT259-Qrl_vahsotrCDCtQrXdiYHR8dboD5ZxR_4DCxUQx9SjMQ

[218] *La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs étatsuniens pour l'enseignement supérieur et la recherche :* https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche?fbclid=IwAR0xaD79Vda5AHNksYhPLy1Kx4x2G1lrzv42q7bTVeiIGXJPkgA4g1Xv3UM

77

Est-il cohérent que la société française de prise de rendez-vous médicaux Doctolib confie les données de santé à Amazon, avec le feu vert du Conseil d'Etat ?

Le développement éclair de Doctolib et sa position de « quasi-monopole » sur le marché des rendez-vous médicaux pose question alors qu'il existe pourtant des concurrents, tels que Maiia, KelDoc, Allodocteur ou Vitodoc. *« Il s'agit d'une activité de santé, sensible en matière de données. La sécurisation de ces données au niveau du stockage et de leur circulation relève elle aussi du service public »*, souligne Frédéric Bizard, qui estime que la France se trouve actuellement *« dans une zone de flou »*. Un avis partagé par plusieurs associations de médecins et de patients qui ont saisi le Conseil d'État en mars. Ils reprochaient à Doctolib d'héberger ses données sur le cloud d'Amazon, soumis en tant qu'entreprise américaine à l'autorité des services de renseignements américains (et craignaient de voir ces informations sensibles utilisées par les États-Unis). Mais le Conseil d'État a donné raison à l'entreprise française, rappelant – bien innocemment … - qu'elle a signé un avenant avec Amazon, comprenant une procédure précise en cas de demande d'accès par une autorité publique. Pour protéger ses données, Doctolib promet aussi avoir mis en place une procédure de chiffrement (ce qui ne résoud d'ailleurs en aucune manière la question soulevée).

Est-il cohérent que la Banque publique d'investissement ait choisi de confier la gestion des données des entreprises bénéficiant des prêts Covid garantis par l'Etat à *Amazon Web Services*, et ce sans que cette opération ait donné lieu à un appel d'offres, ni à une consultation des prestataires français ou européens tels qu'*OVHcloud*, *Scaleway* ou *Rapidspace* ?

Or, pour pouvoir répondre aux exigences techniques et juridiques posées en mai 2021 par l'État français pour la protection maximale des données sensibles des administrations et des entreprises françaises, *Google Cloud* a choisi de s'allier avec Thales, après que Orange, Capgemini et Microsoft se soient alliés pour la mise en place en France d'un *cloud* souverain, que la 'nouvelle stratégie nationale pour le cloud' entend rendre commun à l'ensemble de l'administration française, en lieu et place de solutions ministérielles harmonisées.

Un tel projet soulève naturellement de nombreuses difficultés alors même que le ministère des Armées français a décidé de faire de l'informatique en nuage – ou *cloud computing* – l'un des piliers de sa transformation numérique. [219]

Bien que *Palantir*, une entreprise américaine de *big data* qui a des liens étroits avec les services américains de renseignement, ait été liée à plusieurs dossiers sulfureux (comme *Cambridge Analytica*, qui porte sur des tentatives de manipulation des réseaux sociaux), la DGSI, qui regroupe les services de renseignement intérieur français, a signé avec l'entreprise américaine un contrat en 2016, pour s'en émanciper en 2018 puis le renouveler en 2019.

Par ailleurs, *Palantir Technologies* propose depuis décembre 2021 aux 1000 jeunes pousses françaises « *Foundry for Builders, un programme permettant aux start-ups de souscrire à Palantir Foundry sur un modèle d'abonnement* ». Ce service en ligne met la puissance d'analyse du *big data* à la portée des PME françaises les plus prometteuses.

L'industrie française devrait-elle s'inquiéter ou se réjouir de l'arrivée au sein de la Station F – la pépinière parisienne de start-ups – d'une telle société ?

Dispose-t-on aujourd'hui d'un concurrent français de *Palantir* ?

[219] *Cf.* Clotilde Bômont in *Le cloud défense : défi opérationnel, impératif stratégique et enjeu de souveraineté (IFRI / Focus stratégique, n° 107, novembre 2021)*
https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/cloud-defense-defi-operationnel-imperatif-0

D'après Pascal Jouary, journaliste et auteur du livre '*Secret Défense : Le livre noir'*, ce n'est pas d'actualité : *« Il y avait le projet d'intelligence artificielle Athéa*[220]*, développé par Thales et Atos. D'après les spécialistes, on n'est pas sûr qu'il aboutira ou alors qu'il arrivera au niveau de Palantir. On peut aussi se demander pour quoi faire puisque, comme l'on est sous commandement américain dans l'Otan, quel est le problème d'utiliser un logiciel américain ? Mais on y perd de notre souveraineté. »*

De tels rapprochements interrogent [221] au moment même où ces mêmes entreprises technologiques nationales de premier plan prennent une place centrale dans les processus d'élaboration de notre identité et de notre sécurité numériques comme en témoigne notamment cet article posté sur le blog officiel de Thalès évoqué *supra.*

Or, il est difficile d'imaginer que de tels agissements n'aient pas été validés par les tutelles étatiques respectives, et eu égard à la nature stratégique des enjeux associés, par la présidence de la République, en dépit des efforts déployés par le ministère en charge de l'Economie malgré ses positions rassurantes en 2020 sur la question de la souveraineté ; en particulier celles portées par Thomas Courbe, directeur général des entreprises et commissaire à l'information stratégique et à la sécurité économiques, lors d'un colloque organisé par le MEDEF sur le thème *« Souveraineté et compétitivité des entreprises : plus de temps à perdre ! »* - à l'initiative du comité 'souveraineté et sécurité économiques des entreprises' du MEDEF, au cours duquel il a présenté les instruments et moyens, notamment financiers, que la France et l'Europe doivent mettre en place pour préserver leur autonomie et la compétitivité de leurs entreprises.[222]

Le 18 novembre 2021, à Fort Meade, au sud de Baltimore, où est situé le siège de la toute puissante *National Security Agency* (*NSA*) et de l'*US Cyber Command*, les maîtres espions américains et britanniques du cyberespace ont profité de leur dernier forum annuel pour marquer les esprits, en annonçant mettre en commun leurs forces afin de mieux « *dissuader* » quiconque de s'en prendre à leurs intérêts vitaux.

« *Nous convenons que l'engagement stratégique dans le cyberespace est crucial pour défendre notre mode de vie (…). « Nous y parviendrons en planifiant des opérations cyberspatiales combinées durables qui permettent une défense et une dissuasion collectives* ».[223]

Ce terme emprunté à la grammaire de l'arme nucléaire a aussitôt alerté et intrigué la petite communauté des spécialistes de la guerre numérique, qui s'interrogent sur son sens et sa portée.

Bien que sa position soit isolée chez les experts qui rappellent que « *le cyber est une arme éminemment régalienne, et chacun sait qu'il serait très difficile de collaborer sur ce sujet avec les Allemands* », Bernard Barbier s'est alarmé de l'annonce américano-britannique : « *Cette force combinée représente des moyens humains et techniques impressionnants (plus de dix fois les moyens français). Est-ce que l'Europe veut créer une capacité combinée de cyber dissuasion ? Si l'Europe ne réagit pas rapidement, nous serons encore plus totalement dépendant du couple UK-USA : les GAFAM plus NSA-GCHQ* ».

Les autorités françaises ont donné des gages au grand allié américain en signant des accords de coopération.

---

[220] *Cf. Thales et Atos créent le champion européen du Big Data et de l'Intelligence Artificielle pour la défense et la sécurité :* https://atos.net/fr/2021/communiques-de-presse_2021_05_27/thales-et-atos-creent-champion-europeen-big-data-ia

[221] Voir par exemple Emeline Strentz *in Les GAFAM et la stratégie du cloud de confiance : quid de la souveraineté numérique française ?* https://portail-ie.fr/analysis/2982/les-gafam-et-la-strategie-du-cloud-de-confiance-quid-de-la-souverainete-numerique-francaise

[222] *« Souveraineté et compétitivité des entreprises : plus de temps à perdre ! » :* www.medef.com/fr/actualites/podcast-souverainete-et-competitivite-des-entreprises-plus-de-temps-a-perdre

[223] *Washington et Londres brandissent la cyberdissuasion. Quand la guerre numérique change d'échelle :* https://incyber.fr/washington-londres-brandissent-cyberdissuasion-quand-guerre-numerique-change-echelle/

Pour autant, elles considèrent que le haut niveau de compétence des experts publics autorise la France à demeurer « *autonome* » et « *prudente* ». Posture de principe qui porterait plutôt à sourire si elle n'était pas révélatrice d'une volonté de rassurer malgré le constat édifiant que même les agences fédérales américaines éprouvent les plus grandes difficultés à se mettre au niveau des défis posés à la sécurité nationale des Etats-Unis, au point d'amener le président Joe Biden à leur fixer un ultimatum pour y parvenir.[224]

Dès lors, dans un contexte économique qui privilégie toujours l'internationalisation des chaînes de valeurs[225], que peut-on réellement espérer en France à un horizon prévisible dans ce domaine de l'autonomie - une souveraineté véritable semblant illusoire - pourtant si important aux yeux des Français - et de certains de ses partenaires européens - ?

[224] *Failles de sécurité : ultimatum du président Joe Biden aux agences fédérales :* https://incyber.fr/failles-securite-ultimatum-joe-biden-agences-federales/

[225] *Cf.* Paul Herault *in Comment renforcer la souveraineté à l'heure des chaînes de valeur mondiales ? Études de l'Ifri, décembre 2021 :* https://www.ifri.org/fr/publications/etudes-de-lifri/renforcer-souverainete-lheure-chaines-de-mondiales

En France, l'Etat 2.0 satisfait-il les caractéristiques et les exigences d'un Etat de droit ?

- *Du despotisme doux, à l'ombre de la souveraineté du peuple*

« Je veux imaginer sous quels traits nouveaux le despotisme pourrait se produire dans le monde : je vois une foule innombrable d'hommes semblables et égaux qui tournent sans repos sur eux-mêmes pour se procurer de petits et vulgaires plaisirs, dont ils emplissent leur âme.

Chacun d'eux, retiré à l'écart, est comme étranger à la destinée de tous les autres : ses enfants et ses amis particuliers forment pour lui toute l'espèce humaine ; quant au demeurant de ses concitoyens, il est à côté d'eux, mais il ne les voit pas ; il les touche et ne les sent point ; il n'existe qu'en lui-même et pour lui seul, et s'il lui reste encore une famille, on peut dire du moins qu'il n'a plus de patrie.

Au-dessus de ceux-là s'élève un pouvoir immense et tutélaire, qui se charge seul d'assurer leur jouissance et de veiller sur leur sort. Il est absolu, détaillé, régulier, prévoyant et ... doux. Il ressemblerait à la puissance paternelle si, comme elle, il avait pour objet de préparer les hommes à l'âge viril ; mais il ne cherche, au contraire, qu'à les fixer irrévocablement dans l'enfance ; il aime que les citoyens se réjouissent, pourvu qu'ils ne songent qu'à se réjouir. Il travaille volontiers à leur bonheur ; mais il veut en être l'unique agent et le seul arbitre ; il pourvoit à leur sécurité, prévoit et assure leurs besoins, facilite leurs plaisirs, conduit leurs principales affaires, dirige leur industrie, règle leurs successions, divise leurs héritages ; que ne peut-il leur ôter entièrement le trouble de penser et la peine de vivre ?

C'est ainsi que tous les jours il rend moins utile et plus rare l'emploi du libre arbitre ; qu'il renferme l'action de la volonté dans un plus petit espace, et dérobe peu à peu chaque citoyen jusqu'à l'usage de lui-même. L'égalité a préparé les hommes à toutes ces choses : elle les a disposés à les souffrir et souvent même à les regarder comme un bienfait.

Après avoir pris ainsi tour à tour dans ses puissantes mains chaque individu, et l'avoir pétri à sa guise, le souverain étend ses bras sur la société tout entière; il en couvre la surface d'un réseau de petites règles compliquées, minutieuses et uniformes, à travers lesquelles les esprits les plus originaux et les âmes les plus vigoureuses ne sauraient se faire jour pour dépasser la foule; il ne brise pas les volontés, mais il les amollit, les plie et les dirige; il force rarement d'agir, mais il s'oppose sans cesse à ce qu'on agisse; il ne détruit point, il empêche de naître; il ne tyrannise point, il gêne, il comprime, il énerve, il éteint, il hébète, et il réduit enfin chaque nation a n'être plus qu'un troupeau d'animaux timides et industrieux, dont le gouvernement est le berger.

J'ai toujours cru que cette sorte de servitude, réglée, douce et paisible, dont je viens de faire le tableau, pourrait se combiner mieux qu'on ne l'imagine avec quelques-unes des formes extérieures de la liberté, et qu'il ne lui serait pas impossible de s'établir à l'ombre même de la souveraineté du peuple. » (Alexis de Tocqueville, *'De la démocratie en Amérique'*)

- *De la démocratie*

Lors d'une conférence prononcée en décembre 2021, Norman Eisen, l'un des co-auteurs américains d'un document proposant 10 principes pour la Démocratie applicables au sein de l'Alliance des Démocraties chère au président Biden[226], évoqua la conversation apocryphe entre le Secrétaire d'Etat américain Henry Kissinger et le Premier ministre chinois Zhou Enlai au cours de laquelle on prétend que Kissinger aurait demandé : *« What do you think of the French Revolution ? »*. Et Zhou Enlai est censé avoir répondu : *« It's too soon to tell. ».*

[226] *Cf.* https://www.brookings.edu/research/the-democracy-playbook-preventing-and-reversing-democratic-backsliding/

Il voulut ainsi souligner la très forte différence d'appréciation entre les deux nations de ce qu'a pu produire pour les nations la Révolution française en termes d'avancées démocratiques.

S'il en avait été tenu informé, Zhou Enlai aurait pu alors demander à son interlocuteur ce qu'il pensait du droit des peuples à disposer d'eux-mêmes issu justement de la Révolution française, principalement en vertu du Décret de la Convention du 19 novembre 1792 qui stipule : *« La Convention nationale déclare au nom de la Nation française, qu'elle accordera fraternité et secours à tous les peuples qui voudront recouvrer leur liberté […] »,* et de l'Article 119 de la Constitution de 1793 qui stipule : *« [Le Peuple français] ne s'immiscera en aucune manière dans le gouvernement des autres puissances ; mais [il] déclare en même temps, qu'[il] s'ensevelira plutôt sous ses propres ruines que de souffrir qu'aucune puissance s'immisce dans le régime intérieur de la République […] »,* comme le rappela brillamment Jean Carpentier[227].

A la question fondamentale : *« qu'est-ce qu'une démocratie au XXIème siècle ? »,* le sociologue Alain Touraine, directeur d'études et directeur du Centre d'analyse et d'intervention sociologiques (CADIS) de l'Ecole des hautes études en sciences sociales, répond dans un article mis en ligne sur le site de l'UNESCO[228] :

« La démocratie est plus souvent définie aujourd'hui par ce dont elle libère l'arbitraire, le culte de la personnalité ou le règne de la nomenklatura que par ce qu'elle construit ou par les forces sociales sur lesquelles elle s'appuie. Que célèbre-t-on aujourd'hui ? La chute des régimes autoritaires ou la victoire de la démocratie ? Et nous nous souvenons que des mouvements populaires, qui avaient renversé des anciens régimes, ont donné naissance à des régimes totalitaires pratiquant le terrorisme d'Etat.

Aussi sommes-nous d'abord attirés par une conception modeste, purement libérale, de la démocratie, définie « négativement » comme le régime où nul ne peut s'emparer du pouvoir et s'y maintenir contre la volonté de la majorité. N'est-ce pas un triomphe suffisant que de libérer la Terre de tous les régimes qui ne reposent pas sur le libre choix des dirigeants par les dirigés ? Cette conception prudente n'est-elle pas aussi la plus forte puisqu'elle s'oppose à la fois aux pouvoirs absolus, fondés sur la tradition ou le droit divin, et aux régimes volontaristes, qui en appellent aux intérêts et aux droits du peuple et lui imposent, au nom de sa libération et de son indépendance, une mobilisation militaire et idéologique qui conduit à la répression de toutes les formes d'opposition ?

Cette conception négative de la liberté et de la démocratie, telle que Isaiah Berlin et Karl Popper en particulier l'ont développée, est convaincante, car la grande affaire aujourd'hui est de libérer les individus et les groupes du contrôle étouffant que leur impose une élite dirigeante parlant au nom du peuple et de la nation. Personne, actuellement, ne peut plus défendre une conception anti-libérale de la démocratie et il ne fait plus aucun doute que les régimes qui se qualifièrent de « démocraties populaires » ont été des dictatures imposées à des peuples par des dirigeants politiques s'appuyant sur une armée étrangère. La démocratie se définit bien par le libre choix des dirigeants, et non pas par la nature « populaire » de la politique menée.

Mais une fois rappelées ces vérités, que les événements des dernières années ont transformées en évidences, une question s'impose : la liberté de choix politique, condition nécessaire de la démocratie, en est-elle la condition suffisante ? La démocratie se réduit-elle à des procédures ? Autrement dit, peut-on la définir indépendamment de ses fins, donc des rapports qu'elle établit entre les individus ou les catégories sociales ? Au moment où s'écroulent tant de régimes autoritaires, nous devons nous interroger aussi sur le contenu de la démocratie, même si le plus

[227] *Le droit des peuples à disposer d'eux-mêmes et le droit positif international* : https://www.persee.fr/doc/rqdi_0828-9999_1985_num_2_1_1609

[228] *Démocratie, qui es-tu ?* https://fr.unesco.org/courier/novembre-1992/democratie-qui-es-tu

urgent est de garder en vue que la démocratie ne peut exister là où la liberté de choix politique fait défaut.

[…] Aujourd'hui, dans maintes parties du monde, le conflit semble ouvert entre une modernisation économique, qui bouleverse l'organisation sociale, et l'attachement à des croyances. Il ne peut pas exister de démocratie si modernisation et identité sont ainsi considérées comme contradictoires. La démocratie repose non pas seulement sur un équilibre ou un compromis entre les forces en présence, mais sur leur intégration partielle. Ceux pour qui le progrès suppose qu'on fasse table rase du passé et des traditions sont les adversaires de la démocratie, tout autant que ceux qui voient dans la modernisation une diabolique. Une société ne peut être démocratique que si elle reconnaît à la fois son unité et ses conflits internes.

De là vient l'importance centrale, dans une société démocratique, du droit et de l'idée de justice, définie comme le plus haut niveau possible de compatibilité entre les intérêts en présence. Le critère principal de la justice est le maximum de liberté possible pour le plus grand nombre d'acteurs possible. Le but d'une société démocratique est de combiner le plus de diversité possible avec la participation du plus grand nombre possible aux instruments et aux produits de l'activité collective. »

- *L'Etat de droit comme système garantissant la démocratie libérale*

De manière très synthétique, l'Etat de droit peut se définir comme un système institutionnel dans lequel la puissance publique est soumise au droit.

Raphaël Roger propose une définition à la fois beaucoup plus complète et très claire de l'Etat de droit : *« L'État de droit peut renvoyer à plusieurs objets juridiques ou politiques. Mal défini, il devient l'objet d'interprétations les plus diverses et polémiques.*

L'État de droit renvoie d'abord à une conception limitée du pouvoir, et donc libérale. Le pouvoir est limité du fait de sa soumission à la règle de droit.

Ainsi, comme l'annoncera Hayek : « Le fondement essentiel de l'État de droit est cette confiance dans l'action des règles abstraites régissant les relations entre les individus […], l'État de droit est visiblement une limitation des pouvoirs du gouvernement et en particulier des pouvoirs du législateur ».

Concluant plus loin, il ajoute : « L'État de droit n'est pas une règle de droit mais une règle sur le droit, une doctrine métajuridique ou in idéal politique. Et pour être effectif, le législateur doit se sentir tenu de s'y conformer. En démocratie, l'observance de l'État de droit dépend donc de son acceptation par l'opinion publique, c'est-à-dire, en réalité, du fait qu'elle fasse partie ou non du sens de la justice prévalant dans la communication ».

Ainsi, dans ce passage, Hayek identifie bien ce qu'est l'État de droit. Le principe fondamental est que les gouvernants ne sont pas placés au-dessus de la loi, mais agissent au contraire conformément à celle-ci. C'est le principe de l'habilitation juridique. L'action ne peut se faire qu'en vertu d'une loi, évitant ainsi l'arbitraire d'une mesure réglementaire qui serait par exemple dénuée de fondement légal. En quelque sorte, l'État de droit peut être défini premièrement comme un État qui s'auto-limite par son propre droit.

Cependant, cette définition ne peut suffire, et plusieurs conceptions de l'État de droit apparaissent historiquement, bien distinctes les unes des autres. Outre celle évoquée que l'on pourrait qualifier de conception matérielle, deux autres conceptions existent :

1. *Une conception formelle où l'État agit au moyen du droit*
2. *Une conception substantielle où l'État garantit des droits au travers notamment de procédures juridiques et judiciaires*

En France et en Allemagne au début du siècle dernier, l'État de droit est vu et pensé comme un « régime de droit », autrement dit un État soumis au droit : « Le pouvoir ne peut utiliser que des moyens autorisés par l'ordre juridique en vigueur, tandis que les individus disposent de voies de recours juridictionnelles contre les abus qu'il est susceptible de commettre ». Ainsi, l'administration doit agir en vertu d'une habilitation juridique, une règle de droit doit lui donner compétence, c'est-à-dire la possibilité d'agir, d'user de sa puissance matérielle, mais toujours en respect de la norme d'habilitation.

Cela sous-entend deux choses.

Premièrement, dire que l'administration doit agir en vertu d'une habilitation juridique ne suffit pas. Il faut veiller à ce qu'elle reste dans son champ de compétences et la sanctionner le cas échéant. Pour ce faire, il faut un pouvoir juridictionnel, qu'il soit un tribunal ordinaire ou un tribunal spécial. Le juge est alors un agent de la légalité.

Deuxièmement, l'habilitation juridique issue d'une loi ne doit pas non plus violer les principes fondamentaux de la Nation circonscrits dans un texte, la Constitution. Dès lors, pour en assurer son respect il faut, non plus contrôler les actes administratifs au regard de la Constitution mais contrôler directement la loi eu égard à celle-ci. Dès lors, un juge spécial (ou non) sera chargé d'assurer ce contrôle de la constitutionnalité de la loi. Matériellement, l'État étant le seul créateur du droit, dès lors, c'est dans sa volonté et sa puissance que se trouve la source du droit positif. Pour reprendre Jellinek, il reste « maître de se fixer sans cesse à lui-même les règles qui sont de nature à le limiter ».

L'État de droit est ici alors comme formel et matériel et correspond à la pensée européenne de l'État de droit, qu'il s'agisse de celle du Rechtstaat ou de l'État de droit français, où l'on est passé progressivement d'un État policier où l'administration n'avait pas de limites légales à un État de droit où l'administration est soumise à un ensemble de règles contraignantes qui en cas de violation, fera l'objet d'une sanction de la part du pouvoir juridictionnel.

Ainsi, on constate au travers de l'Histoire que ces conceptions matérielles et formelles s'opposent à la dernière conception, la conception substantielle.

La conception substantielle est historiquement présente dans les pays de common law, où au travers du « due process », le juge encadre le pouvoir de l'État via sa jurisprudence et ses arrêts de précédents (stare decisis). Mais au travers de ces procès il va aussi soulever et ériger des principes et droits fondamentaux dont le citoyen pourra se prévaloir contre l'arbitraire de l'État.

Aujourd'hui, les trois conceptions de l'État de droit se rejoignent dans les démocraties libérales.

Enfin, l'État de droit peut se schématiser pour en faciliter la description. Ainsi, il est la condition fondamentale de la démocratie libérale, car comme l'a précisé Michel Troper, « il n'y a pas de démocratie sans État de droit ».

Cet État de droit repose sur quatre piliers : le principe de légalité ; la sécurité juridique ; la hiérarchie des normes ; la protection des droits et libertés fondamentaux.

Le tout repose sur deux principes : La séparation des pouvoirs avec notamment la garantie de l'indépendance et l'impartialité du pouvoir judiciaire ; Le juge comme garant de l'État de droit au travers de la raison juridique »[229,230]

84

[229] *Etat de droit : clé de voûte de la démocratie libérale* : https://www.contrepoints.org/2021/09/26/406676-etat-de-droit-cle-de-voute-de-la-democratie-liberale

[230] *Les critères de l'Etat de droit* :

De manière plus synthétique, l'État de droit suppose la limitation des pouvoirs à travers le principe de légalité, c'est-à-dire que l'exécutif et l'administration sont soumis à la loi, et plus tard à la Constitution, soumission faisant l'objet d'un contrôle par une autorité juridictionnelle ou une juridiction spécialisée (comme le Conseil constitutionnel).

- *Les rôles fondamentaux de la Constitution et du Conseil constitutionnel dans l'Etat de droit en France*

Le Conseil constitutionnel assure la justice constitutionnelle qui peut être définie dans un sens matériel comme l'activité permettant d'assurer la primauté de la Constitution ou dans un sens procédural comme les techniques permettant de consacrer cette primauté.

Quatre fonctions composent la justice constitutionnelle : l'unification/purification de l'ordre juridique ; la protection des droits fondamentaux ; l'arbitrage entre les pouvoirs publics ; le contrôle de l'expression du suffrage.

Le Conseil constitutionnel, d'abord pensé comme l'arbitre des pouvoirs publics s'est transformé en un véritable défenseur des droits fondamentaux substantiels. Bien que ce contrôle reste imparfait, il n'en demeure pas moins que cette avancée constitue un progrès de la démocratie libérale.

Comme le relève Raphaël Roger Devismes[231] : *« C'est avec la décision du 16 juillet 1971 que le Conseil constitutionnel va se muer en véritable Cour constitutionnelle et permettra, au travers de son contrôle effectif, d'assurer la pleine normativité à la Constitution, la faisant ainsi primer sur les règles normatives inférieures, finalisant ainsi le « principe de légalité » compris dans son sens large de soumission de l'exécutif et de l'administration à une norme juridique supérieure. En faisant de la norme constitutionnelle la norme sanctionnée, elle devient le fondement de validité de l'ensemble de l'ordre normatif.*

La Constitution de la Cinquième République du 4 octobre 1958 n'est pas, a priori, une Constitution libérale dans le sens où elle consacrerait un ensemble de droits fondamentaux. Alors que les autres Constitutions européennes comme celle de l'Allemagne (« clause d'éternité » à l'article 79 al. 3, Loi fondamentale de 1949) ou de l'Italie prévoient des catalogues de droits fondamentaux, celle de la France ne le prévoit pas. La Constitution de la Cinquième République est pensée comme une réponse au régime d'assemblée de la Quatrième République, et le thème principal de la Cinquième République sera le parlementarisme rationalisé, entendu comme une codification juridique des rapports et des actions du parlement.

Cependant, la Cinquième République consacre certains droits comme : le principe de laïcité (art. 1er) ; le principe de souveraineté nationale (art. 3) ; l'égalité devant la loi (art. 1er) ; la liberté individuelle (art. 66) etc.

On le voit, avec ses 89 articles la Constitution stricto sensu, c'est-à-dire matérielle, ne dispose pas de beaucoup de droits et libertés fondamentaux.

Par sa jurisprudence créatrice, le Conseil constitutionnel va consacrer un véritable mur constitutionnel, un trésor constitutionnel, composé de l'ensemble des acquis constitutionnels, trésor auquel on ne peut qu'ajouter de nouveaux principes fondamentaux et jamais en enlever. C'est l'effet cliquet décrivant une « roue de droit fondamentaux constitutionnels » qui ne peut aller que vers l'avant, et qui instaure un seuil en deçà duquel le législateur ne peut descendre.

Dans son rapport sur la prééminence du droit (CDL-AD(2011)003rev) adopté à sa 86e session plénière (mars 2011), la Commission de Venise a dégagé les caractères communs des notions d'Etat de droit, de *Rule of Law* et de *Rechtsstaat* ; le document contient en annexe une première liste de critères d'évaluation de la prééminence du droit dans un Etat https://rm.coe.int/1680700eb7

[231] *Eloge du Conseil constitutionnel* : https://www.contrepoints.org/2021/12/19/417322-eloge-du-conseil-constitutionnel

Par sa jurisprudence, le Conseil constitutionnel a donc consacré la valeur constitutionnelle au préambule de 1958 et a fait découler des diverses déclarations des nouveaux droits comme, à partir de l'article 2 de la Déclaration de 1789, la liberté d'entreprendre, la liberté de la personne et la liberté contractuelle. Bien sûr, ces droits constitutionnels sont souvent antagonistes, contradictoires et donc vont nécessiter une conciliation.

Le Conseil constitutionnel va cimenter le « mur constitutionnel » à la fois par sa méthode générale d'appréciation des lois qui tiendra compte de l'objet, des motifs et du but de la loi, mais aussi par son œuvre créatrice que sont les objectifs de valeur constitutionnels (OVC), et qui permettent cette conciliation par la création d'une norme constitutionnelle qui dans le même temps, élargit le champ d'application des principes constitutionnels originaires. En ce sens que, le Conseil constitutionnel est un « architecte constitutionnel », modulant au gré de sa jurisprudence la structure des droits fondamentaux en tenant compte des situations dans lesquels s'exerce le contrôle.

Le Conseil constitutionnel est l'institution de l'indétermination textuelle, on pourrait alors dire que la Constitution est ce que le juge constitutionnel dit qu'elle est, par son interprétation toujours progressive mais nuancée, permettant la mutabilité de la Constitution.

Selon le professeur Troper, l'interprétation de la Constitution est nécessaire pour au moins trois raisons : l'indétermination normative ; la nature et la signification du texte ; les évolutions institutionnelles et sociétales. Cette œuvre interprétative est en France aux mains du Conseil constitutionnel qui devient un acteur du régime d'énonciation concurrentielle des normes, il est en ce sens un co-législateur. »

- *Le droit et l'Etat de droit se trouvent profondément malmenés par les grandes avancées technologiques*

Fait nouveau dans l'histoire des sciences et des technologies, et plus largement, dans l'histoire de l'humanité, cette 4ème révolution industrielle à l'œuvre participe à modifier la nature des relations, et des rapports de force, entre la puissance publique mondiale et les champions du capitalisme technologique, au point de rendre illusoire toute perspective de rééquilibrage, à court ou moyen terme. C'est dans ce contexte historique qu'il convient d'envisager les développements suivants, la France n'ayant ni la capacité ni l'ambition d'échapper à cette grande révolution civilisationnelle.

D'une manière générale, le droit est très en retard par rapport aux avancées technologiques qui progressent à marche forcée, à la faveur d'investissements colossaux que seules les grandes plateformes numériques systémiques et leurs satellites sont en capacité d'imaginer, de concevoir, de développer et d'imposer au monde, leur puissance capitalistique dépassant largement les capacités d'intervention et de régulation des Etats les plus puissants de la planète.

Dans un ouvrage intitulé '*Repenser la pyramide des normes à l'ère des réseaux – Pour une conception pragmatique du droit*,' Boris Barraud souligne avec force : *« L'an 2000 ne pouvait se contenter de signer sobrement le crépuscule d'un millénaire ; aussi a-t-il marqué avec fracas le passage à une ère nouvelle. Dans la sphère juridique notamment, le postmodernisme – façonné par la globalisation et par son éminent ambassadeur, l'Internet – se déploie de façon exponentielle, conquérant chaque jour d'autres adeptes convaincus que, désormais, les normes se négocient en dehors du cadre de l'État ou que la justice ne se rend plus devant les cours et tribunaux. Ainsi rouillées par l'accélération pharaonique du temps, les munitions de la « pyramide » mériteraient d'être refondues. Il est certain que, jusqu'à lors, le droit et sa philosophie ont toujours su s'accommoder des révolutions – qu'elles soient techniques ou sociales – et que celle du numérique et des réseaux ne mènera pas plus que ses prédécesseurs à la décadence de l'empire juridique. Mais les soldats de la doctrine devront lutter âprement ;*

devant la guerre paradigmatique qui s'annonce, chaque partie fourbie ses armes. « Ubi societas, ubi ius », selon un adage latin que nul ne saurait mettre en doute. Mais, une fois cela dit, une fois cela acquis définitivement, le juriste se trouve néanmoins en délicate posture ; car que renferme au juste ce ius ? Le droit, autant que la norme, est en fait indéfinissable ; et personne ne résiste à la tentation de la définition. Or, prise dans les tourments des mutations portées par les réseaux, la tentation devient obsession. Afin de contrarier cette frustration naissante, la méthode empirique doit être privilégiée. En naviguant sur la mer internetique et en observant les règles régissant l'activité de ses plaisanciers, flibustiers et autres corsaires, peut-être est-il permis d'aboutir à quelque conclusion pertinente. »

Le professeur Julien Bonnet affirme : *« La révolution numérique bouleverse des pans entiers du droit, phénomène désormais largement étudié. Mais ses conséquences sur le droit constitutionnel, plus particulièrement, sont encore peu explorées. Les enjeux sont pourtant nombreux et importants, au regard du double mouvement permanent de déconstruction/reconstruction qui affecte plusieurs fondements de la discipline. Sont ainsi concernés des concepts classiques tels que, par exemple, la souveraineté de l'État, la puissance publique source de la normativité, la hiérarchie des normes, le régime représentatif ou encore la citoyenneté et ses modes d'expression. Sont aussi impliqués les processus politiques et démocratiques de décision et de désignation des gouvernants, et les modalités d'exercice et de protection de certaines libertés fondamentales.*

Le numérique met ainsi à l'épreuve le droit constitutionnel : en se fondant sur l'existant et en se projetant sur son potentiel, le numérique soumet le droit constitutionnel à plusieurs défis, qui concernent autant l'adaptation des objets de la science constitutionnelle que la modernisation de ses méthodes. Quatre principaux défis ont pu être identifiés et étudiés lors des journées nationales décentralisées organisées par l'AFDC en 2016, puis lors de la journée nationale de restitution du 17 mars 2017.

1 – <u>Réinventer la souveraineté et la démocratie</u> : La révolution numérique produit des effets sur l'autorité souveraine des États, sur les modes de gouvernement et sur les processus démocratiques. Au niveau international, cela suscite autant de perspectives que de crispations. Sur le plan interne, cela se traduit d'ores et déjà par des innovations dont les résultats ne sont pas encore pleinement convaincants.

L'État et son autorité, d'abord, sont confrontés au développement des technologies du numérique, et notamment d'Internet, qui favorisent le dialogue et les échanges, grâce à des connexions libres, instantanées, interactives et transnationales, et contribuent à la dilution des frontières, au rapprochement des sociétés humaines, à la construction de nouveaux espaces de construction et d'expression des opinions publiques. Le numérique facilite la comparaison permanente des systèmes constitutionnels et des pratiques politiques grâce aux sites institutionnels, aux plateformes wiki et aux blogs, aux outils d'information et de classification, aux bases de données et de jurisprudence, aux moteurs de recherche, à l'image du « Constitute project », du forum de Venise ou de la base de données CODICES. Ces technologies pourraient ainsi favoriser la convergence, voire la standardisation des pratiques, participant d'un double phénomène d'internationalisation et de « globalisation » du droit constitutionnel.

Après le principe de l'autonomie constitutionnelle des États, c'est le concept classique de souveraineté de l'État qui se trouve mis à l'épreuve. Assimilée à l'exercice d'un pouvoir de commandement suprême et indépendant dans le cadre de frontières délimitées, cette conception classique, déjà fragilisée, est bousculée par les conséquences de la révolution numérique et par la montée en puissance des réseaux. D'autant que, précisément, la conception hiérarchique, pyramidale et unilatérale du pouvoir de contrainte de l'État se heurte aux modes de régulation des espaces numériques. Associant aux techniciens et aux autorités étatiques le secteur privé,

la société civile et les utilisateurs, ils reposent largement sur la soft law et contribuent à la multiplication des sources et des formes de normativité.

Ces évolutions conduisent à d'inquiétants phénomènes de repli et à la revendication, par certains États, d'une « souveraineté numérique » présentée comme nécessaire à la défense de leurs intérêts fondamentaux et de leurs pouvoirs régaliens. Certes, les États ont à protéger leurs intérêts politiques, diplomatiques, économiques, de défense et de sécurité, et doivent garantir le respect du droit, de l'ordre public et des libertés. Mais l'affirmation de leurs droits souverains peut aussi traduire une volonté de prise de contrôle, préjudiciable aux principes libéraux qui structurent les réseaux. La réflexion sur le concept énigmatique et controversé de « souveraineté numérique » est cependant plus ouverte, puisqu'elle renvoie à la maîtrise, non seulement par les États, mais aussi par les entreprises, par les communautés d'utilisateurs, voire par les individus, de leur destin dans un monde numérique. Elle soulève, pour certains, la question de la capacité à s'auto-gouverner, à s'auto-déterminer, à choisir ou à consentir aux règles auxquels on se soumet, dans le monde numérique. Elle est définie, par d'autres, comme le pouvoir de commander et de se faire obéir sur les réseaux, et serait ainsi appropriée par les grandes multinationales américaines, notamment les « GAFA », qui tendent à se substituer aux États dans un nombre croissant de domaines. La souveraineté numérique devrait se reconquérir, à l'échelle européenne, grâce à une politique industrielle ambitieuse, à la réforme des modes de gouvernance des réseaux, afin de clarifier les objectifs et les processus décisionnels, et de « reprendre le contrôle sur les algorithmes ».

Ce sont, d'ailleurs, les failles du système de gouvernance des espaces numériques, mises en évidence par certains scandales récents, qui conduisent à s'interroger sur la perspective d'une transposition aux instances internationales de régulation des principes du constitutionnalisme (légitimité, représentativité, responsabilité, transparence). La réflexion sur une potentielle « Constitution de l'Internet », par exemple, porte l'hypothèse d'une « constitutionnalisation » des principes, droits et des devoirs attachés à la communication numérique (principe de neutralité, ouverture, liberté de l'internet), auxquels la communauté unifiée des concepteurs et des utilisateurs accepterait de se soumettre.

Les processus d'expression de la souveraineté et de construction du débat démocratique sont également bouleversés par l'irruption des technologies numériques. La démocratie connectée (e-democracy) ouvre de nouvelles perspectives pour l'exercice des droits civils et politiques (droit de pétition, vote électronique, consultations publiques, appels à contribution, comptes rendus électroniques en temps réel…). Déjà étudiées dans le champ de la science politique, ces innovations ont des conséquences politiques et normatives qui relèvent désormais pleinement du droit constitutionnel, dans le cadre d'une réflexion déjà internationalisée. Les citoyens sont appelés à contribuer directement aux processus constituants (élaboration de projets de Constitution de l'Union européenne en 2004, en Islande en 2011, ou au Sri Lanka à partir de 2016) et aux processus législatifs (expérience de co-écriture de la loi pour une République numérique du 7 octobre 2016 en France, droit d'amendement citoyen, plateformes e-parlement d'appel à contribution aux études d'impact, à l'évaluation des lois, ou à la simplification des lois, initiative législative populaire à l'échelle nationale ou européenne…). Rendu matériellement possible grâce aux plateformes numériques et aux réseaux sociaux, le « crowdsourcing », méthode de production participative issue du marketing, permet de valoriser les idées et expériences du plus grand nombre dans les processus décisionnels et réanime l'idéal de la démocratie directe. Les « citoyens » (dont l'âge et la nationalité ne sont d'ailleurs pas vérifiés, le plus souvent, sur les plateformes numériques concernées) sont, selon les cas, informés, consultés ou véritablement associés aux processus, ce qui diminue le poids des considérations partisanes, dans le cadre de forums où le débat n'est pas non plus confisqué par les « sachants ». Ils peuvent être appelés à proposer la loi ou à l'enrichir, à la valider ou

à l'évaluer. Ils peuvent aussi contribuer au contrôle de l'action du gouvernement ou de la gestion des services publics. Cette logique collaborative peut aider à reconnecter les élus aux citoyens, à mieux légitimer les processus décisionnels en faisant appel à l'expérience du terrain, à l'expertise des praticiens et des usagers, à la diversité des points de vue. Le rôle des corps intermédiaires, des médias traditionnels, des partis politiques, doit être adapté. En multipliant les outils de communication, d'expression, de mobilisation politique, en modifiant les rapports gouvernants-gouvernés, l'outil numérique fait évoluer la manière de participer à la vie politique pour les citoyens et la manière de « faire » de la politique pour les gouvernants. Cet outil peut être considéré, à de multiples égards, comme un atout pour nos démocraties, un outil permettant de la revivifier.

Pour autant, quels qu'en soient l'intérêt et le potentiel, l'outil numérique soulève aussi des interrogations et des inquiétudes. Certaines expériences déjà menées suscitent quelques réserves, au vu de leur résultat discutable, de leur apport limité ou de leurs effets pervers ou contre-productifs. Le processus de co-écriture de la Constitution islandaise, par exemple, est un échec, les causes de sa défaillance ayant pu être utilement identifiées : impréparation et improvisation, complexité et illisibilité des procédures, concurrence entre la classe politique et les citoyens (entre la méthode représentative et la méthode participative), confrontation des institutions concernées (organe constitutionnel élu, cour suprême, parlement, les experts, les partis politiques et même la communauté universitaire), insuffisant relais des médias, poids des lobbys… De même, en matière de co-écriture de la loi, les résultats concrets des mécanismes participatifs sont assez faibles et le manque de représentativité des « citoyens numériques » peut être critiqué[(15)]. Certains dénoncent le mirage du « clicktivism », qui limite finalement l'engagement politique à un click de soutien seulement virtuel et fugace. D'autres s'inquiètent d'un phénomène paradoxal d'inclusion/ exclusion, pour des raisons matérielles ou sociologiques, de certaines catégories de la population de la citoyenneté numérique. Le risque du cloisonnement, l'enfermement de la réflexion par un phénomène d'entre-soi favorisé par les réseaux sociaux, la sélection des informations opérée par les algorithmes, le court-circuitage des institutions de gouvernement et d'information traditionnelles au profit d'autres acteurs dont la légitimité et la compétence ne sont pas garanties ni contrôlées, figurent au nombre des motifs d'inquiétudes. Les technologies numériques n'étant qu'un outil, c'est la façon dont elles vont être utilisées, développées et encadrées qui déterminera, dans l'avenir, leurs effets bénéfiques ou délétères, à moyen et long terme, sur la démocratie.

2 – <u>Repenser la normativité</u> : Dès lors que le numérique renouvelle les modes de production du droit, le cadre théorique et juridique des caractéristiques de la norme est nécessairement affecté. Si plusieurs dimensions sont d'ores et déjà envisageables, la plus évidente renvoie aux nouveaux registres de légitimité de la norme qui découlent de l'usage du numérique. En effet, les nouveaux processus numériques d'élaboration de la norme renouvellent les débats constitutionnels sur l'élaboration de la Constitution et de la loi. D'autant qu'il n'est pas exclu que ces processus numériques de participation soient, dans un avenir proche, obligatoirement intégrés à l'ensemble des procédures d'adoption des textes constitutionnels et législatifs. Certes, le droit constitutionnel s'était déjà saisi de ces aubes normatives où le jeu politique rencontre le droit. Mais le numérique transforme les modalités de ces processus, les enrichit de la possibilité d'une participation plus importante des individus, et en définitive permet d'envisager une présence fréquente et active du peuple réel. Les expériences récentes de « crowdsourcing », en dépit de leurs limites, montrent que l'élaboration d'une Constitution ou de la loi sous l'effet du numérique sera de moins en moins un processus linéaire concentré entre les mains du pouvoir politique. À terme ces processus seront davantage déconcentrés, diffus et forcément plus complexes. Mais le numérique n'est pas seulement une nouvelle technique d'ingénierie constitutionnelle qui nécessiterait d'amender les ouvrages de droit

parlementaire. Plus qu'un vague gadget technologique qui permettrait d'obtenir plus rapidement un résultat similaire, le numérique génère un objet inédit qui renouvelle les registres de légitimité de la norme. Dans l'absolu, l'usage du numérique renverse les obstacles pratiques et temporels qui rendaient impossible la présence institutionnelle du peuple réel. Sous réserve d'adaptations techniques mineures, l'ensemble des citoyens et des individus vivant sur un territoire donné pourrait demain accéder à des outils de participation politique. Ainsi, les registres de légitimité des normes issues de ce type de processus relèveraient davantage d'une approche procédurale et consensuelle de la démocratie. De même, la possibilité pour le numérique de rapprocher la population locale du pouvoir décisionnel, qu'il soit politique ou administratif, renforcerait la logique de proximité et de la démocratie locale.

Le numérique renforce également, du moins potentiellement, les gages de qualité de la norme. En amont, les dispositifs de consultation via le numérique peuvent élargir les consultations ponctuelles effectuées par les commissions parlementaires ou le rapporteur. En aval, le contrôle de l'application des lois et l'évaluation de la législation et des politiques publiques s'enrichiront d'enquêtes à grande échelle auprès des citoyens, d'un public ciblé ou d'un secteur professionnel particulier.

En outre, le numérique renouvelle de nombreuses questions touchant aux rapports entre les systèmes normatifs, avec en particulier la question récurrente du niveau normatif pertinent pour prévenir un risque pour les droits et libertés ou pour réglementer un secteur d'activité. Le numérique rend en effet insaisissable la norme applicable, en défiant les règles classiques de la territorialité du droit international public ou privé et en suscitant la concurrence accrue des normes produites par le secteur privé. Bien que le problème reste entier, des solutions sont proposées ou ont déjà été amorcées, comme l'adoption d'un traité international sur les réseaux, la création d'un mécanisme international de régulation, ou l'approfondissement des réseaux internationaux et européens de régulateurs.

Enfin, grâce aux métadonnées, le fameux « Big Data », le numérique offre une compréhension approfondie du processus normatif et de la norme elle-même, voire l'anticipation du sens de la norme. Grâce au traitement automatisé à grande échelle des données du droit constitutionnel, des décisions des juges, des textes, des débats parlementaires, le numérique permet d'envisager une analyse exhaustive, dépassant ainsi l'approche sélective de l'exemple choisi par l'observateur. En ce qui concerne plus particulièrement la jurisprudence, la loi du 7 octobre 2016 pour une République numérique oblige les juridictions judiciaires et administratives à mettre à la disposition du public, à titre gratuit et dans le respect de la vie privée des personnes concernées, l'ensemble de leurs décisions. Une telle masse de données nécessite l'élaboration d'algorithme et de programmes informatiques qui permettront de mieux comprendre la décision des juges, voire d'établir des probabilités sur le sens de la décision en se fondant sur les décisions passées. Cette évolution, qui devrait se concrétiser dans quelques mois seulement, permettra d'approfondir les théories de l'interprétation grâce aux modélisations informatiques. Un objectif de prédiction est également poursuivi, l'analyse en « Big Data » de la jurisprudence permettra en effet d'établir des probabilités sur l'issue du litige. Cependant, la démarche a ses limites et le risque est grand de transformer la norme jurisprudentielle en une version réduite à des occurrences dénuées de pertinence, à une représentation numérique de la norme incapable de traduire le véritable sens de la décision du juge, ses non-dits et ses implications.

3 – <u>Interroger les droits et libertés</u> : Les interactions entre les technologies du numérique et le droit constitutionnel se manifestent particulièrement en matière d'exercice des droits et libertés fondamentaux, qu'il s'agisse évidemment des libertés de communication et d'information ou de la protection de la vie privée et des données personnelles. Le perfectionnement de la géolocalisation, l'exploitation commerciale du « Big Data », les nouvelles techniques de

surveillance et de fichage, les dérives possibles dans l'utilisation des données personnelles et de santé, la montée en puissance des réseaux sociaux ou la cybercriminalité sont autant de défis posés à la garantie des libertés. L'outil numérique peut être mobilisé au service de la protection de l'ordre et de la sécurité publics autant qu'il peut être vecteur d'atteintes aux droits, comme l'ont illustré la loi Renseignement du 24 juillet 2015 ou les révélations relatives aux politiques de surveillance généralisée développées par certains services.

Le numérique constituant un nouvel espace d'exercice des droits et libertés, à la lisière de l'espace public et de l'espace privé, il oblige à réaménager les modalités de garanties ainsi que le contenu de ces droits et libertés, voire d'en créer de nouveaux. Outre la redéfinition des contours de la liberté de réunion, de la liberté d'expression et de communication, le droit à l'information et à la participation, par exemple, peut être approfondi. La protection du droit d'auteur, de la vie privée, de la dignité, par exemple, doit être adaptée. D'autres droits, tels le droit à l'instruction ou le droit au secret du vote peuvent être affectés par les nouvelles technologies du numérique. Les droits économiques et sociaux sont également concernés, à l'image du phénomène d'« uberisation », dont le Conseil constitutionnel a été saisi à plusieurs reprises, ou des enjeux relatifs aux droits des travailleurs ou au secret des affaires. La conciliation de la liberté d'entreprendre, de la liberté du commerce et de l'industrie et du droit de propriété doit être repensée. Sans nul doute, l'irruption de problématiques numériques dans le contentieux des droits et libertés interroge le rôle du droit et du juge, confrontés à des évolutions techniques complexes qui supposent une expertise particulière. D'autant que la révolution numérique fait apparaître des droits de nouvelle génération, tel le droit à l'oubli et le droit au déférencement, la liberté d'accès à internet, ou le droit d'accès aux données en open data, dont les fondements et contours doivent être précisés.

Alors que l'individu s'aventure dans un monde déterritorialisé, la protection des libertés doit s'appuyer sur des principes juridiques identifiés et clairement réaffirmés, et sur une large palette d'outils de régulation. Le juge a un rôle majeur à jouer, aux côtés des autorités indépendantes spécialement compétentes, telles la CNIL, forte de son expertise technique et juridique, ou, dans leurs domaines respectifs, le CSA ou la HADOPI. Afin de mettre en lumière les nouvelles dimensions numériques des libertés individuelles et publiques constitutionnellement protégées, la jurisprudence constitutionnelle est « constructive et évolutive », permettant d'accompagner la « consécration de nouvelles dimensions des droits et libertés fondamentaux, voire de nouveaux droits à part entière ». Ainsi, la liberté d'accéder à Internet, proclamée par le Conseil constitutionnel en 2009, pourrait se transformer en droit opposable. La portée et les limites du droit d'accès à l'information sur internet, en lien avec le principe de transparence, sont progressivement précisées. Dans l'attente d'une éventuelle inscription de la protection des données personnelles dans le texte de la Constitution, le principe fait l'objet, avec le droit à la vie privée, d'une jurisprudence nourrie. Et l'on suppose un prochain positionnement du Conseil constitutionnel sur le droit au déférencement, prolongement technique du droit à l'oubli, reconnu par la Cour de Justice de l'Union européenne depuis 2014. Celle-ci joue un rôle majeur, s'appuyant sur la Charte des droits fondamentaux de l'Union et sur la Convention européenne de sauvegarde des droits de l'homme pour protéger les intérêts des utilisateurs européens, dans un contexte tendu par l'affaire Snowden. Elle bataille pour garantir un haut niveau de protection des données personnelles (invalidation du Safe Harbor), et veille à la protection de la vie privée des internautes qui utilisent les services de compagnies américaines (enjeux du Privacy Schield adopté par la Commission européenne et entré en vigueur le 1er août 2016), en liaison avec la CNIL et le réseau des CNIL européennes (G29). Car en matière de gouvernance du monde numérique comme en matière de protection des droits et libertés, c'est aussi et surtout à l'échelon européen que les problématiques peuvent être utilement traitées.

4 – <u>Transformer les discours des acteurs</u> : En adoptant un regard transversal, le support et le contenu du discours des acteurs du droit constitutionnel sont transformés par le numérique. L'analyse approfondie du phénomène ne pourra se faire, à terme, sans un dépassement du droit positif et un croisement des disciplines, par exemple avec les enseignements de la sociologie institutionnelle et de la sociologie de la communication. Certains constats peuvent d'ores et déjà être dressés.

De manière générale, l'avènement du numérique impose une technicisation du discours des acteurs du droit constitutionnel. « Big Data », « open data », « crowdsourcing », « tweet », « ubérisation », algorithme, autant de termes dont la présence dans une réflexion de droit constitutionnel était inimaginable il y a seulement dix ans. Désormais, le pouvoir politique, les juges et la doctrine doivent nécessairement intégrer un niveau minimum de connaissance de ces technologiques afin de les comprendre, les encadrer ou de juger les conséquences de leur mise en oeuvre. À titre d'illustration, les nombreuses questions prioritaires de constitutionnalité relatives à l'entreprise « Uber » ont nécessairement contraint le Conseil constitutionnel à analyser les dispositifs technologiques à l'origine du débat juridique et constitutionnel avec les chauffeurs de taxis. De même, les impératifs de sécurité numérique sont désormais omniprésents sur toutes questions touchant, par exemple, à la protection des données ou au vote électronique. Le règlement juridique de ces questions suppose avant tout de les comprendre, et implique donc pour le droit constitutionnel d'intégrer un aspect technologique à sa réflexion.

Le numérique a également transformé le rythme et l'impact de la communication politique. Grâce aux sites internet et aux réseaux sociaux, dont sont dotés désormais toutes les institutions de la République et tout homme ou femme politique, un système direct et décentralisé de production du message est désormais à l'oeuvre. Par-delà le parti politique, sans devoir emprunter le filtrage des médias traditionnels, une institution ou un responsable politique peut s'adresser directement à un public extrêmement large. Le nombre exponentiel d'utilisateurs des réseaux sociaux, tout particulièrement chez les jeunes, dévoile tout le potentiel futur du numérique comme moyen principal d'information et d'échange sur la politique. Les campagnes politiques sont dès lors particulièrement concernées par le numérique, à l'image de l'usage tout aussi choquant qu'efficace de son compte Twitter par le candidat Trump lors des dernières élections présidentielles aux États-Unis. La France connaît également l'effet à double tranchant de la réduction du débat politique à 140 signes, comme l'avait d'ailleurs laissé augurer dès 2012 un tweet de la compagne du Président de la République dans l'entre-deux tours des législatives.

On remarque également une évolution des rapports entre les pouvoirs publics liée à l'outil numérique, du fait de l'accélération et de la démultiplication des échanges publics, via des communiqués ou des tweets provenant des comptes officiels d'institutions (Élysée, CSA, CSM par exemple), comme certaines affaires récentes l'ont montré.

Signe d'une véritable évolution, il est plus surprenant de constater que les institutions juridictionnelles de la République développent de manière grandissante sur Internet et les réseaux sociaux un discours numérique, en marge de la décision de justice. Mise en ligne de commentaires officiels, dossiers thématiques, communiqués, notes d'information, sélections de décision, vidéos, mais également utilisation grandissante de Twitter et Facebook : le Conseil constitutionnel, le Conseil d'État et la Cour de cassation ne se contentent plus de motiver leurs décisions, ils communiquent. Et leur communication s'opère principalement par la voie du numérique. L'analyse des comptes Twitter des trois cours suprêmes françaises, sur ce point à l'image de la plupart des pratiques constatées à l'étranger, met en évidence plusieurs usages. Au-delà de la diffusion de la jurisprudence, après une sélection préalable en ce qui concerne le Conseil d'État et la Cour de cassation, les juges de la République répondent régulièrement

aux demandes de leurs abonnés, qu'ils soient professionnels du droit ou non, et font la promotion de leur réforme ou de leur action. Au-delà d'une adaptation évidente à la modernité visant à assurer une visibilité des institutions concernées, l'émergence de la communication institutionnelle des juges sur le réseau n'est pas sans risque. Outre l'inévitable effet déformant de toute communication, les juridictions pourraient se banaliser en renonçant totalement à l'autorité de leur silence, sans compter les risques de la personnalisation de la communication institutionnelle des juges par la mise en avant de leurs plus hauts responsables. Sont ainsi révélatrices à cet égard les offensives institutionnelles menées par la Cour de cassation depuis fin 2015 grâce à une communication particulièrement intense sur le site Internet et le compte Twitter de l'institution.

Enfin, le discours de la doctrine, de manière générale et en particulier en droit constitutionnel, s'est également transformé sous l'effet du numérique. Ce nouvel outil affecte effet la pédagogie de l'enseignement ainsi que les méthodes de la recherche, au profit de la comparaison des droits, l'utilisation généralisée des bases de données, ou l'approfondissement des techniques numériques de recherche permettant l'exploitation du « Big Data ». Avec des perspectives prometteuses, mais peut-être, aussi, quelques effets pervers au regard des risques de réduire la part d'analyse et de critique au profit de la promotion de résultats exhaustifs et statistiques. La mise en valeur et la visibilité du discours doctrinal sont également concernées. Les revues électroniques et blogs juridiques se sont multipliés, les universitaires interviennent sur les sites Internet spécialisés et grand public. Les comptes Twitter et Facebook de la doctrine, individuels ou institutionnels, permettent de diffuser la connaissance, de promouvoir la recherche, ou plus largement de susciter l'intérêt de l'auditoire et en particulier des médias. » [232]

Bruno Barraud ajoute *: « Sous le regard noir du droit, le changement n'est pas toujours synonyme de progrès ; et l'extraordinaire outil qu'est le réseau internet apparaît, à ses yeux, comme une source de la lente agonie des frontières et de l'Etat. Or il est un dogme, dessiné par le théoricien positiviste Hans Kelsen, qui se construit essentiellement dans le cadre étatique : la « pyramide » des normes. Cette figure s'est imposée au sein des esprits juridiques avec une telle autorité qu'elle semble, aujourd'hui encore, immuable. Pourtant, qui plonge dans le paysage globalisé du XXIe siècle internetique et s'adonne à une approche pragmatique constate fatalement la déchéance de ce modèle par trop linéaire.*

Traditionnellement réfractaire à l'évolution, le milieu juridico-politique doit alors admettre combien l'insaisissable cadence du temps maltraite ses acquis les mieux ancrés ; et c'est tout naturellement que le droit de l'internet - postmoderne s'il en est - conduit à un nouveau paradigme : le « réseau » de normes. »[233]

- *L'Etat de droit 2.0 face au défi de la défiance*

Corrollaire de cette nouvelle révolution civilisationnelle, le XXI^{ème} siècle voit émerger une nouvelle ère pour l'Etat de droit, celle de l'Etat de droit 2.0.

