Un projet socialiste pour faire face à la révolution numérique

Jean Christophe Schwaab, août 2018

Contenu

Remarques liminaires

Le contenu du présent rapport est politique et subjectif, tant sur le choix des sujets que sur la façon de les aborder. Même si j'ai essayé de faire abstraction de mes propres positions, surtout lorsqu'elles divergent de celles du Parti (p. ex. sur le vote électronique), il n'est pas exclu qu'elles transparaissent toute de même dans mes lignes. Ce rapport n'a en outre pas la prétention d'être exhaustif ou d'analyser chaque problématique évoquée sous toutes ses coutures, ni de présenter des solutions concrètes directement applicables, ou, à tout le moins, immédiatement transformables en interventions parlementaires. Il doit plutôt servir de point de départ ou, mieux, de camp de base pour élaborer des projets politiques plus concrets, en s'appuyant notamment sur les sources citées, plus détaillées. D'ailleurs, certaines problématiques très connues du grand public et déjà largement détaillés dans d'autres publications (p. ex. les risques en matière de protection des données engendré par la révolution numérique ou la neutralité du net) n'ont pas été développées en détails. Il a par ailleurs été difficile de structurer le présent document, tant les thèmes et problématiques à traiter sont transversaux les uns pour les autres et dépendants les uns des autres. Nous espérons que la structure adoptée sera lisible et compréhensible !

Les entreprises, applications, logiciels, produits, machines et autres robots cités ne le sont qu'à titre d'exemple, sans aucune appréciation de leurs agissements, utilité, avantages et inconvénients.

L'utilisation du genre masculin a été adoptée afin de faciliter la lecture et n'a aucune intention discriminatoire.

Mes remerciements vont enfin à Min Li Marti, qui a eu la gentillesse de me transmettre ses abondantes notes sur les conséquences de la révolution numérique.

1. Mandat

Comme convenu par échange de courriels avec Roger Nordmann, voici les objectifs du présent document :

- Mettre en lumière les avantages et opportunités de la révolution numérique pour la population, la vie en société, les collectivités publiques et la place économique, mais sans tomber dans la béatification à la sauce des « technoptimistes ».
- Mettre en lumière les risques de la révolution numérique pour les mêmes acteurs, mais sans tomber dans le pessimisme à la « 1984 » ou « les intelligences artificielles et les robots vont prendre le pouvoir et nous piquer notre boulot ».

2. Définitions et contexte

Révolution numérique

Wikipedia défini la révolution numérique ainsi : « On appelle « révolution numérique » (ou plus rarement « révolution technologique » ou « révolution Internet ») le bouleversement profond des sociétés survenu globalement dans les nations industrialisées et provoqué par l'essor des techniques numériques, principalement l'informatique et Internet. Cette mutation se traduit par une mise en réseau planétaire des individus, de nouvelles formes de communication (courriels, réseaux sociaux) et une décentralisation dans la circulation des idées ».
Dans le présent document, nous employons le terme « révolution numérique » en tant que synonyme pour « numérisation »/« digitalisation » (au sens d'un changement sociétal et non au sens de convertir des documents en code numérique), « transformation digitale ou numérique et de la société et/ou de l'économie », « essor des nouvelles technologies », « [entrer le nom du thème] 4.0 », etc.

Encore une révolution numérique ?

La révolution numérique est une tendance très ancienne. En effet, dès l'invention de l'abaque il y a plus de trois mille ans, les êtres humains ont construit des machines capables de faire des calculs plus rapidement et plus précisément qu'eux-mêmes. Au cours des siècles qui ont suivi, de nouvelles machines et méthodes de calcul, ainsi que de reproduction et de diffusion de l'information, pour certaines très complexes et très efficaces, ont fait leur apparition, entraînant parfois des transformations très importantes de la société[1]. Par exemple, le métier à tisser mécanique inventé en 1805 par Jaccard, il fonctionnait déjà à l'aide… d'algorithmes[2] !
A chaque fois, l'emploi de technologies nouvelles a suscité craintes, critiques et velléités d'interdiction ; dans le « Phèdre », Platon voulait par exemple empêcher l'essor de l'écriture qu'il jugeait « inhumaine » et parce qu'elle « détruirait la mémoire ».
La révolution numérique que nous vivons actuellement contient toutefois des éléments nouveaux, qui vont bien au-delà de la facilité et de la rapidité à faire des calculs de plus en plus complexes : les informations sont mises en réseaux, sauvegardées, combinées, réexploitées. Elles sont aussi sauvegardées par défaut et conservées même une fois leur utilité première périmée (au sens du principe de finalité)[3]. Souvent qualifiées d'« or noir du XXIème siècle », les données, comme le disait en substance Tim Berners-Lee, un des inventeurs du *World Wide Web*, « c'est mieux que du pétrole, car une fois qu'on les a utilisées, données, vendues ou échangées, on les a toujours ! ».
En outre, grâce à l'intelligence artificielle capable d'apprendre (*deep learning*), les machines commencent à ne plus avoir besoin d'humains pour choisir, définir et effectuer leurs tâches, voire pour s'améliorer, se réparer… ou se fabriquer en série. Certains « technoptimistes » font preuve d'une emphase toute publicitaire et n'hésitent pas à parler d'un « deuxième âge de la machine ».
De même, l'économie du partage n'est pas une invention nouvelle. Depuis la nuit des temps, les communautés humaines mettent en commun des ressources rares ou mal utilisées si monopolisées. La révolution numérique ne fait que faciliter ces processus[4]… et beaucoup d'autres ! Certains n'hésitent d'ailleurs pas à rendre les nouvelles technologies responsables de problèmes qui ont d'autres causes qu'il est plus difficile d'assumer dans le débat public et auxquelles il est plus difficile de trouver des solutions. Ainsi, ce furent les smartphones « blackberry » et leur système de messagerie instantanée cryptée « BBM », alors très populaires auprès des jeunes qui furent rendus responsables des émeutes dans la banlieue

londonienne en 2011[5]. Ces troubles sociaux avaient bien entendu d'autres causes, notamment en lien avec la politique sociale, mais il était alors plus simple et plus pratique de rendre la technologie responsable de ces débordements. Il en va de même de la tendance actuelle des supermarchés d'introduire l'auto-scan et de remplacer les caisses tenues par des vendeuses. Cette mode est mise en relation avec l'essor de l'IA et des robots, alors que les caisses auto-scan en question ne peuvent pas vraiment être qualifiées d'« intelligentes ». Quant aux *fake news* créées et diffusées dans le but d'influencer des élections, il s'agit aussi d'un phénomène très ancien, que les nouvelles technologies rendent peut-être plus visible… et plus mesurable (en termes de clics)[6] !

3. Avantages de la révolution numérique d'un point de vue socialiste

Monde du travail

L'essor des nouvelles technologies est une occasion de faire progresser le travail décent. Leur usage permet non seulement de « désautomatiser » l'humain[7], notamment en le déchargeant de certaines tâches pénibles, chronophages ou inintéressantes, voire abrutissantes. Cela est valable dans de nombreux secteurs d'activité[8] : des tracteurs agricoles connectés John Deere[9] au logiciel Watson d'IBM qui facilite le traitement des courriels. Pour de nombreux salariés, la révolution numérique est synonyme de temps gagné : « Alternatives économiques »[10] donne notamment les exemples de salariés d'une banque française gagnant jusqu'à 2 heures par semaine grâce à l'emploi d'une application qui gère les contacts avec la clientèle. Autre exemple, celui d'une employée d'une assurance qui affirme que le traitement d'un dossier prend un mois de moins et que l'efficacité du travail est en hausse. Enfin, dans une autre banque française, jusqu'à 50% des sollicitations (simples) des clients peuvent être réglées sans intervention humaine. Les conseillers peuvent alors se (re)concentrer sur l'expertise, ce qui est, selon eux, la partie la plus intéressante de leur métier.
De nombreuses analyses tablent aussi sur une facilitation de la conciliation entre vie familiale et professionnelle grâce aux nouveaux outils numérique[11].

Environnement

L'emploi de l'IA est considéré par beaucoup comme une chance en matière de protection de l'environnement et de gestion des ressources naturelles[12], en particulier de l'eau, notamment pour adapter les cultures aux changements climatiques[13]. L'usage de l'IA doit aussi permettre d'identifier et de préserver la biodiversité, modéliser l'impact des actions humaines sur cette dernière, mais aussi de réparer les dommages[14]. L'emploi de nouvelles technologies est aussi considéré comme un moyen de faire face à la pénurie de ressources servant à la production desdites technologies, mais aussi de dépasser leurs limites physiques actuelles. Ainsi, l'emploi de processeurs graphiques (*graphics processing unit*, GPU) pourrait compenser la fin annoncée des « Lois de Moore »[15].

Santé publique

Beaucoup voient dans la révolution numérique des opportunités en matière de santé publique non seulement pour les (futurs) patients, mais pour la collectivité dans son ensemble[16]. Ainsi, l'analyse et la recherche médicale, le ciblage thérapeutique, la détection des effets secondaires

et le suivi des patients devraient être facilités[17]. Le maintien à domicile des personnes très âgées et/ou handicapées pourrait lui aussi être facilité, notamment en ce qui concerne la prévention des chutes ou de l'inactivité.
L'économiste de la santé Mascha Madörin (même si elle ne cache par ailleurs pas son pessimiste) est persuadée que la robotique peut améliorer la santé, notamment en matière de rationalisation des soin (au sens positif du terme) ou de lutte contre la pénurie de personnel qualifié[18].