Qu'il s'agisse des grands débats engagés par le gouvernement français qui reposent sur des consultations en ligne, ou des consultations publiques proposées par les institutions européennes ou les institutions parlementaires nationales (notamment lors des phases

[232] *Le numérique : un défi pour le droit constitutionnel :* https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-un-defi-pour-le-droit-constitutionnel

[233] *Repenser la pyramide des normes à l'ère des réseaux – Pour une conception pragmatique du droit*, L'Harmattan, collection -, 2012, 394 pages.
Notamment en incluant un *Dictionnaire du droit postmoderne* (p. 305), cet ouvrage contribue à la délicate mise en lumière des mutations de la sphère juridique, ainsi qu'à la réflexion fondamentale sur le renouveau des notions de droit et de norme.
https://www.academia.edu/15296139/Repenser_la_pyramide_des_normes_%C3%A0_l_%C3%A8re_des_r%C3%A9seaux_Pour_une_conception_pragmatique_du_droit_L_Harmattan_coll_Logiques_juridiques_2012_394_p?email_work_card=title

d'élaboration des études d'impact des projets et propositions de loi[234]), le recours à la démocratie 2.0 est désormais entré dans les moeurs, suscitant ici et là une défiance quasi généralisée au sein d'une population insuffisamment préparée à de tels bouleversements de l'action publique, la protection des droits fondamentaux et des libertés fondamentales semblant malmenée par cette émergence rapide dans l'espace public comme dans l'espace privé du numérique et de la dématérialisation.

En France, une partie importante des citoyens ont le sentiment que l'Etat ne parvient plus à adapter ses mesures à une société qui doute de son efficacité autant que des mobiles de son intervention.

Reconnaissance faciale, intelligence artificielle, 5G … : les controverses sur les risques liés au développement de certaines technologies se sont multipliées.

Les nombreux débats éthiques, philosophiques et juridiques autour du risque d'une emprise irréversible de la technologie sur l'humain [235] ont trouvé dans le douloureux épisode pandémique de 2020 et 2021 et du recours à des technologies profondément innovantes pour tenter d'y mettre un terme (traçage numérique, vaccins à ARN messager, …), comme dans des initiatives privées particulièrement audacieuses articulées sur l'objectif d'optimiser toujours plus le rapport cerveau/machine[236], des terreaux propices à nourrir de très profondes inquiétudes qui appellent des réponses 'appropriées' de la part des pouvoirs publics, notamment.

Dans leur dernier ouvrage[237], Irénée Régnauld et Yaël Benayoun révèlent et dénoncent les dogmes et les manœuvres qui permettent aux industries et aux pouvoirs publics de maintenir les citoyens et les travailleurs à l'écart des choix technologiques, en excluant tout processus démocratique. Les auteurs expliquent pourquoi, après une décennie euphorique, le numérique ne fait plus rêver.

Les promesses d'un monde meilleur laissent la place à une autre réalité, faite d'entraves à la vie privée, de surveillance de masse, de gouffre énergétique et de manque de transparence, supprimant les contre-pouvoirs en ignorant l'avis du citoyen. Ils montrent que notre arsenal juridique et nos institutions apeurées, voire serviles, sont incapables de contrer les servitudes imposées par les plateformes et les industries hyper capitalistes : « *Les controverses liées au numérique se multiplient. Cependant, prises unes à unes, elles ne permettent pas de voir un enjeu plus global : le cruel manque de démocratie dans ces décisions. […] Pas une semaine ne passe sans qu'un scandale lié aux nouvelles technologies n'éclate. A peine voit-on les dégâts*

---

[234] Aux termes des troisième et quatrième alinéas de l'article 39 de la Constitution : *« La présentation des projets de loi déposés devant l'Assemblée nationale ou le Sénat répond aux conditions fixées par une loi organique. - Les projets de loi ne peuvent être inscrits à l'ordre du jour si la Conférence des présidents de la première assemblée saisie constate que les règles fixées par la loi organique sont méconnues. En cas de désaccord entre la Conférence des présidents et le Gouvernement, le président de l'assemblée intéressée ou le Premier ministre peut saisir le Conseil constitutionnel qui statue dans un délai de huit jours ».* Aux termes du premier alinéa de l'article 8 de la loi organique du 15 avril 2009 relative à l'application des articles 34-1, 39 et 44 de la Constitution : *« Les projets de loi font l'objet d'une étude d'impact. Les documents rendant compte de cette étude d'impact sont joints aux projets de loi dès leur transmission au Conseil d'État. Ils sont déposés sur le bureau de la première assemblée saisie en même temps que les projets de loi auxquels ils se rapportent ».* Selon le premier alinéa de l'article 9 de la même loi organique, la Conférence des présidents de l'assemblée sur le bureau de laquelle le projet de loi a été déposé dispose d'un délai de dix jours suivant le dépôt pour constater que les règles relatives aux études d'impact sont méconnues.
Les études d'impact, méthodologie : https://www.legifrance.gouv.fr/contenu/menu/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/les-etudes-d-impact-methodologie

[235] *Cf.* Jean-Yves Goffu *in Humanisme, posthumanisme, transhumanisme : de quoi* ***parle-t****-on exactement ?*
https://theconversation.com/humanisme-posthumanisme-transhumanisme-de-quoi-parle-t-on-exactement-152510

[236] *Cf.* Philippe Menei *in Elon Musk, le singe et les trois cochons : une fable transhumaniste ?*
https://theconversation.com/elon-musk-le-singe-et-les-trois-cochons-une-fable-transhumaniste-164418

[237] *Technologies partout, démocratie nulle part. Plaidoyer pour que les choix technologiques deviennent l'affaire de tous'* : https://www.fypeditions.com/technologies-partout-democratie-nulle-part/
Dans cet ouvrage, les auteurs proposent des actions concrètes et réalistes qui replacent le débat démocratique et les revendications citoyennes au cœur du développement technologique, afin que la question du progrès devienne l'affaire de tous.

qu'a produit la numérisation à marche forcée de certains services de l'Etat que nous voilà rattrapés par le débat à propos de la reconnaissance faciale, talonné de près par le procès à venir de la 5G. Les choix technologiques sont devenus des sujets de société, et non plus seulement des questions réservées aux experts. Pourtant, ces choix restent cantonnés à des sphères très restreintes, pour ne pas dire qu'ils échappent complètement aux citoyens. […] La CNIL a, paradoxalement, perdu du pouvoir depuis l'entrée en vigueur du RGPD. Ses avis sont désormais émis a posteriori des « expérimentations », quand ils ne sont pas tout simplement balayés. Quant aux autres instances chargées de poser un regard distancié sur les choix technologiques, comme le Conseil national du numérique (CNNum) ou le Comité consultatif national d'éthique (CCNE), leurs membres ne sont pas élus, et leurs avis seulement consultatifs. Souvent, ces instances sont sollicitées uniquement dans le but de conforter des politiques publiques. […] Du côté des pouvoirs publics, le discours est tout à fait contradictoire. Elus et institutions en appellent à plus de « démocratie » et de « débat public », mais n'expliquent jamais réellement sous quelle forme ni à quelle fin. Bien souvent, il ne s'agit en réalité que de mettre un peu de « citoyen » dans des organes sans importance, et surtout sans pouvoir, afin de mieux légitimer des décisions déjà prises à l'avance. » [238]

Les représentants des différentes administrations de l'Etat donnent parfois le sentiment d'exercer leurs missions en usant d'excès de pouvoir, d'abus de pouvoir, ou de détournement de pouvoir.

En réalité il n'existe que 5 cas où un abus de pouvoir en droit public sera caractérisé. Ces 5 cas englobent tous les excès de pouvoir[239].

En droit public un abus de pouvoir signifie que l'autorité publique commet une illégalité que le juge administratif a sanctionné. L'autorité publique, c'est l'administration, que ce soit l'Etat et ses représentants, les collectivités locales et les établissements administratifs ou un établissement public industriel et commercial dans l'exercice d'une prérogative de puissance publique. Cette autorité peut être amenée dans le cadre des pouvoirs qui lui sont confiés à dépasser ce cadre. Que ce soit par ses actes, son inaction ou son comportement, une ou plusieurs illégalités outrepassant le cadre de qu'elle pouvait légitimement faire pour l'intérêt général doit être sanctionnée par le juge administratif. Sans décision définitive d'une juridiction administrative établissant l'annulation définitive des actes, il n'y a pas d'abus ou d'excès de pouvoir. C'est le pendant de la présomption d'innocence adapté à l'autorité publique.

---

[238] *Reconnaissance faciale, 5G : les choix technologiques ne doivent plus échapper aux citoyens* : https://www.liberation.fr/debats/2020/01/30/reconnaissance-faciale-5g-les-choix-technologiques-ne-doivent-plus-echapper-aux-citoyens_1776194?fbclid=IwAR1m5j5Smvb3azWOqegNrxtB2VO8WQmbokBZljG0lzfqqeHFuhHxBh98Po

95

[239] Les 5 cas d'abus de pouvoir

D'abord il existe le 'vice d'incompétence' de l'auteur de l'acte contre lequel on saisit le juge administratif d'une requête pour excès de pouvoir.

Ensuite nous avons le 'vice tiré du défaut de motivation' de l'acte administratif que l'on conteste.

Le principe veut que les destinataires des décisions administratives disposent d'une information suffisante. Elle doit contenir les considérations de droit et de fait permettant de la comprendre.

Vient par la suite le 'vice de procédure' qui a été suivie ou qui n'a pas été mise en place pour prendre l'acte reproché. Le principe veut que si l'on organise ou si l'on doit suivre une procédure, celle-ci doit être respectée. Si ce n'est pas le cas, elle ne doit pas priver les usagers d'une garantie qui aurait dû en découler.

Nous trouvons ensuite les 'vices tirés de l'erreur de droit', l'administration s'est trompée dans l'application de dispositions légales ou réglementaires auxquelles elle était soumise. Puis les vices d'erreur de fait quand l'autorité publique a dénaturé les faits pour prendre sa décision.

Enfin, le "détournement de pouvoir" concerne les cas où l'administration utilise un pouvoir dans un but différent de celui qui lui a été confié.

Un excès de pouvoir sera sanctionné si le juge considère que l'un de ces 5 principes a été méconnu.

Par ailleurs, l'explosion du nombre d'actes délictueux sur les réseaux numériques[240] aurait dû conduire l'UE comme les Etats, incapables d'assurer un niveau de sécurité approprié, à modérer leur inclination à la dématérialisation des activités de communication et d'échanges au profit des missions de service public. Or, il n'en a rien été.

Rendu public en mai 2021, le *rapport Tendances digitales 2021 dans le secteur public*, qui présente les principaux points à retenir pour les organismes publics, de la mise en oeuvre de moyens de généraliser les prises de décisions axées sur le numérique au renforcement de la confiance, en passant par l'importance du raffermissement des politiques de données, révèle les succès et les échecs de l'adoption du numérique[241].

Pour la troisième année consécutive, l'Académie des Technologies a cherché à comprendre et analyser la perception des Françaises et Français, et son évolution, à l'égard des nouvelles technologies. Ce baromètre annuel réalisé par l'Ifop montre que les technologies constituent une source croissante d'inquiétude.

Les Françaises et Français sont désormais une majorité (56 %) à se dire inquiets à ce sujet (+ 15 points par rapport à l'enquête précédente). Par ailleurs, ils sont nettement moins nombreux qu'il y a une dizaine d'années à reconnaître leur impact positif sur le quotidien. Malgré ces inquiétudes, 61 % estiment que le progrès technologique reste synonyme de progrès pour l'humanité et 75 % se déclarent majoritairement intéressés par les nouvelles technologies.

Le sondage révèle le sentiment d'un fort déficit d'information sur ces sujets. Seulement 33 % estiment être suffisamment bien informés, un chiffre inchangé depuis 2001. 77 % souhaitent être plus impliqués dans les décisions sur des technologies controversées et 75 % estiment que le gouvernement n'informe pas suffisamment de leurs conséquences. Les résultats mettent également en lumière le nombre limité d'institutions et de personnes suffisamment crédibles pour combler leurs attentes. Ainsi, seuls les scientifiques et les journaux scientifiques ont la confiance d'une majorité de citoyens, loin devant les représentants du gouvernement.[242]

Pour le politologue Eddy Fougier *: « Il existe ainsi une critique de nature militante portée par deux types de courants. Le premier est un courant critique de la « technoscience », cette alliance supposée entre la science, la technique et le marché jugée pernicieuse par des ONG, des scientifiques critiques, certains journalistes, des lanceurs d'alerte, des écologistes ou des leaders d'opinion. Le second est un courant plus radical, critique de la technique en tant que telle, incarné par des intellectuels ou des écrivains anti-technique, des décroissants, des activistes recourant à des actions de désobéissance civile ou à des actions clandestines de sabotage. Cette critique de nature militante est très présente dans l'espace public. Mais les enquêtes montrent aussi l'existence d'une contestation de nature « sociale », peu visible dans l'espace public, qui est le fait de personnes exprimant des inquiétudes vis-à-vis de certaines technologies. Ce sont souvent des femmes, qui se montrent plus sensibles que les hommes aux risques technologiques et industriels et plus prudentes sur les questions de santé. Ce sont aussi des catégories défavorisées : catégories populaires, peu ou pas diplômées, sympathisants RN, voire LFI, soutiens des « gilets jaunes ». […]. Ce sont avant tout des individus socialement fragiles qui ne font plus confiance aux institutions et aux élites pour les protéger de risques par rapport auxquels ils se sentent plus vulnérables que les autres catégories. […] Dans tous les cas de figure, la contestation sociale n'est pas vraiment prise en compte. Les inquiétudes tendent à être ignorées en étant vues à travers le prisme d'une critique idéologique. […] En*

[240] *3 milliards de mots de passe dans la nature : Gmail, Hotmail, Netflix ou encore LinkedIn concernés* : https://www.lesnumeriques.com/vie-du-net/3-milliards-de-mots-de-passe-dans-la-nature-gmail-hotmail-netflix-ou-encore-linkedin-concernes-n160415.html

[241] *Tendances digitales 2021 dans le secteur public : https://www.adobe.com/fr/offer/digital-trends-2021-in-public-sector.html*

[242] *Cf.* https://www.ifop.com/publication/le-regard-des-francais-sur-les-nouvelles-technologies-a-lheure-des-debats-autour-de-la-5g/

définitive, si l'on veut lutter efficacement contre la défiance de ces catégories fragiles et inquiètes, il faut à tout prix entendre leurs cris qui sont, d'une certaine manière, de véritables appels à l'aide. »[243]

- *La gestion de la crise pandémique du Covid 19 a donné lieu à des initiatives inquiétantes en regard des principes qui prévalent au sein d'un Etat de droit*

Lors de cette crise, l'article 15 de la Convention européenne des droits de l'Homme ouvrant la possibilité aux États contractants de déroger à leurs obligations en invoquant des circonstances exceptionnelles, les autorités françaises ont établi un « *état d'urgence sanitaire* » s'inspirant de celui prévu par la loi n° 55-385 du 3 avril 1955.

Plutôt que de recourir à ce système, le pouvoir a élaboré un dispositif *ad hoc*.

Aux termes de l'exposé des motifs du projet de loi d'urgence, la crise sanitaire, *« sans précédent depuis un siècle, fait apparaître la nécessité de développer les moyens à la disposition des autorités exécutives pour faire face à l'urgence "* et, du fait de son *« ampleur jamais imaginée jusqu'ici »*, appelait une réponse *« d'une ampleur qui n'a pu elle-même être envisagée lorsque les dispositions législatives et réglementaires existantes ont été conçues »*.

Si le recours à un état d'exception – en l'occurrence ici, un état d'urgence sanitaire – est venu confirmer la tendance forte observée depuis les attentats terroristes de 2015 à se soustraire à l'Etat de droit en raison de circonstances « exceptionnelles », les modalités de son instauration en mars 2020 interroge.

Pour Maître Jean-Christophe Bontre-Cazals, avocat au Barreau de Paris : *« Cette période a été inaugurée d'une bien curieuse et très inquiétante manière au regard de nos institutions. L'état d'urgence sanitaire n'étant prévu par aucune loi, ni aucun texte, le décret du 16 mars 2020 ordonnant le confinement général de 66 millions de personnes ne repose que sur le principe des circonstances exceptionnelles et l'urgence de la situation. Aucun dispositif législatif n'autorisait l'exécutif à imposer une telle privation de liberté à toute une population. C'est d'ailleurs la raison pour laquelle une loi instaurant un état d'urgence sanitaire dans le Code de la santé publique a été votée dès le 23 mars 2020, légalisant ainsi une situation juridique hors norme en matière d'atteinte à nos droits fondamentaux. Si les circonstances exceptionnelles « ont pu fonder » le décret du 16 mars 2020 ordonnant le confinement, comme l'a relevé avec ambiguïté le Conseil d'Etat, on est légitime à s'interroger sur la nature de l'urgence dont l'exécutif s'est prévalu pour user d'un tel pouvoir de police administrative. La loi sur l'état d'urgence sanitaire aurait pu être votée une semaine avant, donnant ainsi un véritable cadre légal aux mesures prises. Le contournement par l'exécutif de nos institutions, en imposant dans la panique une restriction sans commune mesure de nos libertés fondamentales, est un précédent qui doit nous inquiéter, car c'est une immense brèche dans notre Etat de droit. On sait par expérience que l'exception des circonstances crée toujours un précédent. On sait surtout que les mesures d'exception se retrouvent tôt ou tard codifiées dans notre droit commun, et que l'Etat élargit sans cesse son pouvoir de coercition. Sous le coup de l'émotion ou de la sidération, tout passe, ou presque, et pour longtemps.*

Mais la singularité de la crise sanitaire actuelle est d'avoir ajouté une nouvelle strate aux outils régaliens classiques de contrôle des individus et des corps : celle du contrôle des masses consentantes. On ne peut qu'être interpelé par la docilité avec laquelle une population entière a sacrifié les plus fondamentales des libertés (aller-venir, se réunir, exercer son culte, manifester…) sur l'autel de la santé. Nous assistons à une accélération de ce que Foucault appelait « l'étatisation du biologique », laquelle met en œuvre « une nouvelle technique de pouvoir non disciplinaire ». Dans un cours au Collège de France du 17 mars 1976, qui ne nous

[243] *Le défi de la défiance :* https://www.telos-eu.com/fr/societe/le-defi-de-la-defiance.html

a jamais paru autant d'actualité, Foucault décrypte cette nouvelle forme de contrôle qui, à la différence du pouvoir disciplinaire ne s'adresse pas à l'individu, mais à la masse. Autant le pouvoir disciplinaire était individualisant, autant le pouvoir biopolitique est « massifiant ». Ce qui va intéresser la biopolitique, ce sur quoi elle va agir pour réguler, c'est la morbidité. Non la mort d'un individu, mais le taux de mortalité d'une population globale prise dans un champ « d'évènements aléatoires ». La seule chose qui va compter c'est la vie, le « faire vivre », on pourrait même dire la vie à tout prix. « La biopolitique a affaire à la population, et la population comme problème politique, comme problème à la fois scientifique et politique, comme problème biologique et comme problème de pouvoir ». La technique du pouvoir biopolitique va s'appuyer sur des « prévisions », des « estimations statistiques », des « mesures globales ». Seuls les mécanismes globaux sont pris en considération, l'individu n'ayant pas de sens « au niveau du détail ». Dans « Post-scriptum pour une société de contrôle » (« Pourparlers »), Deleuze décrit cette perspective peu réjouissante d'une société exerçant un contrôle bipolaire avec d'un côté la « signature qui indique l'individu », et de l'autre « le nombre ou le matricule qui indique sa position dans la masse », comme les applications de tracking par exemple. »[244]

Par ailleurs, le gouvernement a autorisé les administrations, et notamment les préfectures, à s'affranchir des normes en vigueur, suivant en cela les recommandations suivantes formulées par Alain Lambert, le président du Conseil national d'évaluation des normes (CNEN) : *« La seule solution est en chacun de nous, et dans le courage de nous sentir, chacun, légitimes dans nos fonctions et responsabilités, pour nous affranchir de certaines règles à raison de circonstances dont notre droit s'épuise à chercher la qualification. »* Cette latitude donnée ainsi aux acteurs de la gestion de crise a donné lieu à des initiatives diverses dont certaines ont confirmé une certaine propension à agir en dehors du cadre constitutionnel national.

Enfin, un épisode ubuesque est venu souligner l'antiparlementarisme du gouvernement lors du débat parlementaire qui s'est tenu le 21 janvier 2021 à l'Assemblée nationale dans le cadre d'une première prorogation de l'état d'urgence sanitaire.

A cette occasion, le ministre de la santé a estimé publiquement qu'il n'était pas du rôle des parlementaires d'évaluer les prises de décision du Conseil scientifique, dont les décisions « trop techniques » échapperaient à l'entendement ordinaire des élus, ignorant alors – ou feignant d'ignorer -, outre les pouvoirs de contrôle de l'action du gouvernement attribués au Parlement par la Constitution, l'existence et les travaux sur les questions sanitaires de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)[245].

Pour Jean-Philippe Feldman : *« L'état d'urgence sanitaire issu de la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19 n'est malheureusement pas un texte isolé. Il n'est que le prolongement de nombreux dispositifs, d'autant plus préoccupants qu'ils se sont multipliés ces dernières années). Il amène à s'interroger dès lors sur la légitimité d'une législation d'exception et plus fondamentalement d'une disposition sur les situations de crise dans une Constitution. […] Il n'est pas inutile de noter que la France a émis une réserve d'interprétation lors de la ratification de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales en 1974 et ce, au sujet de l'article 15 paragraphe 1 relatif au régime dérogatoire à la Convention. En effet, cette dernière disposition prévoit la possibilité exceptionnelle d'une dérogation au texte, mais il énumère les conditions matérielles,*

[244] *Préface pour une société de contrôle :* https://blogs.mediapart.fr/j-c-bonte-cazals/blog/301120/preface-pour-une-societe-de-controle

[245] *Rapport de l'OPECST sur "Les aspects scientifiques et techniques de la lutte contre la pandémie de la Covid-19"*: https://www2.assemblee-nationale.fr/15/les-delegations-comite-et-office-parlementaire/office-parlementaire-d-evaluation-des-choix-scientifiques-et-technologiques/secretariat/a-la-une/lutte-contre-la-pandemie-de-la-covid-19?fbclid=IwAR3mJpQSOOVLwytNG4_Kd3MFfDv1hajfUIwNMQoym36qcB6b403yqAFEIt4

procédurales et temporelles permettant de respecter cette dérogation. La France a alors indiqué que les circonstances exceptionnelles mentionnées à l'article 15 de la Convention devaient se comprendre comme celles prévues tant à l'article 16 de la Constitution qu'à celles prévues par les lois sur l'état de siège et sur l'état d'urgence.

Les réactions des constitutionalistes à la nécessité d'une loi spécifique pour régler la crise sanitaire en 2020 ont été diverses. Pour les uns, il suffisait de s'appuyer sur l'état d'urgence du 3 avril 1955, pour les autres la loi du 5 mars 2007 relative à la préparation du système de santé à des menaces sanitaires de grande ampleur modifiant le Code de la santé publique était suffisante. Il n'en demeure pas moins que l'état d'urgence sanitaire comporte des points communs indiscutables avec l'état d'urgence issu de la loi de 1955, entre autres son instauration par décret et son éventuelle prorogation par la loi. On n'a pas manqué de relever combien les termes de la nouvelle législation pouvaient être larges : qu'est-ce qu'une « catastrophe sanitaire mettant en péril, par sa nature et sa gravité, la santé de la population » ? Certains n'ont pas manqué de relever qu'une simple grippe saisonnière était susceptible d'entrer dans les prévisions du nouveau texte… D'autres ont constaté que l'état d'urgence sanitaire donnait encore plus de latitude à l'exécutif puisque tant l'état de siège que l'état d'urgence requièrent l'intervention du Parlement pour une éventuelle prorogation au-delà d'un délai de 12 jours, alors que la nouvelle loi ne prévoit l'intervention du législateur que pour une prorogation au-delà d'un mois ! Enfin, si la loi de 2020 détaille les pouvoirs du Premier Ministre, elle le fait de manière particulièrement extensive en dix catégories distinctes, ainsi qu'il a été exposé. » [246]

Mais le Gouvernement français semble avoir pris le parti de rester sourd à ces très nombreux appels à la modération et au respect des principes, valeurs et droits les plus fondamentaux qui fondent la République française.

Dans un article intitulé *'L'État de droit est-il malade du Covid-19 ?'* et publié le 21 décembre 2021 [247], la professeure de droit Muriel Fabre-Magnan alerte : « *La dernière décision du gouvernement de transformer prochainement le passe sanitaire en passe vaccinal en est un exemple flagrant. Si l'objectif est d'établir un certificat permettant de limiter la propagation de l'épidémie, comment justifier que quelqu'un qui viendrait de se faire tester et dont le test est négatif serait plus dangereux que le détenteur d'un passe vaccinal qui, comme il est aujourd'hui scientifiquement avéré, peut être porteur du virus ? Les plus hautes juridictions de notre pays se déshonoreraient à ne pas s'opposer fermement à une atteinte aussi patente au principe de proportionnalité.* »

Pour l'historien Gérard-Michel Thermeau[248] : « *l'extension indéfinie de l'intervention de l'État, toujours pour de bonnes raisons, cela va de soi, a fini par miner l'État de droit. À force de multiplier les droits particuliers, on a dilué le droit général. À force de faire de l'état d'urgence le fonctionnement ordinaire de nos démocraties, on finit de vider de toute substance nos régimes de démocratie libérale.*

- *Le débat emblématique autour de l'application StopCovid*

De très nombreuses technologies ont été lancées depuis le début de la pandémie, sans compter les technologies existantes qui sont commercialisées comme outils de surveillance pour lutter contre le Covid-19. Les géants de la technologie et les startups ont proposé une kyrielle de

[246] *Constitution, état d'exception et état d'urgence sanitaire :* https://journaldeslibertes.fr/article/constitution-etat-dexception-et-etat-durgence-sanitaire/#.YR4Um44zaM9

[247] *L'État de droit est-il malade du Covid-19 ?* *https://www.lefigaro.fr/vox/societe/muriel-fabre-magnan-l-etat-de-droit-est-il-malade-du-covid-19-20211221*

[248] *La République d'Emmanuel Macron est-elle une dictature ?* https://www.contrepoints.org/2021/07/20/401877-la-republique-demmanuel-macron-est-elle-une-dictature

solutions qui incluent la détection visuelle de signes vitaux par ordinateur, celle d'appareils portables qui peuvent donner des indications précoces de l'apparition du virus sans compter les multiples applications qui surveillent les paramètres de santé.

Parmi les outils utilisés par le gouvernement français (et bien d'autres) pour tenter de lutter contre la propagation de l'épidémie, les mesures reposant sur ces techniques ont effectivement été nombreuses.[249]

Le passe sanitaire instauré à la faveur de cette crise pandémique s'inscrit dans une dynamique visant à l'établissement d'un passeport vaccinal européen.[250] Il anticipe l'instauration d'un système généralisé où l'identité ne sera plus établie par un document officiel "autonome" comme une carte d'identité, mais bien par un "portefeuille" numérique conservé sur un *cloud* et une application dont l'archivage échappera à l'utilisateur. Comme le révèle la société Thalès, ce portefeuille numérique devrait constituer demain la clé d'accès aux services publics, en même temps qu'il devrait permettre d'opérer numériquement diverses opérations bancaires.[251]

Pour Stéphane Grumbach, directeur de recherche à l'INRIA[252] : *« Si l'efficacité du contact-tracing a été très tôt démontrée théoriquement, les stratégies dites rétrospectives* (*backward tracing*) *déployées notamment en Corée du Sud et au Japon sont aujourd'hui identifiées comme étant beaucoup plus efficaces que les stratégies prospectives (forward tracing) utilisées par les Américains et les Européens. Alors que ces dernières recherchent de manière prospective les contacts des cas détectés puis les invitent à s'isoler, les stratégies rétrospectives reposent sur une approche inverse temporellement : lorsqu'un cas positif est identifié, les autorités recherchent d'où provient la contamination et non pas qui l'individu aurait pu contaminer. Il est indispensable, un an après leur introduction, de questionner l'ensemble des systèmes numériques déployés dans le cadre de la pandémie, en distinguant leurs finalités, les types de données utilisées et les acteurs impliqués dans le traitement de ces données. Une grande diversité de services a en effet été développée impliquant des acteurs publics comme privés très différents. Ces systèmes offrent des degrés très variables d'intermédiation avec les acteurs de la stratégie sanitaire nationale. Les pays membres de l'Union européenne ont majoritairement fait le choix de stratégies de mitigation portées par des outils numériques peu intrusifs et optionnels. La stratégie française reposant sur l'application TousAntiCovid est représentative de ce choix, qui, dès le départ, accorde la priorité absolue à la préservation de l'anonymat des utilisateurs en accord avec les exigences de la CNIL*[253]*. Si l'entrée en vigueur du passe sanitaire et le déploiement de TousAntiCovidSignal le 9 juin 2021 témoignaient déjà d'un changement de stratégie, les garanties imposées par la CNIL*[254] *conditionnaient, de facto, leur fonctionnement en France. Bien que les nouvelles extensions du premier dispositif semblent contrevenir à ces recommandations, le second conserve quant à lui un caractère facultatif et anonyme ; l'historique des visites ne permet ni l'identification des lieux de propagation ni la transmission d'informations vers les autorités de santé. Parmi les principales mesures*

[249] *Cf.* notamment Yoann Nabat *in Les risques de l'avènement de nouvelles formes numériques de surveillance sanitaire :* https://theconversation.com/les-risques-de-lavenement-de-nouvelles-formes-numeriques-de-surveillance-sanitaire-164656

[250] *Roadmap for the implementation of actions by the European Commission based on the Commission Communication & the Council Recommendation on strengthening cooperation against vaccine preventable diseases* https://ec.europa.eu/health/sites/default/files/vaccination/docs/2019-2022_roadmap_en.pdf?fbclid=IwAR0SlRhOXjyOmoLbfdhzyPhRuS8iFPVBDliZMRZ3ujv-PubN5lBBZ1ak0uY

[251] *How Digital ID can help citizens access government services from anywhere* : https://dis-blog.thalesgroup.com/identity-biometric-solutions/2021/07/27/how-digital-id-can-help-citizens-access-government-services-from-anywhere/?utm_source=twitter&utm_medium=Hootsuite&utm_term=&utm_content=&utm_campaign=DIS-Digital-Identity

[252] *Numérique et Covid-19 : la liberté face au contrôle :* https://theconversation.com/numerique-et-covid-19-la-liberte-face-au-controle-162691

[253] *Cf.* https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-evolutions-de-lapplication-tousanticovid

[254] *Cf.* https://www.cnil.fr/fr/la-cnil-revient-sur-la-nouvelle-fonctionnalite-tousanticovid-signal

susceptibles d'être mises en œuvre dans le cadre d'une stratégie d'élimination, les outils numériques jouent un rôle bien plus central, et leur efficacité semble directement liée à leur intrusivité. Ils permettent, face à l'incertitude épidémique, de révéler des données extrêmement précieuses sur l'état individuel des personnes, infectées, immunisées ou à risque, et d'interagir avec la population pour mieux protéger tant les individus que la société dans son ensemble, avec célérité, parfois même en temps réel. Pour autant, leur déploiement suscite à juste titre des craintes pour les libertés publiques et pour la protection de la vie privée, il y a donc lieu de considérer cette question avec le plus grand sérieux. Un système de surveillance épidémiologique présente des risques, l'anonymisation est pour une part illusoire et en tout cas difficilement vérifiable, la sécurité difficile à garantir, l'utilisation détournée des données possibles. De nombreuses associations de défense des libertés comme la Quadrature du Net en France appellent à la plus grande vigilance. »

Les débats relatifs à l'application StopCovid[255] ont mis en évidence les tensions entre les tenants d'un usage intensif du numérique sans souci des libertés fondamentales, imposant des nouveaux rapports à la vie privée, personnelle et intime que cela entraine, et ceux qui refusent radicalement toute surveillance, évoquant un outil dangereux vers le totalitarisme technologique avec tout retour en arrière impossible.

Le Conseil National du Numérique, placé auprès du Premier ministre, a émis un avis favorable au principe de StopCOVID, en tant que brique d'une stratégie plus globale[256].

Tandis que l'ANSSI a apporté son expertise sur les aspects techniques du projet[257], le Comité Consultatif National d'Ethique (CCNE) sur les sciences de la vie et de la santé a contribué à apporter une réflexion de fond sur la base d'une contribution publique[258] et d'une veille dédiée en particulier aux enjeux éthiques[259]. De son côté, la CNIL, dans son avis sur le projet d'application mobile StopCovid[260], a souligné que le dispositif est conforme au RGPD si certaines conditions sont respectées. Elle relève qu'un certain nombre de garanties sont apportées par le projet du gouvernement, notamment l'utilisation de pseudonymes. La CNIL appelle cependant à la vigilance et souligne que l'application ne peut être déployée que si son utilité est suffisamment avérée et si elle est intégrée dans une stratégie sanitaire globale.

En contrepoints, la CNCDH a tenu à alerter les pouvoirs publics sur les dangers pour les droits fondamentaux de toute application de suivi de personnes et des contacts, en particulier sur le droit à la vie privée[261], tandis que La Quadrature du Net a fourni un argumentaire hostile au projet tout en donnant au débat une richesse basée sur l'expertise[262].

Les deux assemblées parlementaires ont finalement donné leur feu vert à la mise en place de cette technologie, finalement remplacée le 22 octobre 2020 par l'application TousAntiCovid.

L'historien, écrivain et homme politique français Sébastien Nadot en retire les enseignements suivants[263] : « *La mauvaise approche du gouvernement qui a d'abord programmé un débat sans*

[255] *L'équipe-projet StopCovid et l'écosystème des contributeurs se mobilisent pour développer une application mobile de contact tracing pour la France :* https://www.inria.fr/fr/stopcovid

101

[256] *Cf.* https://cnnumerique.fr/StopCOVID-Avis

[257] *Cf.* https://www.ssi.gouv.fr/publication/application-stopcovid-lANSSI-apporte-a-inria-son-expertise-technique-sur-le-volet-securite-numerique-du-projet/

[258] *Cf.* https://www.ccne-ethique.fr/fr/actualites/la-contribution-du-ccne-la-lutte-contre-covid-19-enjeux-ethiques-face-une-pandemie

[259] *Enjeux d'éthique concernant des outils numériques pour le déconfinement :* https://www.ccne-ethique.fr/fr/actualites/cnpen-enjeux-dethique-concernant-des-outils-numeriques-pour-le-deconfinement

[260] *Cf.* https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid%C2%A0%20

[261] *Avis sur le suivi numérique des personnes :* https://www.cncdh.fr/node/2069

[262] *Cf.* https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/

[263] *L'application Stop-Covid est morte née. Attention au retour de flamme* https://blogs.mediapart.fr/sebastien-nadot/blog/040520/l-application-stop-covid-est-morte-nee-attention-au-retour-de-flamme

vote sur l'utilisation de l'application stop-covid, puis un vote sans quasiment de débat, puis une déclaration du Premier ministre évoquant le sujet, repoussé à un autre jour finalement etc etc… Bref ! Pour une fois, on ne saurait être plus reconnaissant de la médiocrité de cet exécutif à n'avoir pas su quelle voie emprunter pour imposer à tous un truc fabriqué à quelques-uns sans concertation. On disposera de la sorte d'un peu plus de temps pour prendre des décisions fortes sur un sujet jusqu'ici bien trop éludé. L'application Stop-Covid n'est qu'un énième avatar dans la controverse sur la possibilité d'une intelligence artificielle éthique. Le terme "éthique" vient du grec éthos qui fait référence aux mœurs. L'éthique a pour fonction de transposer la morale dans le fonctionnement et la dynamique de la société. Bien évidemment, l'IA en santé doit respecter des principes éthiques. C'est préférable. Mais l'IA et toutes les formes numériques appliquées à nos vies ne doivent-elle pas aussi et surtout respecter la loi ? (La loi est l'expression de la volonté générale : on considère que chaque citoyen participe, directement ou par l'intermédiaire de ses représentants, à l'élaboration de la loi). En effet, la violation d'un principe éthique n'équivaut pas à celle d'un principe juridiquement obligatoire. Or, fort logiquement, le droit est encore très jeune concernant les dernières avancées technologiques. Pour l'application Stop-Covid, la technicité du dispositif n'étant pas suffisamment fiabilisée et en capacité de répondre à des grands principes juridiques, il y a fort à parier qu'elle ne verra pas le jour. De plus, le politique s'est embourbé... Mais cela est provisoire et la prochaine application pour la prochaine crise (ou celle-là) aura à être reconsidérée à la mesure d'un vrai débat de société. Faute d'un débat démocratique incluant toutes les composantes de notre société, la digue des libertés finira par céder devant les coups de boutoir de quelques ensorceleurs du numérique ayant su séduire des politiques peu éclairés. Sur le modèle de celle pour le climat, une convention citoyenne du numérique aurait du sens. A condition que ses conclusions soient suivies d'effet... La meilleure solution découlera de l'acceptation de règles définies collectivement, donc selon des processus démocratiques - débat, conflit, dialogue, concertation, information publique, va-et-vient entre politiques et citoyens ... »

« La stratégie de déploiement et d'utilisation du numérique relève donc d'un arbitrage politique entre les risques et les bénéfices sanitaires, économiques et sociaux. Toutefois, les bonnes intentions peuvent avoir des effets paradoxaux en la matière. Plus un système numérique aspire à la protection de la sphère privée, plus il a de chance de s'imposer dans la durée. Les systèmes très intrusifs, outre qu'ils offrent une bien plus grande efficacité contre l'épidémie, pourraient donc s'avérer politiquement moins dangereux sur le long terme, précisément à cause de leur caractère exceptionnel que seule l'urgence justifie, un débat que la délégation sénatoriale à la prospective propose désormais d'ouvrir[264]*. »* (Stéphane Grumberg)

Pour le philosophe et historien des sciences Mathieu Corteel, la gestion de la pandémie est largement passée par le recours à des dispositifs techniques de modélisation statistique des comportements. En mettant à l'écart les sciences humaines et sociales, cette gestion techniciste aboutit à des politiques de santé publique qui visent le contrôle plutôt que l'autonomie des acteurs : *« En participant au dispositif du contrôle social, la santé publique a délaissé sa prétention à la promotion de la santé visant l'autonomie des acteurs, pour mieux maîtriser les conduites. L'octroi de capabilités a fait place à une instrumentalisation du choix social qui, en se normalisant au gré des décisions publiques, guide l'agent de manière diffuse, insidieuse et sans contradiction. Ce tournant laisse penser que l'autonomisation des acteurs de la santé et la défense des droits n'ont plus leur place dans l'application des normes sanitaires. Il faut au contraire réguler, inhiber et désinhiber les comportements en appareillant les individus de laissez-passer. Qu'elle est la raison de ce changement de perspective ? Est-ce véritablement la population qui s'est écartée de la raison, en perdant confiance dans la science et les*

[264] *Crises sanitaire et outils numériques : répondre avec efficacité pour retrouver nos libertés* (rapport d'information déposé le 21 juin 2021 au nom de la délégation à la prospective du Sénat) : http://www.senat.fr/rap/r20-673/r20-673.html

institutions ? Ou bien serait-ce plutôt les institutions qui ont perdu confiance dans l'autonomie de leurs administrés ? Alors que la complainte de la défiance s'amenuise et que plus de 50 millions de français sont vaccinés, le gouvernement réaffirme encore une fois sa visée comportementale aspirant à l'adaptation toujours plus astreinte des individus au milieu sociotechnique. Cette conscience dirigiste de l'État est sans doute le signe d'une inquiétude concernant la population, ou pour le moins, celui d'une conviction dans le bien-fondé de sa mise sous tutelle. La défiance, quasi-continue depuis les gilets jaunes jusqu'aux anti-vaccins, aura sans doute conduit le gouvernement à la certitude que les politiques publiques doivent parvenir à maîtriser la conduite en instrumentalisant la raison et la science. À tel point qu'embarquées dans ce dispositif, les valeurs de la santé publique se sont vidées de leur sens.

Sommes-nous encore capables de trouver un équilibre entre le respect des droits de la personne et la protection de la santé collective ? »[265]

Le recours à des dispositifs numériques était-il absolument nécessaire ?

Au cours de la période de confinement, sept Français sur dix ont estimé que l'Etat n'utilisait pas assez les technologies numériques pour lutter contre la maladie, plus d'une personne sur deux étant favorable à l'utilisation de la reconnaissance faciale, du *'tracking'* et des technologies *'big data'* dans ce contexte, et 80% pensant que la France devrait utiliser des caméras thermiques.

Yoann Nabat, doctorant en droit privé et sciences criminelles y voit matière à de nombreuses interpellations démocratiques : *« Si la question a été soulevée pour l'application de traçage, bien que les débats se soient rapidement concentrés sur des enjeux techniques, elle a été quasiment absente ensuite. Le « solutionnisme » technologique a ici trouvé une application nouvelle : face à une difficulté majeure, biologique donc difficilement contrôlable, et inédite, le recours au numérique apparaît comme évident. Pourtant, aucune des technologies utilisées par ces dispositifs n'est neutre. Lorsque des caméras de surveillance sont mises en place dans le métro parisien pour vérifier le bon port du masque par les usagers, tout doit être pris en compte : quelles caméras sont utilisées, et fabriquées par quel opérateur ? Où sont envoyées les données et par qui sont-elles traitées ? Que deviennent les images filmées et les résultats ? La CNIL est d'ailleurs très vigilante sur ces questions.*

Ces questions, relatives notamment au respect de la vie privée et au traitement des données personnelles, mais aussi aux risques du conflit entre intérêts privés et publics, sont intrinsèques au recours à ces technologies, mais pourtant peu soulevées dans le débat public. Si des dispositifs de suivi des cas positifs existaient ainsi déjà pour certaines maladies, la création inédite pour le coronavirus de fichiers nationaux et centralisés n'est pas anodine. Plus fondamentalement, ces systèmes apparaissent avant tout comme des outils de contrôle et de surveillance des individus, à un niveau sans doute rarement égalé dans nos sociétés modernes, au moins à une aussi large échelle. La très récente généralisation du passe sanitaire à de nombreux lieux culturels ou de vie sociale systématise ainsi l'idée d'un contrôle inédit, car mise en œuvre essentiellement par ceux qui ne disposent habituellement pas de ce pouvoir (gérants ou directeurs d'établissements par exemple) et donc par les citoyens eux-mêmes. La « société de vigilance » trouve ici peut-être une nouvelle traduction. L'espace public perd encore un peu plus de son anonymat.

L'idée d'un contrôle par la technologie n'est pourtant pas nouvelle. Elle s'incarne depuis plusieurs années en matière sécuritaire par le développement des fichiers de police, mais aussi des outils de surveillance à la disposition des forces de police judiciaire voire administrative. Elle est également appuyée par les grandes entreprises du numérique (qui en font la source de

[265] *Covid-19 : la santé publique comme laboratoire du contrôle social ;* https://aoc.media/analyse/2021/11/23/covid-19-la-sante-publique-comme-laboratoire-du-controle-social/

leur rentabilité, grâce au développement du « capitalisme de surveillance » dénoncé par Shoshana Zuboff). La perspective originale des processus actuels se trouve alors peut-être dans leur lien étroit et nouveau avec la dimension biologique. Par ces outils, le politique se saisit encore un peu plus des enjeux de santé, non pas à la manière des siècles passés en exerçant une emprise directe sur le corps, mais par une forme plus insidieuse de contrôle, de « biosurveillance ». Ces dispositifs deviennent ainsi ceux de la « biopolitique » telle qu'exposée par Michel Foucault à la fin du siècle passé. Celle-ci ne s'adresse plus au corps individuel, mais « à la multiplicité des hommes comme masse globale affectée de processus d'ensemble qui sont propres à la vie », c'est-à-dire à la population conçue comme un tout. Or, la technologie permet précisément de répondre à ces impératifs, puisqu'elle assure une prise en compte globale de la population, chaque individu se trouvant réduit à un ensemble de données, dont la gestion peut être opérée quasi-automatiquement. Dans cet équilibre, le rôle des nudges ne doit pas être écarté. Ils participent pleinement à la surveillance en s'assurant de la complète coopération de l'individu, et en évitant le plus possible le recours à la contrainte. Si la vaccination n'est pas obligatoire, la présentation du passe sanitaire l'est devenue. Plus subtilement, si le recours à l'application TousAntiCovid n'est pas strictement nécessaire, tout est rendu plus facile pour son utilisateur. D'ailleurs, la communication des chiffres de téléchargement est en elle-même aussi un nudge, car elle incite par le nombre.

L'ensemble de ces outils apparaît comme particulièrement intrusif. Rarement autant de dispositifs de contrôle et de surveillance auront concerné une part aussi importante de la population. Pourtant, leur acceptabilité sociale a progressé très rapidement. Sur ce point, l'exemple du passe sanitaire est particulièrement révélateur : d'une mesure inenvisageable à l'été 2020, il est devenu quasi obligatoire un an plus tard.

Les nudges ne sont pas seuls responsables de cette apparente absence de contestation. C'est ici le phénomène d'accoutumance qui doit être observé, facilité par l'impatience de sortir enfin un jour de la crise sanitaire et celle du tant promis retour à la vie antérieure. La technologie est partout dans notre quotidien, et les mesures de surveillance tendent également, qu'elles soient sanitaires ou sécuritaires, à se banaliser. Le fichier sanitaire devient un parmi d'autres, le passe sanitaire un contrôle de plus lors de déjà fastidieux passages aux frontières, tandis que l'application trouve sa place au milieu de toutes celles installées chaque jour sur nos téléphones.

Face à ce développement, les remparts juridiques sont souvent bien impuissants : états d'urgence à répétition, absence de tout pouvoir de véto de la Commission nationale informatique et libertés (CNIL, chargée du contrôle des outils numériques et de la protection des données personnelles), modifications législatives régulières et action timide du Conseil constitutionnel.

Ce constat est d'autant plus vrai qu'on assiste au recours fréquent à un simulacre de la technique marketing du « pied dans la porte ». Si le passe sanitaire a pu être validé par la CNIL et le Conseil d'État, c'est avant tout grâce à son champ d'application limité. Pourtant, quelques mois plus tard, il est très largement étendu. Trop tard : l'outil est déjà en place. La même technique avait déjà été à l'œuvre pour l'application TousAntiCovid, dont les fonctionnalités n'ont fait que croître, et est très largement mise en application pour certains fichiers sécuritaires. Cette habitude peut être dangereuse. Elle conduit en effet à progressivement déplacer la barrière de l'intolérable, et à accepter toujours plus de dispositifs de surveillance dans nos vies. Si la période exceptionnelle peut bien sûr justifier certaines atteintes aux libertés et des outils inédits, il faut sans doute ici plus que jamais rappeler les risques de l'effet « cliquet », bien connu en matière sécuritaire, qui interdit tout retour en arrière.

Prenons garde à ce que l'ensemble de ces dispositifs, entre technologies et biopouvoirs, ne créent pas un périlleux précédent en constituant un pas de plus vers la société de contrôle, dans laquelle le risque, pour inhérent à tout système libéral, semble de moins en moins bien toléré. »[266]

Dans un article intitulé *'Sécurité et liberté : quel compromis ?'*[267], le psychologue Vincent Berthet et le politiste Léo Amsellem considèrent que, dans un contexte de pression sécuritaire croissante, les nouvelles technologies peuvent mettre en danger les libertés en favorisant une politique de l'anticipation, mais aussi garantir la sécurité sans attenter aux libertés, à condition que ces innovations fassent l'objet d'un contrôle par les instances démocratiques.

« L'efficacité de l'État, en particulier dans les domaines régaliens, est garante de sa légitimité. Mais la recherche d'efficacité dans l'action sécuritaire, qui doit permettre de garantir un niveau optimal de liberté collective, doit s'accompagner des garanties nécessaires pour préserver les libertés individuelles et proportionner strictement toute mesure privative de liberté aux objectifs démocratiquement fixés. Ce principe ne vaut que s'il s'accompagne d'un contrôle rigoureux et permanent des actions du gouvernement et de l'administration, contrôle sans lequel l'État de droit ne serait qu'un paravent. Il peut prendre différentes formes : contrôle par le juge (administratif ou constitutionnel), par des commissions indépendantes, par le Parlement, voire par la société civile.

L'opportunité de mettre en œuvre des mesures à visée sécuritaire doit être évaluée suivant une analyse pragmatique plutôt qu'une position de principe, mettant en balance les gains potentiels d'efficacité et les risques sur les libertés. Cette analyse pragmatique correspond au contrôle de proportionnalité exercé le cas échéant par le Conseil constitutionnel, par lequel celui-ci vérifie qu'une mesure restreignant un droit fondamental est adéquate (susceptible de permettre ou de faciliter la réalisation du but recherché), nécessaire (n'excède pas ce qu'exige la réalisation du but poursuivi) et proportionnée à l'objectif poursuivi. Il veille ainsi à concilier les libertés et les « intérêts fondamentaux de la nation ».

[…] Le compromis efficacité-liberté est souvent bel et bien une réalité. L'endiguement de la première vague de l'épidémie de Covid-19 par le confinement généralisé s'est bien fait au prix d'une privation massive de libertés pour l'ensemble des citoyens pendant une longue période.

Mais le compromis efficacité-liberté est un cadre conceptuel fallacieux dans les cas où il ne s'impose pas : parfois, la protection des libertés ne se fait pas au détriment de l'efficacité, et inversement, la recherche d'efficacité n'est pas nécessairement fatale aux libertés. La technologie peut permettre d'échapper au compromis efficacité-liberté. Peter Thiel, figure de la Silicon Valley, fondateur de PayPal et Palantir, l'illustre de la façon suivante : aux États-Unis, les deux extrêmes du continuum efficacité-liberté peuvent être incarnés par Dick Cheney, vice-président des États-Unis dans l'administration du président George W. Bush d'un côté (sécurité élevée et libertés restreintes) et l'Union américaine pour les libertés civiles de l'autre (sécurité faible et libertés préservées). La haute technologie permet de décorréler efficacité et liberté : il est possible de développer des solutions aptes à préserver à la fois l'ordre public et les libertés.

[…] Partant du principe que le gain d'efficacité permis par la technologie se ferait nécessairement au détriment des libertés, la logique de l'arbitrage nous condamnerait à choisir entre une société efficace mais peu éthique et une société éthique mais peu efficace. En réalité,

[266] *Les risques de l'avènement de nouvelles formes numériques de surveillance sanitaire :* https://theconversation.com/les-risques-de-lavenement-de-nouvelles-formes-numeriques-de-surveillance-sanitaire-164656

[267] *Sécurité et liberté : quel compromis ?* https://aoc.media/analyse/2021/12/06/securite-et-liberte-quel-compromis/

nous ne sommes pas toujours condamnés à choisir entre la liberté et la sécurité, et l'innovation peut nous aider à échapper à ce choix forcé.

Mais la vigilance demeure : la volonté de faire passer des mesures visant à augmenter la sécurité (intérieure ou sanitaire) est légitime si elle poursuit un objectif d'efficacité plutôt que des fins politiques et administratives. Des applications comme StopCovid ne devraient être que des outils permettant un gain d'efficacité dans l'action publique, non les premiers pas vers l'instauration d'une société de surveillance. »

- *Les initiatives de l'Etat pour la protection des données sont-elles suffisantes ?*

Au moment où, en France, l'Etat s'organise pour repenser son rôle de régulateur en l'articulant autour de la donnée[268], ce qui apparaissait encore il y a quelques mois comme la panacée en matière de protection des données, préoccupation principale des citoyens, à savoir le RGPD, a montré ses limites tant ses vulnérabilités sont importantes[269,270,271,272].

Des défaillances importantes dans le respect même de ses règles et principes par l'Etat de droit ont été relevées au point que certains acteurs n'ont pas hésité à recourir à des procédures judiciaires pour obtenir des mesures correctrices.

Les réglementations gouvernementales (portant sur la protection de la vie privée, sur les '*fake news'*, sur les données personnelles, etc.) ne comportent-elles pas aussi des failles patentes ?

Le 'simple' fait que le *European Data Protection Supervisor* (*EDPS*), l'équivalent européen de la CNIL, ait dû ordonner en janvier 2022 à l'agence de police européenne Europol de supprimer sous un an une quantité impressionnante de données issues d'enquêtes - comme celle sur EncroChat - stockées illégalement, suffirait à lui seul à le démontrer, en première lecture.[273] Si le gendarme européen des données personnelles somme Europol d'effacer de sa base de données de 4 pétaoctets celles qui ne concernent pas les suspects, témoins et certaines victimes (c'est-dire les données collectées "au hasard" des procédures judiciaires, mais aussi par des programmes de surveillance (dont certains controversés) qui concernent donc des personnes hors enquête. ; des données collectées "au cas où", mais pas analysées tout de suite) et ce, 6 mois après qu'elles aient été collectées, Europol se défend en plaidant que ses enquêtes, *a fortiori* internationales, durent bien plus longtemps que 6 mois.

Mais d'autres faits sont intervenus en France qui interpellent.

Le choix de confier les données de santé de 67 millions de Français à Microsoft Azure a suscité les inquiétudes de la CNIL, du conseil de la Caisse nationale de l'assurance maladie (Cnam) et du Conseil d'Etat, mais fut finalement validé par ce dernier, faute de mieux[274], et gêné aux encablures le gouvernement[275]. Le ministère des solidarités et de la santé s'était engagé à déposer une demande d'autorisation du GIP *Health Data Hub* (HDH) auprès de la CNIL, à la

[268] *Nouvelles modalités de régulation - la régulation par la donnée :* https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Nouvelles-modalites-de-regulation-la-regulation-par-la-donnee

[269] *La vérification d'identité : une faille importante dans le règlement RGPD :* https://www.decideo.fr/La-verification-d-identite-une-faille-importante-dans-le-reglement-RGPD_a11303.html?fbclid=IwAR0phpVADiJnbaP-uSNzlWzjt23hlxNzxRtqtxzBA4N6ejIhDqrnuybnYOE

[270] *Black Hat 2019 : comment le RGPD facilite le vol de données personnelles :* https://www.lebigdata.fr/black-hat-2019-rgpd

[271] *Cloud Act, l'offensive américaine pour contrer le RGPD :* https://portail-ie.fr/analysis/1902/cloud-act-loffensive-americaine-pour-contrer-le-rgpd?hash=0c8ded38-333b-4310-a215-c6d0484882dd&utm_medium=social&utm_source=facebook

[272] *Tirer profit du Big Data sans compromettre nos libertés :* https://www.contrepoints.org/2020/05/31/372574-rgpd-profit-du-big-data-sans-compromettre-nos-libertes-3-5

[273] *Cf.* https://edps.europa.eu/node/8469_fr

[274] *Cf.* https://www.zdnet.fr/actualites/health-data-hub-pas-de-risque-zero-en-matiere-de-transfert-des-donnees-outre-atlantique-selon-le-conseil-d-etat-39911315.htm

[275] Microsoft hébergeur de nos données de santé : les surprenants bricolages juridiques du Health Data Hub

suite d'une requête de celle-ci, avant même sa création fin 2019 par la transformation de l'Institut national des données de santé. La plateforme technologique du Hub est opérationnelle depuis le printemps, mais elle comprend uniquement des données relatives à l'épidémie de Covid-19 et repose sur des décrets pris dans le cadre de l'état d'urgence sanitaire.

Comme le relève Léa Crébat dans un article publié dans le journal international de médecine[276], d**ès** son origine, les critiques étaient nombreuses et concernaient notamment le choix du gouvernement d'utiliser le cloud public de Microsoft pour héberger les données très sensibles du système national d'information inter-régimes de l'Assurance-maladie (Sniiram), du programme de médicalisation des systèmes d'information (PMSI) et du système national de données de santé (SNDS). Un an plus tard, Olivier Véran ministre de la Santé et Cédric O, secrétaire d'État chargé de la transition numérique s'engageaient à changer d'hébergeur *« d'ici à deux ans au maximum »*. Mais une année après cette promesse, il est vrai encore très marquée par l'épidémie de Covid, il n'y a guère de signe tangible d'une évolution prochaine.

Aussi, comme l'explique dans *Le Monde* le président de la réforme de l'État Christian Babusiaux : *« La frilosité de l'écosystème du Health Data Hub et de leurs responsables est donc parfaitement légitime. S'y ajoutent les piratages relatés par les médias dans de nombreux pays ces derniers mois, dont Microsoft n'est pas exempt »*.

Face à ces difficultés, le Conseil scientifique du HDH lui-même ne cache pas ses inquiétudes. Christian Babusiaux résume : *« le HDH se trouve aujourd'hui dans une impasse »*. Pour lui, qui regrette que beaucoup de temps a été perdu, il faut se ressaisir, en réglant notamment le problème de l'hébergeur. Il relève : *« Si la France a été capable de construire une des plus grandes bases du monde (le système national des données de santé), elle l'est aussi, avec des partenaires européens, pour l'héberger et l'exploiter en se conformant à l'état de l'art des nouvelles technologies. Il est temps de sauver le soldat Health Data Hub et de sortir de cette impasse qui appelle une décision rapide des pouvoirs publics face aux enjeux de santé publique, financiers, industriels et éthiques que représentent les données de santé. »*

Le 8 janvier 2022, le gouvernement a pris la décision retirée sa demande d'autorisation déposée auprès de la CNIL pour le Health Data Hub.

Le député Philippe Latombe, rapporteur de la mission d'information de l'Assemblée nationale sur la souveraineté numérique[277], a réagi à cette décision en ces termes : *« […] Il ne viendrait à personne l'idée de critiquer l'objectif initial d'un projet censé permettre "l'accès aisé et unifié, transparent et sécurisé, aux données de santé pour améliorer la qualité des soins et l'accompagnement des patient". L'exploitation massive des données de santé représente sans conteste un outil essentiel pour la recherche. Sans autorisation de la CNIL, le HDH ne peut pas fonctionner de manière pleine et normale, si tant est qu'il en soit capable. II ne peut donc y avoir que des projets pilotes, très limités et très contrôlés. C'était bien la peine d'ambitionner de "faire de la France un leader de l'analyse des données de santé", pour en arriver là, après plus de deux ans. Du choix malheureux de Microsoft à l'Incapacité fonctionnelle du HDH, ses promoteurs ont accumulé erreurs stratégiques et techniques, sans avoir l'humilité de se remettre en question, persistant dans le déni et se refusant à envisager une alternative. […]Il existe pourtant des solutions nationales souveraines et fonctionnelles, comme le Ouest Data Hub ou l'Entrepôt des données de l'APHP, qui sont d'ores et déjà opérationnelles et conformes*

[276] *Les espoirs déçus du Health Data Hub :* https://www.jim.fr/medecin/jimplus/e-docs/les_espoirs_decus_du_health_data_hub_190034/document_jim_plus.phtml

[277] Mission d'information sur le thème *« Bâtir et promouvoir une souveraineté numérique nationale et européenne »* : https://www.assemblee-nationale.fr/dyn/15/dossiers/alt/batir_promouvoir_souverainete_numerique_mi

aux attentes de la CNN, et aux intérêts des Français. Et si on en profitait pour faire confiance à l'écosystème français du cloud... par appel d'offres ? »

Qu'en est-il de l'espace numérique de santé ?

Pris en application de la loi du 24 juillet 2019, dite "Ma santé 2022", le décret permettant la mise en oeuvre de l'espace numérique de santé (ENS, aussi appelé Mon espace santé) n'a été publié que le 7 août 2021 au Journal officiel. Il s'inscrit dans la feuille de route ministérielle du numérique en santé dont l'ENS est une des mesures phares en permettant à chaque assuré de disposer d'un compte personnel en ligne qui lui donne accès à une sorte de carnet de santé en version numérique. Ce décret définit le contenu de l'ENS, les modalités de sa création et de sa clôture éventuelle, les modalités d'exercice des droits de son titulaire, dont le droit d'opposition à sa création, et d'une manière plus générale l'ensemble des règles de fonctionnement. Il définit également les critères de référencement des services numériques en santé au catalogue de l'espace numérique en santé ainsi que le cadre applicable à la procédure de référencement.

Le dispositif a été testé dans trois départements pilotes avant un déploiement dans toute la France à partir du 1er janvier 2022. Pour l'heure, les assurés n'ont accès qu'à leur dossier médical partagé – partie intégrante de l'ENS - et à une messagerie, notamment utilisée pour préparer les admissions à l'hôpital ou envoyer certains conseils thérapeutiques. À terme, d'autres fonctionnalités devraient être ajoutées avec notamment les résultats d'examens, des outils numériques de prévention, mais aussi de prise rendez-vous, ou encore de télémédecine. L'Assurance maladie a pu « *tester techniquement le fonctionnement* » de ce service. L'hébergement des données est assuré par des sociétés françaises dont Santeos, une filiale de Wordline, et Atos, toutes deux étant certifiées « *hébergeur de données de santé* ».

Par ailleurs, la Cour des Comptes a saisi l'opportunité de ses travaux à l'égard de la situation de la sécurité sociale en France pour émettre des recommandations en faveur de la dématérialisation des prescriptions médicales, considérant qu'elle pourrait permettre des progrès majeurs, notamment en matière de qualité et de sécurité des soins, de pertinence et d'efficience des dépenses de santé, de réduction des coûts de gestion et de prévention des erreurs et fraudes.[278]

La saisine du Conseil constitutionnel à la suite de l'adoption par le Parlement de la loi du 27 mai 2021 relative à la gestion de la sortie de crise sanitaire, a permis à cette plus haute juridiction de l'Etat d'établir la conformité à la Constitution de dispositions inscrites à l'article 7 de ladite loi ayant trait à la protection des données de santé dont le paragraphe I complète l'article 11 de la loi du 11 mai 2020 mentionnée ci-dessus par un paragraphe X afin de prévoir l'intégration au système national des données de santé des données recueillies dans le cadre des systèmes d'information mis en œuvre aux fins de lutter contre l'épidémie de covid-19[279], profitant de cette occasion pour à la fois rappeler - dans les paragraphes 24 à 34 de sa décision – les principales

[278] *Chapitre VIII : La dématérialisation des prescriptions médicales : un facteur d'efficience du système de santé, des chantiers ambitieux à faire aboutir :* https://www.ccomptes.fr/fr/documents/57129?fbclid=IwAR2M2kYoKX6ZmauDkIUGa4B9JNqm5Wl9sJxUFdZwFaa8PtzZdTU9doXPfqM

[279] A propos de cet article, les députés déférant soutiennent que les dispositions contestées méconnaîtraient le droit au respect de la vie privée. En effet, selon eux, le transfert de ces données au sein du système national des données de santé emporte un allongement de la durée de leur conservation qui ne serait ni justifié ni proportionné. La protection de ces données médicales, particulièrement sensibles, ne serait en outre pas assurée par des garanties adéquates, dès lors qu'elles sont traitées sous une forme qui n'est pas réellement anonyme et qu'elles sont susceptibles d'être mises à disposition d'un grand nombre de personnes.

dispositions du code de la santé publique ayant trait aux données de santé, et établir la conformité à la Constitution dudit paragraphe X de la loi du 11 mai 2020.[280,281]

Cette décision juridique se heurte malheureusement au principe de réalité.

Le 20 septembre 2021, l'Assistance publique des hôpitaux de Paris (AP-HP) a informé par courriel 1,4 million de Franciliens ayant réalisé un test PCR dans le cadre de l'épidémie de Covid-19 à la mi-2020 qu'ils avaient été victimes du vol d'une partie de leurs données personnelles et de santé (nom, prénom, adresse, numéro de téléphone, email, numéro sécurité sociale et positivité de leur test PCR).

En fonction des données dérobées, les risques sont plus ou moins importants. Cela peut aller de l'usurpation d'identité à la divulgation d'informations confidentielles. C'est d'ailleurs tout l'intérêt du vol des données de santé, elles sont tellement précises et personnelles qu'elles peuvent facilement permettre l'usurpation d'identité.[282,283]

La legaltech *Data Legal Drive*, qui accompagne les entreprises dans leur mise en conformité RGPD, fait le constat accablant suivant : seuls 38% des professionnels de la santé ont réalisé leur registre des traitements de données personnelles. Un chiffre inquiétant dans un secteur où les données sont de plus en plus nombreuses et dites sensibles.[284]

Plus emblématique encore de l'insécurité numérique qui pèsent désormais sur les individus en raison des choix 'technologistes' de l'Etat, se sont retrouvés publiés sur Internet les QR code des passes sanitaires du président Emmanuel Macron et du Premier ministre Jean Castex.[285]

Le professeur Yannick Chatelain relève que l'État se donne dans l'urgence quelques libertés concernant le traitement des données personnelles des citoyens, par impréparation ou volonté délibérée.[286]

Il alerte sur des faits précis, aux côtés des organismes comme la CNIL ou *La Quadrature du Net* qui veillent et surveillent attentivement les projets de loi et les décrets qui se succèdent à une cadence effrénée : *« Le fait est que l'urgence, qu'elle soit sanitaire ou sécuritaire n'a pas pour vocation d'accorder un blanc-seing au pouvoir qui s'arrogerait le droit de s'éloigner pas à pas de l'État de droit, alors qu'il se dit y être particulièrement attaché. Que ce soit par précipitation ou par intention cet éloignement dessinerait les contours non plus d'un État de droit, mais d'un État policier peu soucieux du droit précisément.*

À ce titre, trois situations posent questionnements et soulèvent des inquiétudes. Il ne s'agit pas de prêter une quelconque intentionnalité de l'exécutif à sortir de l'État de droit, mais de noter au travers de ces trois exemples concrets que ce dernier franchit, ou tente de franchir de façon récurrente la ligne rouge et s'arroge des libertés qui ne peuvent en aucune façon être compatibles avec le fonctionnement usuel d'un État de droit. »

---

[280] Décision n° 2021-819 DC du 31 mai 2021 - Loi relative à la gestion de la sortie de crise sanitaire : https://www.conseil-constitutionnel.fr/decision/2021/2021819DC.htm

[281] *Les données relatives à la santé :* https://www.data.gouv.fr/fr/pages/donnees-sante

[282] *Cf.* notamment : *Ce que vous risquez si vous faites partie du million de Français aux données de santé volées :* https://www.marianne.net/societe/ce-que-vous-risquez-si-vous-faites-partie-du-million-de-francais-aux-donnees-de-sante-volees

[283] *Usurpation d'identité, que faire ?* https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite-que-faire

[284] *62% des entreprises du secteur de la santé négligent les données personnelles :* https://www.globalsecuritymag.fr/62-des-entreprises-du-secteur-de,20210603,112414.html

[285] *Cf.* https://www.lemonde.fr/politique/article/2021/09/21/le-qr-code-d-emmanuel-macron-fuite-sur-Internet-l-elysee-denonce-la-negligence-ou-la-malveillance-de-professionnels-de-sante_6095489_823448.html

[286] *La stratégie du choc : de l'État de droit malmené à l'État policier :* https://www.contrepoints.org/2021/10/13/408430-la-strategie-du-choc-de-letat-de-droit-malmene-a-letat-policier

Alors que le gouvernement s'est passé de l'évaluation de la CNIL - qui n'a pas manqué d'alerter à ce sujet, un projet de loi envisage dans son article 4 de rendre le Fichier SI-DEP (système d'information de dépistages) utilisable par les forces de l'ordre, alors que la loi de mai 2020 prévoyait que seuls quelques acteurs du secteur de la santé étaient habilités à accéder à ce fichier.

Si le sanitaire interpelle, le sécuritaire est d'ores et déjà entré dans une gestion peu en rapport avec le respect de la loi.

Le 24 septembre 2021, la formation restreinte de la CNIL a rappelé à l'ordre le ministère de l'Intérieur pour sa mauvaise gestion du fichier automatisé des empreintes digitales (FAED)[287]. Les contrôles de la CNIL ont ainsi fait émerger de nombreux points mettant en défaut le ministère en charge. Lors de ces contrôles, la CNIL a ainsi identifié cinq manquements majeurs et a sommé le ministère de l'Intérieur de rectifier le tir et se mettre d'urgence en conformité avec la loi. Ses injonctions à l'encontre du ministère de l'Intérieur sont extrêmement claires.

Côté sécuritaire toujours, le ministère de l'Intérieur a été une nouvelle fois pris en défaut de non-respect du droit dans l'usage que font ses services des drones pendant de nombreux mois.

« Il ne s'agit pas de juger du bien-fondé de l'utilisation des drones par les forces de l'ordre si tant est qu'ils puissent être un appui à leurs actions au service des citoyens et de leur sécurité, mais il est impérieux que cet usage se fasse dans le respect du droit. […] Malheureusement, comme le souligne La quadrature du Net : « Après s'être vu à quatre reprises refuser le droit de surveiller la population avec des drones, le gouvernement est revenu une cinquième fois à l'attaque. Deux arrêts du Conseil d'État, une décision de la CNIL et une décision du Conseil constitutionnel n'auront pas suffit. »

L'Assemblée nationale a adopté le 21 septembre 2021 le projet de Loi 'Responsabilité pénale et sécurité intérieure' qui – entre autres –, et après des mois d'usages illégaux, encadre l'utilisation des drones par les forces de l'ordre.

La Quadrature du Net ne peut dès lors que constater avec amertume : « Le texte est quasiment identique à celui censuré par le Conseil constitutionnel en début d'année, les parlementaires n'ont pas hésité à le voter une nouvelle fois. »

En retournant ces trois faits dans tous les sens force est de constater que l'exécutif s'est autorisé à régulièrement sortir du cadre, que l'urgence, si souvent brandie, ne saurait pour autant tolérer que le pouvoir s'affranchisse régulièrement du respect du droit.

Quelle que soit l'urgence, qu'elle soit sanitaire et/ou sécuritaire cette accumulation d'arrangements avec la loi ne peut perdurer, à moins de finalement renoncer définitivement à l'État de droit et assumer l'édification d'un Etat policier prêt à transgresser le droit, jusqu'à celui-ci, à force d'obstination liberticide, et au forceps… finisse par rendre légitimes des transgressions avérées et ce de façon rétroactive. Une approche inquiétante qui ne peut être admise comme relevant de la normalité dans une démocratie en bonne santé. »

- *La CNIL semble servir d'alibi bien commode à la fuite en avant sécuritaire*

Nous avons vu *supra* que la loi relative à la protection des données personnelles promulguée le 20 juin 2018, qui adapte la loi 'informatique et libertés » du 6 janvier 1978 au 'paquet européen de protection des données'[288], confère à la CNIL des missions et des responsabilités étendues.

[287] Le fichier automatisé des empreintes (FAED) est un fichier de police judiciaire d'identification recensant les empreintes digitales de personnes mises en cause dans des procédures pénales. Ces empreintes sont principalement utilisées par les forces de l'ordre dans le cadre de leurs enquêtes.

[288] Ce paquet européen comprend le RGPD, un règlement du 27 avril 2016 directement applicable dans tous les pays européens au 25 mai 2018 ainsi qu'une directive datée du même jour sur les fichiers en matière pénale, dite directive "police"

Mais cette dernière dispose-t-elle des moyens appropriés pour lui garantir sa pleine efficacité ?

« Depuis quarante ans, la CNIL sert d'alibi bien commode à la fuite en avant sécuritaire. […] La CNIL n'a tout simplement pas les moyens humains, juridiques ou politiques d'enrayer la raison d'État, ni la volonté de questionner la surenchère technologique. » (Luc Tréguier)

Les difficultés rencontrées par la CNIL pour faire respecter ses décisions à l'égard des opérations de surveillance illicite par drones effectuées par les services relevant du ministère de l'Intérieur suffisent à illustrer la situation à cet égard.[289]

Devant les échecs de ses démarches, *'La Quadrature du Net'* dénonce publiquement l'impuissance et l'inefficacité de la CNIL devant les comportements répréhensibles des GAFAM en regard des dispositions du RGPD : *« Depuis trois ans, les réseaux sociaux Facebook et Linkedin continuent de violer le RGPD : le fichage publicitaire qu'ils réalisent repose sur un consentement obtenu de façon illégale – sous la contrainte de ne plus pouvoir accéder à leur service. La CNIL n'a aucun souci à reconnaître que cette marchandisation de nos libertés est illégale quand elle est le fait d'acteurs français. S'agissant des GAFAM, la CNIL s'interdit toute intervention, alors même que les articles 60, 65 et 66 du RGPD lui en donnent les pouvoirs. […]*

Sur nos cinq plaintes, deux n'ont jamais été examinées (Google, Amazon), deux autres semblent faire l'objet de manœuvres dilatoires absurdes (Apple, Facebook) et la cinquième n'a pas davantage abouti sur quoi que ce soit de tangible en trois années (Linkedin).

On l'a souligné plusieurs fois : si les GAFAM échappent aussi facilement au RGPD, ce n'est pas en raison de la complexité de nos affaires ou d'un manque de moyens matériels. Le budget annuel de la CNIL est de 18 millions d'euros et elle emploie 215 personnes. Au fil des ans et sur d'autres sujets, nous avons souvent échangé avec les personnes employées par la CNIL : leur maîtrise du droit des données personnelles est sincère. Elles partagent certainement nos frustrations dans une bonne mesure et n'auraient aucune difficulté à redresser la situation si on le leur demandait. Le RGPD leur donne toutes les cartes et, s'il en était besoin, nous leur avons explicitement pointé quelles cartes jouer. Si les causes de cet échec ne sont pas matérielles, elles ne peuvent être que politiques. La défaillance du RGPD vis à vis des GAFAM est si totale et flagrante qu'il est difficile d'imaginer qu'elle ne soit pas volontaire ou, tout le moins, sciemment permise. Les motivations d'une telle complicité sont hélas déjà bien identifiées : les GAFAM sont les fidèles partenaires des états pour maintenir l'ordre sur Internet. Plus que jamais, l'État français, dans sa dérive autoritaire, a tout intérêt à les maintenir au-dessus des lois pour leur laisser gérer la censure et la surveillance de masse.

À leur échelle, en permettant aux GAFAM d'échapper au droit qui devait protéger nos libertés fondamentales, les 18 membres du collège de la CNIL participent de l'effondrement démocratique en cours. »[290]

S'il est indubitable que la CNIL semble pâtir de failles structurelles qui lui interdisent d'agir à la pleine mesure des enjeux, force est d'avoir l'honnêteté de lui reconnaître une réelle expertise et un dynamisme à toutes épreuves qui l'honorent. La présente étude rassemble suffisamment d'éléments concrets qui illustrent son professionnalisme autant que la densité de ses interventions dans un contexte particulièrement complexe, le droit étant en mouvement incessant dans le registre numérique.

Cf. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&from=FR.

[289] *Cf.* https://www.zdnet.fr/actualites/drones-la-sanction-de-la-cnil-mettra-t-elle-fin-a-la-surveillance-illicite-39916223.htm

[290] *Les GAFAM échappent au RGPD, la CNIL complice :* https://www.globalsecuritymag.fr/Les-GAFAM-echappent-au-RGPD-la,20210525,112026.html

Dans son 4ème avis adressé au Parlement sur les conditions de mise en œuvre des dispositifs contre la COVID-19, en date du 30 novembre 2021[291], la CNIL fait un nouveau bilan de ses actions concernant les systèmes et dispositifs mis en place par le gouvernement depuis 18 mois pour lutter contre l'épidémie de COVID-19 : TousAntiCovid, SI-DEP, Contact-COVID, Vaccin COVID. Au total, depuis le début de la pandémie, la CNIL a réalisé 42 opérations de contrôle sur les dispositifs mis en place dans le cadre de la crise sanitaire et plus de cinquante contrôles au total en lien avec la COVID-19. Elle a également adressé plus de 200 courriers à des organismes dans le cadre de ces contrôles.

La CNIL attire de nouveau l'attention du gouvernement sur la nécessité, plus de 18 mois après le début de l'épidémie, de produire des éléments permettant d'évaluer pleinement l'efficacité des fichiers et dispositifs mis en œuvre.

Une cinquième phase de contrôles, qui porte notamment sur la durée de conservation, la suppression et/ou l'anonymisation des données, est d'ores et déjà engagée pour la fin 2021. Les résultats seront communiqués dans le prochain avis public de la CNIL.

La CNIL s'est prononcée en décembre 2021 sur un décret visant notamment à permettre l'utilisation des données contenues dans le passe sanitaire, lorsque l'utilisateur l'a enregistré dans l'application, afin d'afficher des *« recommandations sanitaires personnalisées »*. L'autorité a autorisé l'affichage de ces recommandations qui portent, entre autres, sur la nécessité d'une dose de rappel pour bénéficier d'un schéma vaccinal complet contre la Covid-19.

Selon la CNIL, il s'agit d'une modification « importante » de la fonctionnalité "Carnet" de TousAntiCovid, puisqu'elle ne permettait, jusqu'à présent, que le stockage du passe sanitaire. Or, les nouvelles modalités qui sont envisagées nécessitent d'utiliser les données contenues dans les passes sanitaires enregistrés au sein de l'application, et notamment les données nominatives. Les recommandations visent *in fine* à informer les utilisateurs sur les mesures à prendre afin de bénéficier d'un passe sanitaire valide, ou encore à les informer sur la marche à suivre lorsqu'ils intègrent dans l'application un résultat positif à un examen de dépistage à la Covid-19.

Dans son communiqué, la CNIL affirme que ces évolutions sont justifiées par *« les récentes annonces du gouvernement concernant la nécessité, pour conserver un passe sanitaire valide, d'effectuer pour certaines personnes un rappel vaccinal »*, ou par la diminution de la durée de validité des tests de dépistage à 24 heures au lieu de 72 heures.

Toutefois, l'autorisation de la CNIL est soumise à des *« garanties importantes »*. Les données doivent être lues uniquement en local, sur le terminal de l'utilisateur, et ne doivent pas être associées à d'autres traitements de données, précise la CNIL dans un communiqué de presse. De plus, les personnes doivent pouvoir être informées et s'opposer, si elles le souhaitent, à ce que les données soient utilisées pour ces nouvelles fonctionnalités.

Dans cette même délibération, la CNIL a par ailleurs autorisé la prolongation de l'application jusqu'au 31 juillet 2022.

Toutefois, la Commission réitère ses alertes sur la tentation d'un *« solutionnisme technologique »*, rappelant que *« la multiplication des dispositifs numériques mis en œuvre dans le cadre de la gestion de l'épidémie rend absolument nécessaire une évaluation quantifiée et objective de leur efficacité dans la contribution à la lutte contre la Covid-19 ».*

[291] La CNIL publie son quatrième avis adressé au Parlement sur les conditions de mise en œuvre des dispositifs contre la COVID-19

- *L'exécutif éprouve de profondes difficultés à traduire la loi dans des mesures réglementaires d'application*

L'inflation législative induit nécessairement des difficultés fonctionnelles lors de la phase de mise en application de la loi, puisqu'elle met fortement sous tension les instances en charge de la rédaction et de la validation des mesures réglementaire d'application.

Cet état de fait se manifeste en particulier dans le registre numérique, participant ainsi à entretenir le retard systémique du droit sur les évolutions de la société 2.0.

En effet, le contrôle par le Parlement de l'application de loi pour une République numérique (Loi n° 2016-1321 du 07/10/2016 parue au JO n° 235 du 08/10/2016)[292], s'il fait apparaître qu'un nombre très important de mesures réglementaires ont bien été prises par le Gouvernement, un nombre tout aussi significatif ne l'ont pas encore été en novembre 2021, soit cinq années plus tard.[293]

Bien évidemment, une telle situation est rigoureusement incompatible ni avec la promesse d'une République numérique irréprochable, ni avec les obligations contractuelles et morales qui lient l'Etat aux citoyens.

Mais elle ne procède pas uniquement de cette inflation législative paralysante dénoncée ci-avant. Elle procède aussi, nécessairement, des téléscopages aussi nombreux que stérilisants avec les agendas politiques et juridiques des instances internationales et européennes dont les productions viennent s'imposer au droit national, dès lors qu'elles rejoignent le bloc conventionnel après leur ratification définitive, s'agissant des premières, ou qu'elles sont adoptées, s'agissant des secondes.

Elle procède enfin également de l'affaiblissement structurel de l'administration de l'Etat consécutif aux différentes phases de réforme auxquels il a été soumis depuis l'avènement de la RGPP, ne disposant plus des ressources intellectuelles et physiques requises pour lui permettre d'affronter la variété et la complexe d'un monde soumis aux grandes transformations de l'époque, en prenant la mesure des risques encourus.

- *Le processus législatif connaît une évolution qui inquiète*

La Fondation Robert Schuman, en partenariat avec un réseau universitaire européen de recherches initié par l'Université de Lille en 2016 autour du sujet "*Le Parlement et le temps*", a réalisé une série de rapports visant à rendre compte de "*l'impact de la crise sanitaire sur le fonctionnement des Parlements nationaux*" en Europe. Ont particulièrement été questionnés l'impact de la crise sanitaire sur la procédure parlementaire, ainsi que sur le contrôle parlementaire du gouvernement.

Le rapport sur la France se conclut ainsi : *« L'état de santé du Parlement français durant la crise sanitaire était donc assez alarmant. Il l'était d'autant plus que les règles adaptées pour fonctionner avaient des bases juridiques fragiles (décisions du Président ou de la Conférence des présidents). On peut même se demander si la condition de l'interruption du fonctionnement régulier des pouvoirs publics, nécessaire à l'activation de l'article 16 de la Constitution n'était pas réunie, ce qui aurait pu permettre d'autres garanties, peut-être meilleures, telle la consultation systématique du Conseil constitutionnel. C'est parce que les parlementaires ont été unanimes que les assemblées ont pu fonctionner ainsi. Comme le relève Sylvain Waserman, président du groupe de travail de l'Assemblée nationale chargé d'anticiper le mode de*

[292] *Contrôle de l'application de loi pour une République numérique :* https://www.senat.fr/application-des-lois/pjl15-325.html
[293] *Mesures réglementaires prévues par la loi et non encore prises par le Gouvernement :* https://www.senat.fr/application-des-lois/pjl15-325.html#non_pris

fonctionnement des travaux parlementaires en période de (futures) crises : « Il importe de se demander ce qui se serait passé en l'absence d'unanimité ».

Une réflexion est donc menée pour anticiper de nouvelles situations de crise et les modalités pour y répondre, ce qui permettrait, sans doute, de trouver un fonctionnement plus satisfaisant du Parlement qu'il ne l'a été. Mais, dès à présent, les assemblées françaises pourraient « compenser » cette apathie en donnant un nouveau souffle au travail parlementaire. Pour cela, il leur faudrait examiner et voter de manière sérieuse les projets de loi de ratification des ordonnances prises sur son habilitation pendant la crise ; il faudrait aussi que la commission d'enquête du Sénat et la mission d'information de l'Assemblée procèdent à un contrôle, certes à rebours, mais précis de l'action du Gouvernement et des autorités administratives avant et pendant cette crise. À l'heure où les craintes d'une reprise de l'épidémie se font plus fortes, il en va de la survie même du Parlement français. Donc de la démocratie. »[294]

Abordant la question complexe de l'inflation législative en France, Guillaume Flori relève : *« L'avènement de la société de l'information conduit à légiférer dans l'urgence ou pour répondre à une demande médiatique. Il est clair qu'aujourd'hui la loi est beaucoup plus technique et parfois mal pensée. C'est désormais l'urgence*[295] *qui semble régir l'ordre législatif, plaçant l'efficience au second plan. Le rôle symbolique de la loi n'y est pas étranger. De ce fait, la loi devient peu lisible pour les sujets de droit. Cette illisibilité fait vaciller la sécurité juridique. En effet, une incompréhension ou une instabilité de la norme peut conduire à d'importants préjudices pour le sujet de droit.*

En 1999, le Conseil constitutionnel a dégagé l'objectif à valeur constitutionnelle d'accessibilité et d'intelligibilité du droit[296]*, composante de la sécurité juridique*[297]*, lequel suppose que :*

- *La norme puisse être accessible aux personnes (physiques et morales), par Internet ou dans les codes par exemple ;*
- *La norme puisse être comprise par les personnes. Ce qui suppose une rédaction de qualité et lisible auprès des profanes.*

Dans une autre décision[298]*, le Conseil constitutionnel a précisé la portée de cet objectif, tout en ajoutant aussi un principe de clarté de la loi (portant sur du concret). Ainsi, le législateur doit "adopter des dispositions suffisamment précises et des formules non équivoques". Il s'agit de prévenir les risques d'arbitraire du pouvoir politique. Dans la même décision, le Conseil constitutionnel s'octroie la faculté d'interpréter les textes inintelligibles. Il le fait lorsque l'interprétation de la loi en cause "est nécessaire à l'appréciation de sa constitutionnalité".*

Au niveau européen, la Cour européenne des droits de l'Homme exige que la norme soit « énoncée avec assez de précision pour permettre au citoyen de régler sa conduite"[299]*. Elle ajoute que le texte doit permettre une certaine prévisibilité. Il s'agit de pouvoir se préparer*

---

[294] *Cf.* https://www.robert-schuman.eu/fr/doc/ouvrages/FRS_Parlement_francais_Covid-19.pdf

[295] *Cf.* notamment à cet égard François Saint-Bonnet *in « États d'urgence » in* Revue Esprit https://esprit.presse.fr/article/francois-saint-bonnet/etats-d-urgence-43438?fbclid=IwAR1JQmk3UcS9hRHRlm2E3pf4i6BhBDrvTSSr8qNg7Z-ywnu366YWApxARNM

114

[296] *Décision n° 99-421 DC du 16 décembre 1999 relative à la Loi portant habilitation du Gouvernement à procéder, par ordonnances, à l'adoption de la partie législative de certains codes :* https://www.conseil-constitutionnel.fr/decision/1999/99421DC.htm

[297] La sécurité juridique est un principe du droit qui a pour objectif de protéger les citoyens contre les effets secondaires négatifs du droit, en particulier les incohérences ou la complexité des lois et règlements, ou leurs changements trop fréquents (insécurité juridique). Ce principe peut lui-même se décliner en plusieurs exigences. La loi doit être : - compréhensible ; - prévisible ; - normative ; - et porter sur le domaine de compétence du législateur. La loi, en tant que règle de droit, doit aussi être générale, obligatoire, et coercitive.

[298] *Décision n° 2001-455 DC du 12 janvier 2002 relative à la Loi de modernisation sociale :* https://www.conseil-constitutionnel.fr/decision/2002/2001455DC.htm

[299] *Cf.* https://www.doctrine.fr/d/CEDH/HFJUD/CHAMBER/1979/CEDH001-62140

face à une situation juridique donnée. Cependant, ces gardes fous constitutionnels et conventionnels ne semblent pas avoir eu l'effet escompté. »[300]

Pour mettre en œuvre la première proposition de son étude annuelle 2016 « Simplification et qualité du droit », le Conseil d'État a constitué en novembre 2017 un groupe de travail chargé de concevoir un référentiel de la mesure de l'inflation normative. Dans le cadre des travaux de ce groupe, un tableau de bord des indicateurs de suivi de l'activité normative a été élaboré par le Secrétariat général du Gouvernement. Le Premier ministre en a décidé la mise en ligne sur le site Légifrance le 7 mars 2028. L'assemblée générale du Conseil d'État a adopté le 3 mai 2018 une étude retraçant les travaux d'élaboration de ce tableau de bord, qui est sans précédent à cette échelle, et présente également des propositions susceptibles de conduire à l'enrichissement de ce tableau. *« Le Conseil d'État marque son attachement à ce que ce travail de grande importance pour documenter un phénomène toujours dénoncé, mais jamais documenté jusqu'à présent, fasse l'objet de mises à jour régulières et, le cas échéant, de compléments, en principe sur une base annuelle. Il convient en effet d'enrichir progressivement la liste des indicateurs de l'inflation normative, en l'étendant notamment aux normes émanant des autorités administratives ou publiques indépendantes, et de s'intéresser aussi à des indicateurs proches et importants, comme les indicateurs de stabilité/ instabilité de la norme et ceux permettant de mesurer l'origine de l'inflation normative et les branches du droit qui sont les plus affectées par ce phénomène. »*[301]

Dans un article intitulé '*Crise de la démocratie ou crise dans la démocratie'*[302], Thomas Branthôme, maître de conférence en Histoire du droit et des idées politiques, relève : *« En 2018, dans un essai retentissant sur le sujet*[303]*, le politologue Yasha Mounk, de nature pourtant modéré, alertait les plus incrédules. La « démocratie », écrivait-il, est en danger de mort. Parce que deux périls la menacent : la démocratie illibérale et le libéralisme antidémocratique. En 2020, l'inquiétude est particulièrement vive pour le cas français puisqu'au vu de ces derniers mois, la France semble s'être fragilisée sur l'un et l'autre des deux versants. Alors qu'Emmanuel Macron avait été élu en promettant une version* intégrale *du libéralisme (c'est-à-dire économique et sociétale) comme le préconisaient certains grands libéraux du XIX*e *siècle (Benjamin Constant, Jules Simon), sa majorité multiplie sous son mandat des lois considérées comme liberticides. Dans 'Les Politiques', Aristote définit la « démocratie » comme le régime au sein duquel les citoyens exercent le pouvoir « à tour de rôle ». On ne le dit presque plus, mais c'est là en principe le point fondamental qui doit permettre à la démocratie de tenir et de bénéficier du consentement de ses citoyens. Par une pratique aléatoire et circulaire du pouvoir, chacun étant amené dans son existence à être tantôt « gouverné » tantôt « gouvernant » s'investit pleinement dans la vie démocratique. Aujourd'hui, cette règle d'or de la démocratie est lettre morte. Qui peut penser une seule minute qu'au sein des classes populaires existe ce sentiment d'alternance « gouverné/gouvernant » ? Notre époque est profondément marquée par la disparition de ce cycle mais également – phénomène plus neuf –, par l'affaiblissement significatif de la colonne d'équilibre de la théorie du gouvernement représentatif, la croyance dans le couple « représentant/représenté ». »*

Dans l'ouvrage qu'il consacra à l'Etat de droit[304], le professeur Jacques Chevalier précise que « *L'État de droit substantiel suppose que la règle de droit présente un ensemble d'attributs*

[300] *L'inflation législative en France :* https://juridiquoi.com/linflation-legislative-en-france/
[301] *Mesurer l'inflation législative :* https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes/mesurer-l-inflation-normative
[302] *Crise de la démocratie ou crise dans la démocratie : https://theconversation.com/crise-dans-la-democratie-ou-crise-pour-la-democratie-150188?fbclid=IwAR0NQuORvC0Nxc5f0TyQGoJc25Kw_4erHLb5dUapDXueM-dQu5u6zT3ujYo*
[303] *Le peuple contre la démocratie* : https://www.editions-observatoire.com/content/Le_peuple_contre_la_democratie
[304] *L'Etat de droit* : https://www.persee.fr/doc/polix_0295-2319_1994_num_7_28_1893

substantiels qui lui permettent de remplir la fonction qui lui incombe : elle doit constituer pour les destinataires un cadre clair, précis, stable qui leur apporte des éléments de certitudes nécessaires et leur donne la possibilité de prévoir les conséquences de leurs actes. »

La sécurité juridique est *« une garantie contre l'arbitraire et apparaît comme une exigence fondamentale de l'État de droit ».*

Le principe de sécurité juridique implique l'amélioration de la qualité de la production juridique et la protection contre l'instabilité des règles. Il implique plusieurs choses :

- *L'accessibilité et l'intelligibilité de la loi* : il s'agit ici de simplifier les textes, et de faire en sorte que le droit soit connu de tous et compris par tous. C'est devenu un objectif à valeur constitutionnelle par les décisions de 1999 et 2003 ;
- *La qualité de la loi* : il s'agit d'aller vers une meilleure rédaction en se tournant vers la légistique (la manière dont on fait les lois), et en évitant les neutrons législatifs qui n'ont pas de charge normative ;
- *La prévisibilité* : autrement dit la stabilité de la règle de droit dans le temps, permettant aux individus de s'organiser autour de la règle de droit sans risque pour eux de voir leurs situations changer de manière arbitraire par une intervention législative.

Or, lorsqu'ils sont saisis, le Conseil d'Etat et le Conseil constitutionnel prennent parfois des arrêts et décisions qui viennent bloquer des textes de loi pour leur non-conformité aux dispositions du droit fondamental ou des principes généraux du droit.

En particulier, le 3 décembre 2020, le Conseil constitutionnel a rendu publique sa décision par laquelle il établissait notamment que les articles 30, 51, 63, 65, 66, 68, 69, 71, 74, 80, 81, 85, 86, 88, 102, 103, 104, 110, 115, 116, 123, 129, 135, 136, 137 et 149 de la loi d'accélération et de simplification de l'action publique ne sont pas conformes à la Constitution.[305]

Le 15 janvier 2021, le Conseil constitutionnel décide à l'égard d'une Question prioritaire de constitutionnalité - QPC - portant sur l'utilisation de la visioconférence sans accord des parties devant les juridictions pénales dans un contexte d'urgence sanitaire, que « *le premier alinéa de l'article 5 de l'ordonnance n° 2020-303 du 25 mars 2020 portant adaptation de règles de procédure pénale sur le fondement de la loi n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19 est contraire à la Constitution. »*[306]

Le 1er avril 2021, il juge contraire à la Constitution la résolution adoptée le 1er mars par l'Assemblée nationale, qui vise à organiser les travaux parlementaires en période de crise.[307]

Pour certains juristes français, *« le constat est aujourd'hui sans appel, non seulement la France ne dispose plus d'un pouvoir législatif digne de ce nom, mais l'organe dévalué qui en tient lieu a été absorbé par le pouvoir exécutif. Législatif et exécutif ne sont plus séparés dans notre pays. […] L'abaissement drastique de la valeur normative de la Constitution au cours des 20 dernières années a permis de mettre progressivement en place un nouveau système à valeur de nouveau régime qui entretient des rapports très lointains avec un système légitime de démocratie représentative. Des 92 articles initiaux, après une bonne trentaine de révisions, il n'en reste aujourd'hui que 30 dans une Constitution qui en compte désormais 108. Et n'a plus*

[305] *Cf.* Décision n° 2020-807 DC du 3 décembre 2020 - Loi d'accélération et de simplification de l'action publique : https://www.conseil-constitutionnel.fr/decision/2020/2020807DC.htm?fbclid=IwAR2LVMi3piT47lEczc2Sesjo1_eMwgmOSUhFR89IrLEYfW2Ku4RzA3qX80g

[306] *Cf.* www.conseil-constitutionnel.fr/decision/2021/2020872QPC.htm

[307] *Cf.* Décision n° 2021-814 DC du 1er avril 2021 : https://www.conseil-constitutionnel.fr/decision/2021/2021814DC.htm?fbclid=IwAR0_gti8TtVJB-XgxLSKFKL65ZpV45NKrX-2dCFRYhC2teL4hzdgp6Gtsn8

grand-chose à voir avec le texte proposé par Charles de Gaulle et adopté par le peuple français avec 82 % des voix en octobre 1958. » (Régis de Castelnau, avocat au Barreau de Paris).

Dans son ouvrage intitulé *'Liberté et Droit'*, Bruno Leoni, affirmait en 1921 que la loi est devenue le pire ennemi du droit.[308]

En 2021, Raphaël Roger Devisme prolonge sa pensée en ces termes :

« Dès lors qu'elle est artificielle et arbitraire, elle ne remplit plus sa fonction régulatrice de la société. L'inflation législative a conduit à une instrumentalisation de la loi par le politique, amenant à une dépréciation de sa valeur dans la société. La mise en place au niveau rédactionnel de neutrons législatifs sans aucune charge législative certaine, a obstrué et complexifié les textes normatifs, empêchant une bonne assimilation de ces derniers. La multiplication des textes et leurs plus grandes complexités ont donc diminué leur assimilation et ont donc conduit à un déficit d'exécution de ces mêmes textes. Enfin, les lois sont le plus souvent frappées par leurs obsolescences du fait de leur inapplicabilité.

L'activité incessante du législateur conduit à une baisse de la valeur que l'on accorde à la loi. Le droit, aujourd'hui, ne se découvre plus. Il est produit d'en haut de manière centralisée.

Pour reprendre Bruno Leoni : « Le citoyen s'adapte de plus en plus à l'idée que la législation ne correspond pas à une volonté commune, c'est-à-dire une volonté que l'on suppose partagée par tous, mais à l'expression de la volonté particulière de certains individus et de groupe qui ont eu suffisamment de chance pour mettre de leur côté une majorité contingente de législateurs à un certain moment ».

De même que pour les codes qui ne résultent plus d'une légitimité coutumière, mais comme le dit Philippe Fabry, d'une légitimité législative.

Pour Bruno Leoni : « La législation ordinaire et les codes sont de plus en plus présentés comme l'expression directe de la volonté contingente de ceux qui les décrètent, avec souvent l'idée sous-jacente que leur fonction consiste à énoncer non pas le droit résultant d'un processus séculaire mais ce qu'il devrait être selon une approche complètement nouvelle et des décisions sans précédent. »

Ainsi, le sage législateur, « qui tire instruction des difficultés que les juges rencontrent dans les procès, pour reconnaître les lacunes et les vices de ses propres lois (Emmanuel Kant) », semble disparu *aujourd'hui. L'un des arguments justifiant l'intervention du législateur est celui du vide juridique. [...]*

L'argument du vide juridique est couramment utilisé par le législateur pour justifier son intervention. Les médias reprennent également cette expression pour justifier une intervention du législateur, généralement à la suite d'un fait divers, le plus souvent en matière pénale. Très souvent, le législateur, ne connaissant pas lui-même les textes existants du fait de leur nombre important, fera une loi qui existe déjà, sous une autre dénomination, dans un code déjà existant. Pourtant, et il faut le dire, le vide juridique n'existe pas. » [309]

En réponse à *« cette crise démocratique,* M[me] Yaël Braun-Pivet, présidente de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République de l'Assemblée nationale, établit dans un rapport daté du 1[er] décembre *« 25 propositions concrètes*

[308] *Cf.* à son sujet notamment *Liberté et droit dans la pensée de Bruno Leoni* : https://www.academia.edu/10294820/Libert%C3%A9_et_droit_dans_le_pens%C3%A9e_de_Bruno_Leoni

[309] *La sécurité juridique ou l'idéal du sage législateur :* https://www.contrepoints.org/2021/11/21/414407-la-securite-juridique-ou-lideal-du-sage-legislateur

pour rééquilibrer les pouvoirs » qui font office de *« plaidoyer pour un Parlement renforcé »*[310]. *« On vient de vivre un mandat où le rôle du Parlement, de la démocratie représentative a été très questionné en France ». « Nous allons vite, nous n'arrivons pas à travailler au fond et le tout dans des oppositions stériles… Je comprends qu'il y ait presque un désaveu du Parlement de la part de nos concitoyens. C'est justement parce que trop de gens ont cette vision de nos assemblées qu'il est à mon sens urgent et fondamental de changer les choses. »*

« *Il ne faut toucher aux lois que d'une main tremblante* » conseillait jadis Montesquieu qui ajouta : *« les lois inutiles affaiblissent les lois nécessaires. »*

Le regard que portait jadis Georges Clémenceau sur l'activité parlementaire prend plus que jamais tout son sens : *« Le Parlement est le plus grand organisme qu'on ait inventé pour commettre des erreurs politiques, mais elles ont l'avantage supérieur d'être réparables, et ce, dès que le pays en a la volonté. »*

- *L'exécutif éprouve de profondes difficultés à traduire la loi dans des mesures réglementaires d'application*

L'inflation législative induit nécessairement des difficultés fonctionnelles lors de la phase de mise en application de la loi, puisqu'elle met fortement sous tension les instances en charge de la rédaction et de la validation des mesures réglementaire d'application.

Cet état de fait se manifeste en particulier dans le registre numérique, participant ainsi à entretenir le retard systémique du droit sur les évolutions de la société 2.0.

En effet, le contrôle par le Parlement de l'application de loi pour une République numérique (Loi n° 2016-1321 du 07/10/2016 parue au JO n° 235 du 08/10/2016) [311], s'il fait apparaître qu'un nombre très important de mesures réglementaires ont bien été prises par le Gouvernement, un nombre tout aussi significatif ne l'ont pas encore été en novembre 2021, soit cinq années plus tard.[312]

Bien évidemment, une telle situation est rigoureusement incompatible ni avec la promesse d'une République numérique irréprochable, ni avec les obligations contractuelles et morales qui lient l'Etat aux citoyens.

Mais elle ne procède pas uniquement de cette inflation législative paralysante dénoncée ci-avant. Elle procède aussi, nécessairement, des téléscopages aussi nombreux que stérilisants avec les agendas politiques et juridiques des instances internationales et européennes dont les productions viennent s'imposer au droit national, dès lors qu'elles rejoignent le bloc conventionnel après leur ratification définitive, s'agissant des premières, ou qu'elles sont adoptées, s'agissant des secondes.

Elle procède enfin également de l'affaiblissement structurel de l'administration de l'Etat consécutif aux différentes phases de réforme auxquels il a été soumis depuis l'avènement de la RGPP, ne disposant plus des ressources intellectuelles et physiques requises pour lui permettre d'affronter la variété et la complexe d'un monde soumis aux grandes transformations de l'époque, en prenant la mesure des risques encourus.

- *La possible dématérialisation du processus électoral suscite des interrogations*

Le recours au vote électronique suscite des craintes multiples.

---

[310] *Plaidoyer pour un Parlement renforcé. 25 propositions concrètes pour rééquilibrer les pouvoirs* (Fondation Jean-Jaurès) : https://www.jean-jaures.org/publication/plaidoyer-pour-un-parlement-renforce-25-propositions-concretes-pour-reequilibrer-les-pouvoirs/

[311] *Contrôle de l'application de loi pour une République numérique : https://www.senat.fr/application-des-lois/pjl15-325.html*

[312] *Mesures réglementaires prévues par la loi et non encore prises par le Gouvernement :* https://www.senat.fr/application-des-lois/pjl15-325.html#non_pris

En septembre 2017, le Premier ministre Edouard Philippe déclara : *« Nous nous posons d'ores et déjà la question de savoir comment nous prémunir contre certaines formes d'ingérence ou de piratage de secteurs clés de notre vie démocratique et du dérèglement de notre vie démocratique (média, élections), de notre vie économique (énergie) ou de notre indépendance nationale.* »

Si un rapport sénatorial publié en décembre 2017, en souligne les atouts (facilitation du vote pour les handicapés, accélération du recensement des votes) : « *Leur usage n'a jamais posé de difficultés. Les électeurs, les élus, les agents municipaux s'accordent sur la simplicité et la fiabilité du dispositif. Malgré cela, ces machines suscitent des oppositions souvent très doctrinales* », il pointe néanmoins du doigt l'approbation du Conseil constitutionnel[313] et du Conseil d'Etat[314] sur le fait que ces machines « *conservent le secret du vote* », *tandis que le ministère de l'Intérieur considérait que « leurs fonctionnalités techniques garantissaient la sincérité du scrutin* »[315].

Laurent Nuñez, alors secrétaire d'Etat auprès du ministre de l'Intérieur, a fait valoir la position du gouvernement : *« Le moratoire gelant depuis onze ans paraît constituer, à ce jour, un point d'équilibre. Cela explique d'ailleurs probablement que le ministère de l'Intérieur reçoive autant de demandes d'élus voulant interdire strictement ces machines que d'élus voulant au contraire développer leur usage et faire homologuer de nouveaux modèles ».* Pour justifier la prudence du gouvernement, Laurent Nuñez a rappelé que ces appareils rendent impossible le contrôle du dépouillement – principe *« auquel le Conseil constitutionnel a eu l'occasion de dire son attachement »*, et qu'ils peuvent être potentiellement exposés à un risque « cyber » qui viserait à entraver le bon déroulement du scrutin ou à en modifier les résultats.

Et *quid* alors de l'anonymat qui préside à tout vote lors d'élections démocratiques en France ?

Alors que la France était toujours placée sous le régime exceptionnel de l'état d'urgence sanitaire, le gouvernement a déposé le 16 février 2021 un amendement sur le vote par anticipation sur une machine à voter, dans le cadre de l'examen du projet de loi organique relatif à l'élection du Président de la République, qui précise que ce vote par anticipation peut être effectué sur une machine à vote, dont les suffrages seraient dépouillés « *en même temps que les autres bureaux de la commune afin d'éviter les risques de fraude ou d'influence sur le vote des autres électeurs* ». Parmi les arguments évoqués par la ministre déléguée auprès du ministre de l'Intérieur, en charge de la citoyenneté, qui a présenté l'amendement en séance publique, cette proposition de « *vote numérique favorise notamment le vote de gens isolés, des gens qui travaillent le dimanche, des jeunes et ceux qui viennent de déménager. (...) Nous proposons que ce soit l'Etat qui prenne en charge ces machines, pour ne pas imposer de coûts supplémentaires aux communes* ». Cette proposition se veut être une « troisième voie » entre l'inaction et une modernisation excessive. Les électeurs pourraient choisir une commune de leur choix parmi la liste proposée, et dans un délai imparti. Cette proposition sera d'abord proposée à une échelle « raisonnable » avant d'être étendue davantage.

La commission des lois du Sénat s'est opposée à une large majorité à un tel amendement qui, selon elle, « *relève du bricolage* ».

Dans un communiqué[316], elle a considéré que, sur le fond, l'amendement était de nature à « *alimenter la suspicion sur la sincérité de l'élection présidentielle et à remettre en cause la légitimité du président élu. Les machines à voter, en effet, sont soumises à un moratoire depuis 2008 : seules 66 communes en sont équipées, le gouvernement interdisant aux autres communes*

[313] *Cf.* https://www.conseil-constitutionnel.fr/decision/2012/2012154PDR.htm
[314] *Cf.* https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000023493752
[315] *Cf.* http://questions.assemblee-nationale.fr/q14/14-88162QE.htm
[316] *Cf.* http://www.senat.fr/presse/cp20210217.html

119

d'acquérir des machines à voter ». Depuis 2008 en effet, un moratoire restreint l'utilisation des machines à voter aux seules communes qui avaient opté pour cette modalité à cette date.

La commission rappelle également que « *le Conseil constitutionnel a alerté les pouvoirs publics à de nombreuses reprises sur les risques de fraude liés à l'utilisation des machines à voter, notamment après l'élection présidentielle de 2007, de même que l'Agence nationale de la sécurité des systèmes d'information (ANSSI)* ».

Le président de la commission des lois a par ailleurs souligné dans l'hémicycle que l'insécurité des machines à voter faisait l'objet d'un « *consensus auprès de tout le monde* », y compris du directeur général de l'ANSSI qui a « *confirmé clairement qu'il était hostile à l'utilisation des machines à voter, compte tenu de leur obsolescence et du risque de cyberattaque* », tout en ajoutant : « *la condition substantielle est la sécurité absolue. Et là, nous ne l'avons pas*

- *La docilité présumée d'un Conseil d'Etat*[317] *qui poursuit pourtant son action en faveur d'une meilleure accessibilité au juge comme à ses décisions*

Au moment où l'on s'interroge sur les menaces que fait peser sur la démocratie américaine la politisation de la Cour suprême, plusieurs décisions prises par le Conseil d'Etat français au cours de la gestion de la crise sanitaire interrogent l'état de la démocratie française.

Selon le professeur Dominique Rousseau, s'agissant de la France : *« On est toujours dans un Etat de droit, mais il y a des pistes qui s'effritent, et un jour, où va-t-on se retrouver ? »*

Eugénie Mériau déplore un recul de l'Etat français à l'égard des droits humains, recul également « *noté avec une profonde inquiétude* » par le Haut-Commissariat aux Droits de l'Homme des Nations Unies, ainsi qu'une détérioration de la qualité de la démocratie en France, telle qu'enregistrée par les indicateurs de V-Dem mesurant les évolutions dans le temps des régimes politiques à travers le monde[318].

Depuis le mouvement des *« gilets jaunes »*, et alors même qu'il considère que « *le respect de la dignité de la personne humaine est une des composantes de l'ordre public* »[319], le Conseil d'État est régulièrement accusé de ne pas défendre les libertés fondamentales alors même que la Constitution lui confère les compétences requises à la fois pour nourrir le bloc de constitutionnalité dans sa fonction juridictionnelle en matière contentieuse (le Conseil d'Etat peut alors donner à un principe contenu dans une simple loi, une valeur constitutionnelle), et pour saisir le Conseil constitutionnel si au cours d'une instance devant une juridiction, il est soutenu qu'une disposition législative porte atteinte aux droits et libertés que la Constitution garantit.[320]

Le Conseil d'Etat est une institution qui joue un rôle central dans le fonctionnement de l'Etat. Les projets de loi, les ordonnances et certains décrets sont soumis à l'avis obligatoire du Conseil d'Etat. La Constitution précise les modalités de cette obligation.[321]

Au cours de la pandémie, lors des trois premiers mois, la haute juridiction administrative a été saisie de 327 recours – dont plus de 208 en référé – liés aux mesures prises pour lutter contre l'épidémie de Covid-19. Pour faire face à ce raz-de-marée, une *task force* d'une quinzaine de

[317] *Cf.* https://www.conseil-etat.fr/liens-utiles
[318] *Cf.* https://www.v-dem.net/fr/
[319] *La dignité de la personne humaine :* https://www.conseil-constitutionnel.fr/la-constitution/la-dignite-de-la-personne-humaine
[320] *Le Conseil d'État et la Constitution - rapports entre la norme suprême de l'État et la plus Haute juridiction administrative* : https://www.doc-du-juriste.com/droit-public-et-international/droit-administratif/dissertation/conseil-etat-constitution-459834.html
[321] Voir par exemple *Quels textes le Gouvernement doit-il soumettre au Conseil d'État ? :* https://www.vie-publique.fr/fiches/269095-les-textes-du-gouvernement-soumis-lavis-du-conseil-detat

juges a été constituée par Jean-Denis Combrexelle, le président de la section du contentieux. L'immense majorité des décisions rendues par le Conseil d'État entérinent les choix de l'exécutif. Le gouvernement n'a été enjoint par les juges à se réformer qu'à 10 reprises (comme le lever de l'interdiction de rassemblement dans les lieux de culte).

Lorsque le juge des référés du Conseil d'Etat a rejeté les demandes dirigées contre le décret n° 2021-955 du 19 juillet (abrogé par le décret n° 2021-1059 du 7 août 2021) par lequel le Premier ministre avait fixé à 50 le nombre de clients des établissements de loisirs devant présenter un passe sanitaire, Paul Cassia, professeur des universités en droit, s'exprimant en tant que partie requérante dans ce dossier, déplore : *« Ce lundi 26 juillet 2021 a acté la dégradation d'un Etat de droit déjà très imparfait en raison d'une séparation des pouvoirs défectueuse vers ce qu'il est possible d'appeler un « Etat de covid », où une institution juridictionnelle – ici, le Conseil d'Etat – homologue automatiquement, le doigt sur la couture du pantalon et à l'issue de procédures contentieuses sommaires, toutes les actions réglementaires du Premier ministre labellisées « lutte contre le covid-19 ».*[322]

Les dispositions inscrites dans la décision (ordonnance) de rejet de la part du Juge des Référés du Conseil d'Etat dans le cadre d'une procédure ouverte à la suite d'une requête appelant à suspendre l'exécution du décret n° 2021-1521 du 25 novembre 2021 modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaire à la gestion de la sortie de crise sanitaire, sont de nature à interpeler les citoyens de la République dans la mesure où elles participent à corroborer des décisions du gouvernement fondées sur des éléments d'appréciation très largement contestables et amplement contestés par la communauté scientifique internationale compétente.

« Le Conseil d'Etat a été jusqu'ici incapable de faire preuve d'indépendance et a validé docilement l'ensemble des décrets pris par le Gouvernement. » relèvent conjointement le Cercle Droit & Liberté. *« Il passe pour un auxiliaire de la police administrative »,* accuse le journaliste Yvan Stefanovitch, qui publie une enquête sur l'institution[323].

Si de tels griefs à l'encontre du Conseil d'Etat peuvent apparaître légitimes, il convient également de souligner son attachement constant à faire prévaloir l'intérêt général devant les situations complexes qui motivent son intervention.

Les préconisations contenues dans son étude annuelle de 2014 relative à la question des tensions générée par le numérique sur les droits fondamentaux (*cf. supra*) comme dans illustrent sa capacité à analyser et à anticiper de manière particulièrement pertinente les enjeux comme les risques encourus. Une étude du Conseil d'Etat publiée en 2018vait notamment exploré la question fondamentale de la prise en compte du risque dans la décision publique.

Cette étude formulait 32 propositions afin de mieux armer les décideurs publics dans la gestion des risques, pour qu'ils ne renoncent pas à mener des politiques publiques audacieuses au nom de l'intérêt général.

Une première série de propositions consistait, dans une logique de droit souple, à développer au sein de l'action publique des "bonnes pratiques essentielles" pour renforcer les capacités d'anticipation des risques.

Une deuxième série de propositions visait à transformer la gouvernance et la gestion publiques afin que l'action publique soit plus audacieuse.

[322] *De l'Etat de droit à l'Etat de covid :* https://blogs.mediapart.fr/paul-cassia/blog/080821/de-l-etat-de-droit-l-etat-de-covid

[323] *Petits arrangements entre amis,* Albin Michel

Enfin, plusieurs propositions visaient à améliorer le traitement contentieux de la responsabilité des acteurs publics devant les juges administratif, financier ou pénal.[324]

Sa compétence au fond ne saurait donc être mise en accusation.

Par souci de transparence et aux fins de légitimer son action par le droit, le Gouvernement a décidé de rendre public l'avis rendu par le Conseil d'État sur un projet de loi relatif à l'adaptation de nos outils de gestion de la crise sanitaire.[325]

Conscients que les données ont une importance capitale dans de nombreux domaines, et que leur exploitation suppose des efforts de clarification, de concertation, de normalisation et le cas échéant de régulation en matière de méthode de production et de conservation des données, de règles de partage et d'accès à ces dernières, d'élaboration des principes qui doivent guider leur traitement, de création des régimes d'appropriation et de partage des fruits de leur exploitation, la Chaire « Gouvernance et Régulation » de l'université Paris Dauphine-PSL et le Conseil d'État ont organisé en octobre 2020 un colloque en ligne spécifiquement dédié à la gouvernance et à la régulation des données, sujets au carrefour entre plusieurs domaines mais encore inexplorés par les pouvoirs publics.[326]

Du seul point de vue du droit, une difficulté majeure se pose au juge administratif qui réside dans la recherche de réponses robustes à la double question - cruciale - de la définition et de la fonction de l'intérêt général national en regard du point de vue du droit communautaire et dans le contexte de la Convention européenne des droits de l'homme, car il n'est pas certain qu'elles puissent être appréhendées en termes identiques si l'on s'attache à la jurisprudence de la Cour de Strasbourg et à celle de la Cour de Luxembourg.[327]

La volonté générale et l'intérêt général qui en est l'expression sont des concepts fondés sur une idéalisation de l'homme et du peuple. L'application de ces concepts les confronte à la société réelle et montre leurs limites, largement dépassées par suite de la complexité des sociétés démocratiques modernes.[328]

« Y *a-t-il encore sens aujourd'hui à parler d'intérêt général dans un contexte où les sociétés complexes semblent éclatées en une multiplicité parcellaire de réseaux ? L'intérêt général est-il mort, tué par le pluralisme de la post-modernité, ou à réinventer ?* » s'interroge Camille Chamois (docteure en philosophie dont les travaux se situent à la croisée de la sociologie, de la philosophie et de l'anthropologie politique).