Prestations et services publics

Les nouvelles technologies doivent permettre un meilleur accès aux prestations publiques, pas uniquement en termes d'accès « physique » (guichets virtuels faciles à utiliser et disponibles en permanence). En particulier, l'IA peut être utilisée pour aider les ayant-droit à remplir les formulaires, notamment pour que leur dossier soit complet et qu'ils ne négligent aucune aide à laquelle ils auraient droit, mais dont ils ignorent l'existence[19]. Cela dit, de tels progrès ne sont envisageables qu'à condition de réduire la « fracture numérique » (cf. plus bas p. 9).
Le succès de la politique numérique volontariste de l'Estonie n'est par exemple plus à démontrer. Dans ce pays, la quasi-totalité des démarches administrative peut se faire en ligne, la formation aux nouvelles technologies est intensive (elle a lieu dès le plus jeune âge) et les investissements dans les infrastructures sont conséquents. Toutefois, une telle exposition aux nouvelles technologies ne va pas sans risque pour un Etat, à plus forte raison s'il est voisin (et en mauvais termes !) avec une grande puissance à forte capacité de cyberattaque comme la Russie, qui a d'ailleurs lancé une attaque massive par « botnets » contre l'Estonie en 2007[20].

Economie et consommation

Habituée à tirer profit des mutations technologiques (même si c'est parfois avec beaucoup de retard et de dégâts collatéraux) la place industrielle suisse pourrait se renforcer grâce à de nouvelles technologies sources de croissance, d'innovation et de gains de productivité et donc d'emplois[21]. Ces constats ne sont toutefois valables que s'il ne s'agit pas d'une phase d'innovation sans croissance (et donc sans croissance de l'emploi) : en effet, les progrès technologiques actuels n'ont qu'un impact beaucoup plus limité sur la productivité que bon nombre d'innovations majeures des décennies précédentes. En effet, passer, par exemple, de la diligence au train permet des gains de temps et d'efficacité beaucoup plus importants que de pouvoir réserver son billet avec son smartphone. En outre, les dépenses de R&D donnent actuellement de moins bons retours sur investissements que par le passé. Enfin, ces gains de productivité sont moins bien redistribués aux salariés que par le passé, tendance qui risque de s'aggraver avec la croissance des inégalités, notamment de capital[22].
La véritable « économie du partage » (*sharing economy,* économie collaborative)[23] permet de mettre en commun les ressources (y compris en temps), non seulement pour qu'un grand nombre en profite, mais aussi pour que l'on utilise plus souvent des ressources trop peu utilisées[24] (en particulier si l'on considère l'investissement à consentir pour les obtenir). Elle permet aussi d'intensifier les contacts sociaux (avec toutefois le risque de monétiser des services auparavant rendus sans contrepartie). Cela dit, au-delà des vrais exemples d'économie du partage que sont, par exemple, Wikipedia, Streetbank ou le *couch surfing*, il y a de très nombreux « faux amis » se réclamant de l'économie du partage comme AirBnB, Uber, eBay, Upwork, etc. qui monétisent, voire accaparent les ressources mises en commun et en tirent un bénéfice. Par ailleurs, dans cette variante où les ressources sont monétisées, l'économie du partage encourage les inégalités, car seul celui qui possède peut mettre des ressources à disposition… et tirer profit de leur utilisation plus intensive[25].

La révolution numérique : un processus civilisateur et émancipateur ?

L'essor des nouvelles technologies a le potentiel pour révolutionner la transmission des informations et des savoirs, mais aussi l'organisation collective. Ainsi, certains voient dans les technologies comme le p2p, l'open source ou la véritable économie du partage un nouveau processus émancipateur, comparables aux inventions collectives du mouvement ouvrier à ses débuts (syndicats, sociétés d'assistance mutuelle). Les nouveaux outils numériques pourraient contribuer à renforcer les communautés et leurs actions collectives, la communauté en ligne devenant, en parallèle ou à la place des entreprises, le lieu de la négociation collective[26]. Par exemple, Bauwens et Lievens[27] voient dans ces nouvelles technologies une opportunité vers une société post-capitaliste relocalisée, où le marché serait contraint de se soumettre à la logique du bien commun. Les nouveaux outils de traduction en ligne doivent encore contribuer à faciliter ces contacts et cette auto-organisation.
Il ne faut toutefois pas oublier que ces nouvelles possibilités d'organisation collective décentralisée ne profitent pas uniquement aux mouvements que les socialistes soutiennent ou dont ils se revendiquent : en Italie, le M5S, parti populiste désormais à la tête d'une majorité gouvernementale et parlementaire, est aussi, en partie, né de l'auto-organisation de groupuscules contestataires locaux, grâce aux nouveaux outils informatiques.
Au-delà des questions d'organisation collective, la révolution numérique tend à s'imposer en processus civilisateur posant de nouvelles questions éthiques. Comme le relève Milad Doueihi, paraphrasant Norbert Elias : « nous [les humains] sommes aujourd'hui des sauvages modernes soumis à un nouveau processus civilisateur, le numérique. (…). Notre environnement numérique est comme un laboratoire d'expérimentation et de cohabitation avec le non-humain, mais un non-humain qui relève à la fois du social, du technique, du discursif, du scientifique. C'est bien l'originalité du numérique, de sa spécificité et de son statut unique dans notre histoire. Il interroge l'humain, à la fois dans son comportement, son identité, mais aussi dans ses valeurs et dans le choix qu'il peut faire et dont il dispose [en particulier face aux algorithmes]. »

4. Risques de la révolution numérique d'un point de vue socialiste

Monde du travail

Quelles conséquences sur l'emploi ?

C'est notamment à propos du monde du travail que les impacts de la révolution numérique sont le plus discutés… et le plus fantasmés. En effet, les prévisions les plus pessimistes se mêlent à l'optimisme le plus béat lorsqu'il s'agit de savoir si les nouvelles technologies vont massivement détruire, ou au contraire créer des emplois. La plupart des analyses partent de l'idée qu'il n'y a pas de risque de pertes d'emplois massives et globales[28]. Les prévisions quant aux nombres d'emplois « menacés » sont fort variables : certains tablent sur 6 emplois « détruits » pour chaque robot introduit sur le marché du travail (Acemoglu) ; d'autres parlent de 47% des emplois qui pourraient être automatisables grâce à l'IA et seraient donc voués à une disparition prochaine (Frey/Osborne, ainsi que Rifkin ou Attali, ces derniers étant probablement un peu caricaturaux), pendant que d'autres tablent sur 14% (OCDE), voire moins de 10% (Conseil d'Orientation pour l'Emploi)[29]. Sur le terrain, les premiers constats vont plutôt dans le sens d'un certain optimisme : En Allemagne, pays bien loin de subir la « menace mortelle » crainte par certains, dont le Commissaire européen Oettinger[30],

l'industrie crée pratiquement autant de nouveaux emplois en lien avec la digitalisation que cette dernière n'en supprime.

Concurrence globale accrue

Toutefois, les travailleurs des services pouvant être fournis à distance risquent fort d'être mis en concurrence (déloyale) avec le marché mondial via une plateforme et non plus seulement leur concurrent « locaux »[31]. Tout emploi qui n'est plus tributaire d'un ancrage local et qui implique essentiellement la manipulation d'informations peut être désormais être facilement délocalisé[32]. Et, même au niveau local, la prestation de services basée sur les relations et rapports sociaux, le bouche-à-oreille, le voisinage, etc. peut être remplacée par une plateforme comme Upwork où les artisans font leurs offres. La concurrence s'intensifie aussi au sein d'une même entreprise entre les travailleurs jeunes, surmotivés et en bonne santé et ceux plus âgés, en moins bonne santé et/ou avec des personnes à charge. Ainsi, la planification et le contrôle algorithmique du travail conduisent à des discriminations de ces derniers[33]. Il en va de même de l'évaluation à outrance[34].

Profil des emplois menacés

Quant au type d'emplois menacés, les analyses s'accordent sur le fait que les emplois moyennement qualifiés, les activités productives et administratives pourraient être touchées[35]. Certains craignent un bouleversement du terreau industriel (p. ex. une nouvelle crise horlogère en raison des montres connectées), avec pour conséquence un affaiblissement des syndicats et du partenariat social et des pertes d'emplois à forte valeur ajoutée dans des régions peu favorisées comme l'Arc jurassien.

Conditions de travail

En matière de conditions de travail, les nouvelles technologies entraînent un risque certain de précarisation de nombreux emplois, ainsi que des risques pour la santé au travail (hyperconnectivité, disponibilité permanente générant stress et burn-out)[36]. Il y a aussi un risque de concentration de richesse et de pouvoir tout au long de la chaîne de valeur entre les mains du propriétaire de la plateforme (et donc de la norme de communication) avec pour corollaire une croissance de inégalités[37]. D'une manière générale, les travailleurs de la « *gig economy* » subissent, en plus des incertitudes liées à leur type de contrat et aux lacunes d'assurances sociales qui peuvent en découler, des conditions de travail plus mauvaises et une pression plus élevées (notamment en termes de délais) que dans des entreprises « traditionnelles »[38].
Certes, la révolution numérique entraîne la création de nouveaux emplois haut de gamme (p. ex. analyste de données), mais favorise l'émergence d'un nouveau prolétariat de « galériens du numérique » (les *crowdworkers* du « turc mécanique » d'Amazon). Ces « galériens » sont aussi les travailleurs de la nouvelle économie, mais leur lieu de travail ne se trouve pas dans les bureaux confortables, conviviaux, ludiques et cools des géants de la Silicon Valley, ils ne circulent pas en véhicule autonome… et ne se connaissent pas, ne se voient jamais et ne peuvent donc pas s'organiser collectivement (avec une exception notable : Turkopticon)[39]. Soumis aux ordres des machines dont ils sont les exécutants, ils n'ont même plus à utiliser leur propre savoir-faire[40]. Souvent, ils sont confrontés à des contenus insoutenables (p. ex. les modérateurs de vidéos violentes) et entrent dans l'intimité des utilisateurs à l'insu total de ceux-ci[41].
Quoi qu'il en soit et quel que soit son impact sur le niveau global d'emploi, il faut s'attendre à une transformation en profondeur du monde du travail, avec, selon l'USS, un gros potentiel

d'abus ; la révolution technologique laissera certainement des exclus à qui les compétences obsolètes ne permettront définitivement pas de réintégrer le premier marché du travail[42].

Débat public / Droits politiques

Un débat démocratique sous influence ?

Si les nouveaux outils numériques facilitent certains aspects de l'exercice des droits politiques (p. ex. récole de signatures en ligne, mobilisation massive et durable même sans appareil à l'instar du récent référendum contre la surveillance des assuré-e-s), leur emploi comporte aussi certains risques non négligeables, qui vont bien au-delà de l'accentuation de la « démocratie d'opinion » ou « démocratie du clic/du *like* » ainsi que des désormais célèbres *fake news*. Les GAFA risquent, à terme, de contrôler le débat public, non seulement ses lieux (réseaux sociaux), ses contenus (censure préventive et sélective de certaines opinions jugées à tort ou à raison comme extrémistes ou relevant des *fake news*), mais aussi, et c'est encore plus insidieux, en en fixant les termes pour détourner la discussion. Le risque est en effet non négligeable que les milieux de la « tech » (GAFA, mais aussi les universités qui ont vu naître leurs technologies) dictent, voire confisquent le débat public qui doit avoir lieu sur l'impact politique des nouvelles technologies, en en posant des termes peu utiles, mais qui les arrangent, comme le « jeu » du MIT « moral machine »[43]. Ce jeu, qui doit aider à résoudre le « dilemme du véhicule autonome », fait se poser à ses utilisateurs des questions absurdes (en cas d'accident imminent faut-il plutôt écraser une vielle dame et son chien ou une maman et sa poussette ?) et finalement sans grand rapport avec la réalité. La contribution à la « mise en scène » du débat public sur l'impact des nouvelles technologies, ce en quoi les « tech » excellent, inclut aussi le risque de diriger celui-ci. Ainsi, Watson (IBM) est p. ex. présenté comme « intelligence augmentée » au lieu d'être vendu en tant qu'« IA », afin de ne pas faire peur aux humains en leur promettant une complémentarité au lieu d'un combat entre hommes et machines.
Lorsque l'on légifère sur les conséquences des nouvelles technologies, il faut aussi veiller à ne pas se laisser aveugler par le principe des règles « neutres du point de vue technologique », méthode de légistique dont la Suisse s'enorgueillit souvent. Il ne faut en effet pas confondre la neutralité technologique avec la neutralité du risque[44]. La neutralité technique empêche que l'on créer des règles pour une technologie en particulier. Mais elle rate son but lorsqu'elle ne s'adapte pas aux risques générés par une technologie. Or, ces risques évoluent. Il ne faut donc pas traiter de la même manière la carte de fidélité du magasin du coin que celle d'une chaîne de supermarchés qui, grâce au big data, fait des profils de personnalité extrêmement précis sur la base de données en soi inintéressantes, même si la technologie est la même.

Une aubaine pour les propositions radicales de la droite

Au niveau politique, comme chaque « choc » économique ou social[45], la révolution numérique sert d'occasion ou de prétexte aux classes dominantes pour faire passer, parfois ouvertement, parfois sur l'angle de la « lutte contre la bureaucratie anti-innovation », certaines de leurs revendications les plus radicales qui n'auraient aucune chance dans un contexte politique « normal ». Ainsi, la révolution numérique sert de nouveau justificatif pour bon nombre des « vieilles lubies » de la droite. Par exemple, la boîte à idée de la droite ultralibérale avenir.suisse estime qu'en ces temps de révolution numérique, des acquis importants de la gauche sont devenus obsolètes, comme le partenariat social et la négociation collective, la saisie du temps de travail[46], la couverture sociale et la protection des travailleurs contre la fausse indépendance ou le travail précaire[47]. Ces attaques ne se dirigent d'ailleurs pas toutes contre les travailleurs, mais aussi contre certains employeurs, surtout ceux qui ont

le malheur d'être actifs dans une branche visée par les nouveaux acteurs disruptifs (comme AirBnB ou Uber). La révolution numérique peut aussi être le prétexte idéal à une nouvelle vague de privatisation de tâches publiques, une occasion d'autant plus juteuse que les GAFA disposent d'une capacité d'action (notamment financière) colossale qui leur permet d'entrer rapidement sur n'importe quel marché. De nombreux ultralibéraux ont flairé la bonne affaire. Ainsi, l'ancien conseiller de Donald Trump Steve Bannon a envisagé de confier à Google des missions de service public. La révolution numérique permet enfin à certains de s'attaquer aux fondements mêmes du débat démocratique en visant à remplacer les décisions des autorités par des décisions d'algorithmes.

Aucune de ces revendications n'est nouvelle, mais la numérisation de l'économie suffit à faire croire qu'il s'agit d'un programme politique moderne et innovant. Elles visent aussi à faire croire que le cadre légal actuel n'est pas adapté à l'innovation et à l'essor des nouvelles technologies (et, partant à démontrer l'incompétences des organes démocratiques qui l'ont mis en place), alors qu'en réalité, le modèle d'affaire de certains de ces nouveaux acteurs n'a d'innovant que le fait de se fonder sur le non-respect des règles en vigueur. On relèvera enfin que ces revendications sont souvent mis en scène sous l'angle d'une pseudo « guerre des générations » entre « *millenials* qui sont nés et vivent avec Internet » et « vieux ringards qui n'y comprennent rien ».

Il faut dire que de nombreux acteurs des nouvelles technologies passent sans cesse de la « résistance » anarcho-libertarienne contre un Etat « excessivement régulateur » au capitalisme le plus classique et le plus brutal. Les GAFA résistent volontiers à l'Etat central lorsque cela est bien vu. Il y a eu l'exemple d'« Apple contre le FBI » opposant la défenseuse des liberté publiques à l'Etat fouineur qui voulait décrypter l'iPhone du tueur de San Bernardino. Il y a eu aussi Microsoft, qui a récemment condamné les dérives de la reconnaissance faciale et l'utilisation abusive que pourraient en faire les Etats, alors que son propre logiciel a été largement dénoncé pour ses biais racistes (cf. plus bas p. 14). Mais, lorsque cela est nécessaire à leurs affaires, ces entreprises s'adaptent sans broncher aux désirératas étatiques : FB développe p. ex. des moyens de bloquer les messages, en vue de son entrée le marché chinois. Quant à Google, il a annoncé début août 2018 son intention de revenir sur ce marché (qu'il avait quitté en 2010) avec un moteur de recherche filtrant les sites et mots-clef interdits par le gouvernement.

Souvent, les anarcho-libertariens des premières heures se transforment en bons petits soldats du capitalisme oligopolistique et se profilent de plus en plus comme des anarchos-capitalistes qui maximisent leur profit[48]. Comme le résume Morozov : « Ces startups ont beau avoir des allures hippies, les processus sous-jacents n'en restent pas moins tayloristes. »[49] Il est d'ailleurs intéressant de comparer les deux « Déclaration d'indépendance du cyberespace » ; si la première (1996) avait une tonalité très libertaire, la seconde (2018) vise plutôt à mobiliser la résistance citoyenne contre les abus des GAFA.

Fracture numérique (*digital divide*)

Il n'y a actuellement pas d'égalité d'accès aux nouvelles technologies, ni en termes techniques (disponibilité d'un accès performant sur tout le territoire, prestations uniquement disponibles en ligne ou, pis, sur un smartphone récent[50]), ni en termes de ressources financières (la plupart des nouvelles technologies coûtent cher), ni en termes d'éducation tant à l'utilisation qu'aux risques[51]. Or, maîtriser les outils informatiques s'avère de plus en plus indispensable pour participer à la vie sociale, politique, culturelle et économique. Qui n'a pas accès à Internet risque peu à peu d'être exclu de certaines prestations publiques et privées, ou alors de devoir assumer le coût en temps ou en argent d'une prestation délivrée dans le monde « réel » (p. ex. une facture « papier » surtaxée). Le fait de ne pas avoir d'accès à Internet (ou

pas d'accès performant) contribue également à biaiser les bases de données (cf. ci-après p. 13), entraînant ensuite des discriminations supplémentaires envers les victimes de la fracture numérique[52].
Avec la numérisation constante des activités sociales, politiques, culturelles et économiques, cette « fracture numérique » tend à augmenter… comme ses effets négatifs. Par exemple, la participation à l'économie du partage est corrélée avec le niveau de revenu : ce sont les revenus les plus élevés qui sont les plus enclins à y participer, y compris en tant que bénéficiaires, alors que c'est aux revenus les plus bas que ces pratiques devraient avant tout profiter[53]. Cette fracture conditionne aussi l'offre en matière de services en ligne : il y a notamment beaucoup plus d'applications pour trouver des produits de luxe que des biens de consommation courante ou destinés à un public à faible pouvoir d'achat (p. ex. les personnes souffrant d'un handicap)[54].
Un autre type de fracture numérique : celle des genres. Elle notamment est générée par la structure du personnel des GAFA (et de toutes les entreprises et entités actives dans les nouvelles technologies), dont le personnel est composé essentiellement d'hommes. Cela ne fait pas que générer des barrières à l'embauche pour les femmes, mais il en résulte aussi une aggravation des discriminations, en particulier lorsque les algorithmes, programmés par des hommes, ne prennent pas les problèmes rencontrés essentiellement par les femmes au sérieux ou fonctionnent à l'aide de clichés sexistes (cf. les exemples cités ci-après sous « décisions automatisées » p. 14)[55].
La fracture numérique ne concerne pas que les individus : p. ex. seules les communes dotées de certains moyens et d'une certaine taille peuvent sa lancer efficacement dans une démarche de « smart city »… tout en étant à même de négocier d'égal à égal avec le prestataire de service.