---

[324] *La prise en compte du risque dans la décision publique :* https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes/la-prise-en-compte-du-risque-dans-la-decision-publique

[325] *Cf.* https://www.conseil-etat.fr/ressources/avis-aux-pouvoirs-publics/derniers-avis-publies/avis-sur-un-projet-de-loi-relatif-a-la-gestion-de-la-crise-sanitaire

[326] *Cf.* https://www.conseil-etat.fr/actualites/colloques-seminaires-et-conferences/voir-ou-revoir-gouvernance-et-regulation-des-donnees

[327] *Cf.* à cet égard Denys Simon *in L'intérêt général national vu par les droits européens :* *https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/pdf/Conseil/simon.pdf*

[328] *« L'intérêt général (contrairement à l'intérêt commun) se présente comme une position de surplomb prenant le point de vue de la société et des exigences de rationalisation supposées la structurer. [Il existe] trois options différentes concernant la nature et la détermination de cet intérêt. […]. L'approche du physiocrate, Lemercier de La Rivière dégage un intérêt général comme simple épiphénomène de l'intérêt des membres de la société qui cherchent tous à voir leurs gains individuels maximisés. L'approche de Saint-Simon, étudiée ensuite, renverse celle-ci car, pour ce dernier, les droits des individus dépendent entièrement de leur fonction sociale dans le système industriel de telle sorte que le seul intérêt commun des individus est leur intérêt d'industriel qui converge dans une coopération universelle, de telle sorte que l'intérêt général assumé par l'État exprime les exigences générales de l'industrie, c'est-à-dire de la production et de la distribution optimale des ressources dans tout le corps de la société. Enfin, l'approche de Léon Bourgeois permet d'articuler une thèse basée sur les droits et la protection des individus avec une thèse fondée sur la promotion d'intérêts sociaux irréductibles aux intérêts individuels. L'intérêt général incarné par l'État vise alors à réinscrire l'individu dans les exigences et les obligations civiques notamment par des devoirs comme celui de payer l'impôt. »*
Pierre Crétois - *L'intérêt général au crible de l'intérêt commun :* https://journals.openedition.org/asterion/3031

La transformation numérique à marche forcée voulue, pensée, conçue et mise en œuvre en Europe par les pouvoirs publics sous l'emprise d'une offre technologique agissant comme un couperet les met à mal dès lors que cette idéalisation est altérée par des considérations qui ne relèvent pas de la double promesse démocratique et humaniste.

En particulier dans le contexte de la gestion publique d'une crise systémique qui la mobilise pour opérer les suivis individuels des personnes au travers des instruments exceptionnels dont l'usage est rendu possible par la mise en œuvre d'un régime d'exception, elle participe à miner l'Etat de droit.

Le Conseil d'Etat, dans son étude annuelle de 2021 au titre explicite *« Les états d'urgence : la démocratie sous contraintes »*[329] - mise en ligne le 29 septembre 2021 -, a jugé l'usage de l'état d'urgence délétère puisqu' *« il déstabilise le fonctionnement ordinaire des institutions, en bouleversant le rôle du Parlement et des institutions territoriales, banalise le risque, restreint les libertés de façon excessive et altère, à terme, la cohésion sociale ».*

Il propose une grille de lecture et d'emploi de ce régime d'exception ainsi qu'une série de propositions visant à améliorer l'action publique.

Comme il l'a montré durant la crise sanitaire en répondant, dans l'urgence, à la demande de justice, le juge administratif (Conseil d'État, cours administratives d'appel et tribunaux administratifs) a cherché constamment à améliorer l'efficacité de son action.

Pour traiter de ces enjeux, le Conseil d'État a organisé, le 29 octobre 2021, en partenariat avec l'Ordre des avocats au Conseil d'État et à la Cour de Cassation, un colloque intitulé *« Etre accessible, utile et compris : l'efficacité du juge administratif ».*

S'agissant de la garantie d'indépendance des juges des juridictions suprêmes et des inspecteurs généraux de la haute administration, le 14 janvier 2022, après avoir été saisi par plusieurs organisations de hauts fonctionnaires d'une QPC sur l'indépendance des inspections générales et la composition des commissions d'intégration au Conseil d'État et à la Cour des comptes en regard des dispositions de l'ordonnance n° 2021-702 du 2 juin 2021 portant réforme de l'encadrement supérieur de la fonction publique de l'État, prise sur le fondement de l'habilitation prévue à l'article 59 de la loi du 6 août 2019 de transformation de la fonction publique, dont le délai, prolongé par l'article 14 de la loi du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, est expiré, le Conseil constitutionnel a décidé : *« Article 1er. - Il n'y a pas lieu de statuer sur la question prioritaire de constitutionnalité portant sur l'article 6 de l'ordonnance n° 2021-702 du 2 juin 2021 portant réforme de l'encadrement supérieur de la fonction publique de l'État. Article 2. - L'article L. 133-12-3 du code de justice administrative et l'article L. 122-9 du code des juridictions financières, dans leur rédaction issue de la même ordonnance, sont conformes à la Constitution. »*[330]

- *Ni la Constitution ni le Conseil constitutionnel ne parviennent à rassurer les citoyens*

On perçoit bien, au travers de la grande variété comme de la nature des motifs d'inquiétude présentés ci-dessus que le droit fondamental est souvent sollicité pour statuer sur des enjeux fondamentaux. Des questions prioritaires de constitutionnalité ayant trait aux grands enjeux juridiques de cette transformation numérique ont été déposées en nombre auprès du Conseil constitutionnel.

Mais le droit fondamental lui-même comme les modalités de son élaboration et de son application sont en retard pour encadrer ces développements technologiques particulièrement

[329] *Les états d'urgence : la démocratie sous contraintes* : https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/les-etats-d-urgence-la-democratie-sous-contraintes
[330] *Décision n° 2021-961 QPC du 14 janvier 2022 :* https://www.conseil-constitutionnel.fr/decision/2022/2021961QPC.htm

rapides et les dérives et risques qui y sont associés, et notamment ceux que favorise l'IA, quand bien même les constitutionnalistes tentent, depuis quelques années, de se saisir de cette révolution numérique à l'oeuvre pour l'utiliser, l'encadrer ou le réglementer.

Alors qu'il constitue la plus haute juridiction de la République, et que les modalités de sa saisine ont été élargies à la faveur des dernières révisions de la Constitution [331] le Conseil constitutionnel est parfois mis en cause à l'égard du recul de l'Etat de droit.

Comment ne pas s'interroger devant la situation exceptionnelle qui a résulté du simple fait que le Conseil constitutionnel[332] a déclaré conforme à la Constitution la loi organique dite d'urgence qui a suspendu jusqu'au 20 juin 2020 des délais d'examen des QPC : une loi *« sans précédent qui rend moins efficace le contrôle de constitutionnalité »* selon Nicolas Hervieu, enseignant à Sciences Po et spécialiste des libertés, et jugée *« gravissime »* par le professeur de droit Paul Cassia. Ainsi le Conseil constitutionnel s'est vu imposer par une loi organique le principe de différer ses réponses aux recours citoyens contestant certaines dispositions prises au titre de l'état d'urgence sanitaire ?

Les avocats William Bourdon et Vincent Brengarth ont saisi le Défenseur des droits, constatant que *« Cette loi, c'est une dérive extrêmement préoccupante. C'est une sorte d'instrument pour venir neutraliser le contrôle de constitutionnalité. Sur l'état d'urgence qui a suivi les attentats de 2015, il y avait eu des censures du Conseil constitutionnel postérieures à la loi. Dans le cas présent, imaginez : des personnes peuvent être condamnées par comparution immédiate sur le fondement d'un délit dont elles auraient pu contester la constitutionnalité, notamment en termes de proportionnalité. Sans effet impératif sur les délais, la peine sera déjà exécutée avant de pouvoir être contestée devant le Conseil constitutionnel. Les QPC sont des moyens de droit essentiels aujourd'hui, d'autant plus si l'on considère les circonstances dans lesquelles cette loi a été adoptée : sans concertation, sans temps du débat […] Il est intéressant de constater que les situations de crise amènent à une mutation temporaire de l'Etat de droit dans un sens de restriction du contrôle juridictionnel… Il ne nous reste plus que les autorités administratives indépendantes pour rappeler le droit, dans le cadre de leurs prérogatives. Nous attendons du Défenseur des droits qu'il critique la décision du Conseil constitutionnel (de valider la loi le 26 mars) et qu'il fasse au moins une communication pour rappeler que cette loi n'empêche pas de respecter les délais habituels d'une question prioritaire de constitutionnalité. »*

Or, sur l'essentiel des dispositions soumises à examen (procédure d'examen de la loi, conditions d'engagement de la responsabilité pénale en cas de catastrophe sanitaire, …), le Conseil constitutionnel a établi la conformité à la Constitution et au droit. Néanmoins, il a également établi une non-conformité partielle ainsi que des réserves à l'égard de certaines dispositions de la loi ayant trait à des restrictions de liberté individuelle.

Le Conseil constitutionnel a rappelé que *« La Constitution n'exclut pas la possibilité pour le législateur de prévoir un régime d'état d'urgence sanitaire. Il lui appartient, dans ce cadre, d'assurer la conciliation entre l'objectif de valeur constitutionnelle de protection de la santé et le respect des droits et libertés reconnus à tous ceux qui résident sur le territoire de la République. Parmi ces droits et libertés figurent la liberté d'aller et de venir, composante de la liberté personnelle, protégée par les articles 2 et 4 de la Déclaration de 1789, le droit au respect*

[331] *Comment saisir le Conseil constitutionnel ?*
https://www.conseil-constitutionnel.fr/le-conseil-constitutionnel/comment-saisir-le-conseil-constitutionnel

[332] *4 . Afin de faire face aux conséquences de l'épidémie du virus covid-19 sur le fonctionnement des juridictions, l'article unique de cette loi organique se borne à suspendre jusqu'au 30 juin 2020 le délai dans lequel le Conseil d'État ou la Cour de Cassation doit se prononcer sur le renvoi d'une question prioritaire de constitutionnalité au Conseil constitutionnel et celui dans lequel ce dernier doit statuer sur une telle question. Il ne remet pas en cause l'exercice de ce recours ni n'interdit qu'il soit statué sur une question prioritaire de constitutionnalité durant cette période.*
Cf. Décision n° 2020-799 DC du 26 mars 2020 : https://www.conseil-constitutionnel.fr/decision/2020/2020799DC.htm

de la vie privée garanti par cet article 2, la liberté d'entreprendre qui découle de cet article 4, ainsi que le droit d'expression collective des idées et des opinions résultant de l'article 11 de cette déclaration. »

Mais force est de constater que le Conseil constitutionnel n'a soulevé d'office aucune question de conformité à la Constitution et ne s'est donc pas prononcé sur la constitutionnalité des autres dispositions que celles examinées dans cette décision.

Il ressort de cet épisode important de la vie démocratique nationale française que, si un dispositif de contrôle parlementaire renforcé a bien été intégré à l'article 2 de la loi du 23 mars, sur l'insistance sénatoriale, on ne peut s'empêcher d'observer un certain recul par rapport à ce que prévoyait la loi de 1955.[333]

Cette situation nouvelle soulève l'épineuse question de la limitation des droits fondamentaux constitutionnels par l'ordre public.

L'un des cahiers du Conseil constitutionnel relatif à *'la limitation des droits fondamentaux constitutionnels par l'ordre public'* stipule : *« Que veut, que cherche la Nation dans l'œuvre de la Constitution qu'elle attend de nous ? La conciliation, la consolidation de l'ordre et de la liberté, cet éternel problème que poursuivent depuis si longtemps les sociétés humaines. À l'appui d'une interprétation constructive de la Constitution, le Conseil constitutionnel a progressivement indiqué les sources textuelles de l'ordre public. L'article 34 de la Constitution constitue le fondement principal à l'appui duquel est exposée la conciliation législative entre les exigences de l'ordre public et les droits garantis. À partir de cette clause, combinée avec les dispositions comprenant une réserve spécifique de compétence législative, les articles 4 et 5 de la Déclaration de 1789, ou encore la consubstantialité de l'ordre public et des libertés inhérente à la Constitution, le Conseil précise les composantes de l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public. Outre la sécurité des personnes et des biens et la prévention des atteintes à l'intégrité physique des personnes, il comprend la lutte contre le terrorisme et l'immigration irrégulière, la nécessité de garantir l'exécution des mesures d'éloignement, la lutte contre la fraude, la prévention des actes terroristes et de la récidive, mais aussi les « exigences minimales de la vie en société. Cette expansion des aspects matériel et immatériel de l'ordre public a des incidences sur la détermination des limites aux droits garantis. Sur le plan formel, d'une part, elles se matérialisent par un double mouvement dans la hiérarchie des normes. Certains domaines, comme les fichiers de police et les dispositifs de vidéosurveillance, relèvent dorénavant de la compétence du législateur en raison de leur incidence sur l'exercice des droits garantis, alors que le degré de régulation du législateur dans la définition du champ d'application des limites diminue. Aussi, la détermination des limites aux droits garantis témoigne d'une multiplication des régimes dérogatoires du droit commun et du recours à des techniques propres aux régimes d'exception, telles que les dispositions temporaires. D'autre part, la concrétisation législative de l'ordre public se traduit par une diversification matérielle des limites aux droits et libertés. La distinction, de plus en plus complexe, entre les mesures de police administrative et de police judiciaire, ou entre les peines et les mesures de sûreté, illustre la confusion croissante entre la sauvegarde de l'ordre public et la recherche des auteurs d'infractions. Dès lors, la question se pose de savoir si la diversification des normes engendrée par les exigences renouvelées de l'ordre public s'accompagne, elle-même, d'un renouvellement des « limites aux limites » aux droits fondamentaux dans les décisions du Conseil constitutionnel. »*[334]

[333] *La fin des apparences à propos du contrôle parlementaire en état d'urgence sanitaire :* https://journals.openedition.org/revdh/9022

[334] *La limitation des droits fondamentaux constitutionnels par l'ordre public* https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-limitation-des-droits-fondamentaux-constitutionnels-par-l-ordre-public

Pour Luc Rouban : « *Ce retour brutal à des pratiques d'autorité que l'on croyait révolues, tout comme la résurrection de l'État, viennent amplifier des attentes d'efficacité de l'action publique qui étaient déjà bien présentes dans la population française. Alors même que l'on a vécu la crise des « gilets jaunes » et le grand débat national comme des occasions (plutôt ratées) d'étendre et d'approfondir la vie démocratique en France, la vague 11 du* Baromètre *de la confiance politique du Cevipof*[335] *est venue nous dire autre chose en février 2020, juste avant que n'éclate la crise sanitaire. En effet, 41 % des enquêtés sont d'accord (et 9 % tout à fait d'accord) avec la proposition selon laquelle « En démocratie, rien n'avance, il vaudrait mieux moins de démocratie, mais plus d'efficacité ». L'horizon d'une extension des procédures démocratiques se rétrécit et l'efficacité de l'action publique est devenue prioritaire pour une grosse minorité des enquêtés, ce qui semble évoquer des régimes autoritaires du style chinois où le résultat collectif compte plus que les libertés individuelles. »* [336]

A la différence d'autres Constitutions étrangères telles que la loi fondamentale allemande du 23 mai 1949 (art. 1er) ou la Constitution espagnole du 27 décembre 1978 (art. 10), la dignité de la personne humaine n'est pas consacrée explicitement par la Constitution du 4 octobre 1958 ou par les textes auxquels renvoie son Préambule. La seule occurrence du terme « *dignité* » figure à l'article 6 de la Déclaration des droits de l'homme et du citoyen de 1789, qui impose que tous les citoyens soient admissibles aux dignités, places et emplois publics, selon leur capacité, et sans autre distinction que celle de leurs vertus et de leurs talents. La « *dignité* » renvoie ici à la « *qualité de membre d'un ordre civil ou militaire* »

Dans sa décision « Bioéthique » du 27 juillet 1994[337], le Conseil constitutionnel a déduit le principe à valeur constitutionnelle de sauvegarde de la dignité de la personne humaine contre toute forme d'asservissement et de dégradation de la première phrase du Préambule de la Constitution de 1946 ainsi rédigée : « *Au lendemain de la victoire remportée par les peuples libres sur les régimes qui ont tenté d'asservir et de dégrader la personne humaine, le peuple français proclame à nouveau que tout être humain, sans distinction de race, de religion ni de croyance, possède des droits inaliénables et sacrés* ».

En juillet 2015, il a validé l'essentiel de la loi sur le renseignement, en particulier les boîtes noires algorithmiques destinées à détecter les comportements suspects sur Internet sans que le citoyen ordinaire ne puisse en contrôler l'usage politique (en vertu du 'secret défense').

Pour Frédéric Mas, journaliste et philosophe politique : « *En déclarant que le champ d'application de la loi sur le renseignement ne relève que de la police administrative, et donc de la prévention des infractions et de l'ordre public, le Conseil constitutionnel a clairement interprété le texte comme relevant de l'État de police, au détriment de l'État de droit. En cela, il n'est pas exagéré d'y voir une régression d'ampleur, en particulier en ce qui concerne le contrôle des gouvernants par les gouvernés. En effet, historiquement, l'État de droit succède à l'État de police : le premier vise à limiter par le droit l'empiètement de l'administration sur les droits et libertés de ses administrés, le second formalise l'arbitraire du gouvernement et la généralisation de la surveillance du citoyen. Il est désormais clair pour tout le monde que le Conseil constitutionnel a choisi par son positivisme paresseux d'admettre la disparition de la vie privée en France.* »

[335] *Baromètre de la confiance politique du Cevipof (février 2020) :* https://www.sciencespo.fr/cevipof/sites/sciencespo.fr.cevipof/files/OpinionWay%20pour%20le%20CEVIPOF-Barome%CC%80tre%20de%20la%20confiance%20en%20politique3-%20vague11%20-%20Comparaison.pdf

[336] *Les effets politiques de l'épidémie : l'efficacité contre la démocratie ?* https://theconversation.com/les-effets-politiques-de-lepidemie-lefficacite-contre-la-democratie-134828

[337] *Cf.* https://www.conseil-constitutionnel.fr/decision/1994/94343_344DC.htm

Dans une autre décision en date du 5 février 2021 en réponse à une QPC posée par les sociétés Bouygues Télécom et SFR[338], invoquant des considérations relevant de la sécurité nationale, le Conseil constitutionnel a validé les dispositifs législatifs anti-Huawei mis en place à la faveur de la loi n° 2019-810 du 1er août 2019 que les deux opérateurs considèrent comme présentant un danger au regard des conséquences sur leur activité, notamment les nouveaux pouvoirs attribués à l'ANSSI.[339,340]

Le professeur Yannick Chatelain[341] observe que les arguments sécuritaires invoqués valent aussi pour n'importe quel acteur privé, le passé nous ayant appris que des usages dévoyés des technologies ne sont pas l'apanage de la Chine[342] ; or, celui qui contrôle une partie de l'infrastructure technologique au niveau du réseau peut accéder à des éléments critiques en lien avec les télécommunications, lesquels se doivent d'être protégés.

Pour la France, cette loi jugée conforme à la Constitution ne sera pas sans conséquence. Comme le soulignait la Fédération française des télécommunications : « *Si demain, Huawei était amené à être interdit sur tout ou partie du territoire, il faut bien que chacun ait conscience des retards considérables que nous prendrions dans les déploiements. Ça serait un retard considérable pour les territoires, pour les entreprises françaises, pour la transformation numérique. Cela aurait un coût.* »

Dès 2019, une étude non publique conduite par l'association des opérateurs et constructeurs de téléphonie mobile (GSMA), corroborait ce discours et alertait devant la montée en puissance d'une ostracisation fondée sur le soupçon. Le journal *Le Monde* qui avait pu accéder à ce document indiquait que : « *Une exclusion des vendeurs chinois d'équipements télécoms du marché européen augmenterait la facture du déploiement de la 5G d'environ 55 milliards d'euros pour les opérateurs européens.* »

Au-delà de telles considérations, c'est probablement la manière dont sont envisagés l'intérêt général et son rapport aux droits fondamentaux par le Conseil constitutionnel qui soulève les plus grandes difficultés, comme le relève Thierry Foucart : « *Il s'avère que, parmi les textes constitutionnels de référence, aucun ne renvoie à la notion d'intérêt général. Le silence de la Constitution paraît donc a priori condamner le recours à celle-ci dans la jurisprudence constitutionnelle. Tel n'est pourtant pas le cas. Surmontant l'obstacle textuel, la Haute Instance décide d'intégrer l'intérêt général parmi ses instruments de contrôle de la loi. Plus précisément, elle l'érige en condition de constitutionnalité de la loi. Lorsque le législateur restreint l'exercice de certains principes, droits ou libertés protégés par le Conseil, il doit justifier son action par la poursuite d'un intérêt général*. »[343]

Pour *Michael von Liechtenstein* : *« L'idée que la Constitution devrait protéger les citoyens contre l'État a été abandonnée. »*

Dans son dernier ouvrage intitulé *'Le totem de l'Etat de droit'*, Maître Ghislain Benhessa, docteur en droit public, philosophe et avocat, dont les recherches le conduisirent à étudier les dispositifs d'exception mis en place par les Américains au lendemain des attentats du 11

[338] *Cf.* https://www.conseil-constitutionnel.fr/decision/2021/2020882QPC.htm
[339] *Cf.* https://www.conseil-constitutionnel.fr/decision/2021/2020882QPC.htm
[340] 5G : le Conseil constitutionnel valide la loi « anti-Huweï »
https://incyber.fr/5g-le-conseil-constitutionnel-valide-la-loi-anti-huawei/
[341] Auteur notamment de : *Chroniques du technomonde - les évolutions récentes d'Internet - pour le meilleur ou pour le pire ?* *www.cultura.com/chroniques-du-techno-monde-les-evolutions-recentes-d-Internet-pour-le-meilleu-9782818809174.html*
[342] *Prism, Snowden, surveillance : 7 questions pour tout comprendre :*
https://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html
[343] *Intérêt général et droits fondamentaux :* https://fr.irefeurope.org/Publications/Articles/article/Interet-general-et-droits-fondamentaux

septembre 2001, en se posant notamment la question fondamentale : *« La sécurité doit-elle primer sur le droit commun au détriment des libertés fondamentales ? »*, déplore la mutation de la notion d'Etat de droit depuis la Seconde Guerre mondiale. Selon lui, la mise sous surveillance de la politique par les juges a conduit à mettre la démocratie *« sous tutelle »*. Il y dépeint le passage d'un *« droit de l'Etat »* à un *« droit sur l'Etat »* et regrette l'abandon de la souveraineté nationale au profit d'un concept mal défini.

Selon Philippe Forget, docteur en philosophie morale et politique : *« La République étant ordonnée pour la liberté, l'égalité en droit, la propriété et la sûreté de l'individualité civique, le jugement est dès lors intrinsèquement décidable pour le membre d'une cour suprême. Et les citoyens, pouvoir constituant, sont en droit de le juger à son tour. L'existence civile exige de savoir juger le juge et son jugement. Que constatent-ils ? Les décisions/jugements du Conseil constitutionnel sont la plupart du temps soucieux de l'ordre politique et non la défense des droits de l'homme et du citoyen. Or le Conseil constitutionnel n'a pas à défendre l'ordre politique de l'appareil exécutif de l'Etat, mais à faire respecter les droits de l'homme et du citoyen. Or, il montre une fois de plus qu'il veille à la sûreté du seul gouvernement. Il y a une hiérarchie des normes, mue par une logique de la raison constituante. Mais cette hiérarchie est bafouée, car au fond, le droit n'est qu'un expédient de la politique pour la culture française de gouvernement. La pratique du droit par le législateur même est positiviste car elle ne vise qu'à traduire juridiquement les évolutions morales, politiques et idéologiques de la société : le droit dit est le droit juste. Les principes fondamentaux ont été découverts et déclarés pour la croissance de l'individu, non pour la pérennité de l'Etat (lequel n'est qu'une organisation serve). Telle est la raison universelle du libéralisme, fondé par le bourgeois, que la réaction clanique, le collectivisme bureaucratique et le dispositif technocratique, chacun favorisant l'idiotie de masse, s'efforcent d'abattre sans répit. L'individu comme liberté vive est sacrifié sur l'autel d'une transcendance invoquée (Etat, classe sociale, catégories de sexe, de peau, de victimes, etc.). L'abstraction libératrice des droits de l'homme et du citoyen est abolie par les luttes particularistes (d'où le déluge de lois et règlements). »*

Ayant parfaitement saisi les enjeux de la non-appropriation par les Français des termes de la Constitution, dans sa lettre comme dans son esprit, y compris leurs représentants politiques comme en témoignent ses décisions établissant trop souvent des réserves à l'égard de lois pourtant votées, quand elles ne sont pas reconnues non conformes (partiellement ou en totalité) à la loi fondamentale, le Conseil constitutionnel a pris la sage décision de mettre à la disposition du ministère en charge de l'Education nationale un ensemble de ressources destinées à pallier cette défaillance démocratique, au sein duquel apparaît une entrée transversale spécifiquement dédiée au Numérique (droits et liberté, dématérialisation et digitalisation).[344]

- *Le Défenseur des droits prend position*

Devant cette situation dégradée de l'Etat de droit en France, le Défenseur des droits, Jacques Toubon, ancien garde des Sceaux et ministre de la Justice, a rappelé dans un rapport publié en 2019[345], à la suite d'enquêtes menées en commun avec l'Institut national de la Consommation (INC), les enjeux qui président à la fabrication d'une vraie démocratisation du numérique, à savoir l'égalité devant l'accès aux services des publics, de plus en plus dématérialisés, en pointant le véritable souci social et culturel derrière la question de l'accès à Internet à l'heure où, indique-t-il, *« le taux de connexion varie ainsi de 54 % pour les non diplômés à 94 % pour les diplômés de l'enseignement supérieur ».*

[344] Ressources pour l'étude de la Constitution : https://eduscol.education.fr/2689/ressources-pour-l-etude-de-la-constitution?fbclid=IwAR3I4ocnIQmzr_5owaAWQEITU-MO3brHui9v94iS3XSVE8iDryotlpjeb3E#summary-item-11

[345] *Dématérialisation et inégalités d'accès aux services publics :* https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/dp-rappdemat-16.01.19-num.pdf

Il a alerté sur la nécessité de renforcer l'accompagnement des personnes en précarité numérique et de maintenir les modes alternatifs d'accès aux services publics.

Il s'est à nouveau exprimé publiquement le 1er mars 2020 pour réaffirmer que la dématérialisation des services publics est un progrès, mais à la condition qu'elle se fasse en respectant les principes fondamentaux du service public à la française – égalité et continuité – et de l'accès des usagers à leurs droits, sans pour autant contester l'objectif de l'agenda « Action publique 2022 ».

D'ici 2022, parmi les trois écueils qui doivent être évités selon Jacques Toubon, on peut en dégager les principaux éléments suivants : d'abord, la dématérialisation ne doit pas être utilisée comme une simple substitution à la disparition des services publics pour des raisons budgétaires. C'est là un choix politique et social majeur qui relève du pouvoir. Ensuite, elle ne doit pas être faite à marche forcée, en ignorant toute une frange de la population – 20 % selon l'Insee – qui maîtrise mal, ou pas du tout, les nouvelles technologies et les formalités administratives dématérialisées. Enfin, les réponses apportées aux citoyens doivent être respectueuses de la dignité des personnes, autant que de leurs droits.

Rejoignant la lettre comme l'esprit des dispositions de la Charte des Nations Unies comme de la Déclaration universelle des Droits de l'homme de 1948 relatives à l'Etat de droit, la position du Défenseur des Droits se résume en ces termes simples : *« Il faut remettre de l'humain dans la machine France ».*

Dans cet esprit, la création à l'initiative du gouvernement d'un réseau national de la médiation numérique ainsi que d'un portail dédié à cette médiation numérique[346] permettant de consulter et commenter un texte soumis à l'avis du public avant qu'il devienne un règlement, une charte d'adhésion ou même une loi, constitue une avancée importante qui mérite d'être saluée.

Pour autant, en juillet 2021, la Défenseure des droits, Claire Hédon, a été une nouvelle fois amenée à appeler l'attention du Parlement sur des points essentiels. [347]

En particulier, le recours généralisé au QR code européen a retenu toute son attention eu égard aux faits qu'il regorge d'informations personnelles accessibles librement par un simple scan et qu'il est aisément falsifiable.[348]

A l'occasion des débats parlementaires relatifs à l'extension de l'usage du passe sanitaire en France, elle a souligné dans son point 9 les risques qu'un tel projet de loi faisait courir à la Nation en matière de protection des données et de contrôle social.

« L'article 3 du projet de loi complète l'article 11 de la loi n° 2020-546 du 11 mai 2020 qui permet de traiter et de partager des données à caractère personnel concernant la santé des personnes afin de créer des systèmes d'information pour lutter contre la propagation de l'épidémie de Covid-19.

Ainsi, il prévoit d'ajouter une sixième finalité au traitement de ces données, à savoir l'édiction, le suivi et le contrôle du respect des mesures individuelles de mise en quarantaine, de placement et de maintien en isolement.

[346] *Cf.* http://www.mediation-numerique.fr/

[347] *Avis du Défenseur des droits n° 21-11 du 20 juillet 2021 sur le projet de loi n° 4386 relatif à la gestion de la crise sanitaire :* https://juridique.defenseurdesdroits.fr/doc_num.php?explnum_id=20864

[348] *Cf. https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf*
Que contient le QR code du passe sanitaire ?
https://www.codable.tv/qui-a-t-il-dans-le-pass-sanitaire/
Passe sanitaire : mais qui récupère nos données personnelles ?
https://www.lebigdata.fr/enquete-pass-sanitaire-donnees-personnelles

L'appréciation de la conformité de cette mesure au droit au respect de la vie privée et notamment aux données personnelles sera laissée à la Commission nationale de l'informatique et des libertés (CNIL), chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers.

La Défenseure des droits tient cependant à alerter, comme elle l'avait fait précédemment dans son avis n° 20-03 du 27 avril 2020, sur le risque de glissement vers des pratiques de surveillance sociale générale, auquel pourrait contribuer ce projet de loi. »

Sur la méthode, la Défenseure des droits a tenu à souligner la nécessité d'un débat démocratique : *« Par un avis n° 20-10 du 3 décembre 2020 rendu dans le cadre de la prorogation de l'état d'urgence sanitaire, le Défenseur des droits a appelé de ses vœux l'organisation d'un débat démocratique public de fond en soulignant qu'il « devrait permettre de discuter la nécessité de protéger les droits et libertés et de renforcer les services publics, le caractère adapté, nécessaire et proportionné des mesures sanitaires, afin de préserver le juste équilibre entre les objectifs recherchés. / L'adhésion des citoyens à une mesure repose sur une série d'éléments : la clarté de la mesure envisagée, son caractère exceptionnel et temporaire, le fait qu'elle ait fait l'objet d'un débat démocratique et qu'elle soit le résultat d'un consensus fort (ce qui réduirait la perception du caractère autoritaire ou arbitraire de la mesure que certains pourraient avoir), la conviction que la mesure est justifiée et efficace au regard de la situation sanitaire (cela passerait par la démonstration de sa légitimité, de sa nécessité et de sa proportionnalité), une communication adaptée auprès du public, des contrôles renforcés …*

La Défenseure des droits ne peut que renouveler cette demande et regretter vivement le choix d'une procédure accélérée compte tenu de l'ampleur des atteintes aux droits et libertés fondamentales prévues par ce projet de loi ainsi que du caractère inédit de certaines dispositions qu'il comporte.

Le débat semble même d'autant plus nécessaire en l'espèce que le gouvernement propose un durcissement extrêmement rapide des règles, pourtant édictées il y a peu de temps.

Ainsi que l'a rappelé le Conseil constitutionnel dans sa décision du 11 mai 2020, le législateur a pour rôle d'assurer la conciliation entre l'objectif de valeur constitutionnelle de protection de la santé et le respect de ces libertés. Il est donc indispensable que le Parlement dispose du temps nécessaire à l'examen et aux débats sur ces propositions.

La crise sanitaire sans précédent que nous traversons demande à ce que des mesures soient prises pour protéger la vie de toutes et tous et pour enrayer rapidement cette épidémie. Cependant, la Défenseure des droits constate que, depuis le début de cette pandémie, les garde-fous et garanties mises en œuvre à chaque étape sont régulièrement contournés voire annihilés à la suivante sans que les raisons n'en soient toujours clairement établies. A titre illustratif, alors que le Conseil constitutionnel avait relevé lors de l'examen de certaines dispositions de la loi relative à la gestion de la sortie de crise sanitaire1 que les interdictions de circulation des personnes étaient circonscrites et ne concernaient pas les déplacements strictement indispensables aux besoins familiaux, professionnels et de santé, figure désormais l'obligation de présentation d'un « passe sanitaire » ou vaccinal y compris pour effectuer ce type de déplacements essentiels.

En outre, comme la Défenseure des droits le soulignait en préambule de son avis n° 21-06 du 17 mai 2021 sur le projet de loi relatif à la gestion de la sortie de crise sanitaire, les mesures envisagées doivent être élaborées en concertation avec toutes les autorités publiques compétentes, dans des délais raisonnables, afin que l'inscription des dispositions dans la loi, soumise à un objectif de valeur constitutionnelle de clarté et d'intelligibilité, ne laisse aucune place ni aux interprétations divergentes, ni aux décisions discrétionnaires. Elle alertait à cet

égard sur le renvoi au pouvoir réglementaire de 1 Décision n° 2021-819 DC du 31 mai 2021. 4 nombreuses questions structurantes, susceptibles de porter atteinte aux droits et libertés fondamentales.

A la lecture du présent projet de loi, ces considérations, à la fois de méthode et de fond, conservent plus que jamais leur pertinence, qu'il s'agisse de l'objet même du texte ou des dispositions évoquées ci-après. »

Cette situation illustre bien une certaine faillite de l'Etat de droit en France devant la complexité et la variété des défis numériques qui lui sont posés.

Seul véritable signe positif, la réactivité des réseaux sociaux en cas d'injustices flagrantes témoigne toujours d'une grande vigueur de la part de la société civile, vigueur indispensable à une démocratie qui fonctionne.

Les instruments disponibles pour la protection ou la restauration de l'Etat de droit

Les développements précédents offrent une illustration abondante des motifs d'inquiétude quant à la dégradation de l'Etat de droit en France en raison notamment de l'incapacité des institutions de l'Etat à inscrire leur action en cohérence et/ou en conformité avec les exigences portées par la promesse démocratique dans le pays qui fut à l'origine de la déclaration universelle des droits de l'Homme et qui dispose d'une Constitution.

« Le fait le plus marquant réside dans l'appropriation par les grandes plates-formes numériques non européennes des attributs de la souveraineté : un territoire transnational qui est celui de leur marché et du lieu d'édiction de normes, une population d'internautes, une langue, des monnaies virtuelles, une fiscalité optimisée, un pouvoir d'édiction de normes et de régulation. La composante propre au contexte numérique réside dans la production et l'utilisation de données et dans la maîtrise de l'accès à l'information. Il y a donc une forme de concurrence avec les États ou l'Union européenne.

C'est la souveraineté sous toutes ses formes qui est interrogée. »[349]

Devant une telle situation, il convient de s'interroger sur l'existence d'instruments juridiques susceptibles de participer à la protection ou à la restauration de l'Etat de droit face aux risques et menaces que font porter sur lui les transformations profondes de la société et de l'Etat induites par l'évènement d'un numérique et d'une intelligence artificielle omniprésents.

- *La séparation des pouvoirs et la recherche permanente d'une sécurité juridique constituent les garanties les plus essentielles de la protection ou de la restauration – en cas de défaillance grave - de l'Etat de droit au sein de la République française*

« Dès que le pouvoir est fondé sur la souveraineté de tous, la méfiance paraît sans raison, la vigilance sans objet et les bornes mises à l'autorité ne sont plus défendues. » (Bertrand de Jouvenel)

« Il y a une indétermination consubstantielle à la démocratie : si la démocratie donne la souveraineté au peuple, le problème est de savoir quelles sont les formes de cette souveraineté. » affirme Pierre Rosanvallon, professeur au Collège de France.

Cette souveraineté est déléguée aux institutions de la République au travers du contrat politique et social incarné dans la Constitution, laquelle organise la séparation des pouvoirs.

Le Défenseur des droits veille au respect des droits et libertés (article 71-1 de la Constitution).

Les pouvoirs de contrôle (constitutionnel, conventionnel, de légalité) dont disposent le législateur – en vertu du droit qu'a le Parlement de se réunir dans les conditions prévues aux articles 28 et 29 de la Constitution, de contrôler l'action du Gouvernement et de légiférer), comme les grandes juridictions de la République (Conseil constitutionnel, Conseil d'Etat, Cour de Cassation) constituent les instruments juridictionnels garantissant à la Nation le respect par les institutions de la République des lois et règlements qui satisfont aux exigences constitutionnelles et conventionnelles comme aux principes généraux du droit.

Ces juridictions portent la lourde responsabilité de veiller à pallier, au travers du droit, les atteintes portées de manière directe ou indirecte à l'Etat de droit par les avancées technologiques dans les registres numériques et de l'intelligence artificielle et/ou leurs usages au sein de l'Etat comme de la société.

[349] *Cf.* Annie Blandin-Obernesser *in* ***Souveraineté et numérique : maîtriser notre destin :*** https://theconversation.com/souverainete-et-numerique-maitriser-notre-destin-171014

Lorsqu'elles sont saisies selon les procédures en vigueur, elles arrêtent leurs décisions dans les limites de l'état du droit disponible sur les registres mettant en présence le numérique et l'IA, lequel pâtit d'un retard d'autant plus préjudiciable à la préservation pleine et entière des droits et libertés reconnus à toutes les personnes qui résident sur le territoire de la République, que le rythme de renouvellement des technologies et de leurs usages connaît une accélération qui rend illusoire quelque rattrapage que ce soit du droit à leur égard ; ce qui participe à générer une insécurité juridique de nature systémique.

La sécurité juridique découlant du droit national de sûreté, elle doit par conséquent être traitée au niveau du droit constitutionnel.

Devant l'ampleur et le rythme des bouleversements à l'œuvre, lorsque le droit est disponible pour statuer sur leur conformité aux principes généraux du droit, en particulier du droit administratif, comme au droit fondamental et/ou au droit issus des lois (notamment les différents codes), il est permis de penser que le recours à la sagesse des juges du Conseil d'Etat et du Conseil constitutionnel sera désormais de plus en plus la règle, le gouvernement, l'administration publique, comme le Parlement, ne semblant plus en mesure de garantir par eux-mêmes le respect des éléments les plus fondamentaux du droit.

Par sagesse des juges, il faut entendre leur capacité à apprécier la légalité de manière téléologique, comme le suggère la *« nouvelle légalité »*, « *laquelle ne mesure plus la distance entre l'acte et la norme, mais qui, dans le cadre du droit positif en vigueur, vise à atteindre la finalité propre de la pratique juridique, la justice – qu'il faut concevoir comme un juste équilibre, selon le contexte de l'action et au cours d'un due process of law, entre des intérêts multiples et contrastants à l'aune des principes et des valeurs de la Constitution et des Chartes européennes des droits* - »[350], et attribue une importance première au but de la loi en se fondant sur la volonté déclarée ou présumée du législateur, qui doit pouvoir l'emporter quand la lettre trahit l'esprit de la loi.

- *Le code pénal, un instrument juridique majeur au service de la protection des données*

Au premier rang des principaux défis posés à l'Etat de droit par le numérique et l'IA figure la protection des données privées ou publiques sensibles à l'heure où se généralise au niveau mondial la régulation par la donnée ; une régulation qui intervient dans un contexte où les vecteurs de la constitution, du stockage, de la circulation et de l'usage de cette dernière obéissent à des considérations économiques, commerciales, juridiques, technologiques, infrastructurelles, géopolitiques et sécuritaires qui peuvent échapper aux exigences dictées par le droit national (extraterritorialité du droit auxquels sont soumis les acteurs, confidentialité des transactions avec des tiers non nationaux, captation par siphonage de données[351]…).

Comme le relèvent Aurélie Luttrin et Franck DeCloquement dans leur article cité *supra* : *« Au niveau national, l'arsenal juridique existe déjà et demeure puissant pour défendre nos intérêts fondamentaux : l'article 411-6 du Code pénal selon lequel « le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225 000 euros d'amende. ». Il s'avère d'une rare efficacité sémantique pour convaincre*

[350] *Cf.* Massimo Vogliotti *in Les nouveaux chemins de la légalité - Au-delà de la modernité juridique :* https://books.openedition.org/pusl/26148

[351] *Cf.* par exemple Gilbert Kallenborn *in 'iMessage, WhatsApp, Telegram, Signal... Un document révèle les données que le FBI peut siphonner'* : https://www.01net.com/actualites/imessage-whatsapp-telegram-signal-un-document-revele-les-donnees-que-le-fbi-peut-siphonner-2052024.html

les plus récalcitrants de cette impérieuse nécessité de cesser tout stockage et traitement de données auprès de puissances étrangères pouvant porter atteinte à nos intérêts. »

S'agissant de la lutte contre la cybercriminalité, Marc-Antoine Ledieu, avocat spécialisé dans le numérique, relève que *« la responsabilité des cyberattaques n'est pas une difficulté sur le plan pénal. La loi « Godfrain » du 6 janvier 1988 (article 323-1 à 323-3-1 Code pénal) permet de réprimer l'ensemble des intrusions et autres délits de maintien frauduleux dans un système d'information. La loi « Informatique et Libertés » version 2021*[352] *permet sans aucun problème d'envisager la responsabilité pénale des cyber attaquants qui viendraient à* traiter *sans consentement des données à caractère personnelles. Le droit de mettre en oeuvre des logiciels ou des services de chiffrement est entièrement régulé (et sanctionné pénalement) par la loi du 21 juin 2004 « LCEN » pour la confiance dans l'économie numérique. Il est même possible d'appliquer certaines incriminations pénales « classiques » aux nouveaux délits commis par voie numérique. Nous prendrons l'exemple du délit d'extorsion, tout à fait adapté aux chantages exercés par « ransomware ». Hélas, le peu de jurisprudence pénale disponible conduit à conclure que la répression des cyber attaquants n'a aujourd'hui aucun effet dissuasif. »*[353]

Force est de déplorer que, alors que la cybercriminalité et les autres infractions impliquant des preuves électroniques sur des systèmes informatiques sont en plein essor et que ces preuves sont de plus en plus souvent stockées sur des serveurs situés dans des juridictions étrangères, multiples, changeantes ou inconnues, c'est-à-dire dans le nuage, les pouvoirs des services répressifs sont limités par les frontières territoriales. Seule une très faible proportion des actes de cybercriminalité signalés aux autorités de justice pénale donne lieu à des procédures judiciaires et à des condamnations, et le plus souvent les victimes n'obtiennent pas justice.

- *Le principe de proportionnalité, un instrument juridique protecteur des libertés*

Comme le souligne Jean-Marc Sauvé[354], vice-président du Conseil d'Etat, la mise en œuvre du principe de proportionnalité renseigne sur la place qu'une société reconnaît réellement aux droits et libertés, dès lors que ce principe encadre les atteintes qui peuvent y être portées.

Ce principe s'est affirmé depuis plus d'un siècle en Europe et en France au service d'une protection efficace des libertés et des droits fondamentaux en ce qu'il enclenche un mécanisme de pondération entre les différents intérêts publics et privés en cause, mais il subit une influence européenne qui le transforme en profondeur. Issu du droit allemand, il vise à promouvoir une action publique mesurée et respectueuse des droits fondamentaux. Mais là où en Allemagne la proportionnalité est entendue comme un principe général, dès lors qu'elle répond à la nécessité de réguler l'interventionnisme étatique, elle n'est en droit français qu'un mécanisme de contrôle juridictionnel. Ce principe non-écrit est cependant « au cœur de la démarche logique du juge de l'excès de pouvoir ». Il s'est imposé comme l'*« exigence d'un rapport, d'une adéquation, entre les moyens employés par l'administration et le but qu'elle vise »*.

L'exigence de proportionnalité est également présente en droit constitutionnel, soit que le texte constitutionnel la prévoie expressément, soit que le Conseil constitutionnel ait lui-même affirmé ce contrôle dans sa jurisprudence.

Et, dans la lignée de la jurisprudence *Benjamin* du Conseil d'Etat, le Conseil constitutionnel use assez largement du contrôle de proportionnalité lorsqu'il contrôle des dispositions

[352] *L'information : le droit pénal du numérique :* https://technique-et-droit-du-numerique.fr/le-droit-penal-du-numerique-video-5/
[353] *cyber attaque: responsabilité pénale civile et contractuelle :* https://technique-et-droit-du-numerique.fr/cyber-attaque-responsabilite-penale-civile-contractuelle/
[354] *Le principe de proportionnalité, protecteur des libertés ?* https://www.conseil-etat.fr/actualites/discours-et-interventions/le-principe-de-proportionnalite-protecteur-des-libertes

législatives qui restreignent l'exercice d'un droit ou d'une liberté au nom de la sauvegarde de l'ordre public ou lorsqu'il doit concilier plusieurs droits fondamentaux entre eux.

Le principe de proportionnalité est le complément nécessaire de l'intérêt public. Mais s'il *« manifeste qu'un intérêt public en soi ne peut (…) se réaliser à n'importe quel prix »*, il ne saurait se traduire par une remise en cause du principe même de la séparation des pouvoirs et du principe d'appréciation des Gouvernements et des Parlements. Il est indispensable à la garantie de l'Etat de droit, mais il ne saurait conduire à méconnaître les intérêts généraux dont l'Etat et les collectivités locales ont la charge et qui sont, avec les libertés et les droits fondamentaux, les piliers du vivre-ensemble.

Pour Jean-Marc Sauvé, trois précautions s'imposent dans le maniement de la proportionnalité : ce contrôle doit être stable et cohérent pour être prévisible ; il doit, ensuite, s'appuyer sur une motivation explicite et rigoureuse ; enfin, il doit conduire à une véritable mise en balance des différents intérêts en présence et non à la prédominance systématique des droits fondamentaux sur l'intérêt général.

Les cours européennes ont procédé, au cours des toutes dernières années, à une mise en balance plus attentive et prudente de l'ensemble de ces exigences (*cf. infra*).

La conception des cours européennes de la proportionnalité influe sur les déclinaisons nationales de ce principe qui ont évolué vers une approche plus libérale, principalement sous l'impulsion de la Convention européenne des droits de l'homme et l'interprétation qui en est faite par la Cour de Strasbourg, ainsi que sous celle de la Cour de justice de l'UE qui envisage de manière très stricte les restrictions aux liberté de circulation prévues dans les dispositions du Traité sur le fonctionnement de l'UE.

Cette influence européenne fait ressentir ses effets partout en Europe et, notamment, en France où le droit européen a induit une « généralisation » et une « intensification » du contrôle de proportionnalité.

Sous l'effet de la jurisprudence de la Cour européenne des droits de l'homme, ce contrôle a été étendu à plusieurs hypothèses qui en étaient exclues ou faisaient l'objet d'un contrôle restreint. Le contrôle de proportionnalité exercé par le juge administratif s'est aussi intensifié sous l'effet de la jurisprudence de la CJUE.

Cette évolution a connu, en droit français, de nouveaux développements avec la formalisation d'un contrôle de proportionnalité *in concreto* dans la jurisprudence du Conseil d'État et celle de la Cour de Cassation.[355]

Mais ce phénomène de convergence ne doit pas conduire à de trop hâtives conclusions.

D'une part, les juges nationaux et européens continuent, dans les domaines économiques et sociaux, de préserver une importante marge d'appréciation aux autorités publiques. En outre, si le principe de proportionnalité résulte de la volonté de limiter le pouvoir discrétionnaire des autorités publiques et d'éviter l'arbitraire, il ne saurait conduire le juge à substituer sa propre appréciation à celle des représentants du peuple soumis au contrôle démocratique.

La Cour européenne des droits de l'homme reconnaît aussi aux États une marge nationale d'appréciation, lorsque sont en cause des débats éthiques ou moraux ou des choix de société qui ne font l'objet d'aucun consensus entre les États ou qui résultent de traditions nationales.

[355] *Cf. Le contrôle de proportionnalité in concreto dans les réformes des cours suprêmes françaises (Conseil d'Etat et Cour de Cassation) :*https://www.academia.edu/35868126/Le_contr%C3%B4le_de_proportionnalit%C3%A9_in_concreto_dans_les_r%C3%A9formes_des_cours_supr%C3%AAmes_fran%C3%A7aises_Conseil_dEtat_et_Cour_de_Cassation_?email_work_card=view-paper

D'autre part, le principe de proportionnalité reste surtout envisagé comme une technique ou un mécanisme contentieux. Aux fins d'assurer une protection accrue des droits et des libertés, il pourrait s'élargir à une fonction d'orientation de l'action des autorités publiques, ainsi qu'il l'a été en droit allemand, et en droit de l'Union européenne.

Pour Jean-Marc Sauvé, il est même permis de s'interroger sur l'intégration du principe de proportionnalité à celui, plus général, de bonne gouvernance.

- *Les droits européens sont-ils en mesure d'apporter des réponses à ces défis ?*

Le fait que la France soit membre de l'UE ainsi que partie à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et au Réseau européen des Conseils de la Justice[356] est-il de nature à apporter des éléments de réponse significatifs, en termes de droit notamment, à de tels défis ?

Les initiatives et la panoplie des sanctions de l'UE et de la CEDH à l'égard des violations de l'Etat de droit contribuent-elles à améliorer la performance institutionnelle des Etats ? Garantissent-elles à tous les citoyens les mêmes droits et les mêmes libertés ? Sont-elles de nature à créer de la confiance ?

L'état de droit est inscrit à l'article 2 du traité sur l'Union européenne parmi les valeurs communes à tous les États membres. Il garantit que toutes les autorités publiques agissent toujours dans les limites fixées par la loi, conformément aux valeurs de la démocratie et aux droits fondamentaux, et sous le contrôle de juridictions indépendantes et impartiales. Il recouvre le principe de légalité, qui suppose l'existence d'une procédure d'adoption des textes de loi transparente, responsable, démocratique et pluraliste, ainsi que les principes de sécurité juridique, d'interdiction de l'exercice arbitraire du pouvoir exécutif, de protection juridictionnelle effective assurée par des juridictions indépendantes et impartiales, de contrôle juridictionnel effectif, y compris le respect des droits fondamentaux, de séparation des pouvoirs et d'égalité devant la loi[357]. Ces principes ont été confirmés par la Cour de justice de l'Union européenne – avec une jurisprudence récente particulièrement importante – et par la Cour européenne des droits de l'homme. Par ailleurs, le Conseil de l'Europe a élaboré des normes et formulé des avis et des recommandations qui fournissent des orientations bien établies destinées à promouvoir et à faire respecter l'état de droit.

Sébastien Platon, professeur de droit public, propose un éclairage substantiel sur les fonctions du standard de l'État de droit en droit de l'Union européenne[358] : « *Le standard de l'Etat de droit s'impose indéniablement aux Etats membres. Cela résulte tant de l'article 6 TUE, qui fait de l'Etat de droit une valeur de l'Union, de l'article 7 TUE, qui permet de sanctionner les Etats méconnaissant cette valeur, et de l'article 49 TUE, qui en fait une condition d'adhésion. Au-delà cependant de cette dimension axiologique, le respect du standard de l'Etat de droit par les Etats membres est une nécessité fonctionnelle vitale pour l'Union européenne pour au moins deux raisons. D'une part, le respect de l'Etat de droit par les Etats membres est au fondement du principe de confiance mutuelle, lequel sous-tend toutes les formes de coopération interétatique imposées par le droit de l'Union européenne. D'autre part, le respect de l'Etat de*

[356] Le RECJ, Réseau européen des Conseils de la Justice, créé en 2004, rassemble les « *Conseils supérieurs de la Justice* » nationaux. Ce réseau, qui est actif autour de thèmes tels que l'arriéré judiciaire, la mesure de la confiance nationale et transnationale de la population en la justice et les normes minimales pour l'évaluation des systèmes judiciaires, a vocation à assurer la connaissance réciproque des différents systèmes judiciaires de l'Union européenne, et a également pour mission de remplir un rôle de médiateur entre les institutions de l'UE et les organisations judiciaires nationales.

[357] *La protection des valeurs consacrées à l'article 2 du traité UE dans l'Union :*
https://www.europarl.europa.eu/factsheets/fr/sheet/146/la-protection-des-valeurs-consacrees-a-l-article-2-du-traite-ue-dans-l-union

[358] *Les fonctions du standard de l'État de droit en droit de l'Union européenne :*
https://www.academia.edu/40231820/Les_fonctions_du_standard_de_l_%C3%89tat_de_droit_en_Europe

droit par les Etats membres est également nécessaire pour que les individus bénéficient des mêmes garanties juridictionnelles face au juge national, juge de droit commun de droit de l'Union, que face au juge de l'Union. »

Outre les efforts de la CJUE pour faire prévaloir une hiérarchie des normes abaissant la place des constitutions nationales, il existe dans les traités des dispositions (article 2, par. 2 TFUE) - ainsi qu'un protocole relatif aux compétences partagées (protocole n°25) - qui donnent la primauté à l'UE pour agir dans les domaines en relevant, et interdit aux Etats membres d'agir si l'UE a pris l'initiative : *« Lorsque les traités attribuent à l'Union une compétence partagée avec les États membres dans un domaine déterminé, l'Union et les États membres peuvent légiférer et adopter des actes juridiquement contraignants dans ce domaine. »* Selon cet article, *« les États membres exercent leur compétence dans la mesure où l'Union n'a pas exercé la sienne et les États membres exercent à nouveau leur compétence dans la mesure où l'Union a décidé de cesser d'exercer la sienne. »*

Contrairement à d'autres organisations internationales comme le Conseil de l'Europe ou les Nations unies, l'UE ne prévoit pas de procédure d'expulsion d'un de ses Etats membres pour quelque raison que ce soit. Dès lors, les seules sanctions disponibles en regard de l'objet de la présente étude résultent de l'activation de deux procédures distinctes :

- article 7 TUE : cette clause prévoit un mécanisme complexe de "*sanction pour violation grave des "valeurs" de l'Union"* par un Etat membre. Mécanisme qui ne peut aboutir qu'à "*"la suspension de certains droits découlant de l'application des traités à cet Etat membre, y compris les droits de vote de (son) représentant au sein du Conseil".* Ce qui présente l'avantage d'offrir une large gamme de mesures punitives (y compris financières) jusqu'à la sanction maximale d'exclusion du processus de décision. Toutefois, on sait que l'exigence d'unanimité pour son déclenchement en réduit fortement l'efficacité au cas où un seul autre Etat y opposerait son veto par solidarité ou par opportunité.

- articles 258/260 TFUE : il s'agit de la *procédure générale dite de "manquement"* qui permet à la Commission de constater qu'"*un Etat membre a manqué à une des obligations qui lui incombent en vertu des traités*" et d'attraire cet Etat devant la CJUE. Le cas échéant, la Cour peut alors dans un premier temps reconnaitre ce manquement et, dans un deuxième temps, "*infliger le paiement d'une somme forfaitaire ou d'une astreinte*". Parmi les "obligations" visées figure implicitement celle du respect des "valeurs" fixées par l'article 2 TUE. Toutefois, sur le plan strictement juridique, la démonstration d'un manquement de ce type n'est pas toujours aisée à effectuer au vu du caractère très général des "règles " à respecter. D'autre part, infliger des sanctions de nature *financière* pour une infraction à des *"valeurs"* peut apparaitre quelque peu décalé voire incongru.

La jurisprudence de l'UE a de manière constante reconnu qu'un manquement d'Etat pouvait résulter d'une décision d'une juridiction nationale enfreignant le droit de l'Union. Seule la Cour de Justice a compétence pour sanctionner un manquement d'Etat. Seule la Commission européenne ou un Etat membre de l'Union européenne peut la saisir d'un recours à cette fin.

Si les traités de l'UE proposent des mécanismes et procédures visant à sanctionner un Etat membre violant gravement les valeurs de l'Union ou manquant à ses obligations à leur égard

(en particulier le nouveau cadre de l'UE pour enforcer l'Etat de droit[359]), force est de constater qu'ils sont difficiles à mettre en œuvre d'un point de vue politique.[360,361]

La Commission européenne, qui est l'institution garante des traités européens (TUE et TFUE), ne peut que rappeler les termes des traités – et le cas échéant, appliquer des astreintes financières lorsque les Etats défaillants ne se plient pas aux injonctions des juridictions européennes compétentes !

C'est ce qu'elle fait quand elle rappelle le principe de primauté du droit de l'UE.

D'essence fédérale, ce principe général du droit de l'Union est l'un des plus anciens et importants puisqu'il établit que tout acte de l'UE prime sur le droit national des Etats membres de l'Union et que si une disposition du droit national était contraire à un acte de l'Union, le juge national devait écarter cette disposition nationale et appliquer à la place l'acte de l'Union.[362]

Le *rapport sur l'Etat de droit*[363] est un nouvel outil de prévention et fait partie du nouveau mécanisme européen annuel de protection de l'Etat de droit. Il vise à examiner les principales évolutions – positives et négatives – dans l'ensemble de l'UE ainsi que la situation spécifique dans chaque État membre. Son objectif est de recenser les éventuels problèmes liés à l'état de droit le plus tôt possible, de même que les bonnes pratiques. Il ne s'agit pas d'un mécanisme de sanction. Le rapport s'intéresse aux domaines suivants : les systèmes de justice, les cadres de lutte contre la corruption, le pluralisme et la liberté des médias et les autres questions institutionnelles en rapport avec l'équilibre des pouvoirs. Le rapport sur l'état de droit se compose d'un rapport général et de 27 chapitres par pays présentant l'évaluation spécifique à chaque État membre.