Privatisation du droit / Impunité

L'essor des nouvelles technologies peut rendre l'application des lois nationales beaucoup plus difficile en raison des problèmes générés par l'extraterritorialité et les lacunes de l'entraide judiciaire internationale[56]. Ainsi, plusieurs jugements du tribunal fédéral ont empêché l'application du droit suisse, notamment pénal, à des publications de réseaux sociaux, car leurs serveurs et les données de leurs utilisateurs se trouvent dans des pays qui ne collaborent pas avec la Suisse ou dont le droit national empêche l'application du principe de double incrimination[57]. Or, il ne s'agit pas d'arrêter l'auteur d'un délit qui aurait fui le territoire national, mais tout simplement de l'identifier. Et, si cela est impossible, il bénéficie de l'impunité, non pas parce que la Justice ne peut pas l'attraper, mais parce qu'elle ne sait pas qui il est.
L'impunité peut aussi apparaître lorsqu'un comportement, même s'il met en danger certaines personnes, n'est pas punissable et qu'il suffit d'« excuses » pour s'en tirer. Cela peut être par exemple le cas d'une perte de données ou d'une négligence de sécurité informatique, comme lorsque FB a, en juillet 2018, débloqué par erreur des centaines de contacts de son application de messagerie instantanée Messenger, ce qui a permis à des harceleurs de reprendre contact avec leurs victimes[58].
Le poids toujours plus important des GAFA conduit aussi à une privatisation du droit[59] : ces entreprises fixent leurs propres règles et les appliquent, qu'elles soient conformes ou non au droit en vigueur dans le pays où elles déploient leurs activités. Il n'est d'ailleurs pas sûr qu'elles soient conformes à un droit en vigueur quelque part. Par exemple, le Guardian a révélé les directives internes de Facebook en matière de modération des publications. Ces lignes directives prescrivent par exemple l'effacement de publications tout à fait légales en Suisse, tout en empêchant que d'autres, manifestement illégales comme la représentation de

maltraitance d'enfants, soient retirées[60]. Plus récemment, le fondateur de FB Mark Zuckerberg a déclaré que son réseau social ne bloque par exemple pas le négationnisme de l'Holocauste bien que cela soit clairement illégal dans plusieurs pays, arguant que, parce que les négationnistes sont convaincus de leurs théories, il ne s'agit pas de « fake news » ![61]
Cette tendance peut d'ailleurs être aggravée par des règles étatiques comme le *Netzwerkdurchsetzungsgesetz* allemand prescrivant, sous peine de sanctions importantes, de supprimer très rapidement toute publication « manifestement illégale », sans pour autant que l'illégalité de la publication en question ne soit tranchée par une instance judiciaire.
La révolution numérique génère aussi un risque de Justice privée. Cela peut être le cas lorsqu'il n'y a pas de protection contre un déferlement de la vindicte populaire sur les réseaux sociaux sans respect des droits de la défense et avec un fort risque de « mort sociale » (cf. plus bas p. 18) par lynchage numérique. Dans certains cas, on peut même parler d'« armées privées » au service d'entreprise ou de particuliers, prêtes à déferler sur les réseaux pour mener des raids numériques en rétorsion aux critiques[62]. Il y a aussi privatisation de la Justice lorsque des organisations privées à but idéal, qui, même animées de bonnes intentions, ne font pas que critiquer les choix et décisions publiques, mais les mènent des attaques informatiques pour les faire annuler (p.ex. l'attaque de PostFinance par Anonymous en rétorsion contre la suppression du CCP de Julian Assange[63]).

Le poids des GAFA, mais aussi des grandes entreprises en général, accentue le risque de non-respect généralisé du droit, car leur taille et leur richesse rendent d'éventuelles sanctions pénales, administratives et civiles totalement indolores. Le droit suisse qui ne prévoit en effet que très peu d'amendes dont les montants sont dissuasifs[64] et, même lorsqu'ils le sont en théorie (p. ex. les sanctions de l'art. 49a LCart), ils ne font guère peur à ces entreprises aussi richissimes que gigantesques. Notre droit ne prévoit en outre pas d'action de groupe (*class action*) permettant aux personnes lésées d'intenter action, ce qui, en raison du faible montant du dommage subi par chaque personne n'aurait pratiquement aucun sens à titre individuel.
Cela dit, malgré l'absence de sanctions réellement dissuasive ou la possibilité de se soustraire à l'application du droit suisse pour des raisons d'extraterritorialité, les GAFA ont plutôt tendance à respecter les décisions de justice entrées en force, comme ce fut notamment le cas pour l'arrêt du TF « Google street view ».

Libertés individuelle et publiques

Un contrôle total de nos existences par les GAFA ?

L'essor des nouvelles technologies pourrait conduire à un abandon progressif, inconscient et passif des libertés. Les GAFA prennent petit à petit le contrôle de nombreux aspects de nos vies, voire de la totalité d'entre eux. Kerdellant dit à propos de Google : « Le moteur n'invente rien, ne nous "vole" rien, il se contente de collecter et de donner du sens à tout ce qu'il a récolté sur toutes les sources à sa disposition : le contenu de nos mails pour ceux qui ont une boîte Gmail (Google assure ne plus lire ces contenus), nos recherches sur le moteur, notre historique de navigation (Google Chrome), les images (Google Photos), notre goût pour certains types de vidéos, l'heure de notre réveil ou l'actualisation de notre profil Facebook (avec Android sur le smartphone), nos déplacements (Google Maps – ndla : désormais payant pour les entreprises et institutions !!!), notre emploi du temps (Google Now), le contenu des fichiers partagés (Google Docs), nos notes (Google Drive), nos achats (Android Pay). Chaque nouveau service accroît sa connaissance intime qu'il a de chacun de nous puisque sa mémoire est infinie ». Et Google (par la voix de son CEO Eric Schmidt, Berlin 2010) ne dément pas : « Nous savons où vous êtes, nous savons où vous étiez, nous savons plus ou moins ce que vous pensez. ».

Il n'est enfin pas inutile de rappeler que l'usage liberticide des nouvelles technologies n'est pas l'apanage des entreprises privées et peut aussi grandement faciliter la surveillance de masse par les Etats, légale comme illégale, en particulier par les services de renseignement. Les nouvelles technologies permettent aussi aux Etats répressifs non seulement de mieux contrôler leur population, mais aussi d'en influencer, voire d'en dicter le comportement, à l'instar du système de notation du « comportement social » des citoyens en République Populaire de Chine.

De l'incitation à l'obligation

Certes, personne n'est obligé d'utiliser les nouvelles technologies, ni de les utiliser toutes. Cependant, leur diffusion extrêmement large, pour ne pas dire universelle, risque, à terme, de générer une obligation de fait de les adopter… et de s'y soumettre. Cela commence par des incitations et des rabais (rabais de prime LAMAL en cas d'utilisation du QS, rabais d'assurance auto en cas d'utilisation de *dashcam*), puis suivent les injonctions, par exemple de l'employeur (obligation de suivre un programme interne de santé avec QS), puis une obligation de fait, quand le rabais pour les premiers clients à adopter une technologie se transforme en malus pour ceux qui la refusent[65].
Par ailleurs, l'emploi de nouvelles technologies par les pouvoirs publics peut conduire à imposer certains comportement, voire à la création de nouvelles normes sociales[66] auxquelles les algorithmes forcent les gens à se conformer : cela va de l'obligation absolue du respect d'une norme légale (au demeurant utile) quand un véhicule « intelligent » refuse de démarrer si le conducteur n'a pas bouclé sa ceinture à l'obligation de fait d'adopter un certain comportement pour ne pas paraître « suspect », par exemple lorsque c'est un algorithme qui « détecte » les « comportement suspects » des passagers d'un aéroport en analysant les images de vidéosurveillance[67], forçant ces derniers, sans que cela ne soit prescrit nulle part, à marcher calmement, à ne pas faire de mouvement brusques, à suivre des trajectoires prévisibles, etc. Cette dictature des algorithmes peut, via la multiplication des objets connectés, se manifester sous diverses formes : de la ceinture connectée « Belty » qui oblige à être plus actif (p. ex. à monter plus d'escaliers), au préservatif « i.Con » qui décortique toutes les données d'un rapport sexuel, en passant par le miroir connecté « HiMirror » qui analyse les rides. Certes, la plupart, prêtent pour l'instant, à sourire… jusqu'à ce que leur diffusion ne finisse par créer de nouvelles normes sociales appliquées à large échelle.
Enfin, à l'heure du big data qui permet de catégoriser tout un chacun en fonction de n'importe quel critère, il devient de plus en plus difficile de parler de responsabilité individuelle[68].

La fin de la responsabilité ?

Mais la liberté individuelle n'est pas seulement menacée par ce qui l'entrave, elle l'est aussi par la disparition progressive de son pendant : la responsabilité (en tout cas civile). En effet, de nombreuses tendances issues de la révolution numérique tendent à supprimer totalement la responsabilité. Or, la responsabilité en cas d'action illicite est le pendant inaliénable de la liberté personnelle. Assumer les dégâts que l'on cause aux biens juridiques d'autrui et le revers de la médaille et le complément indispensable de la liberté. C'est aussi un instrument indispensable pour garantir la paix sociale[69].
Or, quand c'est un algorithme qui décide, la responsabilité disparaît[70]. C'est aussi le cas lorsque personne ne veut assumer de responsabilité, par exemple dans le cas d'une plate-forme comme Uber qui se considère comme un « simple intermédiaire » entre le client et le prestataire de service (ainsi que d'éventuels tiers) et ne veut rien savoir de ce qui peut arriver à l'un ou à l'autre en raison d'une faute imputable à l'un ou à l'autre[71]. C'est aussi le cas lorsqu'il est impossible de contacter une entreprise fournissant un service qui génère