Le *mécanisme européen de protection de l'Etat de droit* prévoit un processus de dialogue annuel sur l'état de droit entre la Commission, le Conseil et le Parlement européen, les États membres, les parlements nationaux, la société civile et d'autres parties prenantes. Le rapport sur l'état de droit est la pierre angulaire de ce nouveau processus.

L'un des principaux objectifs du mécanisme européen de protection de l'Etat de droit est de stimuler la coopération interinstitutionnelle et d'encourager toutes les institutions de l'UE à apporter leur contribution conformément à leurs rôles institutionnels respectifs. Cet objectif reflète l'intérêt manifesté de longue date par le Parlement européen et le Conseil. La Commission invite également les parlements nationaux et les autorités nationales à examiner le rapport et encourage la participation d'autres parties prenantes aux niveaux national et de l'UE.

L'établissement du rapport sur l'Etat de droit et les travaux préparatoires connexes avec les États membres ont lieu chaque année dans le cadre du mécanisme ; ils servent de base à des discussions au sein de l'UE et contribuent à prévenir l'apparition de problèmes ou leur

[359] Communication de la Commission européenne au Parlement européen et au Conseil (COM(2014) 158 final) intitulée *« Un Nouveau Cadre de l'UE pour renforcer l'État de droit »* : https://eur-lex.europa.eu/resource.html?uri=cellar:caa88841-aa1e-11e3-86f9-01aa75ed71a1.0011.01/DOC_1&format=PDF

[360] *Cf.* Dimitry Kochenov et Laurent Pech *in Renforcer le respect de l'État de droit dans l'UE : Regards critiques sur les nouveaux mécanismes proposés par la Commission et le Conseil* (Questions d'Europe n°356 – Fondation Robert Schuman) : https://www.robert-schuman.eu/fr/questions-d-europe/0356-renforcer-le-respect-de-l-etat-de-droit-dans-l-ue-regards-critiques-sur-les-nouveaux

[361] *Cf.* Dimitry Kochenov, Laurent Pechet Sébastien Platon *in Ni panacée, ni gadget : le « nouveau cadre de l'Union européenne pour renforcer l'État de droit »* (Revue trimestrielle de droit européen) : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2688353

[362] Comme le rappelle l'avocate Ophélie Omnès, ce n'est qu'en 2009, avec l'entrée en vigueur du Traité de Lisbonne, et de la déclaration n° 17, que le principe fait son entrée dans les traités. Dans l'ordre juridique français, sa consécration est survenue grâce aux arrêts *Société des cafés Jacques Vabre* (1975) de la Cour de Cassation et *Nicolo* du Conseil d'État (1989).
Cf. La primauté du droit de l'Union européenne : un principe cardinal dans la tourmente : https://institutdelors.eu/publications/la-primaute-du-droit-de-lunion-europeenne-un-principe-cardinal-dans-la-tourmente

[363] *Rapport 2020 sur l'Etat de droit – Questions et Réponses :* https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1757

aggravation. Le fait de recenser les problèmes le plus tôt possible et avec le soutien mutuel de la Commission, des autres États membres et des parties prenantes, y compris le Conseil de l'Europe et la Commission de Venise, pourrait aider les États membres à trouver des solutions pour préserver et protéger l'Etat de droit.

Le mécanisme européen de protection de l'Etat de droit est l'un des éléments d'une action plus large menée au niveau de l'UE pour renforcer les valeurs que sont la démocratie, l'égalité et le respect des droits de l'homme. Il est complété par une série d'initiatives, dont le plan d'action pour la démocratie européenne[364], une stratégie renouvelée pour la mise en œuvre de la charte des droits fondamentaux[365] et des stratégies ciblées visant à répondre aux besoins des personnes les plus vulnérables afin de promouvoir des sociétés caractérisées par le pluralisme, la non-discrimination, la justice, la solidarité et l'égalité.

Seule certitude formelle, à ce jour, l'UE n'a pas souhaité activer à l'encontre de la France quelque disposition que ce soit de son arsenal 'coercitif' à l'égard d'un Etat membre exerçant des violations généralisées de l'État de droit par un État membre.

- *La remise en cause récurrente de la primauté du droit européen*

L'ordre juridique européen semble toutefois fragilisé par un arrêt pris le 5 mai 2020 par la Cour constitutionnelle allemande mettant en cause le vaste programme de rachats de dettes souveraines mis en place dans la foulée de la crise de l'euro par la Banque centrale européenne, dispositif pourtant validé par la CJUE.[366,367]

Dans une tribune publiée dans cinq quotidiens continentaux[368], le Président du Tribunal de l'UE, Marc van der Woude, a critiqué avec virulence cet arrêt. Pour lui, cette décision est *« erronée »,* et est d'abord de nature à bouleverser l'ordre juridique et la coopération entre les cours nationales et européennes, bâtis au fil des décennies : *« Cet arrêt soulève de graves préoccupations quant à sa compatibilité avec le droit de l'Union, en particulier les principes généraux d'autonomie, de primauté, d'efficacité et d'application uniforme du droit de l'Union, ainsi que de la compétence de la Cour de justice »* européenne. Et il *« constitue un dangereux précédent pour le droit de l'Union ».*

Il peut aussi avoir pour conséquences d'inciter des Etats en délicatesse avec l'Etat de droit, comme la Pologne et la Hongrie, à contester les décisions de la justice européenne.

La Commission européenne a donc procédé à l'ouverture, le 9 juin 2021, d'une procédure pour manquement à l'encontre de l'Allemagne.

---

[364] *Plan d'action pour la démocratie européenne : renforcer les démocraties de l'UE :* https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0790&from=FR

139

[365] Voir à cet égard la Communication de la Commission européenne COM(2020) 711 final du 2 décembre 2020 intitulée *« Stratégie visant à renforcer l'application de la Charte des droits fondamentaux dans l'Union européenne »* : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0711&from=EN
ainsi que la position du Conseil européen en date du 8 mars 2021 :
https://data.consilium.europa.eu/doc/document/ST-6795-2021-INIT/en/pdf

[366] *Cf. L'arrêt du 5 mai 2020 de la Cour constitutionnelle fédérale concernant le programme PSPP de la Banque centrale européenne :* https://www.actu-juridique.fr/international/international-etrangers/droits-europeen-ue/larret-du-5-mai-2020-de-la-cour-constitutionnelle-federale-dallemagne-concernant-le-programme-pspp-de-la-banque-centrale-europeenne/

[367] *Cf.* Jérémy Bernard *in Guerre des juges au sommet de l'Union européenne : l'arrêt de la Cour constitutionnelle fédérale allemande de Karlsruhe : https://www.delcade.fr/actualites-juridiques/droit-de-la-concurrence/guerre-juges-sommet-de-lunion-europeenne-larret-de-cour-constitutionnelle-federale-allemande-de-karlsruhe/*

[368] *« Que resterait-il de l'égalité entre les justiciables européens si certaines règles devaient s'appliquer dans des Etats membres et pas dans d'autres ? »*
https://www.lemonde.fr/idees/article/2020/06/06/que-resterait-il-de-l-egalite-entre-les-justiciables-europeens-si-certaines-regles-devaient-s-appliquer-dans-des-etats-membres-et-pas-dans-d-autres_6041970_3232.html

Dans un article intitulé *'Les juges et l'Etat de droit en Europe'*[369], Matthieu Febvre-Issaly, doctorant en droit public à l'université Paris 1 Panthéon-Sorbonne spécialisé en droit constitutionnel comparé et en théorie du droit, invite à réexaminer la nature même du contentieux opposant le Tribunal constitutionnel polonais aux institutions européennes compétentes (CJUE et Commission européenne) tout en affirmant que la critique adressée au pouvoir des juges n'a rien d'une question de souveraineté nationale : *« La décision du Tribunal constitutionnel est pourtant moins tranchante que les discours politiques ne le laissent entendre. Le Tribunal estime l'article 19 sur l'accès au juge et l'article 1er qui institue l'Union contraires à la Constitution polonaise en ce qu'ils permettent aux institutions européennes de dépasser leurs compétences, qui ne s'étendent pas à l'organisation de la justice, et portent donc atteinte à la souveraineté nationale*[2]*. En réalité, la question se pose pour tous les États membres, puisque la forme hybride de l'Union européenne, qui se refuse au fédéralisme, coexiste avec une théorie du droit positiviste qui place en haut de la hiérarchie des normes une Constitution. Il a donc fallu que les juges aménagent cette conception, et ils l'ont fait en France en refusant de reconnaître une primauté du droit européen sur la Constitution, comme l'avait d'ailleurs décidé le Tribunal polonais en 2005 tout en reconnaissant que les cas de contrariété étaient très rares.*

Le concept de primauté se comprend mal lorsqu'il est traduit dans le langage commun. La construction juridique européenne n'est pas l'imposition d'un ordre juridique supérieur aux ordres juridiques nationaux qui en deviendraient inférieurs, mais une imbrication dont la complexité résiste mal aux discours simples. Les États y participent eux-mêmes en adhérant aux traités et en prenant part aux décisions du Conseil de l'UE, mais aussi en fournissant des parlementaires et des commissaires. Une fois définies, la plupart des normes européennes doivent être transposées dans chaque pays, puis tous les juges peuvent en être saisis. Quand l'ancien commissaire européen Michel Barnier, au moment de se positionner dans une campagne présidentielle nationale, estime qu'il faut préserver la « souveraineté juridique » de la France face à la CJUE et à la Cour européenne des droits de l'homme, il oublie de préciser que la France y a adhéré elle-même, et surtout que la critique adressée au pouvoir des juges n'a rien d'une question de souveraineté nationale, puisqu'elle se pose autant au sein de l'UE que dans chaque État. Le projet européen ne fait que promouvoir une autre manière d'envisager la souveraineté et l'ordre juridique, qui dans ses formulations ambitieuses ne s'arrête pas au juge.

Le 15 octobre 2021, le Conseil constitutionnel français a rendu une décision qu'il est difficile de ne pas relier à celle du Tribunal polonais, en invoquant pour la première fois un « principe relatif à l'identité constitutionnelle de la France ». Il s'agissait de limiter l'obligation des transporteurs aériens de réacheminer une personne étrangère, prévue par l'accord de Schengen, à l'interdiction faite par la Déclaration des droits de l'homme et du citoyen, selon le Conseil, de déléguer l'usage de la force publique. Le principe de ces principes avait été créé en 2006 par le Conseil, inspiré par le Tribunal fédéral allemand et repris en 2007 par le Conseil d'État. Selon cette jurisprudence, le droit européen prime tant qu'un « principe relatif à l'identité constitutionnelle de la France » n'est pas touché ou qu'il existe dans le droit européen une protection équivalente aux droits français. Pour se défaire de la critique adressée au « gouvernement des juges », les juridictions françaises montaient ainsi en abstraction axiologique et nourrissaient l'image harmonieuse d'un dialogue des juges européens sur l'essentiel. Le principe soulevé pour la première fois le 15 octobre 2021 est d'ailleurs sans incidence sur l'affaire puisque l'obligation pesant sur les transporteurs n'a pas pour effet, selon le Conseil, de leur déléguer une mission de surveillance ou de contrainte.

[369] *Les juges et l'Etat de droit en Europe :* https://esprit.presse.fr/article/matthieu-febvre-issaly/les-juges-et-l-etat-de-droit-en-europe-43682

La différence avec le cas polonais ne se situe pas tant dans l'affirmation de principe que dans le contexte de sa mise en œuvre. Le Tribunal constitutionnel de Varsovie s'est aventuré à faire ouvertement de la politique, ce qui n'a rien d'illogique étant donné la pression inouïe exercée sur les magistrats polonais depuis 2015, sans compter la multiplication de nominations de proches du PiS, y compris au sein du Tribunal. En jugeant contraires à la Constitution polonaise deux articles du TUE, dont le premier, le juge n'en tire pas de conclusions puisqu'il n'a bien sûr aucun pouvoir d'annulation à leur égard. Là aussi la déclaration est de principe, bien qu'elle soit plus sèche et sans aménagement, même rhétorique.

Le Tribunal constitutionnel polonais comme le Conseil constitutionnel démontrent ainsi que les apories de l'autorité supérieure d'un juge non élu dans la détermination de la norme fondamentale ne sont pas l'apanage de l'UE, d'autant que ce sont les juges nationaux tout autant que bruxellois ou strasbourgeois qui dialoguent dans l'élaboration de la jurisprudence. Il ne peut y avoir de gardien omnipotent : une telle protection relève d'un idéal impossible. Au contraire, cet idéal comme le droit sont pris dans des conflits politiques et sociaux qui ne peuvent être niés. La hiérarchie des normes, l'État de droit et les droits fondamentaux ne sont pas des essences protégées de la société mais des constructions idéologiques, dont la substance renvoie à des choix collectifs. Si l'on veut que l'État de droit s'impose, il faut l'accepter comme tel et en déduire une politique ambitieuse, qui ne peut être laissée aux seuls juges mais doit relever d'une délibération commune : le droit avec la politique et le droit comme politique. La CJUE va peut-être trop loin, comme le lui reproche le Tribunal constitutionnel polonais, mais ce dernier n'a plus grand-chose d'une juridiction indépendante. Il revient désormais à la Commission, aux États et à l'espace public européen d'affirmer leur État de droit et nos valeurs. »

Dans un entretien avec le quotidien *'Toute l'Europe'*[370], le Commissaire à la Justice Didier Reynders présente l'approche *« politique »* de la Commission en matière de contrôle du respect de l'Etat de droit par certains Etats membres (Pologne, Hongrie) et affirme *« préférer le dialogue aux sanctions »*.

Il explique notamment les raisons pour lesquelles la Commission se refuse, à ce stade, d'enclencher le mécanisme de conditionnalité budgétaire et d'exiger le paiement sans délai des amendes infligées par la CJUE - ou qui la font renoncer à des recours déjà engagés.

Pour Jean-Guy Giraud, ancien fonctionnaire européen et ancien président de la section française de l'Union pour une Europe fédérale (UEF) : *« Même si le Commissaire en charge confirme aussi que l'Institution bloquera l'agrément des plans de relance polonais ou hongrois liés au NGEU « tant qu'elle n'aura pas d'engagements clairs sur les réformes nécessaires » - il n'en demeure pas moins que cette conception très … souple et permissive du respect des règles en vigueur ainsi que des arrêts de la CJUE peut poser problème.*

On en comprend bien sûr les raisons : laisser le temps aux gouvernements concernés de préparer lesdites réformes mais surtout leur proposer une voie de sortie aussi honorable que possible. Une conciliation vaut toujours mieux que des sanctions qui pourraient aggraver le conflit politique notamment dans le cas où l'opinion serait amenée à prendre partie pour ou contre "Bruxelles".

Mais ceci suppose que ces dirigeants soient disposés à se mettre effectivement en règle - après avoir manifesté leur réticence et leur mauvaise humeur. Si tel n'est pas le cas, l'attentisme de

[370] *Didier Reynders : "Sur l'état de droit, nous préférons le dialogue aux sanctions" :* https://www.touteleurope.eu/institutions/interview-didier-reynders-sur-l-etat-de-droit-nous-preferons-le-dialogue-aux-sanctions/

la Commission pourrait être interprété comme une tentative infructueuse d'"apaisement" affaiblissant l'autorité et l'image des Institutions.

D'autre part, la prolongation indéfinie d'un "délai de grâce" dans l'espoir d'une alternance politique installant une équipe de dirigeants plus coopératifs n'est pas une solution appropriée tant pour des raisons de principe que d'effectivité.

Au total, une telle attitude risque de porter atteinte à l'autorité de la règle de droit en donnant le sentiment que celle-ci est relative et négociable.

Bien sûr, une automaticité quasi-mécanique de l'application de la règle peut, dans certaines circonstances, s'avérer maladroite et contre- productive et une certaine marge d'appréciation doit être laissée à la Commission dans son rôle de gardienne des Traités.

Toutefois, ceci suppose que les gouvernements concernés n'enfreignent pas un principe de base : celui de la "coopération loyale" envers les Institutions tel que fixé par l'article 4 du TUE. Dans le cas des deux gouvernements cités ici, on doit s'interroger sur leur acceptation et leur respect de ce principe dans leur attitude générale vis à vis de l'UE et bien mesurer le risque encouru par des atermoiements répétés.

Enfin, pour ce qui est plus précisément de l'intervention de la CJUE, il faut tout particulièrement prendre garde des effets négatifs de sa saisine répétitive qui lui ferait jouer un rôle d'arbitre de conflits de nature politique - et exiger que ses arrêts soient respectés sans délais et sans conditions. C'est ici le principe même de l'état de droit transposé au niveau européen. »

Comme l'a rappelé le docteur en droit Sébastien Martin en 2012[371] : *« Tous les États membres de l'Union puisent dans leur Histoire certaines caractéristiques qu'ils jugent si essentielles qu'ils entendent les protéger envers et contre tout. Dans ce cadre, la participation à l'Union européenne peut s'avérer parfois problématique. On sait, en effet depuis longtemps, grâce à la jurisprudence de la Cour de justice qui a très tôt posé le principe de primauté du droit des Communautés européennes puis de l'Union européenne, qu'un tel principe impose aux autorités juridictionnelles nationales de faire prévaloir les normes de l'Union européenne sur l'ensemble des normes nationales, fussent-elles constitutionnelles. Cette solution n'était pas sans soulever certaines difficultés. « Le problème [tenait] à ce que la norme constitutionnelle, elle non plus, [n'a pas renoncé] à sa supériorité face à la norme internationale ou européenne. » Les juridictions nationales n'ont dès lors cessé de contester ce principe de la primauté communautaire, lui opposant le principe de souveraineté étatique. Néanmoins, après plusieurs années d'opposition, la Cour de justice de l'Union européenne et les cours constitutionnelles nationales auraient trouvé une certaine voie pour la conciliation de leurs jurisprudences respectives. Ce dépassement de l'opposition résulterait d'un mouvement général, partagé par l'Union européenne et par les États membres, de reconnaissance et de prise en considération sur le plan juridique de particularités spécifiques intrinsèques des États, à la faveur de l'élaboration d'un langage commun relatif à leur identité. En effet, il est possible de constater*

[371] *Cf. L'identité de l'État dans l'Union européenne : entre « identité nationale » et « identité constitutionnelle » :* https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2012-3-page-13.htm

qu'un rapprochement s'est fait empiriquement autour de deux concepts : le concept européen d'identité nationale et d'un concept national d'identité constitutionnelle[372].

[…] En France, le Conseil constitutionnel a ainsi clairement affirmé « que la transposition d'une directive ne saurait aller à l'encontre d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France », partant du postulat de principe selon lequel l'existence du principe de primauté « est sans incidence sur l'existence de la Constitution française et sa place au sommet de l'ordre juridique interne ». Dans les premiers commentaires de cette décision, ce nouveau concept a été beaucoup discuté. Outre le fait que sa signification puisse paraître obscure, il semble certain que cette référence soit faite pour « [permettre] de maintenir le principe du primat constitutionnel » dans un contexte qui n'est pas sans faire référence aux évolutions du droit de l'Union, comme s'il existait entre les dispositions du traité et la jurisprudence des juridictions constitutionnelles, un « lien de parenté ». Cette position n'est pas propre à la France. D'autres juridictions constitutionnelles ont, elles aussi, eu recours au concept d'identité constitutionnelle. Bien que les positions ne soient pas équivalentes sur tous les points, force est de constater qu'il existe bien entre les différents juges des États membres une communauté d'esprit. Par exemple, la jurisprudence allemande récente permet de considérer que le juge de Karlsruhe se reconnaît compétent pour contrôler le respect, par le droit de l'Union, de l'identité constitutionnelle allemande. Dans un certain sens, du point de vue constitutionnel, de telles jurisprudences participent à la démarche, déjà ancienne, de la reconnaissance de réserves constitutionnelles. »

Selon Tania Groppi, professeure de droit public à l'Université de Sienne : *« un élément-clé pour comprendre l'attitude des cours nationales dans un contexte de crise, dans lequel les droits sont mis en danger par des décisions politiques centrées sur l'intérêt publique, est précisément leur relation avec les cours européennes. Les cours constitutionnelles nationales les plus activistes et attentives aux droits y trouvent des alliées très importantes, avec lesquelles elles peuvent développer une véritable stratégie de garantie des droits. Au contraire, les cours les plus timides et les plus influencées par le pouvoir politique peuvent, ainsi que les gouvernements, avoir du mal à accepter les décisions européennes. […] Ce qui s'avère décisif dans l'espace juridique européen n'est pas le dialogue horizontal, mais le dialogue vertical. En conséquence des nouveaux défis, l'interaction des cours nationales avec les cours européennes devient encore plus importante : seulement une alliance, une réponse coordonnée des différents sujets qui composent le système « multilevel » peut conduire – même en temps difficiles – à une plus complète garantie des droits et libertés.* »[373]

Or des signes positifs apparaissent au niveau du Conseil de l'Europe à cet égard, la possibilité d'un recours aux dispositions du protocole n° 16 annexé à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales[374] offrant des garanties nouvelles en matière de consultation de la Cour par des juridictions nationales[375].

---

[372] *« L'« identité constitutionnelle », comme la « supra-constitutionnalité », est un ensemble de valeurs dont le respect s'impose à toutes les autres normes, y compris constitutionnelles ou européennes. Leur rôle à l'égard de l'ordre juridique est à la fois d'en légitimer le fondement et d'en structurer le fonctionnement. Très proches dans les fonctions qu'elles remplissent, les deux notions peuvent également utilement se consolider l'une et l'autre au moment d'en assurer le respect.* »
(Cf. Edouard Dubout *in « Les règles ou principes inhérents à l'identité constitutionnelle de la France » : une supra-constitutionnalité ? par Édouard Dubout (Revue française de droit constitutionnel 2010/3 (n° 83), pages 451 à 482) :*
https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2010-3-page-451.htm

[373] *Nouveaux défis pour l'Etat constitutionnel de droit en Europe: quel rôle pour le « dialogue des juges » ?*
https://www.academia.edu/38140470/Nouveaux_d%C3%A9fis_pour_l_Etat_constitutionnel_de_droit_en_Europe_quel_r%C3%B4le_pour_le_dialogue_des_juges_

[374] *Protocole n° 16 annexé à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales :*
https://www.echr.coe.int/Documents/Protocol_16_FRA.pdf

[375] *Protocole n° 16 à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales - Rapport explicatif :*
https://www.echr.coe.int/Documents/Protocol_16_explanatory_report_FRA.pdf

Pour autant, la tournure des évènements qui se sont succédés à l'occasion du contentieux opposant les institutions de l'Union ainsi que le Conseil de l'Europe à la Pologne à l'égard de la réforme du système judiciaire de cette dernière, et plus fondamentalement encore, à l'égard de la primauté du droit européen sur le droit constitutionnel polonais, illustre les difficultés qu'éprouvent encore les institutions supranationales lorsqu'elles tentent de restaurer un Etat de droit dans un Etat membre.

Sébastien Platon précise dans son article cité *supra : « L'exécution du droit de l'Union européenne est régie par le principe d'administration indirecte, codifié par le traité de Lisbonne à l'article 291 TFUE, en vertu duquel c'est en principe aux Etats membres de prendre « toutes les mesures de droit interne nécessaires pour la mise en œuvre des actes juridiquement contraignants de l'Union ». Ce principe s'applique, mutatis mutandis, à la fonction juridictionnelle : les juridictions nationales constituent les juges de droit commun du droit de l'Union européenne. Le rôle des juridictions nationales est important, comme l'a souligné la Cour de justice dans l'arrêt Unión de Pequeños Agricultores. Selon la Cour, « la Communauté européenne est une communauté de droit dans laquelle ses institutions sont soumises au contrôle de la conformité de leurs actes avec le traité et les principes généraux du droit dont font partie les droits fondamentaux ». Cependant, la recevabilité des recours en annulation formés par les particuliers contre les actes de l'Union est limitée par les conditions de recevabilité posées par les traités. Par conséquent, les « personnes physiques ou morales ne pouvant pas, en raison des conditions de recevabilité visées à l'article 173, quatrième alinéa, du traité, attaquer directement des actes communautaires de portée générale » doivent avoir « la possibilité, selon les cas, de faire valoir l'invalidité de tels actes soit, de manière incidente en vertu de l'article 184 du traité, devant le juge communautaire, soit devant les juridictions nationales et d'amener celles-ci, qui ne sont pas compétentes pour constater elles-mêmes l'invalidité desdits actes (...) à interroger à cet égard la Cour par la voie de questions préjudicielles ». Pour que ce « détour » par le juge national soit possible, « il incombe aux États membres de prévoir un système de voies de recours et de procédures permettant d'assurer le respect du droit à une protection juridictionnelle effective ». Cette obligation jurisprudentielle a été codifiée par le Traité de Lisbonne à l'art. 19§1, al. 2, TUE : « Les États membres établissent les voies de recours nécessaires pour assurer une protection juridictionnelle effective dans les domaines couverts par le droit de l'Union ».*

Il pouvait sembler que cette disposition n'imposait pas de standards spécifiques quant à la qualité des voies de recours offertes par le droit interne, sous réserve d'assurer une « protection juridictionnelle effective », et que la Cour de justice s'appliquerait un self-restraint quant à l'évaluation des systèmes judiciaires nationaux, dont l'organisation pouvait sembler relever d'une compétence nationale réservée des Etats membres. Il pouvait d'ailleurs être argué à ce titre qu'une interprétation de l'art. 19§1, al. 2 TUE comme contenant des standards de bonne justice serait redondant avec l'art. 47 de la Charte des droits fondamentaux, qui pose le droit à un procès équitable et à un recours effectif. C'est pourtant précisément une telle interprétation « substantielle » de l'art. 19§1, al. 2, TUE que la Cour de justice a retenue dans son arrêt Associação Sindical dos Juízes Portugueses. La Cour, estimant que l'article 19 TUE « concrétise la valeur de l'État de droit affirmée à l'article 2 TUE », interprète cette disposition comme interdisant aux Etats membres d'adopter des mesures qui mettent en cause l'indépendance des juridictions nationales susceptibles de se prononcer sur des questions portant sur l'application ou l'interprétation du droit de l'Union – c'est-à-dire, virtuellement, une écrasante majorité voire la quasi-totalité des juridictions nationales. Cette solution permet une applicabilité plus large des standards du procès équitable que l'article 47 de la Charte. En effet, alors que l'article 47 pose un droit subjectif à un procès équitable, lequel n'est applicable aux Etats membres que lorsqu'ils « mettent en œuvre » le droit de l'Union (c'est-à-dire, selon

la jurisprudence de la Cour de justice, dans le champ d'application du droit de l'Union), l'article 19, interprété à la lumière de la valeur de l'Etat de droit, pose un principe objectif et structurel de nature constitutionnelle opposable à des mesures nationales susceptibles d'affecter des juridictions nationales susceptibles d'appliquer le droit de l'Union même si ces mesures ne se situent pas elles-mêmes dans le champ d'application du droit de l'Union.

La fonction immédiate du standard de l'Etat de droit est ici de « substantialiser », c'est-à-dire investir d'un contenu qualitatif, l'obligation découlant pour les Etats membres de l'art. 19§1 TUE de mettre en place « les voies de recours nécessaires pour assurer une protection juridictionnelle effective dans les domaines couverts par le droit de l'Union ». Cette obligation étant une obligation structurelle (voire structurante) du système juridictionnel de l'Union, distincte de l'obligation de respecter les droits fondamentaux qui est fonctionnellement limitée par le champ d'application du droit de l'Union, elle permet en retour d'accroître sensiblement l'applicabilité dudit standard de l'Etat de droit aux Etats membres. Au-delà de cette fonction immédiate dans le raisonnement de la Cour, l'arrêt Associação Sindical dos Juízes Portugueses manifeste aussi une fonction plus globale du standard de l'Etat de droit, à savoir une structuration du pouvoir judiciaire multiniveaux de l'Union dont l'art. 19§1 TUE consacre l'existence. Pour le dire autrement, lorsque les juges nationaux agissent en tant que juges de l'Union européenne, ils sont assujettis aux mêmes standards que ceux auxquels l'Union européenne s'assujettit elle-même. Il en va de la légitimité de l'application juridictionnelle du droit de l'Union mais également de la coopération entre juges nationaux et Cour de justice. En particulier, dans le cadre de la procédure préjudicielle, la Cour de justice se trouve en relation directe avec les juridictions nationales, sur l'indépendance desquelles elle doit pouvoir compter et qui constitue l'une des conditions pour qu'un organe étatique soit considéré comme une « juridiction » au sens de ladite procédure.

En conclusion, on peut constater une « diffusion » du standard de l'Etat de droit dans le système constitutionnel de l'Union. De standard permettant d'étendre, dans une certaine mesure, l'office de la Cour de justice, il est devenu un standard de référence pour le juge national, juge de droit commun de droit de l'Union, dans un contexte de crise de l'Etat de droit dans plusieurs pays européens. Pour l'heure, c'est essentiellement le principe d'indépendance de la justice qui a été mobilisé dans la jurisprudence de la Cour. Cette focalisation résulte probablement du contexte : c'est essentiellement cet aspect de l'Etat de droit qui est en cause actuellement en Pologne et en Hongrie. Or, l'indépendance n'est que l'un des principes constitutifs de l'Etat de droit. On peut alors se demander si, à cette diffusion du standard de l'Etat de droit aux Etats membres, succèdera une densification de celui-ci, incluant l'ensemble des principes constitutifs de l'Etat de droit. »

Dans un autre article, Sébastien Platon aborde les ambiguïtés attachées à la mise en oeuvre nationale du droit de l'Union au sens de l'article 51 de la Charte : *« La portée de l'applicabilité aux Etats membres de la Charte des droits fondamentaux de l'Union européenne souffre d'une certaine ambiguïté liée aux termes utilisés à l'article 51, et notamment à la notion de « mise en oeuvre » du droit de l'Union par les Etats membres. Deux arrêts récents, l'arrêt Akerberg Fransson et l'arrêt Melloni, sont venus apporter certaines précisions. Le premier semble confirmer une conception large mais limitée de l'applicabilité de la Charte aux Etats membres. Le deuxième apporte d'intéressante précisions sur la coexistence des standards européens et nationaux de protection des droits fondamentaux dans le champ d'application de la Charte.*

Ces deux arrêts apportent d'instructifs éclairages sur la notion de mise en oeuvre nationale du droit de l'Union au sens de l'article 51 de la Charte. »[376]

En France, préalablement à la ratification du Traité de Lisbonne par le Parlement réuni en congrès, le président de la République a saisi le Conseil constitutionnel pour requérir son avis sur la compatibilité de ce nouveau traité avec la Constitution française d'alors.

Cette saisine a permis au Conseil constitutionnel, outre sa décision établissant à une non-conformité partielle et appelant en conséquence à une modification de la Constitution rendant possible ladite ratification, de rappeler dans ses considérants :

« 3. Considérant que, par le préambule de la Constitution de 1958, le peuple français a proclamé solennellement « son attachement aux droits de l'homme et aux principes de la souveraineté nationale tels qu'ils ont été définis par la Déclaration de 1789, confirmée et complétée par le préambule de la Constitution de 1946 » ;

4. Considérant que, dans son article 3, la Déclaration des droits de l'homme et du citoyen énonce que « le principe de toute souveraineté réside essentiellement dans la nation » ; que l'article 3 de la Constitution de 1958 dispose, dans son premier alinéa, que « la souveraineté nationale appartient au peuple qui l'exerce par ses représentants et par la voie du référendum » ;

5. Considérant que le préambule de la Constitution de 1946 proclame, dans son quatorzième alinéa, que la République française se « conforme aux règles du droit public international » et, dans son quinzième alinéa, que « sous réserve de réciprocité, la France consent aux limitations de souveraineté nécessaires à l'organisation et à la défense de la paix » ;

6. Considérant que, dans son article 53, la Constitution de 1958 consacre, comme le faisait l'article 27 de la Constitution de 1946, l'existence de « traités ou accords relatifs à l'organisation internationale » ; que ces traités ou accords ne peuvent être ratifiés ou approuvés par le Président de la République qu'en vertu d'une loi ;

7. Considérant que les conditions dans lesquelles la République française participe aux Communautés européennes et à l'Union européenne sont fixées par les dispositions en vigueur du titre XV de la Constitution, hormis celles du second alinéa de l'article 88-1 qui est relatif au traité établissant une Constitution pour l'Europe, lequel n'a pas été ratifié ; qu'aux termes du premier alinéa de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'États qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences » ; que le constituant a ainsi consacré l'existence d'un ordre juridique communautaire intégré à l'ordre juridique interne et distinct de l'ordre juridique international ;

8. Considérant que, tout en confirmant la place de la Constitution au sommet de l'ordre juridique interne, ces dispositions constitutionnelles permettent à la France de participer à la création et au développement d'une organisation européenne permanente, dotée de la personnalité juridique et investie de pouvoirs de décision par l'effet de transferts de compétences consentis par les États membres ;

9. Considérant, toutefois, que, lorsque des engagements souscrits à cette fin contiennent une clause contraire à la Constitution, remettent en cause les droits et libertés constitutionnellement

[376] *La Charte des droits fondamentaux et la « mise en œuvre » nationale du droit de l'Union : précisions de la Cour de justice sur le champ d'application de la Charte (à propos des arrêts Åklagaren et Melloni de la Cour de justice du 26 février 2013) :* https://www.academia.edu/4411322/La_Charte_des_droits_fondamentaux_et_la_mise_en_%C5%93uvre_nationale_du_droit_de_l_Union_pr%C3%A9cisions_de_la_Cour_de_justice_sur_le_champ_d_application_de_la_Charte_%C3%A0_propos_des_arr%C3%AAts_%C3%85klagaren_et_Melloni_de_la_Cour_de_justice_du_26_f%C3%A9vrier_2013_

garantis ou portent atteinte aux conditions essentielles d'exercice de la souveraineté nationale, l'autorisation de les ratifier appelle une révision constitutionnelle ;

10. Considérant que c'est au regard de ces principes qu'il revient au Conseil constitutionnel de procéder à l'examen du traité de Lisbonne, ainsi que de ses protocoles et de son annexe ; que sont toutefois soustraites au contrôle de conformité à la Constitution celles des stipulations du traité qui reprennent des engagements antérieurement souscrits par la France ; »[377]

Plus récemment, en avril 2021, s'opposant partiellement à la reconnaissance d'une décision de la CJUE encadrant la possibilité pour les Etats de recourir à la surveillance généralisée des échanges numériques, le Conseil d'Etat a arrêté à cet égard la position suivante : *« Tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique interne, l'article 88-1 confirme la place de la Constitution de 1958 au sommet de ce dernier. Il appartient au juge, s'il y a lieu, de retenir de l'interprétation que la Cour de justice de l'Union européenne a donnée des obligations résultant du droit de l'Union la lecture la plus conforme aux exigences constitutionnelles autres que celles qui découlent de l'article 88-1, dans la mesure où les énonciations des arrêts de la Cour le permettent. Dans le cas où l'application d'une directive ou d'un règlement européen, tel qu'interprété par la Cour de justice de l'Union européenne, aurait pour effet de priver de garanties effectives l'une de ces exigences constitutionnelles, qui ne bénéficierait pas, en droit de l'Union, d'une protection équivalente, le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige. »*[378]

Invité à aborder la question fondamentale de l'autorité du droit européen lors du Congrès du 25ème anniversaire de l'Académie de droit européen (ERA) à Trèves, en octobre 2017[379], Jean-Marc Sauvé conclut son intervention en ces termes : *« La vigueur des débats et l'acuité des tensions qui ont vu le jour ou peuvent exister entre les juridictions nationales suprêmes et la Cour de justice de l'Union européenne ne doivent pas faire oublier que cette dernière a su faire preuve de mesure et d'esprit de conciliation dans de nombreux cas. Les décisions Melki, Aranyosi, ou même Gauweiler, témoignent de la volonté de la Cour de s'inscrire dans un véritable dialogue avec les plus hautes juridictions nationales. L'une des solutions aux conflits susceptibles de surgir réside, comme la décision Aranyosi l'a montré, dans l'élévation des standards européens de contrôle – en l'occurrence, des mandats d'arrêt européens –, de telle sorte que puisse être évité un écart entre la garantie nationale des droits fondamentaux – qui serait plus élevée – et la garantie européenne – qui serait plus lâche. Seul un dialogue régulier et approfondi des juridictions nationales suprêmes et des juridictions européennes peut permettre une articulation des ordres juridiques qui ne se fasse au détriment ni de l'autorité du droit de l'Union, ni de celle des normes suprêmes de droit national. Ce dialogue peut être rugueux et sans complaisance. Il doit cependant se conclure dans la convergence et la concorde. Parce que nous sommes des juges, il nous appartient de respecter la hiérarchie des normes qui s'impose à nous, le mandat qui nous est donné par les textes fondateurs qui nous instituent et la légitimité démocratique, dès lors que nous appliquons des lois qui sont l'expression de la souveraineté populaire. Parce que nous sommes des juges, nous sommes aussi des sages ou nous devons nous efforcer de l'être. Par conséquent, il ne peut être envisagé de se résoudre à des chocs frontaux et il convient de tout mettre en œuvre pour préserver les acquis de la construction européenne à laquelle les juges ont apporté une éminente contribution. Ce que nous avons entrepris ensemble depuis 60 ans, à tous les niveaux des pouvoirs publics, y compris*

[377] *Décision n° 2007-560 DC du 20 décembre 2007 :* https://www.conseil-constitutionnel.fr/decision/2007/2007560DC.htm
[378] *Décision 393099 du 21 avril 2021* : https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-04-21/393099
[379] *L'autorité du droit de l'Union européenne : le point de vue des juridictions constitutionnelles et suprêmes :* https://www.conseil-etat.fr/actualites/discours-et-interventions/l-autorite-du-droit-de-l-union-europeenne-le-point-de-vue-des-juridictions-constitutionnelles-et-supremes

au niveau juridictionnel, est plus important que ce qui peut séparer les juges nationaux et européens. Il nous faut par conséquent maintenir et faire progresser cette construction. Les techniques de conciliation et d'articulation entre les ordres et les principes juridiques doivent nous permettre de surmonter les difficultés conjoncturelles auxquelles nous pouvons être confrontés. Il y a toujours d'autres solutions à trouver que le refuge ou le repli dans l'absolutisation des principes et des jurisprudences nationales ou le glissement dans l'activisme judiciaire au niveau européen : l'élévation de la garantie des droits fondamentaux pour assurer des protections équivalentes aux plans européen et national en fait clairement partie. C'est ainsi que nous respecterons la primauté, l'unité et l'effectivité du droit de l'Union et que nous sauvegarderons les légitimes identités constitutionnelles nationales. Les premières et les secondes sont appelées à coexister durablement et pacifiquement et à se conjuguer dans une dynamique qui permettra de combler les angles morts de la mise en cohérence de nos systèmes de droit et de surmonter et régler les points de désaccord qui pourraient encore surgir. »

S'inscrivant dans le droit fil de l'avis exprimé par Jean-Marc Sauvé, les grandes juridictions nationales françaises (Conseil constitutionnel, Conseil d'Etat, ...) ont néanmoins pris le parti de composer quotidiennement des "partitions juridiques" qui entérinent *de jure* la suprématie du droit européen en usant des marges de manoeuvre dont elles disposent pour prendre leurs décisions et arrêts.

Ainsi, sous l'influence du droit européen, le Parlement français a introduit une certaine dose de proportionnalité dans certains de ses choix législatifs et le Conseil constitutionnel a approfondi son contrôle, initialement limité au contrôle de l'adéquation et parfois de la nécessité, au profit du triple test de proportionnalité : *« Exempli gratia, les récentes décisions du Conseil constitutionnel postulent pour cette emprise grandissante de la CEDH dans le droit français. Assurément, le Conseil constitutionnel fait désormais une référence explicite et presque systématique, dans ses visas, à la jurisprudence européenne, il opère également un contrôle beaucoup moins abstrait mêlé à un contrôle de proportionnalité, et tente d'uniformiser au maximum sa position aux standards européens. Dans le même temps, la CEDH a fait écho à l'entreprise du juge constitutionnel français en affirmant, implicitement pensons-nous, la compatibilité de celui-ci aux exigences européennes dans l'arrêt Jacky Renard c. France, confortant alors son entreprise. En sus, la puissance de la CEDH touche également le droit supranational, en témoigne l'arrêt Caldararu de la CJUE dans lequel elle tient compte des positions de la CEDH et fait évoluer son contrôle dans le même sens qu'elle – ayant également des conséquences en droit interne. »*[380].

En introduction d'une note du professer Ziller, les membres de l'Observatoire politique du Parlement européen de l'Institut Jacques Delors ont cherché à mettre un terme à toute polémique relative à cette question de la primauté du droit européen[381] :

« La remise en cause par le tribunal constitutionnel polonais de la primauté du droit européen a reçu de plusieurs élus politiques français un soutien inquiétant. Alors que la cour constitutionnelle hongroise pourrait à son tour emboîter le pas à la Pologne, il convient de rappeler les fondements juridiques de cette primauté et de mesurer la portée politique du débat soulevé.

[380] *Cf.* Thomas Escach-Dubourg *in Le contrôle concret de conventionnalité des Lois du Juge administratif et l'exigence de prévisibilité juridique :* https://www.academia.edu/35271196/Thomas_Escach_Dubourg_Le_contr%C3%B4le_concret_de_conventionnalit%C3%A9_des_Lois_du_Juge_administratif_et_lexigence_de_pr%C3%A9visibilit%C3%A9_juridique_M%C3%A9moire_de_recherche_sous_la_direction_de_M_le_Professeur_Xavier_BIOY_Universit%C3%A9_Toulouse_1_Capitole_2017_233_p

[381] *Primauté du droit européen, une fausse querelle juridique, un non problème politique :* https://institutdelors.eu/publications/primaute-du-droit-europeen-une-fausse-querelle-juridique-un-non-probleme-politique/

Dans son explication juridique ci-après, le professeur Ziller, sollicité par notre Institut, remonte à l'origine de cette primauté. Elle découle directement de l'obligation des États de respecter les traités qu'ils ont conclus. Ce principe ancien est au fondement de tout le droit international, selon le vieux principe énoncé dans l'adage « pacta sunt servanda » – tout traité doit être intégralement honoré. Ce principe est repris dans toutes les constitutions européennes, comme le fait l'article 55 de notre constitution en France. L'application de ce principe au droit communautaire a été établie depuis 1964 par une jurisprudence constante de la Cour de justice de l'UE.

Cette primauté vaut pour les traités européens comme pour la Charte européenne des droits fondamentaux et pour tout le droit de l'Union, jugements de la Cour compris. Primauté n'est pas pour autant à confondre avec suprématie, propre à un système fédéral. Le droit européen, créé sur la base des traités et applicable dans chaque pays, prime sur les lois nationales. Mais cette primauté ne fait pas obstacle à la souveraineté des États qui, à la différence par exemple des États américains à l'époque de Lincoln, ont le droit de dénoncer les traités européens et de faire sécession par rapport à l'Union européenne (Brexit). En cas de différend entre une norme européenne et une disposition constitutionnelle nationale, le conflit ne peut se résoudre que par la révision de la norme constitutionnelle ou la modification éventuelle des traités ou de la jurisprudence européenne.

Depuis le premier jour, le problème a été soulevé et réglé a priori avant chaque nouveau traité européen : en cas de contradiction entre le projet de traité et la constitution nationale, celle-ci doit être modifiée. La France l'a fait en 1992 pour le transfert de la compétence monétaire à l'Union. Cette saine pratique limite considérablement les risques ultérieurs de conflit entre droit européen et constitutions nationales. Si, malgré cela, un différend apparaît ultérieurement, le dialogue est ouvert : les cours suprêmes peuvent échanger entre elles ainsi que les gouvernements. En attendant, le droit européen prévaut, jusqu'à une éventuelle révision des traités ou un changement de la jurisprudence européenne sur ce différend.

La primauté européenne n'empêche pas non plus un État d'invoquer son « identité constitutionnelle ». Mais c'est le rôle de la Cour européenne de Justice d'apprécier l'opposabilité de cette identité au regard des principes et règles des traités européens, en dialogue avec les juridictions nationales. Si chaque cour constitutionnelle nationale se considérait comme juge ultime de cette identité, nous nous retrouverions très exactement dans une Europe à la carte, contre laquelle la France s'est toujours battue.

Pour les citoyens, la meilleure comparaison est celle du contrat de droit civil. Si, locataire, je suis en désaccord avec mon propriétaire, c'est à un médiateur ou à un juge, choisis à l'avance, de régler le différend. Le traité est le contrat de la famille européenne, et le juge choisi à l'unanimité par tous les membres est la Cour de Justice de l'Union.

Enfin, cette primauté du droit s'articule parfaitement avec le principe de subsidiarité, en vertu duquel l'UE intervient seulement lorsqu'un objectif ne peut être atteint de manière suffisante par les États membres mais peut l'être mieux au niveau de l'Union. La Cour de Luxembourg ne manque pas de sanctionner les textes européens qui méconnaissent ce principe.

Ces rappels juridiques fondamentaux permettent de mesurer l'enjeu du débat politique qui fait fi de ces principes. À l'approche de la présidentielle française, plusieurs candidats à cette élection proposent un « bouclier constitutionnel » ou un moratoire juridique pour faire échapper la France aux décisions communautaires qui leur déplairaient, en inventant une primauté nationale sur un droit européen, qui est à la fois dépeint comme étranger et échappant aux principes du droit international.

Pays fondateur, moteur reconnu de toutes les avancées européennes, la France se décrédibiliserait si elle mettait en doute sa signature apposée sur les traités européens, qui ont tous été ratifiés par son parlement ou par son peuple. Ce débat politique joue donc avec le feu de notre réputation en Europe et dans le monde, y compris à l'égard des marchés financiers vis-à-vis desquels le niveau de notre dette publique nous rend si vulnérables. Les huit présidents qui se sont succédés depuis le début de la Ve République ont pu avoir des visions différentes de l'Europe, mais tous y ont voulu la France exemplaire.

Respecter la primauté européenne n'enfreint nullement la souveraineté. L'UE est issue de la volonté de ses parties contractantes. Par essence, elle ne dispose pas de « la compétence de sa compétence », selon la définition première de la souveraineté inspirée aux juristes allemands par Jean Bodin. Les institutions européennes préfèrent invoquer une « autonomie stratégique » ou une « capacité d'agir ». Derrière ces formules aux diverses fortunes, l'idée est bien de recourir aux leviers normatifs et financiers, à disposition des Vingt-Sept, et de créer les nouveaux instruments à même de donner à l'UE les moyens de s'affirmer comme puissance. La primauté du droit européen et, son corollaire, l'autorité de la Cour de justice de l'Union, sont gages de confiance entre les Vingt-Sept. Elles cimentent leur unité, à faire valoir au reste du monde. Cette primauté assure la cohérence indispensable au fonctionnement du marché intérieur, qui fait la force première des Européens dans leurs rapports avec les autres puissances.

Sachons voir que si la primauté du droit européen n'était pas reconnue, celui-ci succomberait purement et simplement, chacune des parties prenantes s'estimant autorisée à l'interpréter à sa guise, voire à s'en affranchir. Cessons donc toute inutile querelle sur la primauté du droit européen. Respecter cette primauté, c'est tout simplement permettre à l'Union européenne d'exister. »

- *Le revirement de jurisprudence du Conseil constitutionnel constitue un gage de progrès pour l'Etat de droit*

Pour le professeur Thierry Di Manno, le revirement de jurisprudence est, tout à la fois, un gage de légitimité pour le Conseil constitutionnel et un gage de progrès pour l'État de droit, sans remettre en cause la stabilité de la jurisprudence du Conseil constitutionnel :

« Comme l'a souligné pertinemment P. Pactet, « les revirements de jurisprudence ne (sont) pas plus fréquents que les révisions constitutionnelles ». En effet, le phénomène des revirements ne prend pas dans la jurisprudence du Conseil constitutionnel une ampleur considérable.

[…] Il est possible, néanmoins, que ce phénomène, qui s'est d'ailleurs accentué ces dernières années, connaisse une sorte de progression naturelle dans l'avenir, dans la mesure où le revirement est inhérent au développement de la jurisprudence constitutionnelle. Il reste qu'il serait excessif, caricatural et injuste de voir dans cette vingtaine de revirements l'inconstance du Conseil constitutionnel. Au contraire, le Conseil constitutionnel est attaché à assurer la plus grande continuité à son œuvre jurisprudentielle, qui est d'ailleurs largement facilitée par le renouvellement partiel du collège tous les trois ans. L'autorité persuasive de sa jurisprudence […] joue, donc, pleinement à l'égard du Conseil constitutionnel lui-même. Tout en restant exceptionnel, le revirement apparaît, dans ces conditions, comme l'élément indispensable à la respiration de la jurisprudence constitutionnelle.

[…] les revirements ne s'inscrivent jamais véritablement en rupture avec l'évolution générale de la jurisprudence. Ils en confortent, le plus souvent, la cohérence. Il est possible même d'affirmer que, lorsqu'ils touchent à la garantie des droits, les revirements semblent être à sens unique. En effet, ces revirements-là, qui sont les plus nombreux, marquent tous un renforcement de la protection des droits et libertés constitutionnellement garantis.

Tout entier pétri de son rôle de gardien des droits fondamentaux constitutionnels, le Conseil constitutionnel ne peut raisonnablement pas utiliser le revirement pour porter atteinte à son image. Pour cela, le revirement qui marque une régression dans la garantie des droits, est nécessairement exclu par le Conseil constitutionnel.

Il n'y a sans doute pas là le respect d'une obligation constitutionnelle, mais, plus vraisemblablement, une contrainte que le Conseil constitutionnel s'impose à lui-même.»[382]

[382] *Les revirements de jurisprudence du Conseil constitutionnel français :* https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/les-revirements-de-jurisprudence-du-conseil-constitutionnel-francais

Quelques pistes de progrès sur le registre du droit

« Faisons face au temps comme il nous cherche »

(Shakespeare)

Dans un article traitant de ces sujets, Arnaud Merle et Thibaud Zuppinger se veulent rassurants : *« « Dis-moi ta technologie et je te dirai qui tu es, quels sont tes imaginaires et tes angoisses ». La cyber-infusion du numérique sur le réel matériel a-t-elle donc vidé notre monde de ses mystères ? Si l'on définit l'entropie comme la mesure du degré d'incertitude, alors il faut accueillir les temps numériques comme une chance. Les aborder avec prudence permet d'envisager autant de mondes à faire et pas seulement à taire. »*[383]

« La numérisation est désormais un fait social quasiment total, même si beaucoup d'inégalités d'accès aux réseaux persistent : elle symbolise en tout cas des potentialités considérables d'un point de vue sociétal, politique et économique. Le numérique change nos vies privées et publiques. Les pratiques sociales sont elles-mêmes en métamorphose majeure : l'accès aux réseaux offre des capacités de décentrement dans la construction de soi, intervenant ainsi sur les imaginaires institués, et les expériences de socialité en ligne ont en ce sens une dimension existentielle à part entière. Les individus sont susceptibles d'être ouverts à des sources d'influence culturelles, intellectuelles, affectives ou idéologiques beaucoup plus variées qu'autrefois. La variété des supports technologiques permet de créer des sensibilités plus ouvertes à des expressions culturelles hétérogènes, ainsi qu'à des causes transnationales. Les pratiques politiques, par le biais des mobilisations sociales en ligne, évoluent en faveur de davantage de transparence dans l'organisation de la vie commune. Tour à tour émetteurs, récepteurs et relais d'information, les citoyens sont désormais en mesure de s'attaquer à la traditionnelle culture du secret du pouvoir étatique. De Wikileaks aux Panama Papers, l'ère numérique permet l'ouverture de brèches de contournement des ordres institués assez inédites. Une culture de l'horizontalité s'est imposée depuis que nous vivons en réseau et que nous sommes devenus hyperconnectés. »[384]

Si la construction même de la gouvernance de la toile, tout comme son imaginaire en phase avec les rêves de ses pionniers, portent bel et bien une vision démocratique qui renaît sans aucun doute dans la *Legal-tech*, la *Civic-tech*[385] ou la *Social-tech*[386], les vulnérabilités qui pèsent sur la disponibilité en continu du web et d'Internet[387,388,389,390,391] ou sur l'environnement[392] sont de nature à engager les responsables des principales institutions démocratiques à mener une réflexion approfondie sur les risques pour les nations comme pour les puissances publiques d'un usage exclusif de cette infrastructure vulnérable à plus d'un titre alors même que les capacités

[383] *Cf. Calculabilité et entropie numérique* : https://aoc.media/analyse/2021/07/15/calculabilite-et-entropie-numerique/

[384] *Cf.* Pierre-Antoine Chardel *in Quelles orientations numériques en France : un enjeu démocratique et citoyen :* https://theconversation.com/quelles-orientations-numeriques-en-france-un-enjeu-democratique-et-citoyen-170053

[385] *Cf.* https://digital-society-forum.orange.com/fr/les-forums/878-la-civic-tech-une-revolution-democratique

[386] *Cf.* https://digital-society-forum.orange.com/fr/les-forums/882-la-social-tech-le-numerique-au-service-de-linnovation-sociale

[387] *What would happen if the Internet collapsed?* : https://computer.howstuffworks.com/Internet/basics/Internet-collapse1.htm

[388] *Vulnérabilité des services d'authentification web :* https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_des_services_d%27authentification_web

[389] *Sécurité et vulnérabilité de l'Internet et des réseaux sous les océans :* https://www.mag-securs.com/news/id/36095/securite-et-vulnerabilite-de-l-Internet-et-des-reseaux-sous-les-oceans.aspx

[390] *En 2050, Internet sera-t-il toujours debout ? :* https://www.cnetfrance.fr/news/en-2050-Internet-sera-t-il-toujours-debout-39891341.htm?fbclid=IwAR1ds0GrZ20tS6b2Fb1FYpjTUhNaDLe_APaafIlIP8yLWgWqHoduGxPI6tk

[391] *Sans les câbles sous-marins, plus d'Internet : l'Europe est-elle prête ?* https://theconversation.com/sans-les-cables-sous-marins-plus-dInternet-leurope-est-elle-prete-169858

[392] *Cf.* Anne-Cécile Orgerie et Laurent Lefèvre *in Le vrai coût énergétique du numérique :* https://www.pourlascience.fr/sd/environnement/le-vrai-cout-energetique-du-numerique-20490.php

de calcul et de stockage de l'information continuent de croître[393, 394] et qu'une nouvelle génération d'Internet est en préparation.

Écrivain et philosophe, Éric Sadin analyse dans son dernier essai, *'L'Ère de l'individu tyran'*, l'avènement de l'*« individu tyran »* et l'effacement d'un *« monde commun »*.[395]

« Le traitement de masses de données à l'aide d'algorithmes ad hoc autorise une prédictibilité toujours plus fiable des événements en cours de germination. Certes, il demeure encore de nombreuses failles, néanmoins c'est une disposition technique qui ne cesse de se perfectionner. Cette propension a massivement gagné le régime militaro-sécuritaire à la suite des attentats de septembre 2001, poussant les agences de renseignement, notamment la NSA, à chercher à repérer des projets malveillants avant même qu'ils ne se réalisent. Dimension anticipative qui a par la suite gagné de nombreux autres secteurs : le marketing, la logistique industrielle, la santé… De son côté, le pouvoir politique s'empare peu à peu de ces nouvelles facultés techniques dessinant des scénarios anticipatifs qui conduisent à engager des actions au présent en fonction de l'estimation de l'impact futur sur l'opinion. On voit que c'est la notion de projet et de risque politiques qui ici s'affaiblissent, au profit d'analyses algorithmiques appelées à paralyser toute idée novatrice ou à contre-courant. Ici la technique dicte des règles non dites à l'action publique. […] Nous vivons un moment d'extrême saturation à l'endroit d'un ordre politique et économique en vigueur depuis près d'un demi-siècle qui avive l'intention résolue de ne plus subir les situations les bras croisés. Dorénavant, un grand nombre de personnes se trouvent tiraillées entre deux états contraires. D'une part, entre le constat de ne plus s'appartenir, de faire l'objet de pressions permanentes dans l'exercice du travail, d'être confronté à des situations de plus en plus précaires. Et, d'autre part, le fait d'user de technologies de facilitation de l'existence donnant le sentiment de bénéficier d'un surcroît de puissance. Cette tension est explosive, car elle contribue à nous imaginer tels des sujets autarciques reliés à nos instruments technologiques, supposés nous offrir une plus grande maîtrise et libérant l'expression continuelle de nos rancœurs. »

En 2022, la numérisation et la virtualisation des entreprises et de la société continueront leur développement à un rythme effréné.