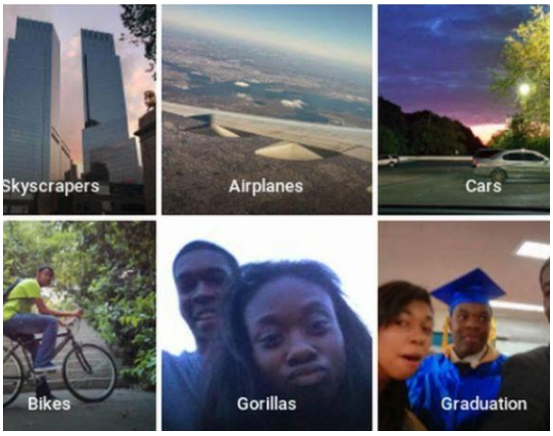
d'importantes nuisances imprévues (comme un service de GPS qui guide le flot du trafic dans une zone résidentielle parce que c'est un raccourci). Cela peut être aussi le cas lorsqu'un dégât est causé par un robot dont l'IA est capable d'apprendre, faute qu'il est difficile d'attribuer à une personne physique ou morale susceptible de la réparer, parce que le fabricant considère que l'action qui a causé le dommage n'était pas prévue dans la programmation initiale de l'IA et parce que l'utilisateur du robot argue que c'était au fabricant de programmer l'IA pour que le dommage ne survienne pas.
Même s'il ne s'agit pas forcément d'un abandon des libertés individuelles et collectives, confier une partie de plus en plus importante de notre existence aux nouvelles technologies pour se faciliter la vie pourrait avoir plus d'effets négatifs qu'espéré, notamment sur nos capacités à choisir nous-même notre mode de vie et à faire nos propres choix[72]. Selon Nicholas Carr[73], essayiste spécialisé en nouvelles technologies, « L'hypertechnologie appauvrit nos vies, car elle nous pousse à négliger nos propres talents et compétences ». Carr dénonce carrément un risque de perte de capacité à émettre des jugements moraux.
Sans en arriver à cette conclusion, il est toutefois clair que le recours généralisé à la technologie peut aussi rendre la vie plus risquée : lors du crash Air France en 2009, le pilote automatique a planté et les pilotes n'ont pas pu rétablir la situation manuellement. Celui qui suit aveuglément la technologie, en particulier les algorithmes, que ce soit par routine, par confort ou par souci d'efficacité, finit par perdre son autonomie : Par exemple, un patient d'Ebola est décédé en octobre 2014 à Dallas à la suite à des erreurs de diagnostic et de questions pas ou mal posées par le personnel soignant qui « suivait la procédure »[74]. Cela dit, ce risque n'est pas forcément lié à la révolution numérique, mais existe aussi avec tout algorithme non numérique comme les formulaires, check-lists et autres recettes.

Décisions automatisées

Un des risques les plus important en matière de liberté personnelle repose sur l'essor des décisions automatisées étatiques ou privées. Les algorithmes commencent à « aider » les décideurs à prendre de plus en plus de décisions, voire les prennent à leur place. Or, nous ne sommes pas égaux devant les algorithmes et cette partialité a de réelles conséquences sur nos vies[75]. En outre, un « décideur » qui suit aveuglément les « recommandations » de l'algorithme ne décide pas, il obéit[76].
Parmi les exemples les plus frappants, on trouve les logiciels de « police prédictive » comme PRECOBS[77], déjà utilisés notamment dans les cantons d'Argovie et de Bâle-campagne, ainsi qu'en ville de Zurich. Fantasmés dans la science-fiction comme dans la nouvelle de Philip K. Dick « The Minority Report » (1956), ils « prédisent » où et quand auront lieu certains délits, notamment des cambriolages, permettant aux forces de l'ordre d'intervenir à temps, parfois de manière préventive. Par ailleurs, si l'IA peut être utilisée par les forces de l'ordre, les criminels s'en servent également pour identifier, surveiller, profiler voire mettre en confiance leurs proies[78].
Le fiasco du logiciel d'attribution des places de formation universitaire « parcoursup » en France (dont le code source est pourtant en grande partie public) montre bien les risques de confier aux algorithmes le soin de prendre des décisions à la place des humains, même si c'est pour gagner en efficacité ou en « objectivité » (cf. à ce sujet ci-après p. 18). La fiabilité attendue n'est pas au rendez-vous : la moitié des candidats n'a pas eu de place d'université lors de la première ronde de sélection (alors que le tirage au sort du système précédent – qui était certes loin d'être parfait[79] – n'écartait… que 1% des candidats). Par ailleurs, l'algorithme semble reproduire les discriminations, car les élèves des établissements les moins bien notés (notamment ceux des quartiers dits « difficiles ») ont plus de problème à trouver une place,

même avec d'excellentes notes[80]. Cela semble se vérifier au niveau de l'attribution des bourses d'étude[81].
« Parcoursup » n'est d'ailleurs pas, et de loin, le seul exemple de discrimination engendrée par les décisions automatisées. En voici quelques autres :

- En raison du racisme ambiant, les chauffeurs noirs sont moins bien notés par Uber, donc reçoivent moins de courses. Le même effet se vérifie chez AirBnB, qui conseille de mettre sa photo sur le profil de l'appartement que l'on souhaite louer. Conséquence : en ville de New York, les non-afro-américains peuvent exiger de leurs hôtes un loyer 12% plus cher.
- Un filtre de sélection des candidats d'une entreprise dont le personnel est surtout composé d'hommes blancs titulaires de MBA ne sélectionnera que ces profils, aggravant les discriminations. On a vu également des annonces google d'offres d'emplois proposés aux femmes… moins bien payés[82].
- Les logiciels utilisés aux USA qui prédisent la récidive (dont certains, comme ROS, sont utilisés en Suisse[83]) pénale désavantagent les minorités ethniques, car, plus pauvres, elles sont plus concernés par la criminalité.
- Siri (Apple), programmé essentiellement pas des personnes de sexe masculin, se moque d'une femme victime de viol qui demande que faire et où trouver de l'aide[84].
- Le moteur de recherche de Google regorge de clichés sexistes, par exemple quand il ne montre que des images de femmes pour une recherche portant sur des emplois peu prestigieux ou suggère un partage des tâches relevant d'un modèle patriarcal quand on fait une recherche « les femmes devraient… »[85].
- Les logiciels de traitement de photo comme FaceApp ou Google Photo qui classent les photos de personnes noires comme « gorilles » ou qui blanchissent la peau pour que la personne en question ait l'air « sexy »[86].
- Le logiciel de reconnaissance faciale de Microsoft « Face API » a dû être corrigé (avec succès selon son éditeur) après que plus de 93% des erreurs concernaient des visages de couleur sombre, en raison d'une base de données de programmation contenant surtout des hommes blancs[87].
- Streetbump (utilisé par la ville de Boston) : les données GPS permettent de déterminer si les trottoirs sont abîmés parce que les gens trébuchent. Mais comme les moins riches ont moins de smartphones et de connexions, les trottoirs de leurs quartiers sont moins souvent réparés…



Une décision d'algorithmes repose en effet toujours sur des données, lesquelles ne sont jamais ni neutres, ni objectives. Les données de programmation sont au contraire toujours biaisées,

car ce sont des constructions sociales et historiques[88]. Ce sont le résultat de jugements collectifs préconçus. Elles dépendent aussi de la localisation des capteurs. Les décisions automatisées entraînent donc un fort risque de « contagion » : p. ex., parce que de nombreux habitants de votre quartier sont de mauvais payeurs, vous serez aussi considéré comme tel par l'algorithme qui fait la corrélation « lieu d'habitation – solvabilité »[89].
Par ailleurs, ce qui intéresse cette nouvelle rationalité algorithmique, c'est de nous connaître jusque dans les moindres détails, sans avoir à nous entendre au préalable, les motivations et justifications des individus n'important plus du tout[90].

Sphère privée / protection des données personnelles

La révolution numérique, en particulier le *big data* engendre des risques aussi évidents que connus pour la sphère privée. Les autorités en prennent petit à petit la mesure, même si le retard est colossal. Villani affirme par exemple (et probablement a-t-il raison) que, si le RGPD européen avait existé il y a 20 ans, les GAFA n'auraient pas pu pénétrer le marché européen aussi facilement et la concurrence aurait été plus saine[91]. Cela dit, la protection des données n'est pas une mesure antitrust contre les GAFA, c'est un moyen de sauvegarder les libertés publiques. La « valeur ajoutée » du droit à la protection des données par rapport à la protection de la vie privée est précisément d'avoir parmi ses objectifs de réduire les asymétries de pouvoir et d'information entre les utilisateurs des services et ceux qui collectent les données[92].
Même si la sensibilisation des collectivités publiques, entreprises et particulier progresse (lentement), les comportements propres à violer la protection des données sont encore nombreux, même quand ils sont le fait de responsables de traitement prudents et consciencieux. Ainsi, le risque de ré-identification par croisement de données anonymes est largement sous-estimé, alors que de nombreux fichiers censés être anonymes et dont les données ont été récoltées dans un but d'intérêt public (p. ex. recherche scientifique) ne protègent pas du tout la personnalité des personnes qui ont fourni les données[93]. Par exemple, trois mois de transactions effectuées par 1,1 million d'utilisateurs « anonymisés » de cartes de crédit permet d'en identifier 90% grâce à seulement 4 données spatiotemporelles[94]. Et, dans tous les cas, l'anonymat en ligne ne permet pas d'éviter la caractérisation des comportements des individus, ni l'analyse prédictive de ces comportements[95].
Un risque important généré par la révolution numérique se cache derrière le « je n'ai rien à cacher », argument dont se sert une part importante de la population (l'auteur du présent document y compris) pour prendre à la légère la protection de ses données personnelles. En effet, dans un monde où le seul moyen d'obtenir des données sensibles (p. ex. les opinions politiques ou religieuses, l'état de santé, etc.) est que ces données aient été explicitement transmises, on peut légitimement prétendre que, tant qu'on ne livre pas de détails intimes, personne ne peut les connaître. Mais cet ancien Monde n'existe plus. A l'heure du « big data », où il est possible d'élaborer des profils de personnalités extrêmement détaillés à l'aide de données en soi anodines (p. ex. une statistique d'achat), nul ne peut plus prétendre que des tiers ne détiennent pas ses données sensibles[96]. En outre, tant que l'on ne sait pas ce que cherche celui ou celle qui cherche, impossible de prétendre que l'on a « rien à cacher », car c'est uniquement du point de vue de celui qui cherche que l'on peut déterminer ce que l'on devrait « cacher ». Cette tendance peut aussi mener à une suppression du droit à la sphère privée, lequel est jugé inutile par certains, étant donné que « quiconque raconte sa vie sur les réseaux sociaux n'a de facto plus de vie privée ». Or, le droit à la sphère privée n'inclut pas seulement le droit de rester caché, mais aussi celui de l'autodétermination en matière d'information (cf. plus bas p. 29), à savoir le droit de choisir ce qui est rendu public (ce que

fait – même si c'est parfois avec peu de discernement – celui qui choisit de dévoiler certains détails intimes sur le net).
D'une manière générale, la révolution numérique risque de faire de la sphère privée un droit que l'on doit acquérir ou « que l'on peut se payer »[97]. Selon le futurologue Gerd Leonhard « être hors-ligne devient un luxe accessible à moins de 1% de la population. »[98]

Environnement / Energie

Certaines analyses prédisent que, d'ici 2040, la demande en capacité de stockage pourrait dépasser la production disponible globale de silicium. La consommation d'énergie du numérique augmente fortement et sa part à la création de gaz à effet de serre aussi[99]. « Selon Alex Wissner-Gross, physicien à l'Université de Harvard, deux requêtes sur Google consommeraient autant de carbone qu'une tasse de thé bien chaud. Selon les travaux de ce scientifique, deux requêtes sur Google généreraient 14 grammes d'émission de carbone, soit quasiment l'empreinte d'une bouilloire électrique (15 g). (…) Selon un récent rapport du cabinet d'analyse Gartner, l'industrie informatique génère à elle seule 2 % des émissions de gaz à effet de serre, devant l'industrie aéronautique. Le simple fait d'utiliser un ordinateur consomme entre 40 g et 80 g de carbone par heure, explique John Buckley, directeur de carbonfootprint, un cabinet d'expertise environnementale britannique. La consultation d'une simple page Web consommerait à elle seule environ 0,02 gramme de carbone par seconde, le chiffre étant multiplié par 10 pour une page enrichie d'images complexes ou de vidéos (0,2 gramme). Plus surprenant : maintenir en vie un avatar dans le jeu de réalité virtuelle Second Life pendant un an consommerait autant d'énergie qu'un Brésilien moyen, soit 1 752 kilowatts-heure. »[100]. Autre exemple, les cryptomonnaies : l'Islande a, « grâce » à son climat frais (ce qui permet de refroidir les serveurs à moindre coût) et son prix de l'énergie très bas, attiré en grand nombre les « mineurs » de bitcoin. Or, en 2018, la consommation énergétique du minage dépassera celle de tous les ménages de ce pays. En outre, ces activités n'ont généré pratiquement aucun emploi ni rentrée fiscale[101].
La multiplication des canaux de communications (m2m, internet des objets) risque de conduire à la saturation des infrastructures (sans et avec fil), ou à leur multiplication. Selon Bradley et al., en 2050, il y aura 50 milliards d'objets connectés, il faudra donc multiplier les antennes, notamment pour introduire de nouvelles technologies de transmission : comme il faut transférer moins d'informations, beaucoup de communications entre objets n'ont pas besoin de canaux aussi performants que p. ex. la 4G. Le même raisonnement vaut pour les nouveaux services en ligne gourmands en capacité de transfert de données : Par exemple, aux USA, Netflix utilise un tiers de la bande passante aux heures de pointe !
Enfin, les progrès en matière de gestion du trafic routier attendus de l'introduction généralisée des véhicules autonomes pourraient paradoxalement mener à une augmentation du trafic, parce que des utilisateurs renonceraient aux transports publics pour leur préférer des voitures individuelles robotisées[102].

Economie/Consommation

Concentration des acteurs

Bien qu'elles se disent libérales et attachées à une économie de marché, le but des GAFA n'en est pas moins de créer des oligopoles, voire des monopoles[103]. C'est en tout cas l'avis d'un des dirigeants de ces entreprises, Peter Thiel, créateur de PayPal. Ces énormes entreprises bénéficient tout d'abord de leur taille (et de la taille de leur réserve de liquidités), qui leur permet de racheter sans problème des concurrents plus innovants, établis (comme whatsapp ou instagram rachetés par FB) ou en train de percer, afin de tuer dans l'œuf toute

concurrence. Plus une entreprise est grosse, plus elle peut investir pour améliorer ses algorithmes et instaurer de nouveaux services afin d'entrer en force dans d'autres domaines et y étendre son monopole. Google planche p. ex. sur le service public de l'emploi – Google for jobs, la santé – intégration des logiciels dans un robot opératoire Johnson & Johnson – la recherche sur Alzeihmer, l'optique – lentilles de contact connectées et intelligentes, le matériel de guerre – drones de combat… Situation comparable (bien qu'à moins échelle) : Swisscom qui, collabore au « service public » en proposant des solutions de *smart cities* aux communes… et en profite pour collecter des données pour son propre compte.
Ces entreprises bénéficient aussi des « effets des réseaux » : pour celui qui a déjà beaucoup de clients et une taille critique, il est très rentable de lancer un nouveau service (quitte à racheter les prestataires émergents)[104]. Ces effets de réseaux accentuent encore l'effet de la « prime au vainqueur » (*the winner takes it all*) : la technologie qui s'impose sur le marché devient le marché, excluant toute concurrence[105]. Cette tendance est aussi renforcée par ce que Villani appelle l'API-sation de l'économie, c'est-à-dire la possibilité d'innover sur la base des interfaces mises à dispositions par les plateformes, ce qui renforce encore le pouvoir de ces dernières, alors que ce sont des développeurs de services externes qui investissent, tout en restant captifs[106].
Une autre conséquence de cette concentration est que d'autres prestataires de service deviennent rapidement dépendant des services des géants du net : booking.com/tripadvisor, etc. pour les hôtels, facebook/twitter pour les médias, ce qui leur permet d'étendre leurs monopoles à de nouvelles branches, sans toutefois y avoir investi un centime. Ces situations de monopoles peuvent avoir des effets désastreux sur toute une branche, en témoigne le changement d'algorithme de FB pour privilégier les publications des « amis » au détriment de celles des médias, ce qui a mis en difficultés plusieurs « *pure players* » (ex. : brut.fr), qui ne sont pas tous des « putaclics » (comme buzzfeed France), qui sont désormais moins visibles et donc moins partagés[107]. Les effets désastreux se manifestent aussi lorsque la plateforme abuse de sa position dominante pour imposer des clauses contractuelles léonines, comme booking.com qui interdit à ses clients captifs de proposer des prix plus bas à leurs clients directs.
Il faut enfin relever que la concentration des acteurs n'est pas que le fait des entreprises : Ainsi, moins de 20 « mineurs » contrôlent désormais le *blockchain* du bictoin[108]… une cryptomonnaie qui se voulait pourtant libre (si ce n'est libertaire) et décentralisée… AirBnB, à ses débuts un des chantres de la véritable économie du partage, n'échappe pas non plus à la concentration du marché : En Suisse, les professionnels de l'hébergement proposant plus de dix objets à louer proposent déjà 19% des locations (contre 5% en 2015) et le plus gros acteurs gère… 184 logements[109]. Nous sommes donc bien loin des particuliers qui se rendent service !

Concurrence déloyale

Il est de notoriété publique que la révolution numérique facilite la concurrence déloyale lorsque de nouveaux acteurs « disruptifs » entrent en force sur un marché en basant leur modèle d'affaire sur le non-respect total ou partiel des règles auxquelles sont assujettis leurs concurrents (p. ex. Uber et le droit du travail, des assurances sociales ainsi que les règles en matière de transports de personnes). Un des slogans en vogue dans la Silicon Valley est d'ailleurs : « *move fast and break things* ». Si cette tendance n'est pas nouvelle en soi, elle a ceci de dangereux que, contrairement à la sous-enchère « classique », elle est vue d'un bon œil par la droite et les milieux patronaux ; certains sont aveuglés par le côté « disruptif-nouvelle économie innovante 4.0-qui-va-changer-le-monde », d'autres y voient une opportunité de faire (enfin) passer des propositions radicales de démantèlement social (cf. p. 8). Les GAFA et autres géants du net profitent aussi de leur taille et de leur pouvoir financier

pour s'établir sur un marché en subventionnant leurs propres prestations (p. ex. Amazon qui livre gratuitement lors de son entrée sur un marché), ou en les proposant à perte le temps d'étouffer la concurrence (Uber, qui n'est toujours pas rentable).
Mais la concurrence déloyale peut prendre d'autres formes, que la numérisation de l'économie facilite grandement. Il y a p. ex. le « *review bombing* » (ou la simple menace de le déclencher), à savoir le bombardement d'évaluations négatives sur les réseaux sociaux ou les sites spécialisés[110]. Toutefois, les évaluations en en ligne représentent plutôt une chance pour les commerces et les consommateurs : les études tendent à montrer qu'il y a plus de commentaires positifs que négatifs[111]. Le bon fonctionnement des marchés peut enfin être perturbé par l'émergence de profils de solvabilité bidons, qui causent un tort considérable aux personnes faussement considérées comme insolvables… ainsi qu'à leur partenaires commerciaux potentiels qui risquent de rater des opportunités sur la base d'informations farfelues[112].
Par ailleurs, vue l'ampleur que prennent les conditions générales d'utilisation de la plupart des services en ligne, on peut de moins en moins parler de marchés libres où preneurs et prestataires de services négocient d'égal à égal. Quiconque veut recourir aux principaux services en ligne n'a pas d'autres choix que d'abandonner bon nombre de ses libertés en acceptant des conditions générales léonines sans avoir le temps d'en lire les milliers de pages, et sans bénéficier de la moindre alternative, car, en raison des monopoles des géants du Net, il n'y en a souvent pas. Et même lorsqu'il y a un concurrent, il exige lui aussi l'approbation de conditions générales similaires.
Enfin, la révolution numérique pourrait favoriser l'émergence de cartels contre lesquels la législation actuelle serait impuissante, grâce à l'usage d'algorithmes créant un parallélisme des prix qui n'a été concerté par personne[113].