Toutefois, le besoin de durabilité, l'augmentation constante des volumes de données et l'accroissement des vitesses de calcul et de réseau commenceront à retrouver leur statut de moteurs les plus importants de la transformation numérique.[396]

---

[393] *Cf.* Jean-Paul Delahaye *in Le monde numérique passe au Zetta :* https://www.pourlascience.fr/sd/informatique/le-monde-numerique-passe-au-zetta-22402.php

153

[394] *« En 2020, l'humanité a produit 45 zettaoctets1 de données numériques. Ce volume devrait atteindre 175 Zo en 2025. Face à cette croissance vertigineuse des données, les supports actuels (optiques, bandes magnétiques ou disques durs) semblent avoir atteint leurs limites : fragiles, ils ont une espérance de vie de 5 à 7 ans ; énergivores, les data centers qui les accueillent consomment désormais près de 2 % de la production électrique mondiale ; volumineux, enfin, car la surface occupée par ces infrastructures ne cesse de croître elle aussi : 167 km² à l'échelle mondiale. Or, avec l'essor de l'intelligence artificielle et l'avènement du big data, la demande en octets n'est pas près de diminuer.* « *En matière de stockage de données générées, nous vivons à crédit depuis quelques années. Si nous sommes aujourd'hui capables d'en stocker 30 %, sans rupture technologique, ce chiffre pourrait tomber à 3 % dans les prochaines décennies* », *alerte Stéphane Lemaire, chercheur au Laboratoire de biologie computationnelle et quantitative. Pourtant, stockée sur de l'ADN, l'intégralité des données mondiales pourrait tenir dans le volume d'une boîte à chaussures. L'ADN constituerait ainsi une solution envisagée et envisageable pour les données dites froides (environ 70 % des données générées chaque année), rarement consultées mais néanmoins précieuses, telles les archives. L'idée d'utiliser l'ADN comme support d'information numérique n'est pas nouvelle : dès 1959, le physicien américain Richard Feynman, prix Nobel en 1965, l'avait déjà suggérée. Mais ce n'est qu'en 2012 que celle-ci s'est concrétisée.* « Toutefois, les technologies de stockage actuelles sont toutes basées sur des méthodes chimiques, physiques et mathématiques ; la piste biologique n'avait pas encore été explorée », *souligne Stéphane Lemaire. »*
Source : *https://lejournal.cnrs.fr/articles/stockage-de-donnees-la-revolution-sur-adn)*

[395] *Cf.* cet entretien avec Eric Sadin sur notre impuissance politique : https://www.youtube.com/watch?v=UlFGkut-j8s

[396] *Technologie : les 5 plus grandes tendances qui vont faire 2022 :* https://www.forbes.fr/technologie/technologie-les-5-plus-grandes-tendances-en-2022/

Les éléments d'analyse exposés *supra* démontrent la nécessité de repenser le droit pour que la promesse démocratique ne soit pas irréversiblement altérée par l'incapacité de l'Etat et des institutions européennes et internationales à anticiper les risques et menaces que font peser sur elle des usages inappropriés du numérique.

Le professeur Dominique Rousseau affirme : *« Comme la musique, le numérique mène nécessairement au droit ! Et, dans cette configuration historique, le droit est et reste le seul médium laïc où enraciner les règles de vivre ensemble. À une triple condition. Qu'il soit pensé et posé au niveau global et non plus au niveau des États. Qu'il soit élaboré par une délibération connectée de la société civile globale. Qu'il soit animé par le principe de libre accès à l'espace et à la culture numérique en raison, selon les mots du Conseil constitutionnel dans sa décision du 10 juin 2009, « du développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions ». Si la civilisation numérique est globale, le droit doit être global.* »[397]

Est-il opportun de procéder à un *aggiornamento* des droits de l'homme pour l'adapter à une technique, alors que la technique est, par nature, changeante et évolutive ?

Cet objet nouveau qu'est le numérique peut générer l'émergence de règles nouvelles, de limites nouvelles, d'extensions nouvelles. Ces spécificités suffisent-elles à changer l'essence d'un droit ? Et si oui, à partir de combien de spécificités change-t-on de nature juridique ? Faut-il en réalité, au-delà de l'existence de règles spécifiques (on en trouvera toujours) un paradigme spécifique ? Bien que des réponses multiples aient pu être apportées à ces interrogations fondamentales[398], on voit bien que l'identité numérique, en substituant à l'individu un corpus de données intangibles d'un genre nouveau, appelle à l'élaboration de nouveaux droits fondamentaux à l'instar de celui d'*« autodétermination informationnelle »,* ou de celui de *« déconnexion »*.

Que ce soit au niveau mondial, au niveau européen ou au niveau national, plus que jamais, le juriste doit être innovant et le droit novateur.

[397] *Le numérique, nouvel objet du droit constitutionnel :* https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-nouvel-objet-du-droit-constitutionnel

[398] Voir par exemple à cet égard Sébastien Platon *in La fondamentalité des droits à l'ère du numérique :* https://www.academia.edu/35420878/La_fondamentalit%C3%A9_des_droits_%C3%A0_l_%C3%A8re_du_num%C3%A9rique

Il est indispensable de poursuivre et développer les initiatives internationales déjà engagées en leur donnant un socle institutionnel prenant en compte les bouleversements profonds à l'œuvre

Devant les grands bouleversements induits par les technologies issues de la 4ème révolution industrielle et par les recommandations puissantes du '*Great Reset*'[399] qui a trouvé dans la pandémie de la Covid19 une occasion historique pour son amorçage[400], aucune réponse nationale ou régionale ne parviendra seule à résoudre les problématiques soulevées en matière d'éthique ou de droit.

- *La société mondiale s'est mise en mouvement*

« L'intervention des régulateurs internationaux pour encadrer le développement et l'application de l'intelligence artificielle vient en réponse à une inquiétude croissante dans l'opinion publique, confortée par la recherche, quant aux effets directs et indirects de cette technologie sur les droits des individus et la société. Les propositions de cadres éthiques n'ayant pas semblé apporter une réponse satisfaisante et convaincante, des organisations intergouvernementales telles que le Conseil de l'Europe, l'Union européenne, l'OCDE et l'UNESCO ont produit, sous l'impulsion de leurs États membres, de nombreux rapports, études, lignes directrices ou recommandations. Si ce qui pourrait être considéré comme du « droit souple » (*soft law*) *présente une influence politique, technique et morale bien plus substantielle que de simples déclarations de bonne volonté des acteurs de l'IA, l'année 2021 marque toutefois un nouveau tournant, avec le premier texte juridiquement contraignant proposé par la Commission européenne en avril 2021 pour renforcer la sécurité des produits d'IA. Le Conseil de l'Europe envisage également un mélange d'instruments juridiques contraignants et non contraignants pour prévenir les violations des droits de l'homme et des atteintes à la démocratie et à l'État de droit. »*[401]

Réservée jusqu'à présent aux travaux de l'Assemblée générale des Nations Unies, la question de la cybersécurité a pour la première fois été traitée de manière formelle par le Conseil de sécurité, lors d'un débat public organisé ce matin, en visioconférence, à l'initiative de la présidence estonienne. Cet échange de haut niveau a été l'occasion pour l'ensemble des délégations d'appeler à une réponse unie aux menaces que font peser sur la paix et la sécurité internationales les activités malveillantes dans le cyberespace.[402]

Le principal défi géopolitique à l'heure actuelle est d'établir des normes juridiques communes dans le cyberespace à l'échelle internationale.

Depuis 2004 cinq groupes d'experts gouvernementaux planchent sur le sujet au sein des Nations unies mais il a fallu attendre 2019 pour que l'ensemble des États membres des Nations unies soit représenté dans un groupe de travail à composition non limitée (*Open-Ended Working Group, OEWG*) afin d'engager concrètement la transposition et la mise en œuvre des mesures proposées par les experts gouvernementaux. Les conclusions de cet *OEWG* ont été adoptées en mars 2021.

[399] *The Great Reset* : https://www.weforum.org/great-reset/

[400] *Cf. Global Technology Governance Report 2021* : https://fr.weforum.org/reports/global-technology-governance-report-2021?fbclid=IwAR2SFZPDYYCBGfqY8AeZr0ym9Y_uNYQaQ5a1kndzPIXNJIglr8mBkD_2QRM

[401] *Cf.* Yannick Meneceur in *'analyse des principaux cadres supranationaux de régulation de l'intelligence artificielle : de l'éthique à la conformité'* : https://lestempselectriques.net/index.php/2021/05/27/analyse-des-principaux-cadres-supranationaux-de-regulation-de-lintelligence-artificielle-de-lethique-a-la-conformite/

[402] *Le Conseil de sécurité tient son premier débat formel sur la cybersécurité et les risques liés à l'utilisation malveillante des nouvelles technologies* – Communiqué de presse : https://www.un.org/press/fr/2021/sc14563.doc.htm

D'autres initiatives internationales émergent, comme le *Global Coalition for Digital Safety* du Forum économique mondial de Davos[403], ou encore comme le projet TrustStamp[404] de Mastercard et de l'organisation internationale Gavi.

L'édition 2020 du Rapport sur le commerce mondial de l'OMC, qui analyse le recours aux politiques publiques à l'ère numérique, souligne qu'il est important que les pays travaillent ensemble afin d'obtenir des résultats globaux positifs tout en réduisant au minimum les retombées négatives.[405]

Mark Hunyadi, professeur de philosophie sociale, morale et politique à l'UCL et Hugues Bersini, directeur du Laboratoire d'IA à l'ULB le concèdent tous les deux, l'IA exige un encadrement qui fait aujourd'hui défaut : *« Pour affronter ces problèmes sociétaux fondamentaux, nous ne sommes pas équipés éthiquement, ni politiquement. Car l'horizon ultime des institutions normatives, ce sont les droits, les libertés et la sécurité individuels, qui protègent les individus [...] Pour le reste, on n'a pas d'instances pour légiférer. Il faut faire preuve d'inventivité et d'imagination institutionnelle, imaginer une nouvelle institution, au niveau continental au minimum, une espèce d'ONU pour réfléchir à ces questions. »*

Les travaux d'Aurélie Jean évoqués *supra* l'ont amené à constater qu'*« il ne peut pas exister de régulation mondiale stricto sensu pour la simple et bonne raison que nous n'avons pas tous le même fonctionnement de construction et d'application des lois, sans parler des différences culturelles. Cela étant dit, on peut avoir des accords entre les nations ou une influence des textes sur d'autres pays. Ce qui fut le cas du RGPD européen qui inspira le texte californien. »*

Mireille Delmas-Marty appelle à prendre pleinement acte que : *« Gouverner la mondialisation par le droit implique de construire un Etat de droit sans État mondial, donc de repenser l'outil que représente le droit, traditionnellement identifié à l'État, face aux interdépendances nées de la mondialisation et aux défis qu'elles engendrent. […] Notre conception de la souveraineté doit être renouvelée. Pour créer un Etat de droit sans véritable État mondial, l'universalisme est trop ambitieux et le souverainisme, par repli sur les communautés nationales, trop frileux. Concilier souverainisme et universalisme nécessite de les penser de façon interactive, car il ne s'agit pas de choisir entre les deux, mais de les combiner afin de les concilier. C'est pourquoi nous avons encore besoin des communautés nationales pour responsabiliser les principaux acteurs de la mondialisation (États et entreprises transnationales – ETN -), mais seule la communauté mondiale pourra définir les objectifs communs et les responsabilités qui en résultent. Et seul leur entrecroisement évitera que les deux dynamiques s'opposent et se neutralisent, aboutissant à une société « à irresponsabilité illimitée ». […] Au niveau européen et a fortiori au niveau mondial, on ne peut pas directement transposer la théorie classique de la séparation des pouvoirs, ne serait-ce parce qu'il n'existe pas de pouvoir exécutif mondial, ni de législateur mondial. En revanche les juridictions sont impliquées dans la gouvernance mondiale, même quand leur statut reste lié au cadre national. La théorie de Montesquieu n'est donc pas transposable, car elle supposerait un État mondial, ni faisable, ni souhaitable. Il faut donc chercher à transposer l'idée démocratique des contre-pouvoirs. À défaut d'une véritable séparation entre les trois pouvoirs, l'agrégation savoir-vouloir-pouvoir pourrait assurer une sorte de rééquilibrage, chacun des acteurs ayant un rôle dans l'élaboration et l'application des normes. À condition de respecter l'indépendance, et de garantir la compétence, des*

[403] *« The Global Coalition for Digital Safety aims to accelerate public-private cooperation to tackle harmful content online and will serve to exchange best practices for new online safety regulation, take coordinated action to reduce the risk of online harms, and drive forward collaboration on programs to enhance digital media literacy. »*
Cf. notamment *Advancing Digital Safety: A Framework to Align Global Action :*
https://www.weforum.org/whitepapers/advancing-digital-safety-a-framework-to-align-global-action

[404] le projet TrustStamp est une application combinant une identité biométrique, un carnet de vaccination et un système de paiement avec reconnaissance biométrique.

[405] *Cf.* https://www.wto.org/french/res_f/reser_f/wtr_f.htm

scientifiques et d'assurer l'impartialité des acteurs civiques. D'où l'importance d'une régulation d'éventuels conflits d'intérêts. En résumé, il ne s'agit plus de séparer les pouvoirs, mais d'agréger le savoir et le vouloir face à des pouvoirs qui, tantôt économiques, tantôt politiques, tantôt les deux, sont la véritable incarnation d'une communauté qui émerge d'un droit en mouvement. […] À l'évidence, le droit est en mouvement : c'est pourquoi les phénomènes normatifs émergents ne peuvent être pensés à la seule lumière de la métaphore de la pyramide des normes. En dépit des piliers, des socles, des droits fondamentaux, nous sommes entrés dans une zone de turbulence, par nature instable. Certes la métaphore des réseaux rend mieux compte des horizontalités (réseaux des villes, des juges), que celle de la pyramide, mais elle ne suffit pas à exprimer cette instabilité croissante qui caractérise nos sociétés. D'où la métaphore des nuages et des vents. Au-delà des problèmes habituels de traduction (l'Etat de droit n'est pas un synonyme de rule of law, les droits de l'homme peuvent renvoyer à l'État soumis au droit comme à l'État qui fait des lois, le droit commun n'a pas le même sens que la common law, etc.), il faudrait remplacer les « concepts fondateurs » par des « processus transformateurs ». Dès lors, petit à petit, subrepticement on subvertit le sens des mots : c'est ainsi que la souveraineté qui se voulait « solitaire » pourrait devenir « solidaire ». En résumé, on ne peut ni choisir entre le souverainisme et l'universalisme, ni enfermer les systèmes de droit dans une logique hiérarchique et binaire ; ni admettre l'appropriation des biens communs mondiaux par les États ou les ETN ; ni transposer la séparation des pouvoirs à l'échelle d'un gouvernement du monde ; ni penser la communauté mondiale comme une communauté de mémoire. C'est pourquoi le juriste doit être innovant et le droit novateur. Certes, il ne s'agit pas de donner libre cours à une imagination débridée, mais simplement de sortir des sentiers battus, parce que la réalité n'y passe plus. Elle passe par une complexité qui pourrait paradoxalement renforcer la justice et par de nouveaux récits d'anticipation qui devraient contribuer à équilibrer la force. »[406]

L'intelligence artificielle recèle un énorme potentiel pour améliorer la santé de millions de personnes dans le monde si l'éthique et les droits de l'homme sont au cœur de sa conception, de son déploiement et de son utilisation, a indiqué l'OMS dans un rapport publié en juin 2021.[407]

« Comme toute nouvelle technologie, l'intelligence artificielle peut aussi en être fait mauvais usage et elle peut entraîner des effets préjudiciables », a indiqué Tedros Adhanom Ghebreyesus, Directeur général de l'OMS.

Pour réglementer et gouverner l'IA, l'OMS a publié de nouvelles orientations qui proposent six principes pour limiter les risques et maximiser les opportunités intrinsèques à l'intelligence artificielle pour la santé.

Six principes ont été développés par l'OMS qui guideront les travaux futurs de l'agence de la santé en vue de garantir que le plein potentiel de l'IA en matière de soins de santé et de santé publique soit mis au service du bien de tous.

Ainsi le premier principe directeur est de protéger l'autonomie humaine pour que les personnes puissent garder le contrôle des systèmes de soins de santé et des décisions médicales.

En effet, la vie privée et la confidentialité doivent être protégées et les patients doivent donner un consentement éclairé valide au moyen de cadres juridiques appropriés en matière de protection des données.

[406] *A l'ère du coronavirus, gouverner la mondialisation par le droit :* https://legrandcontinent.eu/fr/2020/03/18/coronavirus-mondialisation-droit-delmas-marty/
[407] *Cf.* https://news.un.org/fr/story/2021/06/1099252

Afin de promouvoir le bien-être humain et l'intérêt public, le deuxième principe invite les concepteurs d'IA à garantir les exigences réglementaires en matière de sécurité, de précision et d'efficacité, y compris les mesures de contrôle de la qualité.

Le troisième principe indique qu'il faut garantir la transparence, la clarté et l'intelligibilité. Les informations doivent être publiées ou documentées avant la conception ou le déploiement de la technologie d'IA, être facilement accessibles et permettre une consultation et un débat publics constructifs sur sa conception et son utilisation.

Bien que les technologies d'IA effectuent des tâches spécifiques, le quatrième principe insiste sur le fait qu'elles doivent être utilisées de manière responsable, dans des conditions appropriées, par des personnes correctement formées. Des mécanismes efficaces doivent être mis en place pour permettre aux individus et aux groupes lésés par des décisions fondées sur des algorithmes de contester ces décisions et d'obtenir réparation.

Le cinquième principe consiste à garantir l'inclusion et l'équité afin que l'IA pour la santé soit accessible au plus grand nombre de personnes possible, indépendamment de l'âge, du sexe, de l'origine ethnique ou d'autres caractéristiques protégées par les codes relatifs aux droits humains.

Enfin, il est important de promouvoir une IA réactive et durable. Le dernier principe invite donc les concepteurs, les développeurs et les utilisateurs à évaluer de manière transparente les applications lors de leur utilisation réelle afin de déterminer si l'IA répond de manière adéquate et appropriée aux attentes et aux exigences.

Les systèmes d'IA devraient également être conçus de sorte à réduire au minimum leurs conséquences environnementales et à accroître leur efficacité énergétique. Les gouvernements et les entreprises devraient anticiper les bouleversements qui seront occasionnés au niveau du travail, notamment la formation des agents de santé qui devront se familiariser avec l'utilisation des systèmes d'IA, et les pertes d'emploi que le recours à des systèmes automatisés est susceptible d'engendrer.

De son côté, Michelle Bachelet, la Haute Commissaire aux droits de l'Homme de l'ONU réclame une meilleure réglementation de ces technologies, suivant en cela les recommandations formulées par des experts réaffirmant, avant la tenue en juin 2021 du sommet sur les droits humains à l'ère numérique, la nécessité pour les États de promouvoir et de protéger les droits humains, notamment par le biais de réglementations respectueuses des droits imposées aux entreprises technologiques.[408]

Le 15 septembre 2021, le Haut-Commissariat de l'ONU aux droits de l'homme (HCDH) a appelé la communauté internationale à imposer un moratoire sur certains systèmes d'intelligence artificielle (IA) comme la reconnaissance faciale, le temps de *« mettre en place un dispositif pour protéger les droits humains quant à leur utilisation ».*[409]

« Le monde a besoin de règles pour que l'intelligence artificielle profite à l'humanité et la Recommandation sur l'éthique de l'IA est une réponse forte », a déclaré la Directrice générale de l'UNESCO, Audrey Azoulay, en présentant la toute première norme mondiale sur l'éthique de l'intelligence artificielle (IA), qui a été adoptée par les États membres de l'UNESCO lors de la Conférence générale le 25 novembre 2021.

Ce texte historique énonce des valeurs et principes communs qui guideront la mise en place de l'infrastructure juridique nécessaire pour assurer un développement sain de l'IA.

[408] *Les droits numériques sont la clé d'un monde inclusif et résilient :* https://news.un.org/fr/story/2021/06/1097522

[409] *Cf.* https://news.un.org/fr/story/2021/09/1103762

Selon Mme Azoulay la Recommandation sur l'éthique de l'IA fixe le premier cadre normatif mondial *« tout en donnant aux États la responsabilité de l'appliquer à leur niveau ». « L'UNESCO soutiendra ses 193 États membres dans sa mise en œuvre et leur demandera de rendre compte régulièrement de leurs progrès et de leurs pratiques. »*

Cette Recommandation vise à concrétiser les avantages que l'IA apporte à la société et à réduire les risques qu'elle comporte. Elle veille à ce que les transformations numériques favorisent les droits de l'homme et contribuent à la réalisation des Objectifs de développement durable, en abordant les problématiques liées à la transparence, la responsabilité et la vie privée.

Elle comprend des chapitres politiques orientés vers l'action sur la gouvernance des données, l'éducation, la culture, le travail, les soins de santé et l'économie.

Protection des données : la Recommandation appelle à aller au-delà de ce que les entreprises technologiques et les gouvernements font pour garantir aux individus une plus grande protection en assurant la transparence, la capacité d'agir et le contrôle de leurs données personnelles. Elle affirme que tous les individus devraient pouvoir accéder aux enregistrements de leurs données personnelles, et même les effacer. Elle prévoit également des actions visant à améliorer la protection des données et la connaissance qu'ont les individus de leurs propres données, ainsi que leur droit de les contrôler. Elle renforce également la capacité des organismes de réglementation du monde entier à faire respecter ces dispositions.

Interdiction de la notation sociale et de la surveillance de masse : la Recommandation interdit explicitement l'utilisation de systèmes d'IA pour la notation sociale et la surveillance de masse. Ces technologies sont très invasives, elles portent atteinte aux droits de l'homme et aux libertés fondamentales, et elles sont utilisées de manière généralisée. La Recommandation souligne que, lors de l'élaboration de cadres réglementaires, les États membres devraient tenir compte du fait que la responsabilité et l'obligation de rendre des comptes incombent toujours aux êtres humains en dernier ressort et que les technologies de l'IA ne devraient pas être dotées elles-mêmes d'une personnalité juridique.

Aide au suivi et à l'évaluation : la Recommandation jette également les bases des outils qui contribueront à sa mise en œuvre. L'évaluation de l'impact éthique vise à aider les pays et les entreprises qui développent et déploient des systèmes d'IA à évaluer l'impact de ces systèmes sur les individus, la société et l'environnement. La méthode d'évaluation de l'état de préparation aide les États Membres à évaluer dans quelle mesure ils sont prêts en termes d'infrastructure juridique et technique. Cet outil contribuera à renforcer la capacité institutionnelle des pays et recommandera les mesures appropriées à prendre afin de garantir la mise en œuvre pratique de l'éthique. En outre, la Recommandation encourage les États Membres à envisager d'ajouter la fonction d'un responsable de l'éthique de l'IA indépendant ou un autre mécanisme pour superviser des audits et une surveillance continue.

Protection de l'environnement : la Recommandation souligne que les acteurs de l'IA devraient privilégier les méthodes d'IA économes en données, en énergie et en ressources qui contribueront à faire de l'IA un outil majeur dans la lutte contre le changement climatique et la résolution de problèmes environnementaux. La Recommandation demande aux gouvernements d'évaluer l'impact environnemental direct et indirect tout au long du cycle de vie du système d'IA. Cela comprend son empreinte carbone, sa consommation d'énergie et l'impact environnemental de l'extraction des matières premières pour soutenir la fabrication des technologies d'IA. Elle vise également à réduire l'impact environnemental des systèmes d'IA et des infrastructures de données. Elle incite les gouvernements à investir dans les technologies vertes, et si les systèmes d'IA ont un impact négatif disproportionné sur l'environnement, la Recommandation préconise de ne pas les utiliser.

- *Aller au-delà en organisant de nouvelles 'roues de secours juridiques'*

Pour le philosophe Jean-Michel Besnier : *" il est urgent de maintenir unies deux grandes figures mythologiques, dont nous sommes les héritiers, et que Platon à mis en scène dans le Protagoras. Le mythe de Prométhée est souvent raconté de manière incomplète. Prométhée a volé le feu aux dieux ce qui a permis aux humains d'accéder à un processus d'hominisation, à travers la technique et la culture. Mais Platon dit aussi que Zeus savait que si les hommes n'avaient que la technique en leur possession, ils créeraient des sociétés dans lesquelles les rivalités, les conflits seraient constants. Cela les conduirait à l'hybris, la démesure. Comme Zeus ne veut pas la perte de l'humain, il a fait appel à une deuxième figure : Hermès, le dieu du langage, du message, de la pacification et de la politique. C'est cela qui fait contrepoids : la science du langage et de l'organisation politique. Ce mythe est profondément actuel. Nous devons continuer de préserver l'équilibre entre les outils et la parole, le langage.*

L'être humain possède une fonction « symbolique » qui le distingue, et des animaux, et des machines. Cette fonction symbolique repose sur trois points : Le langage, qui nous permet de prendre des distances avec l'immédiateté et de nous représenter les choses, il nous permet de mettre en perspective notre environnement ; L'intelligence humaine. Nous avons une intelligence qui consiste à rompre avec les automatismes. C'est cette faculté qui permet aux enfants de rompre avec les automatismes de l'instinct, à travers l'éducation ; La gratuité : nous sommes capables de jeu, de poésie, de choses qui ne servent « à rien » a priori mais qui sont importantes. Si la culture numérique se développait dans la démesure que dénonce Platon, alors elle attenterait au langage et ne ferait plus de l'intelligence que la faculté à résoudre des problèmes à travers des machines. Nous serions contraints par un utilitarisme qui nous enlèverait cette dimension de gratuité. En outre, cette fonction symbolique est capitale si nous voulons conserver la spécificité de l'humanité. "[410,411]

Le professeur Serge Sur identifie les raisons structurelles qui expliquent le retard du droit dans ce domaine comme dans d'autres, et suggère deux pistes qui permettent de le réduire : *« Ce sont les blocages, incertitudes, ambiguïtés, contradictions des changements souhaités qui entravent une transformation ordonnée et conduisent à la complexité de mesures partielles, d'autorité discutable. La codification du droit international en offre une illustration. Dans le cadre de l'ONU, depuis 1948, la Commission du droit international, organe subsidiaire de l'Assemblée générale, a été chargée de proposer des projets de codification du droit et de son développement progressif. Elle a connu de notables succès, avec de grandes conventions, sur les relations diplomatiques, consulaires, avec le droit des traités entre États. Mais elle n'a pas su adapter le droit de la mer, qui a fait l'objet de négociations séparées, et depuis quelques décennies elle semble incapable d'assurer la réussite de nouvelles conventions. Le projet sur la responsabilité internationale est ainsi resté sur cales. Alors, quelles solutions alternatives ?*

Quelles roues de secours juridiques ? La première de ces roues de secours est le contrat, la technique juridique la plus souple, la plus universelle, qui peut relever aussi bien du droit interne que du droit international, voire d'un droit ad hoc qui rentre dans la catégorie indéfinie du droit transnational. Le contrat est aussi la formule la plus inégalitaire en la matière, puisque dans le domaine des nouvelles technologies les accords sont le plus souvent d'adhésion, et que le choix du droit de référence comme de la juridiction compétente font la part belle à ceux qui maîtrisent les services et leurs infrastructures. L'exemple le plus manifeste est le droit d'Internet, largement soumis au droit interne américain et plus spécialement californien. Il

[410] *Du transhumanisme au posthumanisme : fantasmes et imaginaires technologiques) :* www.cigref.fr/du-transhumanisme-au-posthumanisme

[411] *Technological Approaches to Human Performance Enhancement :* https://iatranshumanisme.com/wp-content/uploads/2021/11/Technological-Approaches-to-Human-Performance-Enhancement-RAND_RRA1482-2.pdf

n'offre que des garanties limitées aux utilisateurs, réserve faite de l'ordre public interne des États concernés, comme les dérives dans l'utilisation des données personnelles par Facebook l'ont récemment illustré. Malgré les inconvénients de la formule, les États, incapables de s'entendre sur des conventions internationales, s'accommodent par défaut du droit américain, même si la tendance à restreindre davantage la liberté de ces nouvelles puissances non étatiques, puissances économiques et intellectuelles, se développe. Mais l'intervention des États en la matière se manifeste plutôt par la négociation avec les entreprises concernées que par l'édiction de mesures unilatérales, comme si des contrats devaient permettre d'encadrer et de régulariser d'autres contrats. Certains pays ont même nommé des « ambassadeurs » auprès des GAFA.

La seconde roue de secours est la jurisprudence, solution a posteriori et aléatoire, puisque la compétence des juridictions internes demande préalablement à être établie. La jurisprudence est également le fruit d'une régulation par défaut, puisque, en l'absence d'un droit interne spécifique, il lui faut s'appuyer sur des principes généraux pour sauvegarder des droits particuliers. Elle est surtout interne, mais la C.E.D.H. peut également être impliquée. Les solutions particulières peuvent conduire à des normes imparfaites puisqu'au statut incertain comme celui de toute jurisprudence. Ces normes reposent sur une conception réticulaire plus que pyramidale du droit, celle du dialogue des juges relevant de systèmes juridiques différents afin de rechercher des réponses compatibles à des problèmes comparables. Ce n'est cependant qu'un pis-aller, sans certitude et sans légitimité. … »[412]

Selon Mireille Dumas-Marty, professeure honoraire au Collège de France et membre de l'Académie des sciences morales et politiques *: « Pour y parvenir, il faudra changer nos repères. Dans ce monde déboussolé, il n'y a plus de pôle nord, en ce sens qu'il est impossible de choisir parmi les vents contraires de la mondialisation. Mais on peut imaginer une boussole inhabituelle. Au centre, engendré par la spirale des humanismes juridiques, un réceptacle octogonal recueille l'eau, symbole de la vie, où se rencontrent les principes régulateurs réconciliant les vents contraires de la mondialisation. Plongé dans ce réceptacle, le fil à plomb de la bonne gouvernance stabiliserait les mouvements désordonnés sans pour autant immobiliser ce monde en mouvement. C'est ainsi qu'inspiré par les « forces imaginantes du droit », le juriste peut tenter de répondre au constat désabusé de Pascal au 17ème siècle : « ne pouvant fortifier la justice, on a justifié la force, afin que la justice et la force fussent ensemble et que la paix fût, qui est le souverain bien ». Si la spirale des humanismes fortifiait la justice, l'octogone des principes régulateurs équilibrerait la force. Il ne s'agit pas pour autant d'adhérer au rêve utopique des deux K : la « Grande paix » des classiques chinois, reprise à la fin du 19ème siècle par le juriste Kang Youwei et la « Paix perpétuelle » du philosophe Emmanuel Kant au 18ème siècle. De façon plus modeste, il s'agit de mettre en place des dispositifs d'apaisement, de faire la paix avec la Terre. »*

- *De l'urgence d'une plus forte mobilisation internationale autour des défis posés par la technologie 'blockchain'*

Un chantier considérable se trouve encore devant nous, celui qu'ouvre le chapitre encore très inexploré des impacts considérables de la technologie 'blockchain' sur la société.

« Cette technologie, que certains imaginent aussi révolutionnaire que l'internet — elle serait aux transferts de valeurs ce que l'internet a été aux échanges d'informations —, interroge le droit à plus d'un titre. Elle pourrait contribuer à remplacer ou, du moins, renouveler le droit,

[412] *Réflexions sur l'inventivité et le droit* (Actes du colloque du 30 mars 2017 sur le thème *'L'inventivité - Aspects de sciences politique et juridique' in Revue du Centre Michel de l'Hospital*, n° 14, juin 2018, pp. 90-97)
https://www.afri-ct.org/wp-content/uploads/2018/07/Contribution-S.-SUR.pdf

notamment en lui permettant de se passer d'État et, plus généralement, de tiers de confiance. Les blockchains possèdent un potentiel disruptif à l'égard de la production et de la pratique du droit dont il faut prendre conscience afin de ne pas se laisser surprendre par les bouleversements qu'elles provoquent. Elles remettent en cause des modèles de génération et de garantie de la confiance qui existent depuis des siècles : droit, État, banques, notaires etc. Les blockchains sont le meilleur témoin du grand mouvement de technologisation des sociétés : les hommes s'en remettent de moins en moins à autrui et de plus en plus à la technologie. Et cela concernerait y compris le monde juridique. Le futur que les blockchains rendent possible est un monde plus horizontal. Le nouveau droit qu'elles forgent serait par conséquent un droit plus horizontal, se passant d'organes de tutelle et de contrôle. » (Boris Barraud[413])

[413] *'Les blockchains et le droit'*, Revue Lamy droit de l'immatériel (Wolters Kluwer), n° 147, avr. 2018, p. 48-62 https://www.academia.edu/36141168/_Les_blockchains_et_le_droit_Revue_Lamy_droit_de_l_immat%C3%A9riel_Wolters_Kluwer_n_147_avr_2018_p_48_62

Le Conseil de l'Europe doit poursuivre les adaptations nécessaires de ses juridictions et des dispositions juridiques (Conventions, Protocoles, …)

Le Conseil de l'Europe s'est pleinement saisi des nombreux enjeux et défis posés au droit, et en particulier au respect des droits fondamentaux et des droits de l'homme, par la convergence technologique, le numérique et l'intelligence.[414]

- *Poursuivre les adaptations requises des Conventions et des protocoles associés*

Dans sa Recommandation sur les impacts des systèmes algorithmiques sur les droits de l'homme en date du 8 avril 2021[415], le Comité des Ministres du Conseil de l'Europe a appelé les 47 États membres à appliquer le principe de précaution dans la réalisation et la mise en œuvre de systèmes fondés sur des algorithmes et à se doter de lois, de politiques et de pratiques respectant pleinement les normes des droits de l'homme, en y énonçant une série de lignes directrices invitant les gouvernements à garantir qu'ils n'enfreignent pas les droits de l'homme dans le cadre de l'utilisation, du développement ou de l'acquisition de systèmes algorithmiques, et en leur rappelant que leur pouvoir réglementaire donne à ces derniers l'obligation d'établir des cadres législatifs, réglementaires et de supervision efficaces et prévisibles, capables de prévenir, de détecter, d'interdire et de remédier aux violations des droits de l'homme, qu'elles soient imputables à des acteurs publics ou privés.

On entrevoit dans certains des droits et principes de la *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales* dont nous avons souligné *supra* le rôle fondamental, notamment ceux liés au respect de la vie privée et familiale, la possibilité d'une prise en compte *de jure* de certaines considérations de droit et d'éthique relatives aux défis numériques identifiés dans la présente analyse.

Mais est-ce suffisant pour couvrir l'ensemble des défis relevés ici ?

Il faudra le vérifier, et si tel n'est pas le cas, engager un processus d'extension du socle des droits et principes énoncés et protégés par la Convention à ces nouveaux défis. Comme il faudra le vérifier également pour la liste des critères de l'Etat de droit telle que définie par la Commission de Venise (*cf. supra*).

Le Conseil de l'Europe œuvre à l'élaboration et à l'adoption d'un 2ème protocole additionnel à la Convention de Budapest qui permettra de relever plus efficacement les défis liés aux preuves électroniques dans les juridictions étrangères, multiples ou inconnues.

Le protocole est conçu pour répondre aux défis suivants :

- Comment obtenir plus efficacement l'utilisation d'un compte ou d'une adresse de protocole Internet utilisés pour commettre une infraction ? Ces "informations sur l'abonné" sont essentielles pour mener à bien une enquête.
- Comment et dans quelles conditions coopérer directement avec un fournisseur de services d'une autre partie pour obtenir ces informations ?
- Comment obtenir sans délai la communication de données - y compris de données relatives au contenu - d'une autre partie en cas d'urgence où des vies sont en danger ?

[414] *Cf.* les nombreux travaux qui y sont consacrés au sein de ses différentes institutions : https://www.coe.int/fr/web/artificial-intelligence/home
Voir également les travaux en cours au sein du Conseil : https://www.coe.int/fr/web/artificial-intelligence/work-in-progress#05FR

[415] *Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme* : https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016809e1124

- Comment rendre plus efficace la coopération entre gouvernements, y compris l'assistance mutuelle, et mettre à disposition des outils supplémentaires pour la coopération en matière de cybercriminalité et de preuves électroniques ?
- Et comment concilier des moyens de coopération innovants et efficaces avec les exigences de l'État de droit et de la protection des données ?

Le Protocole prévoira des outils innovants pour obtenir la divulgation de preuves électroniques, notamment :

- Coopération directe avec les fournisseurs de service ((Article 6 et Article 7)
- Formes accélérées de coopération entre les parties pour la divulgation des informations sur les abonnés et des données relatives au trafic (Article 8)
- Coopération et divulgation accélérées dans les situations d'urgence (Articles 9 et 10)
- Outils supplémentaires pour l'entraide (Articles 11 et 12)
- Protection des données et autres garanties de l'État de droit (Articles 13 et 14)

Les dispositions de ce Protocole seront utiles sur le plan opérationnel et politique et permettront à la Convention de Budapest de continuer à défendre un Internet libre où les gouvernements s'acquittent de leur obligation de protéger les personnes et leurs droits dans le cyberespace.

Il est prévu que le Protocole soit ouvert à la signature en mars 2022.

- *Poursuivre les efforts entrepris pour garantir l'indépendance de la justice*

Lors de sa 16e réunion plénière (25-26 novembre 2021, Strasbourg/en ligne), le Conseil consultatif des procureurs européens (CCPE) a adopté l'avis n° 16 (2021) sur les implications des décisions des cours internationales et des organes de traités concernant l'indépendance pratique des procureurs.[416] En préparant cet Avis, le CCPE a pris en compte les différents systèmes de justice pénale, mais aussi le facteur de convergence le plus important, à savoir l'exigence d'indépendance des ministères publics en tant que condition préalable à l'État de droit et à l'indépendance du pouvoir judiciaire.

L'Avis donne un aperçu de la jurisprudence pertinente des juridictions internationales, principalement celle de la Cour européenne des droits de l'homme et d'autres cours et organes de traités concernant l'indépendance du pouvoir judiciaire en général, et des ministères publics et des procureurs en particulier. Il souligne que, comme il s'agit d'une condition préalable à l'Etat de droit et à l'indépendance du pouvoir judiciaire, l'indépendance et l'autonomie des procureurs et des services de poursuite devraient être encouragées et garanties par la loi, au plus haut niveau possible, de la même manière que pour les juges. Cette jurisprudence fournit des éléments utiles qui peuvent avoir un effet important sur l'impartialité et l'indépendance, en droit et en pratique, des procureurs. Ces éléments contribuent à renforcer l'indépendance institutionnelle des ministères publics, ainsi que l'indépendance fonctionnelle des procureurs individuels. Il peut guider utilement les réformes judiciaires et de poursuites afin d'aider l'État à développer ou à améliorer le cadre législatif de l'autonomie organisationnelle des ministères publics, le processus de nomination, d'évaluation et de révocation des procureurs, la durée de leur mandat, la non-ingérence dans leur travail et d'autres aspects importants relatifs à leur carrière.

Une autre urgence est de vérifier si les « *juges non élus et n'ayant de comptes à rendre à personne* » qui siègent à la CJUE et à la CEDH sont vraiment indépendants et impartiaux.

Et d'agir si nécessaire pour sanctionner et corriger les écarts avérés éventuels.

[416] *Avis n° 16 du CCPE (2021) : Implications des décisions des tribunaux internationaux et des organes de traités concernant l'indépendance pratique des procureurs :* https://rm.coe.int/opinion-no-16-2021-fr/1680a4bd27

C'est dans cette optique que le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe, a recommandé en 2017 « *que les gouvernements des États membres : – établissent ou renforcent, selon le cas, un cadre cohérent et global pour la réglementation juridique des activités de lobbying dans le contexte de la prise de décision publique, conformément aux principes directeurs énoncés dans l'annexe ci-jointe et à la lumière de leurs propres situations nationales; – veillent à ce que la présente recommandation soit traduite et diffusée aussi largement que possible, notamment aux groupes de lobbyistes, au milieu des affaires, aux syndicats, aux organisations sectorielles, aux organes publics, aux autorités de régulation, aux ONG de la société civile, aux responsables politiques, aux universitaires.* »[417]

- *Tirer pleinement parti d'une bonne articulation entre les Conventions de Budapest et d'Istanbul pour lutter contre toutes les formes de cyberharcèlement liées au genre*

Le Conseil de l'Europe observe que, sous l'effet des technologies numériques, les inégalités entre les femmes et les hommes tendent à se reproduire et à s'amplifier. Il observe également que les mesures de restriction et de confinement prises récemment face à la pandémie de covid-19 entraînent une augmentation de la cybercriminalité, à cause du développement des activités en ligne. Par conséquent, les femmes et les filles sont exposées à de multiples risques liés au harcèlement (notamment sexuel) en ligne et facilité par la technologie et à la cybercriminalité fondée sur le genre.

S'agissant de la lutte contre toutes les formes de cyberharcèlement liées au genre, dans une étude publiée en décembre 2021[418], la consultante internationale Adriane van der Wilk montre que la Convention d'Istanbul et la Convention de Budapest peuvent se compléter de manière dynamique : la puissance de la Convention d'Istanbul réside dans le fait qu'elle reconnaît que la violence à l'égard des femmes est une violence fondée sur le genre, tandis que la Convention de Budapest prévoit des moyens d'investigation complets permettant d'obtenir des preuves électroniques d'infractions commises en ligne et par le biais des technologies de l'information.

La Convention d'Istanbul, qui englobe toutes les formes de violence à l'égard des femmes et de violence domestique, est, en la matière, le plus ambitieux des traités juridiquement contraignants relatifs aux droits humains. Elle peut donc être un instrument particulièrement utile pour lutter contre la violence à l'égard des femmes en ligne et facilitée par la technologie.

La Convention de Budapest, quant à elle, est le traité international juridiquement contraignant le plus pertinent dans le domaine de la cybercriminalité et des preuves électroniques. Elle offre donc des possibilités d'exercer des poursuites dans les affaires de violence à l'égard des femmes. Grâce à plusieurs dispositions de droit pénal matériel, elle aborde en effet de manière directe et indirecte certaines manifestations de cette violence.

[417] *Recommandation CM/Rec(2017)2 du Comité des Ministres aux États membres relative à la réglementation juridique des activités de lobbying dans le contexte de la prise de décision publique (adoptée par le Comité des Ministres le 22 mars 2017)* https://rm.coe.int/la-reglementation-juridique-des-activites-de-lobbying-dans-le-contexte/168073ed67

[418] Du harcèlement sexuel en ligne *(« cyber flashing »,* diffamation et calomnie à caractère sexuel, usurpation d'identité à des fins sexuelles, *« doxing », « flaming »,* etc.) au harcèlement sexuel sur la base d'images comme les *« creepshots »* (images suggestives ou intimes prises sans consentement et partagées en ligne), la nouvelle étude classe et définit différentes formes de violence à l'égard des femmes en ligne et facilitée par la technologie. Elle s'intéresse plus particulièrement aux articles 33, 34 et 40 de la Convention d'Istanbul, ainsi qu'aux dispositions pertinentes de la Convention de Budapest. Elle analyse ensuite les dispositions de la Convention d'Istanbul sur les politiques intégrées, la prévention, la protection et les poursuites et commente leur application aux divers aspects du phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie.

L'Union européenne doit continuer d'aménager son droit primaire et mettre fin au monopole des géants du numérique en Europe

Pour Eric Maurice *« La démocratie est le fondement politique et moral de l'Union européenne et des Etats qui la composent. Par son bon fonctionnement, elle tend à pacifier les alternances politiques, atténuer les tensions sociales et supprimer l'arbitraire judiciaire, ce qui garantit la paix civile et la prospérité des sociétés européennes.*

En outre, dans un monde où les marqueurs de la démocratie libérale issue des Lumières européennes sont en recul, la valeur démocratie est un outil de la puissance et de l'influence de l'Union.

Sans démocratie fonctionnelle en leur sein, l'Union et ses Etats membres perdraient leur capacité à agir et défendre leurs intérêts, par le maintien d'un multilatéralisme basé sur des règles, ou par la projection de leurs valeurs et de normes suivies par d'autres. »

- *Renforcer l'Etat de droit au sein de l'UE*

Le renforcement de l'Etat de droit au sein de l'UE est l'une des conditions *sine qua non* du renforcement de la démocratie en Europe. Le cadre juridique du numérique est fondé sur des valeurs qui façonnent une voie européenne, notamment la protection des données personnelles et de la vie privée, la promotion de l'intérêt général, par exemple dans la gouvernance des données.

Le texte emblématique de l'approche européenne est le RGPD adopté en 2016, qui vise la maîtrise de ses données par le citoyen, maîtrise qui s'apparente à une forme de souveraineté individuelle. Ce règlement est souvent présenté comme un succès et un modèle, même si cela doit être relativisé.

Les autorités européennes chargées de la protection de la vie privée, regroupées sous l'égide du Conseil européen de la protection des données (CEPD), ont adopté en novembre 2020 plusieurs recommandations faisant suite à l'arrêt *'Schrems II'*, par lequel la CJUE a invalidé le *'Privacy Schield',* remettant en question la manière dont les entreprises, et en particulier les géants technologiques américains, transmettent des données aux Etats-Unis.

« En vertu de l'arrêt du 16 juillet, les responsables du traitement qui s'appuient sur les clauses contractuelles types (CCT) sont tenus de vérifier, au cas par cas et, le cas échéant, en collaboration avec le destinataire des données dans le pays tiers, si la législation du pays tiers assure un niveau de protection des données à caractère personnel transférées qui est essentiellement équivalent à celui garanti dans l'Espace économique européen (EEE). […] La CJUE permet aux exportateurs d'envisager des mesures complémentaires aux clauses contractuelles pour assurer le respect effectif de ce niveau de protection lorsque les garanties contenues dans les clauses ne sont pas suffisantes. »

Dans son discours sur l'état de l'UE devant le Parlement européen, le 16 septembre 2020, la présidente de la Commission européenne a appelé l'UE à faire des prochaines années la *« décennie numérique »* de l'Europe. Le 9 mars 2021, l'institution qu'elle préside a présenté une communication [419] qui répond à l'invitation du Conseil européen à présenter une *« boussole numérique »*[420] ; et elle s'appuie sur la stratégie numérique de la Commission de février 2020[421]. Cette communication propose de convenir d'un ensemble de principes numériques, de lancer

[419] *Une boussole numérique pour 2030 : l'Europe balise la décennie numérique :* https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021DC0118&from=en
[420] https://www.consilium.europa.eu/media/45918/021020-euco-final-conclusions-fr.pdf
[421] *Façonner l'avenir numérique de l'Europe :* https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_fr.pdf

rapidement d'importants projets multinationaux et de préparer une proposition législative établissant un cadre de gouvernance solide pour suivre les progrès – la boussole numérique.

Cette communication met en exergue la question fondamentale des principes numériques permettant de garantir le respect des droits et valeurs de l'Union.

« Les droits et les valeurs de l'UE sont au cœur de la voie centrée sur l'humain balisée aujourd'hui en matière de numérique. Ils devraient pleinement se refléter dans l'espace en ligne, comme dans le monde réel. C'est pourquoi la Commission propose d'élaborer un cadre de principes numériques, tels que l'accès à une connectivité de haute qualité, à des compétences numériques suffisantes, aux services publics, à des services en ligne équitables et non discriminatoires et, de façon plus générale, de faire en sorte que les droits applicables hors ligne puissent être totalement exercés en ligne. Ces principes seraient discutés dans le cadre d'un large débat sociétal et pourraient être inscrits dans une déclaration interinstitutionnelle solennelle du Parlement européen, du Conseil et de la Commission. Ils se baseraient sur le socle européen des droits sociaux[422] et le compléteraient. Enfin, la Commission propose de vérifier au moyen d'un Eurobaromètre annuel si les Européens ont le sentiment que leurs droits numériques sont respectés. »

Lors de son allocution devant le Parlement européen le 19 janvier 2022, le président de la République Emmanuel Macron, a également mis un accent particulier sur l'Etat de droit et la démocratie libérale : *"Je veux ici vous dire que la présidence française sera une présidence de promotion des valeurs qui nous font et qui, à force d'être considérées peut-être comme des acquis, on finit ces dernières années par se fragiliser. Nous sommes cette génération qui redécouvre la précarité de l'État de droit et des valeurs démocratiques.*

D'abord, la démocratie libérale au sens politique du terme, ces dernières années, on disait ce régime que l'Europe a inventé, devenu fatigué, incapable de faire face aux grands défis du siècle. Cependant, je veux ici dire combien ces derniers mois l'ont montré, la gestion de la pandémie par les démocraties, avec du débat parlementaire, avec une presse libre, avec des systèmes de recherche et des systèmes académiques libres et ouverts a conduit à des décisions beaucoup plus protectrices des vies et des économies que celles des régimes autoritaires. Nous avons in concreto, tous ensemble, démontré l'inverse d'une idée reçue qui était en train de s'installer. C'est pourquoi nous serons au rendez-vous du combat pour la démocratie libérale.

Combat pour défendre nos processus électoraux des tentatives d'ingérence étrangère, combat pour continuer de faire progresser la souveraineté des peuples. À cet égard, nous aurons des travaux qui d'ici au printemps, continueront de progresser dans le cadre de la conférence sur l'avenir de l'Europe. Et si elle en fait la recommandation, la présidence française portera avec l'Allemagne, l'accord de coalition a été très clair sur ces termes, le droit d'initiative législative pour votre Parlement.

Combat pour l'Etat de droit, pour cette idée simple qu'il y ait des droits universels de l'homme qui doivent être protégés des fièvres de l'histoire et de leurs dirigeants. Des voix s'élèvent aujourd'hui pour revenir sur nos grands textes fondamentaux qui ont pourtant été décidés souverainement par les Etats membres lors de leur adhésion. Mais revenir sur quoi ? Sur l'égalité des hommes en dignité et en droit ? Sur le droit pour chacun à disposer d'un procès équitable par une justice indépendante ? Et s'installe comme une idée au fond que pour être plus efficace il faudrait revenir sur l'Etat de droit, confondant le changement légitime de tout gouvernement élu de changer l'état du droit, mais considérant que nous tous avons à nous

[422] *Les 20 principes du socle européen des droits sociaux :* https://ec.europa.eu/info/sites/default/files/social-summit-european-pillar-social-rights-booklet_fr.pdf

inscrire dans cet Etat de droit qui est existentiel de notre Europe, dont les principes ont été bâtis par notre histoire et sont le fruit de nos engagements communs.

La fin de l'État de droit, c'est le règne de l'arbitraire. La fin de l'Etat de droit, c'est le signe du retour aux régimes autoritaires, au bégaiement de notre histoire. Oui, derrière tout cela, il y a un combat idéologique. Ce combat est d'ailleurs porté par plusieurs puissances autoritaires à nos frontières et il revient chez plusieurs de nos pays. Nous voyons cette révolution à l'œuvre qui vient saper les fondements mêmes de notre histoire. Là où la tolérance et la civilité étaient au fond au cœur du processus de civilisation qui est le nôtre, revient une idée qui renaît au sein de nos peuples. Nous ferons donc tout pour œuvrer en ce sens et pour que, par le dialogue toujours, mais sans faiblesse, nous puissions défendre dans toutes les situations connues la force de cet État de droit. Je le dis dans le dialogue parce qu'il ne s'agit pas de laisser s'installer l'idée que l'État de droit serait au fond une invention de Bruxelles dont le seul dépositaire serait Bruxelles, qui est un discours que nous entendons naître dans certaines capitales. Non, c'est le fruit de nos histoires à tous, le combat même de révolutions pour se libérer du joug des totalitarismes durant le siècle passé. L'État de droit est notre trésor. Et il s'agit partout de reconvaincre les peuples qui s'en sont éloignés. Il s'agit partout, avec beaucoup de respect et d'esprit de dialogue, de venir convaincre à nouveau. Parler de cette singularité démocratique européenne, c'est évidemment donner aussi une force à ce nouveau combat.

Dans cet esprit, je souhaite que l'on consolide nos valeurs d'Européens qui font notre unité, notre fierté et notre force. 20 ans après la proclamation de notre Charte des droits fondamentaux, qui a consacré notamment l'abolition de la peine de mort partout dans l'Union, je souhaite que nous puissions actualiser cette charte, notamment pour être plus explicite sur la protection de l'environnement ou la reconnaissance du droit à l'avortement. Ouvrons ce débat librement avec nos concitoyens de grandes consciences européennes pour donner un nouveau souffle à notre socle de droits qui forge cette Europe forte de ses valeurs qui est le seul avenir de notre projet politique commun. Cette singularité que j'évoque, c'est aussi un rapport à la solidarité unique au monde. Nos sociétés ont ceci de singulier qu'elles ont inventé avec l'Etat providence un système de protection pour chacun face aux risques de l'existence. C'est un legs de nos démocraties européennes. Et cette pandémie a montré que la solidarité, loin d'être une faiblesse, est une force incomparable. »[423]

Pour Eric Maurice : *« Le mécanisme européen de protection de l'Etat de droit, dont le premier rapport annuel*[424] *a été débattu pour la première fois par les Etats membres le 17 novembre 2020, est un premier pas vers une action systématique et préventive. Le mécanisme de conditionnalité sur le budget de l'Union, qui doit être mis en œuvre avec le nouveau cadre financier pluriannuel et le plan de relance, est également un outil d'intervention directe dans les Etats qui ne veulent plus suivre les règles. Les stratégies contre les cybermenaces, les ingérences et la désinformation, développées en parallèle, dotent l'Europe d'une panoplie large pour défendre sa démocratie. L'enjeu à venir est une articulation plus affirmée et plus directe de ses multiples dimensions, internes et externes. »*[425]

Dans le rapport 2020 sur l'Etat de droit au sein de l'UE, des pistes de progrès ont été identifiées qui appellent à être mises en oeuvre.[426] Mais en prenant rigoureusement en compte les recommandations formulées par Mireille Dumas-Marty rappelées ci-dessus.

[423] *Discours du Président Emmanuel Macron devant le Parlement européen (19 janvier 2022)* : https://www.elysee.fr/emmanuel-macron/2022/01/19/discours-du-president-emmanuel-macron-devant-le-parlement-europeen

[424] *Rapport 2020 sur l'Etat de droit - La situation de l'Etat de droit dans l'Union européenne :* https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0580

[425] *La démocratie européenne, un système fondamental à protéger :* *https://www.robert-schuman.eu/fr/questions-d-europe/0578-la-democratie-europeenne-un-systeme-fondamental-a-proteger*

[426] *Cf.* notamment à cet égard : *Protéger les contre-pouvoirs pour sauver l'État de droit*

Si l'UE semble avoir renoncé à proposer des alternatives crédibles aux GAFAM, elle campe en position de régulateur. Après le succès du RGPD, les Vingt-Sept s'attaquent à deux sujets d'ampleur : la modération des contenus en ligne (*Digital Services Act, DSA*) et la préservation de la sacro-sainte concurrence libre et non faussée sur les places de marché numériques (*Digital Markets Act, DMA*).

En décembre 2020, les commissaires européens au Numérique et à la Concurrence ont présenté deux propositions de règlements : le règlement sur les services numériques (*'Digital Services Act'*) et le règlement sur les marchés numériques *('Digital Markets Act'*) qui seront d'application immédiate dans toute l'Union européenne après leur adoption définitive, aucune transposition en droit national n'étant nécessaire à la différence des directives européennes. Les Etats membres disposeront de dix-huit après leur adoption définitive pour les transposer dans leur droit interne.

En novembre 2021, après plusieurs mois de discussions, le Parlement européen et le Conseil de l'Union européenne, se sont accordés sur le périmètre du futur *Data Governance Act* (*DGA*)[427]. Ce texte, proposé par la Commission européenne en novembre 2020, est la première initiative pour tenter de réguler le marché des données au sein de l'Union. Ce marché unique européen des données vise à mettre en place divers mécanismes de partage des données en faisant la promotion de la disponibilité des données pour alimenter différents cas d'usage dans différents domaines : la santé, l'agriculture, l'administration publique, l'automobile, la finance, *etc*.

Le *Data Governance Act* a également été pensé pour stimuler de nouveaux modèles commerciaux et favoriser l'innovation sociale. Avec le *DGA*, l'UE se dote d'un cadre capable de fournir un environnement sécurisé, dans lequel les entreprises ou les particuliers pourront partager des données. Un moyen également de faciliter le respect des obligations de partage de données fixées par le RGPD. En effet, en utilisant les plateformes numériques qui seront créées dans le cadre de l'application du *Data Governance Act*, les entreprises pourront partager leurs données *« sans craindre qu'elles soient mal utilisées ou qu'elles perdent leur avantage concurrentiel »*.

Il est intéressant de relever la position adoptée par le Conseil des ministres à ce sujet, laquelle se résume par cette formule : *« Ce qui est illicite hors ligne devrait aussi l'être en ligne. »*[428]

Concernant les particuliers, les législateurs européens précisent que le *DGA* permettra aux citoyens de l'Union d'avoir un *« contrôle total sur leurs données, et de les partager (ou pas) avec une entreprise en qui elles ont confiance »*.

Deux autres textes de régulation sont par ailleurs attendus pour 2023. L'un vise à mettre un peu d'éthique dans l'intelligence artificielle. Le second, *European Chips Act (ECA)*, entend aider l'industrie locale moribonde des semi-conducteurs.

Le premier vise à responsabiliser l'ensemble de opérateurs (les grandes plateformes comme les intermédiaires) qui devront disposer des moyens pour modérer les contenus qu'ils accueillent et coopérer avec les autorités publiques. Mais, reprenant la logique de la loi Avia, il comporte le risque de pousser les acteurs du Net au sens large à pratiquer, par précaution, une censure extrêmement large sur les contenus qu'ils publient.

---

https://www.robert-schuman.eu/fr/questions-d-europe/0590-proteger-les-contre-pouvoirs-pour-sauver-l-etat-de-droit

169

[427] *Promotion du partage des données : la présidence parvient à un accord avec le Parlement concernant l'acte sur la gouvernance des données :* https://www.consilium.europa.eu/fr/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/

[428] *Ce qui est illicite hors ligne devrait aussi l'être en ligne : le Conseil arrête sa position sur la législation sur les services numériques :* https://www.consilium.europa.eu/fr/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/

Le second impose des contraintes spécifiques aux seuls acteurs 'systémiques' dont la toute-puissance menace le libre jeu de la concurrence, précise les critères définissant cette catégorie d'entreprises, et prévoit des sanctions dissuasives en accompagnement du cadre réglementaire.[429] En limitant fortement leur possibilité à une collecte large des données personnelles, leur principal moteur économique, il limitera la rentabilité des sites et les obligera à trouver de nouveaux moyens de financement, par exemple en faisant directement payer leurs services.

Le séquençage de la définition du cadre réglementaire européen dans le secteur numérique doit être minutieux ; car il s'agit de défendre les préférences collectives européennes tout en préservant un espace de coopération avec les États-Unis et d'autres partenaires sans bloquer prématurément toute négociation par une politique du fait accompli.

Mais seront-ils efficients dans l'univers du métavers ?