Nouveaux risques de spéculation

Enfin, comme à chaque fois que des nouveaux produits très demandés sont mis sur le marché, la révolution numérique est susceptible de générer des bulles spéculatives : noms de domaines, cryptomonnaies, etc. Cela est d'autant plus inquiétant que les entreprises technologiques étatsuniennes des années 2010 partagent avec celles qui spéculaient sur l'immobilier dans les années 2000 le fait d'essayer de créer de la richesse en comptant sur la valorisation de leurs actifs, alors même que l'économie dite « réelle » battait de l'aile[114].

Santé et sécurité individuelle et publique

En plus des risques déjà connus (et abondamment décrits !) causé par l'hyperconnectivité et la disponibilité permanente, il est malheureusement clair que la révolution numérique ne sera pas sans conséquences sur la santé publique. Par exemple, aux USA, le taux de dépression et de suicides a augmenté, essentiellement à cause des réseaux sociaux[115].
Au-delà des problèmes individuels de santé, curables ou non, l'essor des nouvelles technologies, en particulier des réseaux sociaux fait peser un nouveau risque : celui de la « mort sociale », à savoir le fait de voir sa réputation réduite durablement à néant en quelques heures par la diffusion inarrêtable d'informations, d'images ou de citations (ainsi que de leurs commentaires par les internautes), véridiques ou non, mais qui deviennent ineffaçables et vont souvent s'amplifiant[116]. Ce phénomène de « mort sociale » (qui peut mener à la mort tout court)[117] peut aussi être causé par une « attaque » (ou une grave négligence comme le montre la navrante histoire #PlaneBae[118]), coordonnée ou pas, à coup d'insultes et de menaces rendant impossible l'utilisation d'un réseau social, mais se répercutant aussi sur la vie réelle lorsqu'adresse, noms des conjoints et des enfants et autres informations personnelles sont

diffusées à des fins de nuire[119]. Pour les centaines, voire les milliers d'auteurs ayant lancé, inspiré ou relayé ces attaques, l'impunité est souvent totale en raison de l'impossibilité pratique de les identifier, puis de les poursuivre. Cette certitude de ne pas être inquiété pousse bon nombre de ces auteurs à agir à visage découvert, ce qui soit dit en passant infirme l'avis fréquemment émis comme quoi « sur Internet, les gens se lâchent parce qu'ils peuvent rester anonyme »...
En plus des risques individuels de santé et de sécurité, la numérisation croissante des infrastructures publiques et privées génère un risque quasi-systémique en cas de défaillance des réseaux, en particulier pour les infrastructures publiques considérées comme critiques (énergie, santé, communications)[120].

« *Data-driven policy* » : la dictature des données (et de leurs experts)

L'essor des nouvelles technologies, en particulier du big data, augmente le poids des données en tant que justificatifs des politiques publiques. Certains rêvent d'une société post-actuarielle, post-assurancielle où le risque doit disparaître, car il tout a été calculé, prévu[121]. D'autres croient à la fin des controverses scientifiques, tout pouvant être prouvé, démontré[122]. Or, tout n'est pas numérisable (p. ex. l'épuisement des ressources, les rêves, les utopies, les idéologies, l'art, la culture). On confère une « rationalité immanente » aux données issue du big data ; mais la rationalité, fut-elle immanente, n'est pas la vérité. Par ailleurs tous les jeux de données comportent des erreurs (et des biais, cf. plus haut p. 13 à propos de la discrimination) ; aucun n'est objectif, ni exhaustif[123]. Décider en fonction des données, c'est prétendre décider objectivement, mais ce n'est pas la Justice qui, elle, demande que l'on tienne compte des faits et du contexte[124]. Une décision est juste non pas parce qu'elle suit le calcul, mais parce que celui qui la prend peu se justifier et adhérer à sa décision.
Par ailleurs, indépendamment de la qualité des données utilisées, les erreurs de programmation sont nombreuses : en moyenne, sur 1000 lignes de code, il y a 50 erreurs. Et, une fois que le programmeur originel n'est plus là, il y a un très fort risque que plus personne ne maîtrise rien[125]. Certains programmeurs spécialisés en IA vont d'ailleurs jusqu'à considérer les algorithmes apprenants comme de l'« alchimie »[126]. Fonder l'action publique sur les données et les algorithmes n'est donc pas un moyen vers des décision publiques plus « justes » (quel que soit le sens que l'on donne à ce terme).

Un Etat impuissant et indigne de confiance ?

La révolution numérique comporte un risque majeur d'un point de vue des socialistes, qui défendent depuis toujours un Etat fort et des solutions collectives et démocratiques : la perte de confiance dans l'Etat et dans sa capacité à protéger (contre les cyberrisques, le cyberharcèlement de masse, la « mort sociale », etc.), à fixer souverainement son propre droit et à le faire appliquer, mais aussi fournir les prestations et infrastructures de base, notamment en matière d'accès et de formation aux nouvelles technologies. Par exemple, en ville de New York, il y a tant d'annonces d'AirBnB qui violent l'interdiction de louer un logement pour plus de 30 jours qu'il est impossible de faire appliquer la loi[127]. Et, face à la montée en puissance des GAFA, la capacité des pouvoirs publics à garantir la cohésion sociale s'en trouve limitée. Certains promoteurs des nouvelles technologies d'obédience libertaire veulent enfin supprimer certaines prérogatives de l'Etat pourtant considérées comme « régaliennes » p. ex. le contrôle la légalité des transactions immobilières à confier à un système de blockchain[128].
L'Etat risque par ailleurs de ne plus être en mesure de protéger les libertés fondamentales (y compris économiques, y compris des libertés fondamentales qui ne sont pas reconnues en tant que telle aujourd'hui dans la Constitution fédérale comme le travail décent ou le droit à la

sécurité sociale), dont le contenu risque d'ailleurs d'être vidé de sa substance, voire dicté par des entreprises privées. La participation à la vie numérique, donc, en grande partie, à la vie sociale toute court, nécessite de plus en plus de se soumettre aux règles fixées par les prestataires de services privés, ce qui signifie bien souvent abandonner sa liberté individuelle et renoncer à bon nombre de ses droits fondamentaux via des conditions générales que personne n'est en mesure de refuser (ni même de lire, d'ailleurs). Les réseaux ne peuvent en effet pas s'encombrer d'une multitude d'accords individuels ; ils font donc tout pour obtenir un accord global de faire ce qu'ils veulent (si besoin par le biais de « nudges »), indépendamment des bases légales. Le seul « oui, j'accepte » se fait en réalité au moment du premier choix (pour autant qu'il s'agisse d'un vrai choix, cf. plus haut p. 15) : « est-ce que je veux une vie digitale ou pas ? »[129]. Ensuite, il ne peut en général plus être fait, notamment en raison de l'effet de « lock-in » : en l'absence d'un droit à la portabilité des données, on ne change plus de prestataire une fois qu'on a toute ses données chez lui et que tous les services que l'on utilise au quotidien sont imbriqués les uns dans les autres (et deviennent inutilisables les uns sans les autres) ! L'accord peut aussi être extorqué et l'autodétermination réduite à néant : Par exemple, même celui qui refuse de donner ses données pour une statistique fait finalement tout de même partie de la statistique[130].

L'humanité reléguée au second rang ?

(Le Chat, © Ph. Geluck, 1986)

Une analyse sur les risques de la révolution numérique se doit d'aborder, ne serait-ce que brièvement, le « risque philosophique » posé par la « singularité », c'est-à-dire le moment où les IA dépasseront les intelligences humaines. Par exemple, en 2004, Larry Page prédisait : « Google sera inclus dans le cerveau des gens. Ils auront un implant, et quand ils penseront à quelque chose, Google leur donnera automatiquement la réponse. »[131]. Il faut dire que les GAFA sont, en tout cas pour l'avis de certains, animés par une idéologie de la prééminence de la technologie sur l'homme[132].

La crainte de la singularité est à notre avis infondée. Les IA battent certes les humains aux échecs depuis les années 1980… mais sont encore incapables de manipuler correctement les pièces de ce jeu, activité pourtant à la portée des enfants humains âgés de quelques années ! Quoi qu'il en soit, le Monde n'est pas modélisable, ni calculable en totalité. Comme le dit très justement Ito, développer la puissance de calcul ne nous rend pas plus intelligents, mais seulement capable de faire de meilleurs calculs. Il convient donc plutôt d'envisager les IA non pas en tant que concurrentes ou que remplaçantes, mais en tant que complément de l'intelligence humaine[133].
Enfin, quels que soient les progrès technologiques, certaines capacités humaines ne seront probablement jamais transférables à des machines ou à des IA, qui ne peuvent p. ex. pas reproduire la maladresse, l'imprévisibilité, l'instinct, l'intuition, le biomimétisme[134], l'empathie ou les émotions.

5. Propositions : adapter les droits fondamentaux à la révolution numérique

Introduction

Depuis toujours les socialistes défendent les droits fondamentaux. Ils ont toujours été du côté des bénéficiaires des libertés fondamentales et ont toujours été en première ligne pour qu'elles s'appliquent de manière universelle, mais aussi pour en instaurer de nouvelles partout où cela a été nécessaire. Comme la révolution numérique apporte de grandes chances, mais aussi de grands risques pour la population, renforcer les droits fondamentaux permet aux individus de profiter des chances tout en se protégeant là où apparaissent les risques. Chacun a le choix d'utiliser ou non les chances de la révolution numérique s'il le juge utile, tout en se sachant protégé si cette utilisation génère des risques.
Nous avons choisi de sélectionner quelques-uns des principaux droits fondamentaux ancrés dans la Constitution fédérale. Notre approche n'est pas juridique, mais politique : nous tenons donc compte des droits fondamentaux donnant droit à des prétentions juridiques, mais aussi du but que se donne la Confédération (art. 2 Cst.) et des buts sociaux (art. 41), qui ne sont pas justiciables. Notre but n'est pas de forcément compléter ces droits ou d'en créer de nouveaux, mais d'examiner là où leur interprétation ou leur traduction dans la législation doivent être précisées. Nous avons aussi examiné quelques tâches centrales de l'Etat, qui, sans être de véritables droits fondamentaux comme la définition de l'identité ou le service public, sont particulièrement concernées par la révolution numérique.