Dans une tribune publiée le 13 janvier 2022 dans *Les Echos*[430], André Loesekrug-Pietri et Romain Forestier, respectivement directeur et chef de projet scientifique de la *Joint European Disruptive Initiative*[431] (équivalent de la DARPA américaine), tirent la sonnette d'alarme, notamment à l'égard du métavers que META tente de bâtir *:*

« Les Gafam, qui fixent leurs propres règles, continuent de grignoter les pouvoirs souverains des Etats. […] Désormais, ce ne sont plus les Etats qui franchissent le Rubicon, mais les réseaux sociaux qui décident de leur propre chef et avec force comités Théodule d'éthique de lignes rouges de plus en plus brumeuses. La propension des réseaux à bannir visent à compenser leur incurie en matière de gestion des contenus. […] Face à cela, l'ambitieux DMA européen est une première base, mais il faudra s'assurer que cette nouvelle réglementation européenne ait un vrai impact, efficace et rapide, dans le monde réel. Il faut aller au-delà, résister à l'offensive de charme des Gafam. […] Dans cette prime à la rapidité, nous devons être plus innovants que les Gafam. Plus innovants politiquement (nos institutions doivent être capables de réagir aussi rapidement qu'une entreprise technologique, dans un cadre bien défini), mais aussi technologiquement. C'est pour cela que se préparent plusieurs grands défis « Démocratie 2.0 » pour faire de la technologie une arme pour défendre nos systèmes démocratiques et nos valeurs humanistes : comment rendre l'intelligence artificielle explicable – et donc responsable ; comment faire de la reconnaissance faciale sans base de données centralisées ; développer des réseaux sociaux qui ne fragmentent pas les mouvements d'opinion ; comment lutter contre la manipulation cognitive … Aux démocraties et à la société civile de se réinventer pour faire face aux défis du XXIème siècle. »[432]

---

[429] Ces sanctions pourront s'élever jusqu'à 10 % du chiffre d'affaires pour de graves infractions à la concurrence, et dans les cas extrêmes, pourront déboucher sur l'obligation de céder des activités en Europe. En matière de contenus illégaux en ligne, les amendes pourront atteindre 6 % du chiffre d'affaires, en plus d'une interdiction de poursuivre son activité en Europe en cas de manquement grave et répété.

[430] *Ne laissons pas la politique aux Gafam' :* https://www.lesechos.fr/idees-debats/cercle/opinion-ne-laissons-pas-la-politique-aux-gafam-1378940

[431] *Joint European Disruptive Initiative (JEDI) :* https://jedi2020.wixsite.com/monsite
A l'image de la DARPA, JEDI a créé sa propre méthodologie, adaptée à l'Europe. Quatre grandes missions sont définies par JEDI : le changement climatique, la santé, la transition digitale centrée sur l'humain et les nouvelles frontières. Pour chacune de ces missions, l'objectif est de lancer un challenge et de sélectionner un nombre limité de projets rapides et disruptifs que JEDI subventionnera (entre 15 et 20 millions d'euros.) En plus de cette aide financière, chaque projet sera accompagné de « *Programme Managers* » : 15 experts charismatiques, détachés de leurs entreprises pour 4 ans, ayant le recul nécessaire pour ne pas s'initier opérationnellement dans les projets et rester neutres. L'objectif de la démarche est d'arriver rapidement à un prototype et de pouvoir le tester, mais surtout d'être les premiers sur le marché. Pour compléter ces challenges, JEDI organise des « *MoonShot Days* » ou usines à idées.

170

Les 11 et 12 janvier 2022, profitant de son statut de président 'temporaire' du Conseil de l'UE pour le format en charge de ces dossiers, Cédric O, le secrétaire d'Etat au numérique a procédé à plusieurs échanges de vue avec des régulateurs, des parlementaires et des *think tanks* américains à propos du DMA et du DSA, et de manière plus large, de la régulation des géants du numérique.

« Un des buts de mes échanges avec Washington était de montrer que les textes européens ne sont pas antiaméricains. Ils visent des acteurs en raison de leur position dominante », répondant ainsi publiquement aux accusations portées le 8 décembre 2021 à l'égard du DMA et du DSA par la secrétaire d'Etat au Commerce, Gina Raimondo.

Cédric O s'est entretenu avec les élus démocrates David Cicilline et Richard Blumenthal, chacun auteur d'une proposition de loi dans l'esprit du DMA et du DSA, l'une sur la concurrence, l'autre sur la protection des enfants sur les réseaux sociaux, ainsi qu'avec des figures du mouvement pour une régulation des *« monopoles »* du numérique : Lina Khan, la présidente de l'Autorité de la concurrence (*la Federal Trade Commission, FTC*), Jonathan Kanter, responsable de l'antitrust au département de la Justice, et Tim Wu, du *National Economic Council*, qui conseille la Maison Blanche.

De son côté, le Conseil européen a tenu à manifester formellement son attachement à voir l'UE poursuivre ses diverses initiatives en faveur de la transformation numérique. Dans une déclaration en date du 27 mars 2021, les chefs d'Etat et de gouvernement ont tenu à souligner notamment les différents points suivants :

« Nous soulignons l'importance de la transformation numérique pour la reprise en Europe, pour sa prospérité, sa sécurité et sa compétitivité ainsi que pour le bien-être de nos sociétés. Dans ce contexte, nous rappelons les conclusions du Conseil européen des 1er et 2 octobre 2020 et celles des 10 et 11 décembre 2020. De plus, nous insistons sur la nécessité d'accroître la souveraineté numérique de l'Europe de manière autodéterminée et ouverte, en tirant parti de ses atouts et en atténuant ses faiblesses et au moyen d'une action intelligente et sélective, en préservant des marchés ouverts et la coopération mondiale.

La communication de la Commission intitulée "Une boussole numérique pour 2030 : l'Europe balise la décennie numérique" constitue une étape en vue de tracer les contours du développement numérique de l'Europe pour la prochaine décennie. Nous invitons le Conseil à procéder rapidement à l'examen de cette communication en vue de l'élaboration du programme de politique numérique envisagé.

6. En outre :

a) nous invitons la Commission à recenser d'autres systèmes concernant des technologies critiques et d'autres secteurs stratégiques afin de renforcer et d'affiner l'approche stratégique européenne à leur égard ;

b) nous invitons la Commission à étoffer la boîte à outils stratégique de l'Union européenne pour la transformation numérique, tant à l'échelon de l'Union européenne qu'au niveau national, et à utiliser tous les instruments disponibles dans les domaines des politiques industrielle, commerciale et de la concurrence, des compétences et de l'éducation, de la recherche et de l'innovation, ainsi que les instruments de financement à long terme, afin de faciliter la transformation numérique ;

c) nous recommandons de mieux exploiter le potentiel que recèlent les données et les technologies numériques, dans l'intérêt de la société, de l'environnement et de l'économie, tout en veillant au respect des droits pertinents en matière de protection des données et de vie privée et des autres droits fondamentaux et en assurant la conservation des données nécessaire pour permettre aux services répressifs et aux autorités judiciaires d'exercer leurs pouvoirs légaux

pour lutter contre les formes graves de criminalité; nous sommes conscients de la nécessité d'accélérer la création d'espaces communs de données, et notamment d'assurer l'accès aux données et leur interopérabilité; nous attendons avec intérêt la proposition de la Commission concernant un cadre réglementaire relatif à l'intelligence artificielle, ainsi que le réexamen du plan coordonné qui l'accompagnera, afin d'accélérer l'adoption de cette technologie tout en garantissant la sécurité et le plein respect des droits fondamentaux ; nous invitons la Commission à présenter rapidement les progrès accomplis et les mesures qu'il reste à prendre pour établir les espaces de données sectoriels annoncés dans la stratégie européenne pour les données de février 2020 ;

d) nous invitons les colégislateurs à faire avancer rapidement les travaux sur les propositions relatives à la législation sur les services numériques, à la législation sur les marchés numériques et à l'acte sur la gouvernance des données, en vue d'améliorer l'accès aux données ainsi que leur partage, leur mise en commun et leur réutilisation et de renforcer le marché unique des services numériques en créant un espace numérique plus sûr et des conditions équitables pour favoriser l'innovation et la compétitivité ;

e) nous invitons le Conseil à faire avancer les travaux sur le plan d'action pour la démocratie européenne ;

f) nous recommandons que les efforts de concertation internationale déployés par l'Union européenne et les États membres soient renforcés tant au niveau bilatéral que dans le cadre des instances et organisations concernées, en vue de promouvoir les normes numériques de l'UE et d'élaborer des règles numériques mondiales en étroite coopération avec des partenaires attachés aux mêmes principes. »[433]

Quand bien même la nécessité de proposer des réponses européennes et internationales aux défis posés à l'Etat de droit n'y figurent pas de manière explicite, il ressort néanmoins très clairement de cette déclaration une préoccupation commune des chefs d'Etat et de gouvernement de voir l'UE veiller au respect des droits pertinents en matière de protection des données et de vie privée et des autres droits fondamentaux.

Le 3 décembre 2021, le Conseil est parvenu à un accord important sur un projet de texte ambitieux qui vise à assurer un niveau commun élevé de cybersécurité au sein de l'Union européenne**.** Il conforte les travaux menés par l'ANSSI au niveau national et européen pour harmoniser les cadres nationaux et renforcer la coopération entre Etats membres.

La France a pour charge pendant sa présidence tournante du Conseil au premier semestre 2022, de négocier ce texte avec le Parlement européen, sur la base de l'orientation générale adoptée par le Conseil.

- *Adapter la Charte des droits des droits fondamentaux de l'UE pour mieux prendre en compte les spécificités du numérique et de l'IA*

La Charte des droits fondamentaux de l'UE devra elle aussi être revisitée en vue de son adaptation à cette nouvelle réalité sociétale décrite par Mireille Dumas-Marty. Et ce d'autant plus nécessairement que la force juridique - que lui confère sa portée constitutionnelle acquise dès l'entrée en vigueur du Traité de Lisbonne – lui assure un effet démultiplicateur à l'échelle de l'Union (aux restrictions près résultant du protocole n°30 sur l'application de la Charte des droits fondamentaux au Royaume Uni et à la Pologne annexé au Traité sur le fonctionnement de l'Union européenne).

[433] *Déclaration des membres du Conseil européen :* https://www.consilium.europa.eu/media/49010/250321-vtc-euco-statement-fr.pdf

Le 10 décembre 2021, la Commission européenne a publié son rapport annuel sur l'application de la Charte des droits fondamentaux au sein de l'UE, en focalisant ses travaux sur le thème de la protection des droits fondamentaux à l'âge digital.[434]

Ce document tout à fait remarquable se termine ainsi : *« Joining forces to make the digital age an opportunity for fundamental rights : Looking at the interrelated challenges and the corresponding measures examined in this report, there is no doubt that the EU and its Member States are committed to protecting and promoting fundamental rights in the digital age and that they are working together to identify the best ways to do so. The examples mentioned in the preceding chapters are some of many opportunities to learn from one another and to shape the changes brought about by the digital transition in a positive way. The Commission uses many tools to ensure the rights enshrined in the Charter are respected – both in the design of its legislative and policy initiatives as well as when enforcing EU law. In particular, the Commission will closely assess the effects on fundamental rights and aim to balance those effects in the upcoming Commission initiatives in 2022, such as legislative proposals on : - a right to repair, - cyber resilience, - digital mobility services, - instant payment, - reciprocal access to security-related information for frontline officers between the EU and key non-EU countries, - a Media Freedom Act, and - binding standards for Equality Bodies. Furthermore, in the context of the Digital Decade, the Commission will propose to include a set of digital principles in an inter-institutional solemn declaration between the European Commission, the European Parliament and the Council. This declaration will inform users and guide policy makers and digital operators about the European way to the digital transformation. The Commission calls on the European Parliament, the Council and Member States to use this Annual Report on the Application of the EU Charter of Fundamental Rights to engage in exchanges about the challenges and opportunities for protecting fundamental rights in the digital age. It welcomes the Council's commitment to exchange views based on the Commission's reports and would also welcome a discussion in the European Parliament. In particular, these exchanges could help to better address the challenges ahead, in particular the fight against hate speech and disinformation, how to ensure checks and balances on surveillance measures, and more generally how to effectively enforce laws to protect fundamental rights in the digital environment. These exchanges can help frame policy developments in a constructive and beneficial way. These joint efforts to render the Charter effective in the digital age, together with the European Democracy Action Plan136 and the European rule of law mechanism, illustrate the EU's commitment to promoting and protecting the values on which it is founded. »*

Outre son adaptation aux nouvelles réalités sociétales induites par le numérique et l'intelligence artificielle, entreprendre la « fédéralisation » de la Charte des droits fondamentaux de l'UE, option mise en avant par l'ancienne Commissaire à la Justice Vivian Reding en 2013, aurait également pour effet d'étendre la compétence de la Cour de justice.

« Il s'agirait d'étendre le champ d'application ratione materiae de la Charte pour la rendre opposable aux États membres dans toute situation, et non seulement lorsqu'ils « mettent en œuvre » le droit de l'Union au sens de son article 51. L'extension de compétence qui en résulterait pour la Cour de justice serait cependant beaucoup plus importante et radicale que celle suggérée par l'avocat général M. Poiares Maduro : elle ferait de la Cour de justice une véritable Cour fédérale, garante d'un standard minimal de protection des droits fondamentaux sur l'ensemble du territoire de l'Union européenne. » [435]

[434] *Protecting Fundamental Rights in the Digital Age - 2021 Annual Report on the Application of the EU Charter of Fundamental Rights :* https://ec.europa.eu/info/sites/default/files/1_1_179442_ann_rep_en_0.pdf

[435] *Cf.* Dimitry Kochenov, Laurent Pechet Sébastien Platon *in Ni panacée, ni gadget : le « nouveau cadre de l'Union européenne pour renforcer l'État de droit »* (Revue trimestrielle de droit européen) : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2688353

- *Entreprendre l'adhésion de l'UE à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales*

L'adhésion de l'UE à la *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales* est prévue à l'article 6, paragraphe 2 du TUE.

Bien que chacun de ses Etats membres y soit partie, l'UE n'est pas elle-même partie à la Convention en tant qu'organisation. Elle n'a notamment aucune compétence pour édicter des règles ou conclure des accords internationaux en matière de droits de l'homme.

Le respect de la Convention est cependant assuré par la Cour de Justice de l'UE qui s'y réfère parfois explicitement.

En accordant la personnalité juridique à l'UE, le Traité de Lisbonne rend désormais cette adhésion possible – le texte de la Convention ayant été amendé dès 2010 au travers de son protocole n°14 qui introduit un nouvel article 59.2 *(« L'Union européenne peut adhérer à la présente Convention »)* pour la rendre possible -, ce qui placerait alors l'UE souhaite sur un pied d'égalité avec ses Etats membres en ce qui concerne le système de protection des droits fondamentaux. Cela lui permettrait d'être entendue dans les affaires examinées par la CEDH, ainsi que d'y désigner un juge.

Cette adhésion offrirait également une nouvelle possibilité de recours aux particuliers, qui pourraient alors, après avoir épuisé toutes les voies de recours nationales – saisir la CEDH d'une plainte pour violation supposée des droits fondamentaux par l'UE (et non seulement par ses Etats membres).

Lancés en 2010, les pourparlers entre la Commission européenne et le Conseil de l'Europe ont achoppé en 2014 sur un avis négatif de la Cour de justice de l'UE. Cette dernière a estimé que la proposition d'accord d'adhésion n'était pas conforme aux lois européennes en raison d'incompatibilités liées notamment à l'autonomie du droit de l'Union ou à la politique étrangère et de sécurité commune (PESC)[436].

L'adhésion reste cependant une priorité de la Commission européenne. Dont acte. [437]

- *La Commission européenne élève la barre des exigences pour le secteur technologique*

Le 21 avril 2021, la Commission a établi de nouvelles règles et actions visant à faire de l'Europe le pôle mondial d'une intelligence artificielle (IA) digne de confiance[438,439] .

[436] *Cf.* notamment à cet égard Carlos Luis Miguel *in Les droits fondamentaux au carrefour de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne* (notamment les pages 129 à 135)
https://www.academia.edu/36805479/Les_droits_fondamentaux_au_carrefour_de_la_Cour_europ%C3%A9enne_des_droits_de_lhomme_et_de_la_Cour_de_justice_de_lUnion_europ%C3%A9enne

[437] *Cf.* notamment le Rapport d'information n° 562 (2019-2020) de MM. Philippe Bonnecarrère et Jean-Yves Leconte, fait au nom de la commission des affaires européennes du Sénat sur *l'adhésion de l'Union européenne à la Convention européenne des droits de l'homme* : https://www.senat.fr/rap/r19-562/r19-562_mono.html
ainsi que Jose m. Cortes Martin *in Sur l'adhésion à la CEDH et la sauvegarde de l'ordre juridique de l'Union dans l'identification du défendeur pertinent : le mécanisme du codéfendeur :*
https://www.academia.edu/7626146/SUR_L_ADHESION_A_LA_CEDH_ET_LA_SAUVEGARDE_DE_L_AUTONOMIE_DE_L_ORDRE_JURIDIQUE_DE_L_UNION_DANS_LIDENTIFICATION_DU_DEFENDEUR_PERTINENT_LE_MECANISME_DU_CODEFENDEUR

[438] *Une Europe adaptée à l'ère numérique : La Commission propose de nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle : https://ec.europa.eu/commission/presscorner/detail/fr/IP_21_1682*

[439] *A European approach to artificial intelligence :*
https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

« La combinaison du tout premier cadre juridique sur l'IA[440] et d'un nouveau plan coordonné avec les États membres[441] garantira la sécurité et les droits fondamentaux des citoyens et des entreprises, tout en renforçant l'adoption de l'IA, les investissements et l'innovation dans l'ensemble de l'UE. Cette approche sera complétée par de nouvelles règles concernant les machines, qui visent à accroître la confiance des utilisateurs dans la nouvelle génération polyvalente de produits en adaptant les dispositions relatives à la sécurité.

Le nouveau règlement sur l'IA garantira aux Européens qu'ils peuvent faire confiance à l'IA. Des règles proportionnées et souples, prévues pour faire face aux risques spécifiques liés aux systèmes d'IA constitueront l'ensemble de normes le plus strict au monde.

Le plan coordonné décrit les réorientations et les investissements qui seront nécessaires au niveau des États membres pour renforcer la position de premier plan de l'Europe dans le développement d'une IA centrée sur l'humain, durable, sûre, inclusive et digne de confiance.

Les nouvelles règles, fondées sur une définition de l'IA à l'épreuve du temps, seront directement applicables dans tous les États membres. »

En ce qui concerne la gouvernance, la Commission propose que les autorités nationales compétentes de surveillance du marché veillent au respect des nouvelles règles dont la mise en œuvre sera facilitée par la création d'un comité européen de l'IA qui sera également chargé de stimuler l'élaboration de normes pour l'IA. En outre, la proposition prévoit des codes de conduite facultatifs pour les systèmes d'IA ne présentant pas de risque élevé, ainsi que des « bacs à sable réglementaires » afin de faciliter l'innovation responsable.

Par cette proposition de loi qui réglemente l'IA au travers une approche articulée sur une catégorisation des risques (risque inacceptable, risque élevé, risque limité et risque minimal), la Commission élève la barre des exigences pour le secteur technologique, comme elle l'a fait avec le *Digital Market Act* et le *Digital Services Act* ; par la cybersécurité, par la protection des données personnelles, par une garantie à la concurrence, et maintenant par la réglementation de l'IA.

La proposition de loi cite une longue liste de droits mis en question par l'IA, et que l'on trouve dans la Charte Européenne des droits fondamentaux. Parmi eux, le respect de la vie privée, la protection des données personnelles, la non-discrimination. Pour ce qui est de la responsabilité, l'accent est mis sur le fournisseur de service, même si les développeurs seront tenus de suivre tout un processus de mise en conformité avant d'introduire leur produit sur le marché. Le tampon CE sera utilisé pour manifester cette conformité, et attester du respect du règlement.

Margrethe Vestager**,** vice-présidente exécutive pour une Europe adaptée à l'ère du numérique, a déclaré à ce propos : *« En matière d'intelligence artificielle, la confiance n'est pas un luxe mais une nécessité absolue. En adoptant ces règles qui feront date, l'UE prend l'initiative d'élaborer de nouvelles normes mondiales qui garantiront que l'IA soit digne de confiance. En établissant les normes, nous pouvons ouvrir la voie à une technologie éthique dans le monde entier, tout en préservant la compétitivité de l'UE. À l'épreuve du temps et propices à l'innovation, nos règles s'appliqueront lorsque c'est strictement nécessaire : quand la sécurité et les droits fondamentaux des citoyens de l'Union sont en jeu. »*

[440] *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) :* https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

[441] *Coordinated Plan on Artificial Intelligence 2021 Review :* https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

Une fois adoptés, les règlements seront directement applicables dans l'ensemble de l'UE. Parallèlement, la Commission continuera de collaborer avec les États membres à la mise en œuvre des actions annoncées dans le plan coordonné.

En France, en matière de santé, l'Association Pour la Sécurité des Systèmes d'Information de Santé, l'APSSIS, formule un certain nombre de recommandations qui prennent leur source dans ce texte de l'UE.[442]

- *L'UE doit veiller à répondre aux inquiétudes légitimes*

Mais cette initiative de réglementation inquiète. D'un côté les entreprises s'alarment de risques sur leurs investissements, de l'autre les associations redoutent qu'un texte trop vague amène à des dérives.

Selon l'Union des libertés civiles pour l'Europe : « *Ces systèmes constituent une menace pour nos libertés individuelles, notamment le droit à l'éducation, le droit à un procès équitable, le droit à la vie privée et le droit à la liberté d'expression. Ils créent souvent une situation de déséquilibre des pouvoirs et ont d'énormes répercussions sur les droits fondamentaux des personnes. Il est inacceptable de déléguer leur évaluation des risques à des entreprises à but lucratif qui se concentrent sur l'obéissance aux règles lorsqu'elles y sont contraintes et non sur la protection des droits fondamentaux* ».

Access Now, association de défense des droits civils numériques, a rejoint une centaine de parlementaires européens pour appuyer le bannissement de plusieurs autres champs. C'est le cas des IA permettant le contrôle des frontières et de l'immigration. Pour l'association, le projet est trop vague et par conséquent contient trop de failles. *Access Now* estime que le niveau de risque considéré comme inacceptable doit être plus clairement défini pour qu'il puisse servir à interdire de nouvelles formes d'IA par la suite.

La CNIL a également pointé cette nécessité de tracer des lignes rouges aux futurs usages de l'IA. Si dans l'ensemble, elle semble plutôt satisfaite des règles proposées par l'UE, elle fait tout de même part de quatre points de vigilance.[443]

L'ONG *Future of Life Institute* insiste sur le fait qu'une IA doit être abordée pour toutes ses utilisations et non pas pour une fonction unique. L'ONG craint que cela « *permette à des technologies de plus en plus évolutives d'échapper à l'examen réglementaire* ».

Parmi les entreprises s'étant prononcées sur la loi européenne d'encadrement de l'intelligence artificielle se trouvent Nokia, Philips, Siemens, le groupe BMW, Facebook, Google, IBM, Intel, Microsoft ou encore OpenAI. La majorité des commentaires apportés à la loi sur l'IA proviennent de structures issues de Belgique, de France, d'Allemagne et des États-Unis.

Eric Schmidt, l'ancien patron de Google juge que ce texte était un « désastre », en s'attaquant à un domaine encore trop récent pour être réglementé.

META s'inquiète particulièrement des articles de loi concernant la publicité ciblée. Le patron de sa recherche en intelligence artificielle, le Français Yann Le Cun, qui est l'un des scientifiques à l'origine des intelligences artificielles modernes, regarde ainsi d'un oeil prudent le projet de réglementation européenne sur l'IA. Il estime qu'il ne faut pas chercher à réglementer l'IA en tant que telle, mais plutôt ses usages. *« Je suis plutôt partisan de réglementer »* une *« application particulière plutôt qu'une technologie »*.

[442] *Cf.* Marguerite Brac de La Perrière *in Quel cadre pour les systèmes d'IA dans le secteur de la santé ?* https://www.apssis.com/actualite-ssi/519/quel-cadre-pour-les-systemes-d-ia-dans-le-secteur-de-la-sante.htm

[443] Voir notamment *Ce que la CNIL pense du futur règlement sur l'intelligence artificielle :* https://siecledigital.fr/2021/07/09/cnil-lintelligence-artificielle-reglement-europeen/

Pour Yann Le Cun, le projet européen « *part d'une bonne intention* ». *« Il faut que les systèmes d'intelligence artificielle soient sécurisés, qu'ils ne mettent pas les personnes en danger, qu'ils respectent la vie privée »*, explique-t-il. *« Mais il faut se méfier de ne pas ralentir la recherche et la créativité des chercheurs, qui sont un peu le moteur de l'innovation de l'économie. L'Europe prendrait le risque de prendre du retard »* avec une réglementation de l'IA trop contraignante, a-t-il ajouté. En matière de reconnaissance faciale par exemple, il faut arriver à faire la part des choses entre les applications qui serviront *« de bonnes fins »*, et les autres, explique-t-il : *« La reconnaissance faciale ou la reconnaissance biométrique se révèlent absolument indispensables pour certains pays qui n'ont pas de moyens très simples de faire de l'authentification de l'identité »*, indique-t-il. *« Cela peut permettre à des gens d'avoir accès à un compte bancaire, à des services sociaux »*, voire, comme le fait la fondation Bill Gates, d'arriver à identifier des bébés par une photo de leur plante des pieds, pour éviter de les vacciner deux fois. « *En revanche, il faut des réglementations très strictes pour protéger la vie privée, éviter qu'on reconnaisse le visage de n'importe qui passe dans un espace public* ».

Mastercard s'oppose à ce que des programmes jugeant la solvabilité des personnes soient considérés comme à risque élevé arguant que cela diminue les évaluations de crédit. Plusieurs cas ont pourtant mis la lumière sur des discriminations au sein des algorithmes de prêts et de services financiers.

De son côté, Google indique qu'il sera très difficile, voire impossible, pour les développeurs de programmes d'IA de se conformer aux nouvelles règles européennes. Probablement pour simplifier les choses, Google souhaite qu'il y ait une distinction entre « *développeurs* », « *fournisseurs* », « *distributeurs* » et « *importateurs* ». Ainsi, l'ensemble des responsabilités ne reposerait pas uniquement sur le développeur mais aussi sur l'utilisateur de l'IA. Microsoft a formulé une demande similaire.[444]

Par ailleurs, la présidence tournante du Conseil de l'UE a élaboré la définition des systèmes d'IA afin de mieux les distinguer des programmes logiciels classiques. Les systèmes d'IA sont donc considérés comme ayant la capacité de traiter des données ou d'autres types d'entrées *« pour déduire la manière d'atteindre un ensemble donné d'objectifs définis par l'homme par l'apprentissage, le raisonnement ou la modélisation »*, selon le compromis.

Un fournisseur d'IA est désormais défini comme un individu ou une organisation *« qui fait développer un système d'IA et qui met ce système sur le marché ou le met en service »*. Les fournisseurs auront la responsabilité d'assurer la conformité avec les exigences du règlement.

Une nouvelle catégorie de système d'IA *« à usage général »* a été ajoutée, qui ne doit pas être considérée comme relevant du champ d'application du règlement, sauf si le système appartient à une marque commerciale ou s'il est intégré dans un autre système soumis au règlement.

Un fait majeur est intervenu le 29 novembre 2021 quand la présidence tournante du Conseil de l'UE a partagé un premier texte de compromis pour accompagner un rapport d'étape sur la loi européenne sur l'IA ; un texte comprenant des changements majeurs dans les domaines du *scoring social*, des systèmes de reconnaissance biométrique et des applications à haut risque.

Alors que la proposition de la Commission comprend une interdiction des applications d'IA considérées comme présentant des risques inacceptables (l'une d'entre elles est le *scoring social* ou notation sociale, une pratique initiée en Chine qui est considérée comme favorisant la surveillance de masse), la présidence du Conseil propose maintenant d'étendre l'interdiction de la notation sociale des autorités publiques aux entités privées. En outre, la définition de l'interdiction a également été étendue pour inclure l'exploitation d'une *« situation sociale ou économique. »* Ces changements pourraient avoir de profondes répercussions sur le secteur

[444] *Cf.* notamment https://siecledigital.fr/2021/09/07/craintes-loi-europeenne-intelligence-artificielle/

financier, car, par exemple, les taux d'intérêt des prêts sont actuellement calculés en fonction de la probabilité de remboursement. L'utilisation de systèmes d'IA pour l'estimation des primes d'assurance a également été incluse dans les systèmes à haut risque.

Dans ce même texte de compromis, les systèmes d'identification biométrique couverts par la législation ne sont plus définis comme des systèmes *« à distance »*, mais comme tout système permettant d'identifier des personnes *« sans leur accord ».* La possibilité d'utiliser des systèmes d'identification biométrique en temps réel a été étendue à des acteurs qui ne sont pas des autorités répressives mais qui collaborent avec elles. La raison de l'utilisation de ces systèmes a été étendue à la protection des infrastructures critiques. Les systèmes biométriques ne peuvent être utilisés qu'avec l'accord de l'autorité judiciaire. En cas d'urgence, la proposition initiale prévoyait que l'autorisation pouvait également être demandée a posteriori. En revanche, selon le nouveau texte, l'autorisation doit *« être demandée sans retard excessif pendant son utilisation, et si cette autorisation est rejetée, il est mis fin à son utilisation avec effet immédiat ».*

Comme nous venons de le montrer, les différends en matière de réglementation de l'intelligence artificielle ont pris de l'importance au cours des dernières années.

Mais un ensemble unique de règles mondiales, ou même simplement transatlantiques, est-il le moyen de résoudre ce problème ?

L'économiste Sylvain Zeghni estime que pour l'UE, dont les ambitions éthiques sont immenses, la réponse pourrait être "non".

« Début 2021, l'UE est devenue la première grande juridiction à publier un projet de règles pour l'intelligence artificielle (IA). Il y a de bonnes raisons de surveiller de près la technologie de l'IA sur le plan législatif. Les préoccupations vont de la discrimination algorithmique et de la distorsion de la démocratie à la surveillance omniprésente et à l'oppression pure et simple.

Au-delà de ces questions se profilent des préoccupations plus profondes. Un monde saturé de machines capables de prédire et d'exploiter nos peurs et nos désirs remet fondamentalement en cause l'autonomie humaine. Dans le même temps, l'automatisation par l'IA risque de priver de nombreuses personnes de leur emploi une fois que le boom post-pandémique alimenté par la dette publique aura disparu. L'automatisation a déjà creusé un fossé entre les échelons supérieurs et inférieurs du marché du travail. Aidés par des machines intelligentes, de nombreux travailleurs hautement qualifiés ont vu leur productivité augmenter, tandis que les emplois comportant des tâches plus routinières ont, en revanche, lentement disparu.

La Commission européenne vante fièrement une troisième voie européenne en matière de réglementation de l'IA : plutôt que de laisser les algorithmes servir l'État (comme en Chine) ou les grandes entreprises (comme aux États-Unis), l'approche de Bruxelles vise à les mettre au service des personnes – une " IA digne de confiance ", selon le slogan de l'UE. Cela implique de restreindre la liberté accordée aux maîtres de l'IA – qu'il s'agisse de gouvernements ou d'entreprises. Cette approche européenne se heurtera à deux obstacles majeurs.

Premièrement, le secteur technologique de l'UE est déjà à la traîne par rapport à ceux de la Chine et des États-Unis. En mettant un frein aux applications de l'IA, on ne peut que creuser l'écart. Après tout, les algorithmes se nourrissent de l'apprentissage par la pratique. La création d'un espace européen des données [445] et la coordination des investissements d'amorçage par les États membres de l'UE sont censées stimuler le secteur. Mais personne ne sait si cela suffira à faire de l'IA européenne autre chose qu'une attraction sur la scène mondiale.

[445] *A European Strategy for data :* https://digital-strategy.ec.europa.eu/en/policies/strategy-data

Deuxièmement, les hommes politiques et les experts américains considèrent de plus en plus l'IA comme un problème de sécurité. Au début de l'année, le rapport final publié par la Commission de sécurité nationale américaine sur l'IA[446] décrivait l'IA comme une course technologique entre la Chine et les États-Unis, le perdant étant vulnérable à la suprématie de l'IA du gagnant. Le rapport laisse entendre que les Européens seraient bien avisés de s'installer dans le siège passager d'une alliance de puissances technologiques "éprises de liberté" dirigée par les États-Unis et de laisser le gouvernail à Washington et à la Silicon Valley.

Ces forces tirent les États européens dans des directions opposées. Les préoccupations éthiques incitent à la prudence, les préoccupations en matière de compétitivité encouragent l'audace européenne, tandis que le cadre sécuritaire de l'IA suggère que l'Europe devrait jouer un rôle secondaire dans une alliance occidentale. Alors, quelle est la voie à suivre ?

Une grande partie du débat actuel sur la dynamique mondiale de la réglementation de l'IA est indûment simpliste, traitant la "réglementation de l'IA" comme s'il s'agissait d'un bloc unique et monolithique, à aborder seul ou en coopération avec l'un ou l'autre partenaire. Au lieu de cela, une perspective nuancée consisterait à reconnaître l'énorme étendue des utilisations et des préoccupations réglementaires actuellement regroupées sous le terme d'IA.

Il est certain qu'avec des frontières économiques ouvertes, l'efficacité des règles européennes en matière d'IA dépend de ce que font les autres grandes juridictions – le domaine de l'IA est riche en "interdépendance réglementaire". À quoi servent les règles européennes contre la discrimination invisible dans le tri automatique des CV si les clients peuvent simplement utiliser des services basés aux États-Unis ? À quoi servent des règles strictes en matière de protection de la vie privée si nous pouvons importer des systèmes d'IA formés à partir de données récoltées de manière non éthique auprès de citoyens étrangers ?

Cette interdépendance réglementaire est toutefois variable : dans certains domaines, comme la diffusion mondiale des systèmes d'armes automatisés[447], l'UE dépend entièrement de la coopération avec les autres grandes puissances. Dans d'autres, comme les normes de sécurité pour les voitures à conduite autonome, elle peut élaborer ses propres règles et procédures de test, indépendamment de ce que font les autres. Certaines applications, comme la résilience des infrastructures alimentées par l'intelligence artificielle, ont un rapport direct avec l'OTAN en tant qu'alliance de sécurité ; d'autres, comme les règles applicables aux algorithmes Twitter ou à l'approbation automatique des prêts, n'ont aucun rapport avec la sécurité.

Cette interdépendance réglementaire variée – élevée dans certains cas, faible dans d'autres – invite à une approche différenciée de la réglementation mondiale de l'IA. Lorsque des normes mondiales peuvent s'aligner sur les objectifs réglementaires européens, elles sont clairement préférables. Lorsqu'un tel accord est hors de portée, des options de second choix apparaissent telles que des normes partagées élaborées au sein du tout nouveau Conseil technologique transatlantique[448]. La reconnaissance mutuelle de normes différentes, mais tout aussi strictes est également une option, tout comme le soutien aux normes privées de l'industrie.

---

[446] *« The mandate of the National Security Commission on Artificial Intelligence's (NSCAI) is to make recommendations to the President and Congress to "advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States." This Final Report presents the NSCAI's strategy for winning the artificial intelligence era. The 16 chapters in the Main Report provide topline conclusions and recommendations. The accompanying Blueprints for Action outline more detailed steps that the U.S. Government should take to implement the recommendations. » -* https://www.nscai.gov/2021-final-report/

[447] *Background on LAWS in the CCW :* https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/

[448] *EU-US Trade and Technology Council: Commission launches consultation platform for stakeholder's involvement to shape transatlantic cooperation :* *https://ec.europa.eu/commission/presscorner/detail/en/IP_21_5308*

Mais lorsque les objectifs éthiques de l'UE sont mieux servis par Bruxelles qui va de l'avant toute seule – comme elle l'a fait avec le règlement général sur la protection des données (RGPD) – elle devrait avoir le courage de le faire. Il n'y a aucune raison de penser que l'UE sera bien servie par une approche unique de la coopération réglementaire internationale en matière d'IA. Elle ne doit pas céder aveuglément à la logique du "êtes-vous avec nous ou contre nous" qui prévaut dans la pensée américaine. Les divers compromis éthiques que soulève l'IA pèsent trop lourd pour être abordés dans un moule international uniforme.

Toujours attentive à l'approche qui lui permet de maximiser sa souveraineté numérique sur une question donnée, l'UE doit coopérer lorsque cela est possible et oser faire cavalier seul lorsqu'elle le doit. Une telle approche à la carte de la réglementation mondiale a bien servi l'UE dans de nombreux autres domaines, de la finance à la sécurité alimentaire en passant par les produits pharmaceutiques. Il n'y a aucune raison de penser qu'elle échouerait dans le domaine de l'IA. »

Comment ne pas partager pleinement un tel constat.

Dans un article publié sur Linkedin le 27 décembre 2021[449], Yannick Meneceur, magistrat, chef de la division centrale (Direction générale des droits de l'homme et de l'État de droit) du Conseil de l'Europe[450], revient sur la question complexe de la définition juridique de l'intelligence artificielle en ces termes : *« En avril 2021, la Commission européenne posait, dans son projet de réglementation sur l'intelligence artificielle (« IA »), une définition de cette technologie dont les mérites, et les défauts, ont été largement débattus. Trop large pour certains, trop précise pour d'autres, il semble que les dernières orientations du Conseil de l'Union européenne tendent maintenant à en restreindre le champ pour concentrer les efforts réglementaires sur les dernières technologies en vogue.*

Si les enjeux de ces discussions semblent paraître très techniques, nous aurions tort d'en réduire la portée. Dans sa carte blanche dans le journal Le Monde, Nozha Boujemaa soulignait avec justesse l'enjeu « juridico-commercial » de l'exercice[451] car si cette définition s'avérait « trop large, elle serait très contraignante en matière d'évaluation et de gestion des risques pour les entreprises », la loi devenant « applicable pour beaucoup de services numériques, y compris ceux n'utilisant pas d'apprentissage profond ».

Les grandes manœuvres en cours autour du projet de réglementation de « l'IA » à Bruxelles, mais aussi à Strasbourg avec l'ouverture en 2022 de négociations sur un projet de Convention dans une autre institution (le Conseil de l'Europe), ne se nourrissent donc pas que de la seule approche scientifique et objective de la question. Il ne fait en effet guère de doute que le terme commode, vague et plastique « d'IA » englobe depuis sa création en 1955 bien plus que l'apprentissage profond. L'inquiétude qui semble saisir nombre d'acteurs de cette régulation serait une forme de contamination de la dynamique d'encadrement juridique à la plupart des systèmes automatisés de prise de décision dont les limites, en Europe du moins, n'étaient alors tracées qu'au travers du concept de protection des données à caractère personnel.

---

[449] *Cf. Le piège de la définition juridique de l'intelligence artificielle :* https://www.linkedin.com/pulse/le-pi%C3%A8ge-de-la-d%C3%A9finition-juridique-lintelligence-yannick-meneceur

180

[450] Intervenant occasionnel à l'ENM, à l'ENA et enseignant-vacataire à l'Université de Strasbourg (M2 Cyberjustice et droit de l'économie numérique), Yannick Meneceur, auteur de *« L'intelligence artificielle en procès »* - Prix du Cercle Montesquieu 2021 est également membre des conseils scientifiques des pôles numériques du Club des Juristes et de l'Institut PRESAJE. J'ai rejoint en 2020 les experts de l'observatoire Éthique et IA de l'Institut Sapiens et en 2021 le conseil consultatif de l'initiative Z-Inspection ainsi que les expert d'AI for Tomorrow.

[451] *Cf. La définition de l'intelligence artificielle, enjeu juridico-commercial* (Le Monde, 15 décembre 2021) : https://www.lemonde.fr/sciences/article/2021/12/15/la-definition-de-l-intelligence-artificielle-enjeu-juridico-commercial_6106094_1650684.html#xtor=AL-32280270-%5Bdefault%5D-%5Bios%5D

Pourtant, sans nier les spécificités des systèmes fondés sur des approches statistiques, l'on devrait bien reconnaître que l'enjeu pour nos sociétés contemporaines est de parvenir à maintenir le délicat mécanisme des équilibres institutionnels et de protection des droits dans un contexte de profonde transformation numérique. Investir un système algorithmique d'une capacité de prise de décision, même sous la responsabilité d'un humain, pose les mêmes questions en ce qui concerne les garanties à apporter, quelle que soit la technologie employée.

Si l'on s'en tient à tenter de prévenir de manière efficace les dérives d'emploi de ces systèmes dans le temps, revenir à une certaine forme de neutralité technologique dans les instruments juridiques à bâtir pourrait donc paraître comme évidente et économiser un temps précieux de débat. Les différentes générations de textes relatifs à la protection des données nous l'ont déjà démontré, en se concentrant sur les effets à prévenir moins que sur les moyens. Ici il serait donc question à notre ère d'aller plus loin que la protection de la vie privée, mais aussi de prévenir le renforcement des discriminations, de continuer de garantir des voies de recours effectives ou de mieux assurer l'équilibre entre liberté d'expression et censure des discours de haine par exemple, quels que soient les formes de traitement informatique.

Mais peut-être n'est-ce pas aujourd'hui l'objectif partagé par tous les acteurs de la régulation de « l'IA », certains pouvant être tentés de gagner du temps en alimentant des débats voués à être sans fin et à répondre aux sérieuses préoccupations sociétales par des textes aux effets extrêmement limités. Entre blanchiment juridique de pratiques extrêmement contestables si elles n'étaient pas noyées sous un vernis technologique et peur irrationnelle de se voir dépasser (technologiquement et économiquement) par les autres, la grille de lecture fondée sur des valeurs humanistes est loin d'être partagée. L'innovation en vient à être considérée comme un objectif cardinal teinté de « sacré », inconditionnellement et inextricablement lié à une évolution positive de la société si cela créé de la richesse économique.

Il n'en sera malheureusement rien si cette innovation n'est pas encadrée par des valeurs et la solide conviction que tout ce qui est faisable n'est pas nécessairement souhaitable. Et c'est bien dans cet exact objectif que le droit devrait conserver toute sa vigueur. »

Sur un tout autre registre, économique et financier, le *Center for Data Innovation'*[452] a produit en juillet 2021 une vaste étude intitulée *'How Much Will the Artificial Intelligence Act Cost Europe?'*[453] dans laquelle les *« Big Tech »* dénoncent essentiellement les obligations *a priori* qui pèseraient sur les développeurs et les exploitants de systèmes à risque « élevé ». Et le coût financier des mesures à prendre en conséquence. Pour lui donner du crédit, le *Center for Data Innovation* précise qu'elle se fonde – entre autres – sur l'analyse d'impact de la Commission européenne.

Il laisse par ailleurs entendre que les chiffres indiqués pourraient être plus défavorables, certains aspects n'étant pas pris en compte. Par exemple, les effets dissuasifs sur l'investissement dans les start-ups, la fuite des cerveaux et le ralentissement de la numérisation de l'économie.

Sur le volet macroéconomique, l'argumentation contre l'AIA peut se synthétiser ainsi :

- Le PIB de l'UE s'élève à 13 300 milliards d'euros ; environ un quart de ce PIB (3 400 milliards) est issu de secteurs qui relèvent de la catégorie des risques « élevés » (santé, éducation, finance, IT, infrastructures critiques…) ;

[452] Derrière cette organisation à but non lucratif de droit américain, il y a un géant du lobbying tech : *l'ITIF (Information Technology and Innovation Foundation).* La liste de ses soutiens financiers comprend notamment tous les GAFAM : https://itif.org/our-supporters

[453] *How Much Will the Cost Europe?* : https://www2.datainnovation.org/2021-aia-costs.pdf

- Si on se base sur un taux d'usage de l'IA à 7 %, environ 230 milliards d'euros de PIB tombent à l'heure actuelle sous le coup de l'AIA ; dont environ 20 % (46 milliards) en R&D IT ;
- Si l'objectif des 75 % est atteint, 25 000 milliards d'euros de PIB – dont 5 000 milliards en R&D IT – seront soumis à l'AIA en 2030.

L'UE est à un tournant de son histoire.

Son autonomie stratégique comme son modèle de civilisation et de démocratie sont en jeu plus qu'ils ne l'ont jamais été.

La capacité des institutions européennes et internationales (Nations Unies) à réguler les innovations technologiques de rupture par le droit est mise d'ores et déjà l'épreuve des faits à l'égard des technologies convergentes de type NBIC[454] comme à l'égard des systèmes d'armes létales autonomes[455].

Si une volonté d'agir s'est bien manifestée, que parviendra-t-elle à produire *in fine* au regard des jeux et enjeux qui opposent les Etats ?

Franck DeCloquement avertit : *« Bien qu'il existe un consensus émergeant sur la menace que les entreprises de Big Tech font peser sur l'esprit de nos démocraties, il y a en réalité peu d'accords factuels sur la façon d'y répondre : certains ont fait valoir aux Etats-Unis que le gouvernement devait rompre avec Facebook et Google. D'autres ont appelé à des réglementations plus strictes pour limiter l'exploitation des données par ces firmes géantes. Sans une voie à suivre claire, de nombreuses critiques ont fait pression sur les plateformes pour qu'elles s'autorégulent, les encourageant à supprimer préalablement les contenus dangereux, et à mieux gérer les publications de leurs sites. Mais peu reconnaissent que les préjudices politiques posés par ces plateformes « sociales » sont bien plus graves que les préjudices économiques. En tout état de cause, les GAFAM sont consubstantiels de la puissance Américaine. Nul doute qu'il est fort improbable que les Etats-Unis se laissent spolier ou endiguer la puissance qu'offrent de tels outils par d'autres à l'extérieur de ses frontières. Gardons-le à l'esprit. »*

---

[454] *« Les NBIC permettent de manipuler la matière à l'échelle des atomes et des molécules. Or, à cette échelle, l'organique ne se distingue plus de l'inorganique, le vivant de l'inerte, l'homme de la machine, ce qui rend possible la combinaison des deux. Les ambitions des NBIC sont portées, à leur plus haut niveau, par les transhumanistes, qui souhaitent que l'humanité prenne en charge sa propre évolution. Ils prônent le passage de l'humanité telle que nous la connaissons actuellement à une post-humanité, c'est-à-dire à une humanité technologiquement augmentée et débarrassée des limites naturelles de l'être humain : d'une part combattre la maladie, le handicap, la vieillesse et la sénescence, et empêcher la mort ; d'autre part augmenter les capacités humaines et notamment les facultés cognitives et physiques. »*
Cf. Nicolas Crozatier *in Transhumanisme et héritage prométhéen : cartographie des mondes posthumains :* https://dumas.ccsd.cnrs.fr/dumas-01146997?fbclid=IwAR1P5SGL50fU8UZD87SLCGAIcXylnD4n-EE9RV0rqsuZYcS13OuQ9U5pcQ4
Thierry Berthier *in Convergence technologique : l'homme, la machine et la société :* https://theconversation.com/convergence-technologique-lhomme-la-machine-et-la-societe-76044
Françoise Roure *in Nanosciences et technologies convergentes : quelle économie politique ? :* https://www.dailymotion.com/video/x5hc38v
Patrice Cardot et Bertrand de Montluc *in Nouvelles sciences et technologies : enjeux de sécurité et problématique de responsabilité internationale :* http://regards-citoyens.over-blog.com/article-28826015.html
ainsi que *Du besoin de gouvernance des activités bio et nanotechnologiques convergentes :* http://regards-citoyens.over-blog.com/article-27955331.html

[455] *Quels principes juridiques pour les systèmes d'armes létales autonomes ?* https://theconversation.com/quels-principes-juridiques-pour-les-systemes-darmes-letales-autonomes-153581?utm_term=Autofeed&utm_medium=Social&utm_source=Facebook&fbclid=IwAR3VXofQ4iJxKaqQzNo6BxTJpNPhDh_aIC_YXGQtc5Qso4OP4gOxW7X5HDw#Echobox=1613343694

Des initiatives industrielles apparaissent qui proposent la constitution de *clouds* 'européens' telles qu'*EUCLIDIA* dont les fondateurs veulent proposer des technologies *cloud* 100 % européennes garanties sans fournisseurs américains ou chinois[456].

L'Europe a encore toutes ses chances pour créer les futurs champions mondiaux du Li-Fi.[457] Elle dispose d'un écosystème riche et propice au déploiement de cette solution sur son territoire, tant au niveau de la recherche (CEA Leti en France, Institut Fraunhofer en Allemagne) que de l'industrie. En atteste la création de la LCA en 2019, première alliance mondiale entre des centres de recherche d'excellence, des producteurs de Li-Fi et de grands équipementiers européens tels que Nokia ou Orange. Si elle veut être en ligne avec sa politique de souveraineté en matière de numérique – auquel la Défense est intrinsèquement liée-, l'UE a un donc rôle clé à jouer dans la compétition internationale engagée autour du développement de cette technologie prometteuse dont la première standardisation mondiale sur cette technologie est attendue pour mai 2022. Elle le fait déjà en finançant depuis 2019 les programmes de recherche ELIoT et ENLIGHT'EM, visant à intégrer la communication optique dans les systèmes IoT (essentiels dans le domaine spatial, l'industrie 4.0, et les futures villes intelligentes). Elle doit continuer à soutenir ses efforts de développement d'un écosystème européen du Li-Fi.

Le développement du projet de résolveur DNS souverain pour l'Europe (*DNS4EU*), prévu dans la stratégie de cybersécurité de l'UE pour la décennie numérique[458,459], témoigne d'une réelle volonté politique commune d'agir. Un appel à propositions à été lancé le 12 janvier 2022.

Mais la perspective de voir l'UE développer un *'Internet européen'* a fait long feu, car cela supposerait une escalade incontrôlable des tensions entre grandes puissances dans le domaine

---

[456] *Euclidia, l'alliance cloud 100 % européenne qui veut détrôner Gaia-X* : https://siecledigital.fr/2021/07/12/euclidia-alliance-cloud-europeenne/?__FB_PRIVATE_TRACKING__=%7B%22loggedout_browser_id%22%3A%22f6eee4987680fdf5e43eed2f2c339425fd226260%22%7D&fbclid=IwAR1QYbHQ0TWBb-0WcclvK0jAZ39wwC3zIfX5hCaF8wAAvim9MUgHE51shJk

183

[457] Le Li-Fi est actuellement considéré comme le réseau le moins aisé à brouiller et pirater. Contrairement aux ondes radio, la lumière a en effet cet avantage de résister aux interférences et de ne pas traverser les murs. La sécurité et la discrétion qu'offre le Li-Fi sont des caractéristiques auxquelles les entreprises à haute valeur stratégique, et plus particulièrement le secteur de la défense, prêtent un intérêt majeur. L'armée américaine est ainsi la première à sauter le pas en avril 2021, en investissant 4,2 millions de dollars pour équiper ses postes de commandement de cette technologie. D'autres armées se montrent également intéressées, et suivront sans aucun doute dans cette voie.
Coupler internet à un éclairage LED - peu énergivore - permettrait de réduire significativement la facture des utilisateurs (entre 15% et 60% selon EDF Entreprises). Il s'agit d'un critère mis en avant notamment pour des activités aérospatiales, où la réduction de la consommation énergétique est un enjeu majeur pour l'ensemble de la filière. Installer du Li-Fi à bord de plateformes aériennes permet par exemple de limiter l'emport de câbles, donc d'alléger celles-ci et de réduire leur consommation de carburant in fine.
Dans l'aéronautique civile, cette technologie offre une connexion internet de haute qualité aux passagers. Du côté du spatial, la lumière est également envisagée pour effectuer des communications inter et intra-satellitaires – voire satellite-Terre par émission de laser optiques, comme le propose la société française Cailabs. Concernant la Défense, les perspectives d'application sont multiples : assurer une bonne connectivité à bord d'avions, de frégates ou de postes de commandement avancés, établir des communications sécurisées de bâtiment à bâtiment (terrestre, marin ou sous-marin), gérer un convoi de véhicules autonomes, géolocaliser du personnel, améliorer la maintenance des appareils navigants… ne sont que quelques exemples parmi tant d'autres. La quantité d'applications possibles dans ces secteurs équivaut à celle des solutions à proposer, ce qui est un signe encourageant l'essor du marché du LiFi dans ces secteurs.
Dans un rapport publié en février dernier, la société *Emergen Research* estimait le marché mondial du Li-Fi à hauteur de 6,9 milliards de dollars en 2028 – dont 9% dédié au secteur aérospatial et défense-, contre 214 millions actuellement. Un marché non négligeable donc, mais qui reste encore en phase de structuration. A ce jour, on recense un peu moins d'une quarantaine de producteurs de Li-Fi, dont plus de la moitié sont européens – les Français n'étant pas en reste avec des sociétés comme Oledcomm, Lucibel, Lifineo.
(Source : https://www.forbes.fr/technologie/souverainete-numerique-le-li-fi-une-technologie-strategique-pour-leurope-de-laeronautique-du-spatial-et-de-la-defense)

[458] *The EU's Cybersecurity Strategy for the Digital Decade :* https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[459] « *DNS4EU offrira un service européen alternatif pour accéder à l'Internet mondial. DNS4EU sera transparent, conforme aux normes et règles les plus récentes en matière de sécurité, de protection des données et de respect de la vie privée dès la conception et par défaut* », était-il annoncé alors. Celui-ci s'adressera au public, aux administrations et aux entreprises.

« cyber », alors que des discussions ont lieu, notamment entre les USA, la Chine, la Russie, la France, le Japon et le Royaume-Uni, pour éviter justement de franchir certains seuils de conflictualité. La tentative russe a permis de clarifier les choses.

Dans le texte de compromis de la présidence du Conseil évoqué *supra,* les pays de l'UE réaffirment leur compétence exclusive en matière de sécurité nationale[460], et insistent sur le fait que les systèmes d'IA développés exclusivement à des fins militaires devraient être retirés du champ d'application du règlement. Les systèmes d'IA développés dans le seul but de la recherche scientifique et du développement ont également été exclus du champ d'application.

Cette position des Etats à l'égard de leur compétence 'exclusive' en matière de sécurité nationale et leur insistance sur le fait que les systèmes d'IA développés exclusivement à des fins militaires devraient être retirés du champ d'application du règlement est totalement incohérente avec celles qu'ils ont adoptées, en permettant de voir figurer dans la partie des Traités de l'UE ayant trait à l'espace européen de justice, de liberté et de sécurité des dispositions ayant trait à la sécurité nationale sans en avoir défini le champ d'intervention, en créant un fonds de recherche pour la défense au sein de l'UE ; et surtout en donnant leur feu vert à la création d'un Conseil technologique transatlantique qui aura bien évidemment dans ses objectifs de traiter de numérique et d'IA ayant des impacts directs ou indirects en matière de sécurité nationale comme de dépendance stratégique, et en autorisant l'UE à contracter un accord de coopération avec les Etats-Unis pour le Commerce et la Technologie dans les domaines de la Défense et de la Sécurité qui inclut de nombreuses dimensions ayant trait au numérique et à l'IA[461] .

Nous relèverons que ce nouvel accord de coopération transatlantique intervient au moment où *l*a montée en puissance technologique de la Chine inquiète les militaires américains, et où le département de la Défense américain vient d'annoncer une réorganisation de ses agences chargées de l'IA et de la data[462].

Début décembre 2021, Eric Schmidt, ancien PDG de Google, et Graham Allison, professeur en sciences politiques à Harvard University, enfonçaient le clou dans le « *Wall Street Journal » : « La Chine va bientôt dépasser les Etats-Unis sur le plan de la technologie. »*

« Le Pentagone a besoin d'une nouvelle stratégie d'IA pour rattraper la Chine », alertait fin novembre l'ancien directeur des logiciels de l'armée, Nicolas Chaillan, dans une tribune publiée par le *« Financial Times »*.

Alors que le Centre Commun de recherche de la Commission européenne constate le recul de l'Europe technologique au cours de la période de crise pandémique après avoir identifié les dépendances stratégiques les plus critiques dans des secteurs clés[463] auxquelles l'UE tente de

[460] Cette position des Etats membres procède d'une lecture restrictive des dispositions des traités qui traitent de la sécurité nationale (articles 4 TUE et 73 TFUE) ; il semble qu'une autre interprétation soit possible : http://regards-citoyens.over-blog.com/article-de-la-securite-nationale-dans-le-traite-de-lisbonne-deuxieme-partie-nouvelle-edition-82372181.html

[461] *U.S.-EU Trade and Technology Council Inaugural Joint Statement :* https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/

[462] La première puissance militaire mondiale aura bientôt un *« Chief Digital and Artificial Intelligence Officer » (CDAO).* Le 8 décembre dernier, Kathleen Hicks, la secrétaire adjointe à la Défense de Joe Biden, a annoncé la création de ce poste, qui va de pair avec une refonte en profondeur de tous les services du Pentagone s'occupant des technologies numériques. A partir du 1er février, le CDAO, qui reportera directement au secrétaire à la Défense, *« sera responsable pour renforcer et intégrer la data, l'intelligence artificielle et les solutions numériques »*. Il succédera au *Joint Artificial Intelligence Center*, créé en 2018 par l'administration Trump, et chapeautera deux autres services du Pentagone, chargés des données et du développement de logiciels.

[463] *In-depth reviews of strategic areas for Europe's interests :* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_fr

Ce rapport recense 137 produits dans des écosystèmes sensibles pour lesquels l'UE est fortement dépendante de sources étrangères.

proposer une réponse pertinente au travers de sa stratégie industrielle pour l'Europe[464], que peut-on réellement attendre de cette nouvelle coopération transatlantique qui ne viendrait pas perturber les tentatives d'autonomisation stratégique de l'UE, dès lors que la déclaration commune publiée dès son lancement précise :

« The United States and the European Union intend to enhance their cooperation in the following areas:

- *Technical consultations on current and upcoming legislative and regulatory developments to promote the global convergence of controls and ensure legal security for U.S. and EU companies, including regular adjustments to control lists and specific license exceptions/General Export Authorizations, development of guidelines, as well as relevant regulatory developments in third countries;*
- *Technical consultations and development of convergent control approaches on sensitive dual-use technologies, as appropriate;*
- *Information exchange on risks associated with : the export of sensitive technologies to destinations and entities of concern, exchange of good practice on the implementation and licensing for listed or non-listed sensitive items ; technology transfers and dual-use research of concern and exchange of best practices to support the effective application of controls while facilitating research collaboration between U.S. and EU research organizations;*
- *Technical consultations on compliance and enforcement approaches (i.e. legal and regulatory basis, institutional and administrative arrangements) and actions;*
- *Capacity building assistance to third countries to develop appropriate capabilities to implement guidelines and lists of multilateral export control regimes, appropriate export control policies and practices, as well as relevant enforcement measures; and,*
- *Technical consultations regarding multilateral and international cooperation, including prior to the introduction of controls outside the multilateral regimes, as appropriate. » ?*

- *Associer davantage la société civile aux avancées européennes sur les registres numériques et de l'IA*

- *Mieux prendre en compte les résolutions du Parlement européen*

Le Parlement européen est particulièrement actif dans les domaines de la démocratie, des droits fondamentaux et de l'Etat de droit. Ses membres, sur la base des travaux de la commission des libertés civiles, de la justice et des affaires intérieures, débattent et adoptent des résolutions lors des sessions plénières du Parlement européen sur la situation des droits fondamentaux dans l'Union ainsi que sur des problèmes spécifiques concernant la sauvegarde de ces droits dans les États membres[465].

---

[464] *Cf. L'Europe traîne des pieds dans la course à la technologie :* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_fr

185

Les investissements en R & D des entreprises européennes ont globalement chuté de 2,2 % en 2020 pendant la crise de la Covid-19, alors que partout ailleurs dans le monde elles sont en hausse ou stagnent, rapporte la Commission européenne dans un document publié pour l'année écoulée, qui analyse les dépenses des 2 500 premiers investisseurs au niveau mondial.

Une baisse remarquée pour la première fois depuis 10 ans, due principalement aux difficultés dans les secteurs de l'automobile, de l'aérospatial et de la défense, alors que les secteurs de la santé et des TIC ont continué à croître, démontre le rapport. Le secteur automobile, notamment, qui représente près d'un tiers de la R & D en Europe, a diminué de 7,2 % en 2020, marqué par les pénuries dans la chaîne de production.

Ces chiffres placent l'Europe loin derrière les Etats-Unis et la Chine en termes de capacité de recherche et de développement dans des secteurs clés de l'économie. Aux Etats-Unis comme en Chine, les investissements ont augmenté quant à eux respectivement de 9,1 % et de 18,1 % l'an passé.

[465] *Cf.* https://www.europarl.europa.eu/committees/fr/fundamental-rights/product-details/20160229CDT00541

Dans une résolution adoptée le 21 janvier 2021[466], le Parlement européen démontre également sa capacité à affronter les grands défis posés à nos sociétés et Etats par l'intelligence artificielle.

En particulier, en matière de droit international privé, le Parlement européen *« note que, un nombre croissant de litiges relevant du droit international privé étant engendré par l'internationalisation des activités humaines, en ligne ou dans le monde réel, l'IA peut aider à les résoudre en créant des modèles permettant de repérer la juridiction compétente et le droit applicable pour chaque affaire, mais aussi d'identifier les conflits de lois les plus délicats et de proposer des solutions pour les régler (Point 88). Il estime que les utilisations de l'IA en droit international privé doivent faire l'objet d'une information appropriée du public et éviter les discriminations par des biais de programmation, qui aboutiraient à favoriser systématiquement un droit national plutôt qu'un autre, et qu'elles doivent également respecter le droit conféré au juge par la loi, le droit de faire appel selon le droit applicable et le droit de tout juge de rejeter la solution suggérée par l'AI (Point 89). […] Il relève qu'au regard de l'importance croissante de la recherche et du développement dans le secteur privé et des investissements considérables de pays tiers, l'Europe est confrontée à une forte concurrence; soutient, par conséquent, les efforts déployés par l'Union pour continuer à développer ses avantages concurrentiels et estime que, dans un monde hyperconnecté, l'Union devrait s'efforcer de définir des normes pour l'IA en adoptant une stratégie efficace à l'égard de ses partenaires extérieurs et en renforçant son action pour fixer des normes éthiques pour l'IA à l'échelle mondiale dans le respect des règles de sécurité et des exigences de protection des consommateurs et conformément aux valeurs de l'Union et aux droits des citoyens, dont les droits fondamentaux; estime que cela est également essentiel pour la compétitivité et le caractère durable des entreprises européennes; invite la Commission et les États membres à renforcer leur coopération et le dialogue avec les pays tiers et les organisations internationales telles que les Nations unies, l'OCDE, le G7 et le G20 afin de relever les défis découlant de l'évolution rapide de cette technologie; estime que ces efforts doivent notamment viser à établir des normes communes et à améliorer l'interopérabilité des systèmes reposant sur l'IA; invite la Commission à favoriser le dialogue, une coopération plus étroite et des synergies entre les États membres, les chercheurs, les universitaires, les acteurs de la société civile, le secteur privé, en particulier les entreprises de premier plan, et les forces militaires, pour garantir le caractère inclusif des processus d'élaboration des règles relatives à l'IA appliquée à la défense. (Point 91) »*

Dans un chapitre intitulé « Principes directeurs », cette même résolution précise sa position à l'égard du droit. *« Le Parlement européen estime que les technologies et les systèmes de réseaux d'IA devraient viser à assurer la sécurité juridique des citoyens ; souligne par conséquent que les règles relatives aux conflits de lois et aux conflits de compétences devraient continuer à s'appliquer compte tenu de l'intérêt des citoyens ainsi que de la nécessité de réduire le risque de recherche de la juridiction la plus indulgente; rappelle que l'IA ne saurait remplacer l'être humain dans le processus judiciaire lorsqu'il est question de rendre des jugements ou de prendre une quelconque décision définitive étant donné que ces décisions doivent toujours être prises par un être humain et être strictement soumises à une vérification humaine et à une procédure régulière; souligne que, lors du recours à des éléments de preuve émanant de technologies faisant appel à l'IA, les autorités judiciaires devraient avoir l'obligation de motiver leurs décisions (Point 92) ; il rappelle que l'IA est un progrès scientifique qui ne doit pas entraîner de régression du droit, mais qu'elle doit au contraire toujours être encadrée par celui-ci — dans l'Union européenne par le droit émanant de ses institutions et de ses États*

[466] Résolution du Parlement européen du 20 janvier 2021 intitulée « *Intelligence artificielle: questions relatives à l'interprétation et à l'application du droit international dans la mesure où l'Union est concernée dans les domaines des utilisations civiles et militaires et à l'autorité de l'État en dehors du champ d'application de la justice pénale* » (2020/2013(INI)) : https://www.europarl.europa.eu/doceo/document/TA-9-2021-01-20_FR.html

membres — et qu'en aucun cas l'IA, la robotique et les technologies connexes ne peuvent enfreindre les droits fondamentaux, la démocratie et l'Etat de droit (Point 93). »

Mais on peut déplorer que rien n'y figure s'agissant de la nécessité d'instaurer un régime de droit propre aux robots[467], ni même des recommandations à l'égard de la protection de l'humain face au robot[468], ou encore d'autres à l'égard du développement et de l'usage des systèmes d'armes létales autonomes (SALA) alors même que les enjeux éthiques et juridiques considérables qu'ils soulèvent font l'objet de discussions internationales.[469,470]

Pour le Comité international de La Croix-Rouge, le ciblage d'êtres humains avec des robots autonomes doit être exclu. L'institution juge leur comportement trop imprévisible et pointe la question de la responsabilité des actes de la machine. Des discussions sont en cours à Genève entre les pays membres de la Conférence pour le désarmement afin de s'accorder sur la définition des Sala. Une position commune doit être adoptée sur le sujet.

En 2009, l'UE a adopté un règlement sur les échanges de biens et technologies à double usage (civil et militaire) basé sur les lignes directrices de l'arrangement de Wassenar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage ; un arrangement international qui ne réunit que 42 pays – dont les Etats-Unis, la Russie, le Royaume-Uni ou la France, mais pas Israël, par exemple.

Si les Etats doivent contrôler leurs exportations et en faire rapport, ce cadre ne pose aucune interdiction. Ce système devait être adapté à l'évolution de l'environnement technologique, économique et politique.

Un nouveau règlement adopté au printemps 2021 par les institutions compétentes de l'UE vient renforcer les exigences de conformité pour les exportateurs et les obligations de contrôle au regard des risques pour les droits humains.[471]

---

[467] La singularité du robot dans l'espace juridique a vocation à s'accentuer ; symétriquement, tandis que la pertinence de la qualification de bien meuble décroît, la nécessité de doter le robot intelligent d'un statut juridique inédit se fait plus pressante. Ce mouvement en vase communiquant a ceci de particulier qu'il semble à la fois unilatéral et irréversible : la puissance de l'industrie robotique, l'implication des plus grands acteurs de l'économie numérique, l'importance des enjeux financiers, l'engouement de la recherche et l'appétence sociale constituent, ensemble, une assise particulièrement solide à l'avènement de la robotique intelligente. Une fois la rupture technologique consommée – résultant de la liberté dont disposera le robot, elle-même alimentée par ses capacités d'apprentissage –, le droit n'aura d'autre choix que de s'aligner.
L'ouvrage « Droit des robots » coécrit par Alain Bensoussan et Jérémy Bensoussan apporte de premières orientations juridiques. https://www.alain-bensoussan.com/droit-des-robots/
Voir également : *Droit des robots : quelle est l'autonomie de décision ?*
https://www.dailymotion.com/video/x5j5g1o

187

[468] Voir par exemple à cet égard Nathalie Nevejans *in Comment protéger l'être humain face aux robots ?*
https://www.dailymotion.com/video/x5j5god

[469] *Cf.* notamment à ce sujet le rapport d'information établi par les députés Claude de Ganay et Fabien Gouttefarde en conclusion des travaux d'une mission d'information *sur les* systèmes d'armes létaux autonomes :
https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b3248_rapport-information
Cf. également Christine Dugoin-Clément *in Armes autonomes et soldats augmentés : quel impact sur les valeurs des armées ?*
https://theconversation.com/armes-autonomes-et-soldats-augmentes-quel-impact-sur-les-valeurs-des-armees-168295

[470] La France surveille de près les Sala. Dès 2018, Florence Parly, ministre des Armées, a exclu l'utilisation de « robots tueurs » et assuré que le pays respecterait le droit international. Si les robots autonomes sont rejetés, ceux qui agiraient en autonomie, mais sous les ordres d'un officier, retiennent l'attention des militaires. En 2021, une unité dénommée Vulcain a été créée pour tester les différents robots que pourrait utiliser l'armée à partir de 2025. Parmi les projets en cours de réflexion, des drones autonomes capables de surveiller une zone seuls et de faire des comptes rendus. Au Mali, de petits drones pilotés par des soldats permettent déjà de surveiller les abords des bivouacs.

[471] *Règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte)*
https://data.consilium.europa.eu/doc/document/PE-54-2020-INIT/fr/pdf
Les principaux éléments du règlement sur lequel l'accord est intervenu sont les suivants :

- afin de prévenir les violations des droits de l'homme et les menaces pour la sécurité liées à l'éventuelle utilisation abusive des technologies de cybersurveillance, les nouvelles règles prévoient des dispositions qui soumettent ces technologies à des contrôles à l'exportation plus stricts dans certaines circonstances

« Ce sont des instruments utiles mais clairement insuffisants. On voit bien que les Etats continuent d'approuver des licences pour des technologies de surveillance, malgré les preuves d'abus » (Katia Roux, chargé de plaidoyer 'libertés' chez *Amnesty International*, cette association plaidant pour un renforcement drastique des contrôles, et une interdiction pure et simple de vendre de tels outils lorsqu'il existe un risque substantiel qu'ils soient utilisés pour porter atteinte aux droits humains).

Dans une résolution intitulée *'L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales'* et adoptée le 6 octobre 2021[472], le Parlement européen constate que le recours de plus en plus fréquent à l'IA ne tient pas toujours ses promesses, par exemple sur la réduction de certains types de criminalité et une prise de décision plus objective. D'autant que les outils utilisant l'IA peuvent présenter des degrés très divers de fiabilité et ne respectent pas la jurisprudence de l'UE en matière de protection des données. De plus, le déploiement systématique d'algorithmes, même avec un faible taux de faux positifs, peut entraîner bien plus de fausses alertes que de vraies alertes selon les parlementaires européens.

Les eurodéputés se montrent également critiques à l'égard de la police prédictive. *« Si elle permet d'analyser des séries de données en vue de l'identification de modèles et corrélations, elle ne peut répondre à la question de la causalité et prédire de manière fiable le comportement des personnes, et ne peut donc pas constituer à elle seule une base d'intervention. »*

Autre danger, des biais inhérents aux données collectées ont tendance à se renforcer progressivement et ainsi à perpétuer et amplifier les discriminations existantes, en particulier pour les personnes appartenant à certains groupes ethniques (personnes racisées, personnes âgées, LGBTI, femmes…).

Dernier grand risque pointé par les élus européens, une trop grande confiance dans la nature en apparence objective et scientifique des outils d'IA pousserait les forces de l'ordre et la justice à ne pas envisager la possibilité que leurs résultats soient incorrects, incomplets, dépourvus de pertinence ou discriminatoires.

Les eurodéputés demandent donc *« que toute utilisation de l'IA incompatible avec les droits fondamentaux soit interdite »*. Respect à la vie privée, non-discrimination et contrôle par la justice de la proportionnalité des moyens utilisés par la police sont ainsi mis en avant comme outils de prévention d'éventuels abus. *« Les décisions finales doivent toujours être prises par*

- en outre, le règlement comprend désormais un mécanisme de coordination au niveau de l'UE qui permet un plus grand échange entre les États membres en ce qui concerne l'exportation de biens de cybersurveillance
- le règlement introduit deux nouvelles autorisations générales d'exportation de l'UE pour l'exportation de biens à double usage (l'une pour les biens cryptographiques et l'autre pour les transferts intragroupes de technologies dans certaines circonstances), réduisant ainsi considérablement la charge administrative tant des entreprises que des autorités chargées de délivrer les licences
- le règlement renforce également l'application des contrôles grâce à une meilleure coopération entre les autorités douanières et celles qui octroient les licences, et introduit des mécanismes permettant aux États membres de renforcer leur coopération dans ce domaine
- le règlement comporte une nouvelle disposition relative aux "contrôles transmissibles" qui autorise, dans certains cas, un État membre à introduire des contrôles à l'exportation sur la base de la législation établie par un autre État membre, permettant ainsi aux contrôles à l'exportation effectués par les États membres d'avoir une dimension transfrontière
- le règlement harmonise au niveau de l'UE les règles applicables à certains services en ce qui concerne les biens à double usage actuellement réglementés au niveau national (assistance technique)
- de nouvelles dispositions en matière d'établissement de rapports permettront d'accroître la transparence du commerce des biens à double usage tout en respectant la confidentialité des secrets d'entreprise et des intérêts nationaux en matière de sécurité.

188

[472] Résolution du Parlement européen du 6 octobre 2021 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales (2020/2016(INI)) : https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_FR.pdf

un être humain et les personnes soumises à des systèmes alimentés par l'IA doivent disposer de voies de recours ».

Le Parlement européen demande qu'une étude d'impact obligatoire sur les droits fondamentaux soit réalisée avant la mise en œuvre ou le déploiement de tout système d'IA à des fins répressives ou judiciaires.

Les eurodéputés demandent également une interdiction de toute notation à grande échelle des individus au moyen de l'IA. Le Parlement européen estime ainsi que *« toute forme de notation normative des citoyens à grande échelle par les autorités publiques, en particulier dans les domaines répressif et judiciaire, entraîne une perte d'autonomie, menace le principe de non-discrimination et ne peut être considérée comme conforme aux droits fondamentaux, en particulier à la dignité humaine. ».*

Pour respecter la vie privée et la dignité humaine, les députés demandent une interdiction permanente de la reconnaissance automatisée des individus dans les espaces publics, faisant remarquer que les citoyens ne devraient être surveillés que lorsqu'ils sont soupçonnés d'un crime.

Le Parlement européen demande également d'interdire l'utilisation de bases de données privées de reconnaissance faciale[473] (comme le système *Clearview AI*, qui est déjà utilisé) et la police prédictive basée sur des données comportementales. Le Parlement tente également de bannir l'utilisation des données biométriques pour l'identification à distance. Notamment lors de contrôles frontaliers. Même chose pour le projet *iBorderCtrl* (*« un système intelligent de détection de mensonges »*).

- *Adapter le cadre commun des agences de régulation de l'UE pour mieux prendre en compte les spécificités du numérique et de l'IA*

L'Agence des droits fondamentaux de l'UE aide les institutions et les États membres de l'UE à comprendre les enjeux de la sauvegarde des droits fondamentaux de chaque citoyen dans l'UE et à résoudre les difficultés dans ce domaine.[474]

Par ailleurs, l'UE dispose de plusieurs agences de régulation.[475]

Ces agences sont régies selon les dispositions d'un cadre commun.

Dans le domaine des systèmes d'information, elle dispose de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)[476]

Comme le relève Laurent Dechatre : *« Devant le développement parfois anarchique des agences européennes et les problèmes qui en découlaient, le Parlement européen, la Commission et le Conseil ont adopté en 2012 une déclaration comprenant notamment des lignes directrices en matière d'organisation, de gestion financière, et d'évaluation. Si ce cadre commun a permis de corriger certains des problèmes antérieurs, l'application de ses recommandations est inégale, pour une bonne part en raison de contraintes politiques, elles-mêmes plus ou moins justifiées selon les cas. De plus, alors que les objectifs de rationalisation et d'équilibre des intérêts au sein de la structure organisationnelle des agences y ont une place centrale, le cadre commun comporte un certain nombre de lacunes concernant les*

[473] NB : Il faut rappeler qu'il n'y a pas de réelles bases de données européennes communes, ce qui oblige les sociétés européennes à recourir fréquemment à des bases de données provenant des États-Unis ou de la Chine.
[474] *Cf.* https://epso.europa.eu/job-opportunities/institutions-and-agencies/2232-fra-european-union-agency-fundamental-rights_fr
[475] *Cf.* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles_fr
[476] *Cf.* https://eulisa.europa.eu/

recommandations de principes tels que l'inclusion d'une chambre de recours dans les cas où l'agence peut adopter des décisions contraignantes. Enfin, une dernière limite de la déclaration concerne son périmètre et l'absence de différenciation relativement à l'applicabilité de ses lignes directrices. »[477]

De telles lacunes sont incompatibles avec les exigences démocratiques attachées à la nécessité d'une régulation appropriée - conforme avec les impératifs de l'Etat de droit – du numérique et de l'IA au sein de l'espace européen.

En particulier, l'UE doit envisager la création d'une chambre de recours dans les cas où les agences existantes ou à naître dans ces domaines viendraient à adopter des décisions contraignantes.

- *Tirer le meilleur parti des exercices de démocratie participative engagés au sein de l'Union européenne*

Les révolutions technologiques ne sont pas qu'une question de technologie.

Ce constat est notamment celui de Marianna Epicoco, Maitre de conférences en sciences économiques à l'Université de Lorraine, qui conclut un article éponyme par ces termes : *« Un débat politique sérieux et inclusif nous semble alors nécessaire afin de discuter quelles sont les trajectoires de changement technologique et sociale à prioriser et quelles sont les directions à négliger ou à reporter, de manière à concentrer les investissements dans des directions de changement partagées et capables de tracer une phase de développement économique plus équitable. »*[478]

Annie Blandin-Obernesser, Professeur de droit à l'IMT Atlantique – Institut Mines-Télécom souligne : *« Les enjeux de souveraineté numérique se manifestent dans toutes les activités humaines. Une des grandes prises de conscience initiale, en 2005, concerne la culture avec le constat fait par Jean-Noël Jeanneney d'un Google qui défie l'Europe en numérisant son patrimoine culturel lorsqu'il crée Google Books. La période récente renoue avec cette vision et l'enjeu culturel et démocratique s'affirme comme essentiel, à l'heure de la désinformation en ligne et son cortège d'effets pervers, notamment sur les élections. Cela implique de placer le citoyen au cœur du dispositif et de démocratiser le monde numérique en affranchissant l'individu de la tutelle des géants du net dont l'emprise ne se limite pas à l'économie et au régalien. C'est sur le système cognitif, sur l'attention et la liberté que la toile des grandes plates-formes se tisse. La souveraineté, celle du peuple, rimerait donc ici avec résistance. »*[479]

La Convention sur l'avenir de l'Europe destinée à engager une nouvelle série de réformes politiques et institutionnelles de l'Union a constitué en 2021 une fenêtre d'opportunité exceptionnelle qui doit être saisie. [480]

Au cœur de ce dispositif, une plateforme numérique citoyenne visant à associer les citoyens européens aux décisions qui seront prises au terme de la démarche. Pensée pour créer un débat ouvert et transparent à l'échelle des 27 États membres, elle avait comme objectif d'inclure le

[477] *Cf. Le cadre commun pour les agences de régulation de l'UE :* https://www.academia.edu/38523540/Le_cadre_commun_pour_les_agences_de_r%C3%A9gulation_de_l_UE_pdf?email_work_card=abstract-read-more

[478] *Les révolutions technologiques ne sont pas qu'une question de technologie :* https://theconversation.com/les-revolutions-technologiques-ne-sont-pas-quune-question-de-technologie-172785

[479] *Souveraineté et numérique : maîtriser notre destin :* https://theconversation.com/souverainete-et-numerique-maitriser-notre-destin-171014

[480] La Conférence sur l'avenir de l'Europe, grand exercice de démocratie participative, ambitionne de dessiner les contours de ce que sera l'Union européenne pour les prochaines décennies. Repoussée en raison de la pandémie, elle est finalement lancée ce 9 mai 2021, à l'occasion de la fête de l'Europe, à Strasbourg, siège du Parlement européen.
Cf. https://ec.europa.eu/info/sites/default/files/fr_-_declaration_commune_sur_la_conference_sur_l.pdf

plus grand nombre dans un processus participatif. Le site, en ligne depuis le 19 mars 2021, a permis aux Européens d'exprimer leurs craintes, de partager leurs rêves et leurs attentes, d'engager le dialogue avec leurs représentants.

Parmi les grands thèmes privilégiés figurent notamment : les valeurs et les droits[481] ; l'Etat de droit, la sécurité ; la transformation numérique ; la démocratie européenne[482]. Un champ « Autres idées » a permis de recueillir les avis et idées transversales et de compléter les autres thèmes car chacun est libre de soulever toute question importante à ses yeux.

Les propositions ont été mises en ligne sur la plateforme et ont formé le point de départ des discussions de panels de citoyens et des séances plénières.

Il est intéressant de relever que, parmi les recommandations formulées par le Panel de citoyens dédiés à ces questions[483], figurent notamment les préconisations suivantes :

7. « Nous recommandons que les entités qui traitent des données à caractère personnel soient agréées au niveau de l'Union. Ces entités devront également être soumises à un audit annuel externe et indépendant sur la protection des données. Ces entités seront sanctionnées pour les violations de la protection des données proportionnellement à leur chiffre d'affaires annuel, d'une manière plus stricte que dans le cadre du règlement actuel. L'agrément devrait être retiré après deux violations consécutives, et immédiatement après une violation grave. »

8. « Nous recommandons de renforcer les compétences de l'Union dans les domaines suivants : 1) l'éducation à la protection des données, 2) la sensibilisation à la protection des données et 3) la protection des données à caractère personnel des mineurs. Nous recommandons de préciser et de renforcer les règles concernant le traitement des données des mineurs dans le RGPD, y compris les règles relatives au consentement, la vérification de l'âge et le contrôle par les tuteurs légaux. Nous recommandons également d'introduire dans le RGPD une catégorie spéciale pour les données sensibles des mineurs (par exemple, le casier judiciaire, les informations relatives à la santé, la nudité) afin que les mineurs soient protégés contre toute forme d'abus et de discrimination. »

9. « Nous recommandons de mettre en place des politiques de confidentialité normalisées et des formulaires de consentement faciles à comprendre, concis et intuitifs, qui indiquent clairement quel traitement de données est strictement nécessaire et ce qui est facultatif. Nous recommandons que le retrait du consentement soit facile, rapide et permanent. Nous recommandons d'interdire aux entités de limiter leurs services plus que nécessaire si le consentement n'a pas été donné à un traitement facultatif de données. »

10. « Nous recommandons que le règlement relatif à la conditionnalité (2020/2092, adopté le 16 décembre 2020) soit modifié de manière à ce qu'il s'applique à toutes les violations de l'état de droit plutôt qu'aux seules violations ayant une incidence sur le budget de l'Union. »

11. « Nous recommandons que l'Union organise des conférences annuelles sur l'état de droit après la publication du rapport annuel sur l'état de droit (le mécanisme de la Commission permettant de contrôler le respect de l'état de droit par les États membres). Les États membres

[481] *Cf.* https://futureu.europa.eu/processes/ValuesRights
[482] *Cf.* https://futureu.europa.eu/processes/Democracy
[483] *Cf. Panel de citoyens européens 2: «Démocratie européenne; valeurs et droits, état de droit, sécurité» Recommandations :* https://prod-cofe-platform.s3.eu-central-1.amazonaws.com/z6eyhqgf0q3bo8k8inem55xso51z?response-content-disposition=inline%3B%20filename%3D%22Panel%202%20recommendations%20FINAL_FR.pdf%22%3B%20filename%2A%3DUTF-8%27%27Panel%25202%2520recommendations%2520FINAL_FR.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA3LJJXGZPDFYVOW5V%2F20211230%2Feu-central-1%2Fs3%2Faws4_request&X-Amz-Date=20211230T104637Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=f9d8fd5ed81d066d9cf71b87936e16a81e87c07a877bdd1a4e96a5c47a045dc2

191

devraient être obligés d'envoyer à la conférence des délégations nationales diverses sur le plan social, comprenant à la fois des citoyens et des fonctionnaires. »

12. « Nous recommandons que l'Union applique plus rigoureusement ses règles de concurrence dans le secteur des médias afin d'assurer la protection du pluralisme des médias dans tous les États membres. L'Union devrait empêcher les grands monopoles médiatiques et les nominations politiques au sein des conseils d'administration des médias. Nous recommandons également que le futur acte législatif de l'Union sur la liberté des médias comprenne des règles visant à empêcher les responsables politiques de posséder des médias ou d'avoir une forte influence sur leur contenu. »

13. « Nous recommandons aux institutions de l'Union de jouer un rôle plus important avec tous les outils à leur disposition, y compris les centres nationaux de cybersécurité et l'Agence de l'Union européenne pour la cybersécurité (ENISA), afin de protéger les citoyens, les organisations et les institutions contre les nouvelles menaces provenant des violations de la cybersécurité et de l'utilisation de l'intelligence artificielle à des fins criminelles. Nous recommandons en outre que les directives émanant de l'Europe et de ses agences soient correctement mises en œuvre et diffusées dans tous les États membres. »

Les conclusions, qui ont vocation à traduire les principales propositions et questions des Européens, devraient être connues au printemps 2022, alors que la France assurera la présidence tournante du Conseil de l'Union européenne (janvier-juin 2022)**.**

Les préoccupations comme les pistes de progrès présentées dans la présente analyse revêtant une nature transversale par rapport à plusieurs thématiques identifiées ci-dessus devraient être prises en considération dans le corpus d'analyse et de propositions de chacune d'elles.

Le processus de réforme de l'Etat en France doit faire l'objet de profondes remises en cause

La quatrième révolution industrielle à l'œuvre introduit quelque chose de nouveau dans la tension entre vie et politique, en produisant une intensité nouvelle et critique des tensions entre vie et justice.

Cela vaut en particulier pour la France.

« Oui, il y a quelque chose de nouveau, et c'est bien le problème principal du moment. Mais ce problème n'est pas nouveau dans sa nature. La tension entre vie et justice n'est, comme telle, pas nouvelle. C'est au contraire le problème principal de la politique, celui qui, en réalité, la définit. Ne croyez pas ceux qui vous disent le contraire. Cela ne veut pas dire que ce problème soit réglé – au contraire, puisqu'il est plus profond qu'on ne le croit – mais cela veut dire que sa nouveauté est ailleurs, et que, si des solutions existaient déjà, il faudrait les renouveler en profondeur. Mais si ce n'est pas dans la nature du problème, où est la nouveauté du présent ? C'est simple : dans une intensité nouvelle et critique des tensions entre vie et justice. Et si des solutions, même précaires et à renouveler en profondeur, existaient déjà, quelles sont-elles ? Ce sont, selon nous, celles de la démocratie, et même de la « social-démocratie ». Mais il faut les renouveler, à travers ce que l'on appellera ici la vital-démocratie. »[484] (Frédéric Worms, philosophe)

En prenant acte que la France est une République, ce qui emporte des exigences supplémentaires qui vont bien au-delà des enjeux de droit.

« Une démocratie peut fonctionner selon la lettre, sans une relative indifférence, en se confiant à la froide objectivité de textes juridiques. 50 % d'abstentions aux élections privent une république de substance, mais n'entament pas une démocratie. Le gouvernement des juges n'est pas républicain. Pas seulement parce qu'il dépossède le peuple législateur de sa souveraineté, il dispense chaque citoyen de vouloir, en son âme et conscience ce que les lois lui dictent. […] Une République se fait d'abord avec des républicains, en esprit. Parce qu'elle est une idée, philosophique, la république est interminable. Elle se poursuit elle-même indéfiniment dans l'histoire, et ce qui la porte en avant est cet infini même, cette insatisfaction de soi. […] Se sachant imparfaite, et toujours trop particulière au regard de la République universelle qu'elle appelle de ses vœux, une république ne sera jamais qu'un exemple. » (Régis Debray)[485]

Lors d'un entretien journalistique réalisé en novembre 2015, le futur président de la République Emmanuel Macron - alors ministre de l'économie - insista sur le fait qu'il avait bien pris acte du rôle de l'Etat devant la révolution numérique, ce dernier devant veiller à la protection des données et des libertés individuelles. Et surtout lutter contre la tendance française à voir le numérique comme une menace.

Or, les conditions de déploiement au sein de la puissance publique française des évolutions technologiques ne sont pas suffisamment encadrées par ce qui apparaît aux citoyens comme la plus efficace des protections de la liberté : le droit, et principalement le droit constitutionnel.

[484] *Les minima de la vital-démocratie : une orientation politique :* https://aoc.media/opinion/2021/09/29/les-minima-de-la-vital-democratie-une-orientation-politique/

[485] *Etes-vous démocrate ou républicain ?* https://www.les-crises.fr/etes-vous-democrate-ou-republicain-par-regis-debray/?fbclid=IwAR2XZNXR62ghsReykhuvHZ8htsGpqKPLPl_ULMD82XgmSRKjuCHnMaNsFRg

Les sujets cruciaux de la souveraineté numérique[486,487] , de la pollution numérique[488] et de la sobriété numérique [489] auxquels le Parlement a consacré plusieurs rapports d'information doivent pouvoir rapidement trouver dans le droit national une concrétisation à la mesure des enjeux, dans le droit fil des mesures inscrites à cet égard par l'Etat allemand dans sa nouvelle loi anti-trust[490], s'agissant de la souveraineté.

L'Etat français s'est saisi des enjeux numériques de manière plus marquée qu'au préalable à l'occasion des Etats généraux des régulations numériques qui se sont tenus en juillet 2018, et dont les grands objectifs consistaient à réfléchir à la cohérence des initiatives existantes et poser les bases d'un cadre global de régulation des « géants du numérique ».

Animés par le Conseil national du numérique, les travaux issus de ces états généraux sont appelés à nourrir une réflexion internationale sur ces enjeux. *« La France porte une vision à la fois performante et humaine [du numérique] que nous devons faire valoir auprès de nos partenaires européens et à l'international », a précisé le secrétaire d'État en charge du numérique en exercice : Mounir Mahjoubi. « Bien sûr, il existe déjà des rapports sur différents sujets, des textes législatifs qui apportent des solutions pour répondre à l'urgence sur certains problèmes »*, a-t-il précisé dans un entretien accordé au quotidien *Le Figaro*. *« Mais nous manquons d'un cadre global pour donner de l'unité à tout cela, pour exprimer une véritable vision à long terme ».*

Les réflexions engagées portent sur quatre axes prioritaires : économique (quelle régulation pour le numérique et ses plateformes ?) ; social (l'économie collaborative et la protection de ses travailleurs) ; sociétal (de la protection des données à la protection des personnes) ; méthode (quels outils juridiques et techniques à disposition des régulateurs ?).

L'Etat français s'est également saisi des enjeux de sobriété numérique en 2020 comme l'illustrent ses initiatives en faveur d'un 'numérique écoresponsable', concept dérivé de celui plus ancien d''innovation responsable'.

« Soucieux de son exemplarité, l'État développe une stratégie volontariste de maîtrise du numérique et de ses effets. Ces engagements de l'État sont notamment formalisés par le dispositif « Services publics écoresponsables » (circulaire du Premier ministre n°6145/SG du 25 février 2020 portant engagements de l'État pour des services publics écoresponsables).

Les administrations, les collectivités territoriales, les agents, tout un écosystème recherche cette cohérence et participe aux côtés d'acteurs privés, coopératives et associations, à la mise en œuvre du numérique responsable sur l'échelle du territoire.

---

[486] *Le devoir de souveraineté numérique : rapport du sénateur Gérard Longuet fait au nom de la commission d'enquête :* http://www.senat.fr/notice-rapport/2019/r19-007-1-notice.html

[487] *Rapport d'information sur le thème « Bâtir une souveraineté numérique nationale et européenne »* présenté par les députés Jean-Luc Warsmann et Philippe Latombe (rapporteur) : https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information.pdf

[488] La notion de pollution numérique intègre :

- la fabrication des objets électroniques ce qui comprend les smartphones, les tablettes mais aussi tout le matériel connecté par exemple dans les maisons ou les voitures ;
- l'utilisation de ressources naturelles comme les minerais, la terre excavée pour l'extraction de ces minerais, l'eau ou encore l'énergie nécessaire à ces opérations.
- le réchauffement climatique ;
- le stockage des données et les centres informatiques ;
- l'infrastructure et les réseaux de téléphonie.

[489] *Rapport d'information de la mission d'information sur l'empreinte environnementale du numérique :* http://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2020/2020-Documents_pdf/20200624_Conf_presse_Dev_Dur/20200624_Conf_Dev_Dur_Synthese_du_rapport.pdf

[490] Voir à cet égard *Taming Big Tech: What Can We Expect From Germany's New Antitrust Tool ?* https://promarket.org/2021/02/07/germany-antitrust-bundeskartellamt-19a-dma-big-tech/

Cette vague porteuse de sens, de valeurs, et d'innovations participe à la cohésion des équipes qui se tournent vers des objectifs communs alliant aspirations professionnelles et citoyennes. Des dispositions réglementaires récentes, notamment la loi relative à la lutte contre le gaspillage et à l'économie circulaire, confortent cela.

En parallèle, est menée une mission interministérielle « Green Tech » co-pilotée par la direction interministérielle du numérique (DINUM) et le Ministère de la Transition numérique. Elle s'inscrit dans la feuille de route gouvernementale « Numérique et Environnement ». Elle associe pour ces différents travaux les ministères et l'écosystème du numérique responsable.

Un effort de prise en compte des décrets est opéré en continu, afin de [..] partager un guide sur l'achat numérique responsable qui soit le plus pragmatique, actuel et opérationnel possible. C'est pourquoi ce guide est développé et construit avec une volonté d'itérations continues et de nouvelles versions seront régulièrement mises à jour. »[491]

Le Parlement a adopté en novembre 2021 une proposition de loi visant à réduire l'empreinte environnementale du numérique, faisant de la France un pays précurseur dans ce domaine. Ce texte consensuel, comprend de nombreuses mesures visant en particulier à soutenir le recyclage et le réemploi des appareils numériques pour réduire leur impact sur l'environnement.

Le 11 janvier 2022, la commission présidée par le sociologue Gérald Bronner a remis son rapport au président de la République.

Riche d'un très grand nombre de recommandations répondant au mandat fixé dans la lettre de mission présidentielle[492], ce rapport propose un éclairage très partiel des défis numériques auxquels la République est confrontée, faisant référence à deux reprises à l'urgence qu'il y aurait à trouver des solutions à la « désinformation » (pp. 15 et 105) et mentionne le temps très contraint qu'il a pu y consacrer (100 jours), allant jusqu'à affirmer avoir « *abandonné immédiatement l'objectif d'exhaustivité* ».

La synthèse de ce rapport dégage les éléments suivants ayant trait plus spécifiquement aux aspects juridiques : « *En matière de droit et numérique (chapitre V), l'étude des dispositions juridiques pouvant potentiellement être utiles pour prévenir ou sanctionner les différentes formes de désinformation (au sens de la diffusion de mauvaise foi de fausses nouvelles) incitent à ne pas modifier ou remplacer l'actuel article 27 de la loi de 1881 sur la liberté de la presse (R16 et R17). En revanche, la sanction pénale pourrait être complétée par un mécanisme de mise en cause de la responsabilité civile des diffuseurs de mauvaise foi de fausses nouvelles pouvant porter préjudice à autrui, responsabilité qui pourrait notamment être proportionnée au niveau de viralité de la diffusion et de la popularité numérique de son auteur (R18). Les délais de procédure judiciaire, en particulier pour obtenir une décision définitive au fond, demeurent largement inadaptés à la réaction rapide qu'exige la diffusion virale de certaines fausses nouvelles. Le Conseil supérieur de l'audiovisuel, qui va devenir l'Autorité de régulation de la communication audiovisuelle et numérique au 1er janvier 2022, sera chargé de veiller au respect par les plateformes de leurs obligations de retrait rapide de certains contenus illicites graves et dispose d'ores et déjà d'une compétence plus générale de lutte contre la diffusion de fausses nouvelles. On peut estimer qu'il manque au moins une procédure formalisée de signalement auprès de la future ARCOM qui soit ouverte à tout citoyen (R19) afin de faire connaître a posteriori à l'ARCOM les difficultés rencontrées dans la prise en compte de la*

[491] Les différentes feuilles de routes ainsi que la circulaire du Premier ministre relatives à cette stratégie de l'Etat sont disponibles sur ce lien : https://ecoresponsable.numerique.gouv.fr/a-propos/

[492] Rapport de la commission *« Les Lumières à l'ère numérique » :* *https://www.elysee.fr/admin/upload/default/0001/12/127ff0d2978ad3ebf10be0881ccf87573fc0ec11.pdf*

réclamation par la plateforme ou, au contraire, les cas de retrait unilatéral d'un contenu qui ne justifiait pas une mesure aussi radicale, afin que la plateforme lui apporte une réponse appropriée. Enfin, dans le cadre de la loi européenne sur les services numériques, pour responsabiliser les plateformes, la commission propose d'introduire explicitement une disposition qui reconnaît que les fausses nouvelles susceptibles de troubler l'ordre public constituent des contenus répréhensibles (R21), de mettre en place un organe d'expertise extérieur pour coopérer avec les plateformes (R22) et de créer un régime de co-régulation entre plateformes, régulateurs et société civile (R23). »

Cette même synthèse se conclut en ces termes : *« En conclusion, une réflexion prospective nous fait entrevoir de nouvelles questions qui surgiront demain. Le concept de métavers, notamment, esquisse un univers où nous seront immergés dans une confusion croissante entre les mondes réels et virtuels, et nécessite une réflexion éthique (R30). Notre rapport avait pour seule ambition de penser, dans l'urgence, des solutions pour juguler un problème amplifié, voire transformé par le numérique. Ce travail ne nous exonère en rien de la réflexion collective que nous devons mener en parallèle pour penser quelle société et quelle démocratie nous souhaitons construire dans ce monde numérique en devenir. »*

Le Président de la République a salué le travail fondateur de la commission et a annoncé *« le lancement d'une série de chantiers qui ont vocation à faire de la France un pays pionnier dans la lutte contre la désinformation et la régulation des grandes plateformes : le renforcement de l'esprit critique et l'éducation de toutes et tous aux médias et à l'information à l'ère numérique ; l'intensification de la recherche portant sur ces phénomènes (cette recherche pourra s'appuyer sur l'ouverture des données des plateformes grâce aux avancées du Digital Services Act au niveau européen ; elle permettra de coordonner les efforts pour identifier et prévenir la désinformation et les ingérences numériques étrangères) ; la nécessité d'empêcher la mise en avant ou le financement d'acteurs qui nuisent à l'information, à la cohésion sociale et in fine à la démocratie ; l'intensification de la pression sur les plateformes qui tirent parfois d'immenses revenus de l'exploitation de ce qu'il y a de pire dans les comportements sociaux de leurs utilisateurs (les recommandations de la commission concernant les algorithmes, le design des interfaces ou la mise en avant de certains contenus permettront de poursuivre ce combat indispensable pour les démocraties). »*

Le Président de la République a souhaité que le travail de cette commission *« Les Lumières à l'ère numérique »* puisse être diffusé largement et permette d'enrichir le débat démocratique.

S'il convient de saluer de telles initiatives, dont les agendas, les méthodologies et les motivations réelles peuvent interroger (s'agissant notamment du rapport Bonner, au-delà du moment politique choisi, en ce qui concerne le contenu, des généralisations sont hâtives et grossières, des termes ne sont pas définis, des auteurs importants sur les questions du numérique ne sont pas cités, la majorité des références concerne des travaux en sciences cognitives, de neurosciences ou en psychologie sociale, ce biais naturaliste empêchant toute portée plus large des constats), il va néanmoins de soi qu'un numérique pleinement responsable requiert d'élargir le socle des enjeux à adresser.

Sur le plan technologique et industriel, si la *French Tech* est indéniablement en grande forme[493], l'écosystème tricolore souffre toujours de quelques grosses faiblesses.

[493] 11,6 milliards d'euros levés en 2021 par les startups tricolores soit plus du double de 2020, 12 nouvelles licornes en 12 mois, l'objectif des 25 licornes en 2025 fixé par Emmanuel Macron en 2019 atteint avec trois ans d'avance..

A commencer par sa dépendance envers les Gafam et les investisseurs étrangers, mais aussi l'absence de champions européens et mondiaux, le manque flagrant de mixité et de diversité, et la difficulté pour les entreprises technologiques françaises de s'introduire et de prospérer en Bourse.

L'Etat de droit doit pouvoir trouver dans les pratiques institutionnelles des ressorts nouveaux garantissant à la nation des protections contre les abus d'un droit de l'Etat dérogeant trop souvent aux fondements même du libéralisme politique qui préside à toute démocratie libérale.

Naguère axé sur l'activité gouvernementale proprement dite, le contrôle parlementaire tend à prendre plus de champ, pour s'intéresser à l'efficacité des politiques publiques dans leur ensemble (et non pas simplement l'action du Gouvernement dans tel ou tel domaine), ce qui peut amener les assemblées à s'interroger sur les dispositifs législatifs qu'elles ont elles-mêmes adoptés : au contrôle classique s'ajoute désormais un effort d'évaluation[494]. Dont acte.

S'agissant du contrôle de conventionnalité (qui consiste à vérifier la conformité d'une loi aux traités internationaux ratifiés par la France), les juridictions compétentes pour l'exercer (Cour de Cassation et Conseil d'Etat) doivent pouvoir voir les résultats de leur contrôle prolongés par un processus de renvoi 'automatique' de la loi en cause devant le Parlement, en particulier lorsque cette loi comporte des dispositions ayant trait au numérique et/ou à l'intelligence artificielle.

Le Conseil constitutionnel doit également poursuivre le développement de sa capacité à dire le droit de manière incontestable dans ce registre numérique qui bouleverse les grands équilibres du droit fondamental[495], en particulier en mobilisant davantage, lorsque les circonstances le requièrent, sa capacité à entreprendre un revirement de sa propre jurisprudence.

Faut-il aller jusqu'à le transformer en une véritable Cour constitutionnelle[496] sur le modèle allemand ? L'heure est venue de trancher.

Des potentialités de contrôle et d'implication démocratiques par les citoyens dans le fonctionnement de cette nouvelle puissance publique 2.0 dont les modes modernes de gouvernance, de gouvernement et/ou d'administration trouvent dans le numérique des potentialités, des exigences mais aussi des inquiétudes et des limites nouvelles qui ne sauraient rester sans traduction dans la loi fondamentale. De nouveaux principes démocratiques inspirés par un humanisme et une éthique numériques doivent pouvoir y trouver place.

Un nouveau contrat social prenant en compte les impacts comme les attentes démocratiques de cette révolution numérique sur le rapport de la nation aux différentes formes de cette puissance publique 2.0 en action doit rapidement émerger pour traduire explicitement dans la lettre et l'esprit de la loi fondamentale la promesse démocratique qu'elle entend et prétend servir.

Consécutivement aux recommandations formulées par le groupe de travail interparlementaire informel constitué en vue de réfléchir à l'inclusion de droits et libertés numériques dans la Constitution[497,498], une proposition de loi constitutionnelle, qui vise à faire inscrire dans le

---

[494] *Le contrôle parlementaire en France :* https://www.senat.fr/role/fiche/controle_gouvernement.html

[495] *Le numérique saisi par le juge, l'exemple du Conseil constitutionnel :* https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-numerique-saisi-par-le-juge-l-exemple-du-conseil-constitutionnel

[496] *Vers une Cour suprême ?* https://www.conseil-constitutionnel.fr/les-membres/vers-une-cour-supreme

[497] Députés et sénateurs ont planché sur trois projets, avant de privilégier le premier :

1. L'intégration d'une « *Charte du numérique* » dans le préambule de la Constitution
2. La reconnaissance du « *rôle du numérique dans l'expression démocratique* » dans l'article 4 de la Constitution
3. L'entrée de « *certains enjeux liés au numérique* » dans la liste des sujets relevant du domaine de la loi (au sens de l'article 34 de la Constitution)

Cf. https://cdn2.nextinpact.com/medias/gt-numerique.pdf

[498] *Proposition de Charte du numérique* : https://cdn2.nextinpact.com/medias/projet-charte-constit.pdf

préambule de la Constitution une référence à la « *Charte de l'Intelligence Artificielle et des algorithmes 2020* » [499] dans l'optique de responsabiliser juridiquement les créateurs de systèmes d'intelligence artificielle, a été soumise à l'Assemblée nationale le 15 janvier 2020.

Mais son contenu s'est révélé très en-deçà du niveau des réponses attendues devant les défis posés à la nation et auxquels la loi fondamentale devra apporter des réponses, notamment à l'égard des impératifs de souveraineté et de sobriété numériques, et plus largement, à l'égard des quatre grands défis identifiés par le professeur Bonnet (*cf. supra*).

Aucune concrétisation n'a encore été opérée à cet égard.

Les textes proposés par l'ISOC [500], par *Privacy Tech* [501] ou par le Cercle de la Donnée [502] apportent à cet égard des préconisations de choix.

L'initiative remarquable prise par l'Etat chilien à l'automne 2021, qui a pris le parti d'introduire dans la Constitution des dispositions garantissant des 'neurodroits' [503] doit constituer une incitation forte pour que la France, notamment, agisse dans le même sens.

Au-delà, un enjeu fondamental se pose : trouver les voies et moyens de garantir en toutes circonstances le respect de l'esprit comme de la lettre de la Constitution par les institutions et juridictions impliquées, à un titre ou à un autre, dans le fonctionnement de l'Etat de droit.[504]

Enfin, l'Etat français doit profondément repenser sa stratégie d'études d'impact des textes législatifs et réglementaires qu'il élabore, comme le requiert le Conseil économique, social et environnemental (CESE). France Stratégie a reçu la mission de rechercher les voies et moyens qui permettront de moderniser les méthodologies requises pour la conduite de ces études.[505]

« Sur le plan intellectuel, la France dispose d'atouts pour faire entendre la voix d'une culture numérique éthiquement soutenable, par exemple avec les travaux menés à l'Institut de Recherche et d'Innovation ou plus amplement avec le courant des études digitales. Mais, pour les faire valoir, elle doit réaffirmer, dans les processus d'innovation eux-mêmes, les valeurs auxquelles elle est démocratiquement attachée. » (Pierre-Antoine Chardel)

Plus que jamais la France a besoin du souffle d'une République des solutions.

---

[499] *Proposition de Loi constitutionnelle relatif à la Charte de l'Intelligence Artificielle et des algorithmes :* http://www2.assemblee-nationale.fr/documents/notice/15/propositions/pion2585

[500] *Pour la consécration constitutionnelle des droits fondamentaux des utilisateurs du numérique :* https://www.isoc.fr/petition-charte-du-numerique/

[501] *#DigitalHumanRights : pour une déclaration des droits fondamentaux numériques, 4ème génération de droits de l'homme* https://www.privacytech.fr/livre-blanc/

[502] *Intelligence Artificielle : Le Cercle de la Donnée présente 12 propositions pour une meilleure utilisation de la donnée :* https://www.lemondedudroit.fr/publications/248-etudes-et-documents/66278-intelligence-artificielle-cercle-donnee-presente-12-propositions-meilleure-utilisation-donnee.html?fbclid=IwAR3b7GcCjvy2WCimDgNmFwfPYlF7TqXJ6PlUzN6zkjlF_sCLns5cUr1Xxi8

[503] L'article 19 de la Constitution chilienne comporte désormais la disposition suivante : « *Le développement scientifique et technologique doit être au service des personnes et s'effectuer dans le respect de la vie et de l'intégrité physique et mentale. la loi réglemente les exigences, les conditions et les restrictions de son utilisation sur les personnes, et protège tout particulièrement l'activité cérébrale, ainsi que les informations qui en découlent. ».*

[504] *Comment garantir le respect de la Constitution ?* https://www.doc-du-juriste.com/droit-public-et-international/droit-constitutionnel/dissertation/garantir-respect-constitution-455198.html?fbclid=IwAR0J_konUWn3Sa4rsjzAZgET9ob-T3A3HkvuF2LLLPVZwrD5IaqAHSqM9f8

[505] *Vingt ans d'évaluations d'impact en France et à l'étranger – Analyse comparée des pratiques dans six pays :* https://www.strategie.gouv.fr/publications/vingt-ans-devaluations-dimpact-france-letranger-analyse-comparee-pratiques-six-pays

Epilogue

En épilogue aux nombreuses réflexions exposées dans la présente étude comme aux développements abondants qu'elles ont pu nourrir et aux recommandations multiples qu'elles ont pu inspirer, je me contenterai d'inviter le lecteur à poursuivre ses propres réflexions et analyses en prenant acte des termes de la conclusion que Boris Barraud choisit d'inscrire au terme de sa thèse de droit intitulée *'Le renouvellement des sources du droit – Illustrations en droit de la communication par internet'*[506] :

« Toutes les branches du droit ne suivent pas le modèle du droit de la communication par internet, bien au contraire, ce qui est peut-être heureux pour l'État. Cependant, la tendance ne semble pouvoir être qu'au développement des branches du droit « postmodernes » et « globales » et au retrait des branches du droit modernes et nationales, ainsi qu'à la transformation de certaines branches du droit modernes en branches du droit « postmodernes ». C'est pourquoi le droit de la communication par internet a pu être envisagé tel un « exemple prospectif ». « Le temps des États-Nations et des droits nationaux est révolu », gage-t-on désormais sans ambages. Aussi le regard porté sur le droit de la communication par internet, droit en avance sur son temps, pouvait-il peut-être servir à anticiper quelques phénomènes d'ordre général à venir, à court ou moyen terme, au premier rang desquels figureraient l'avènement d'une « nouvelle constellation politique » et juridique. Il apparaît de plus en plus contestable que les travaux portant sur l'abandon de l'État ne seraient là que pour « faire sensation », à mille lieues de toute réalité factuelle. Et l'observation du droit de la communication par internet pourrait également être utile à ceux qui recherchent les solutions pertinentes afin de « sauver l'État » ; à moins qu'il faille comprendre que la meilleure solution serait de « sauver le droit » sans « sauver l'État ». Qu'on se souvienne, avec Raymond Carré de Malberg, combien « l'État n'est pas une fin mais un moyen ».

L'État « ne mérite ni l'excès d'hommage que lui rendent les uns ni la honte dont le couvrent les autres ; il exige une analyse aussi froide que lui-même ». D'une telle analyse entreprise dans le domaine de la communication par internet, il ne semble pouvoir ressortir qu'un bilan peu satisfaisant pour l'État et pour les sources du droit qui en relèvent. Partant, s'il lui est encore possible de suivre la voie de la « renaissance » plutôt que celle de l'« érosion », l'État devrait peut-être se réformer et, en particulier, ne plus élaborer le droit applicable aux objets « postmodernes » en suivant les canons modernes de la production du droit. En un mot, il devrait devenir cet « État postmoderne » que d'aucuns imaginent, soit un État plus ressemblant qu'antinomique par rapport aux caractéristiques de l'internet. Ce cadre étatique « postmoderne » pourrait, notamment, correspondre au passage d'un « régime de sujétion », de « puissance dominatrice » et de « puissance coercitive » à un « régime de collaboration », ce qu'imaginait déjà Raymond Carré de Malberg au début du XXe siècle. Et l'« État postmoderne » produirait un « droit postmoderne », c'est-à-dire un droit « mou, négocié, pluraliste et réflexif ». Le pluralisme des sources du droit ne serait dès lors plus le symptôme de la « crise » de l'État mais le résultat de la réforme de l'État.

En tout cas l'État d'aujourd'hui ne saurait-il être celui d'hier — à moins qu'il faille plutôt envisager que l'État de demain ne puisse être celui d'aujourd'hui. Selon Maurice Hauriou, il incomberait à l'État de « s'appuyer sur le passé et s'élancer vers l'avenir ». À l'heure de l'internet, il lui appartiendrait surtout de savoir « s'élancer vers l'avenir ». Or, en matière de

[506] *'Le renouvellement des sources du droit – Illustrations en droit de la communication par internet'*, Presses universitaires d'Aix-Marseille, 2018, 596 pages : https://www.academia.edu/25103935/Le_renouvellement_des_sources_du_droit_Illustrations_en_droit_de_la_communication_par_internet_Presses_universitaires_dAix_Marseille_2018_596_p

sources du droit, ainsi que l'indique l'étude qui s'achève, il tend surtout à « s'appuyer sur le passé ». Si des concepteurs de l'« État postmoderne » en font le fruit d'une « pensée de la déconstruction de l'État », n'est-il pas possible de penser la reconstruction de l'État en pensant l' « État postmoderne » ? En particulier, il s'agirait de penser la reconstruction des sources étatiques du droit, de penser le dépassement de la loi mais aussi la refondation de la loi.

Peut-être l'État n'a-t-il jamais été aussi contesté et menacé qu'actuellement et continue-t-il d'exister seulement parce qu'aucun modèle alternatif efficace n'est proposé. Rien n'assure que cette situation puisse se prolonger durant des décennies et peut-être la « crise de l'État », phénomène préoccupant à plus d'un titre que la problématique du renouvellement des sources du droit permet d'éclairer, doit-elle être prise au sérieux.

Selon Jean-Jacques Rousseau, « Le corps politique, aussi bien que le corps de l'homme, commence de mourir dès sa naissance et porte en lui-même les causes de sa destruction. Mais l'un et l'autre peuvent avoir une constitution plus ou moins robuste et propre à les conserver plus ou moins longtemps. La constitution de l'homme est l'ouvrage de la nature, celle de l'État est l'ouvrage de l'art. Il ne dépend pas des hommes de prolonger leur vie, mais il dépend d'eux de prolonger celle de l'État aussi loin qu'il est possible, en lui donnant la meilleure constitution qu'il puisse avoir. Le mieux constitué finira, mais plus tard qu'un autre, si nul accident imprévu n'amène sa perte avant le temps. »

Or la Constitution ne comporte-t-elle pas l'essentiel du « droit des sources », si bien que, pour rénover les sources étatiques, il faudrait nécessairement rénover la Constitution ? Peut-être importe-t-il en tout cas de retenir la leçon selon laquelle un État dont les institutions sont adaptées à son environnement et sont capables de s'ajuster en fonction de l'évolution de cet environnement aurait autrement plus de chances de survivre aux crises qu'il pourrait devoir affronter qu'un État sclérosé et se reposant sur une structure qui, étant ancestrale, risque fort d'être aussi archaïque. « La véritable mesure de performance des organisations modernes, écrit-on, est leur capacité de lire et de comprendre la situation, et de se transformer rapidement afin de pouvoir répondre de façon créatrice aux défis que posent les nouveaux contextes ».

[…] Qui sait quels objets « néo-postmodernes » les normes seront bientôt chargées d'encadrer et quelles conséquences le droit « néo-postmoderne » qui en résultera emportera pour la doctrine des sources du droit ? En définitive, le renouvellement des sources du droit et le droit de la communication par internet enseignent que la seule règle universelle et immuable de la pensée et de la science juridiques pourrait être : Le droit est mort, vive le droit ! »

« L'histoire de la pensée humaine montre que la science, et donc également la science du droit, se libère toujours de l'état de dépendance dans lequel le pouvoir tente continuellement de la maintenir. […] Dans la lutte incessante du pouvoir contre la pensée, […] la victoire du pouvoir n'est jamais définitive ; la pensée résiste jusqu'à atteindre à nouveau ce qui seul correspond à sa nature propre, à savoir la liberté. »

(Hans Kelsen)

" La sauvegarde de notre monde humain n'est nulle part ailleurs que dans le coeur humain,

la pensée humaine, la responsabilité humaine."

(Vaclav Havel)

« Il ne sert à rien de dire "Nous avons fait de notre mieux". Il faut réussir à faire ce qui est nécessaire. »

(Winston Churchill)