Une charte ou un nouveau préambule à la Constitution fédérale ?

Plusieurs Etats réfléchissent au moyen d'ancrer les nouveaux droits fondamentaux rendus nécessaires par la révolution numérique dans leur constitution. En Allemagne, le ministre Heiko Maas (SPD) a, suite à une proposition de Martin Schulz (alors candidat à la Chencellerie), esquissé un projet de « Charte de l'Internet : nos droits fondamentaux digitaux ». En France, les membres de la mission parlementaire Fortezza/Frassa propose de compléter la Constitution avec une charte en préambule. Celle-ci ne créera pas de nouveaux droits en tant que tels, mais entend consolider quelques grands principes en les fixant dans le texte suprême. Ces droits et libertés, garantis à divers niveaux, pourront ainsi faire l'objet d'un contrôle de constitutionnalité[135]. Ces deux projets de chartes contiennent notamment ces droits :

- Droit d'accès égal et sans discrimination
- Neutralité du net
- Développement des réseaux dans l'intérêt collectif
- Le numérique facilite la participation à la vie publique et le débat public
- Droit d'accès aux informations utiles à un débat d'intérêt public
- Protection des données personnelles et autodétermination en matière d'information
- Droit à l'éducation et à la formation au numérique
- Droit de ne pas être soumis aux algorithmes
- Droit à un travail décent, aussi en ligne
- Mêmes droits en ligne que dans le Monde « réel »
- Droit à une vie « hors-ligne », dans le Monde « analogique »
- Interdiction des abus de monopoles et de position dominante
- Injonction aux Etats de créer un droit international de l'Internet

Le concept français de charte constitutionnelle (comme la Charte de l'environnement adoptée en 2004) est toutefois étranger au droit constitutionnel suisse, ainsi qui ne connaît pas non plus de juridiction constitutionnelle comparable à la France ou à l'Allemagne. Ces projets sont néanmoins très utiles pour définir quels sont les compléments qu'il est nécessaire d'introduire à notre arsenal de droits fondamentaux.

Art. 2 Cst. But de la Confédération

[1] La Confédération suisse protège la liberté et les droits du peuple et elle assure l'indépendance et la sécurité du pays.
[2] Elle favorise la prospérité commune, le développement durable, la cohésion interne et la diversité culturelle du pays.
[3] Elle veille à garantir une égalité des chances aussi grande que possible.
[4] Elle s'engage en faveur de la conservation durable des ressources naturelles et en faveur d'un ordre international juste et pacifique.

L'art. 2 Cst. n'a pas besoin d'être complété ou modifié en raison de la révolution numérique. Mais cette dernière doit conduire à de nouvelles interprétations tenant compte des risques qu'elle génère.
Ainsi, la Suisse ne doit pas devenir ou rester une « colonie numérique »[136]. Notre pays doit affirmer sa souveraineté sur Internet en appliquant le principe suivant : toute activité en ligne qui a un résultat ou un impact en Suisse est soumis au droit suisse, peu importe où se trouve l'auteur, l'entreprise qui a fourni le ou les services (y compris si c'est une plate-forme mettant en relation fournisseur et client), ses serveurs, les données, etc.
La Suisse doit continuer à créer son propre droit (ou contribuer à créer le droit international qu'elle appliquera) et pas subir le « droit » créé par des privés ou d'autres Etats. Elle doit aussi initier et collaborer à l'élaboration de nouvelles « conventions de Genève digitales » afin d'ancrer dans le droit international des règles de fonctionnement et d'accès aux réseaux, les nouveaux droits fondamentaux rendus nécessaires par la révolution numérique, mais aussi garantir non-prolifération des armes autonomes[137].
La Suisse doit par ailleurs veiller à protéger ses infrastructures critiques, lesquelles doivent être déconnectables (respectivement pouvoir fonctionner hors ligne) en cas de problème ou d'attaque informatiques.
La Suisse doit par ailleurs (mais ce constat est valable indépendamment de la révolution numérique) veiller à garantir la cohésion sociale, fort mise à mal par l'émergence d'immenses entreprises disposant de monopoles sur leurs propres marchés, mais aussi de la capacité d'entrer sur n'importe quel autre marché (y compris pour des prestations relevant du service public) en y acquérant d'entrée une position dominante. L'accumulation de capital par les GAFA met en danger la cohésion sociale et la prospérité *commune,* à plus forte raison s'ils se soustraient à l'impôt[138] et au droit. La cohésion sociale pourrait enfin être menacée par la fin de la solidarité, si l'usage intensif du big data permet aux entreprises et collectivités publiques, notamment aux assurances, d'optimiser la « chasse aux mauvais risques » en individualisant à l'extrême les prestations et leur financement[139].

Art. 5 Cst. : Etat de droit (cf. aussi les droits procéduraux aux art. 29, 29a, 30 et 32)

Un Etat de droit se doit d'attendre de toute technologie, en particulier des algorithmes, qu'ils se conforment à ses lois et normes sociales[140]. A notre avis, l'art. 5 doit être précisé afin que cela soit le cas. Il convient notamment de garantir l'application des principes suivants[141] :

- **Explicabilité et transparence des IA et des algorithmes** : Le fonctionnement d'un algorithme et les données dont il se sert doivent pouvoir être rendus publics et explicables aux personnes concernées (idéalement sans qu'il y ait besoin de connaissances particulières en informatique), à plus forte raison s'il aide à prendre une décision étatique (ou pis : la prend tout seul). Les décisions des IA prises par des « boîtes noires » doivent être protocolées afin que l'on puisse déterminer qui est responsable des erreurs[142]. Cela dit, l'exigence d'explicabilité et de transparence risque fort de ne pas être très utile au commun des mortels, comme le montre l'exemple de « Parcoursup », dont près de quarante fichiers informatiques ont été dévoilés par le ministère, auxquels il faut ajouter une documentation technique d'une vingtaine de pages qui détaille les choix techniques opérés[143]. Par ailleurs un algorithme, à plus forte raison s'il est auto-apprenant, reste une « boîte noire » difficile, si ce n'est impossible à comprendre pour la population, qui, de toute façon, ne comprend plus depuis longtemps le fonctionnement de la plupart des machines qui l'entourent, fussent-elles vitales. Certains en concluent que la transparence des algorithmes pourrait être un leurre[144].
- **Responsabilité** : pour tout système algorithmique, il doit y avoir une personne ayant le pouvoir de faire face à ses effets indésirables.
- **Exactitude** : les sources d'erreur doivent être identifiées, consignées et comparées.
- **Auditabilité** : les algorithmes doivent être développés pour permettre à des tiers d'en sonder et d'en revoir le comportement). Les résultats et critères de ces évaluations devant être expliqués et publiés.
- **Justiciabilité** : pour éviter les biais des décisions automatisées, les algorithmes qui prennent des décisions au sujet des individus doivent être évalués pour notamment que leurs effets discriminatoires puissent être mesurés.

Art. 6 Cst. Responsabilité individuelle

L'art. 6 Cst. doit être complété afin de mieux faire respecter ce pendant indispensable de la liberté qu'est la responsabilité. En effet, la révolution numérique crée un nombre important de situations générant des dommages pour lesquels personne n'est responsable ou alors parce le ou les responsables bénéficient de l'impunité, soit en raison de leur trop grand nombre, soit en raison des difficultés d'identification, soit pour des questions d'extraterritorialité. Or, à notre avis, il existe un droit fondamental à la réparation civile d'un dommage par son responsable (cf. plus haut), mais aussi à ce que l'auteur d'un crime ou délit soit poursuivi au pénal (cf. ci-après à propos de l'art. 10 Cst.). Pour cela, il faut que, sauf pour les cas où aucune responsabilité humaine n'est en cause (notamment les catastrophes naturelles inévitables), il doit y avoir une personne physique ou morale responsable. Il ne doit donc plus y avoir de dommage sans responsable (personne physique ou entreprise), ni d'entreprises sans responsables « humains » ou dont les responsables sont impossibles à contacter (p. ex. parce qu'il n'est possible de prendre contact que via un formulaire en ligne dont on ne sait pas s'il est traité ou qui est traité par un chatbot). Cela ne doit toutefois pas conduire, cela serait absurde, à ce que certaines machines autonomes doivent en permanence être sous supervision humaine (p. ex. la Convention de Vienne prescrit que tout véhicule doit avoir un conducteur « prêt à intervenir », ce qui est en contradiction avec le concept d'autonomie !). A l'heure actuelle, certains fabricants acceptent volontairement d'endosser la responsabilité en cas de dommages causés par leur produit autonomes (Volvo, Google ou Mercedes)[145], mais cela reste une démarche volontaire.

Comme le prescrit l'art. 27 CC, la protection de la liberté individuelle vaut aussi en cas d'abandon volontaire (et plus ou moins conscient) de cette dernière, p. ex. lorsqu'on livre une grande partie de sa vie intime « par confort » en confiant la gestion de son foyer à un assistant comme Alexa (Amazon). La protection de la liberté individuelle doit aussi être améliorée afin d'éviter les effets « lock-in » ou « take it or leave it » qui font que, pour bénéficier des prestations en ligne, il faut accepter toutes les conditions générales, sans possibilité de négociation ni de trouver une alternative lorsque le prestataire, ce qui est souvent le cas, bénéficie d'un monopole.
Enfin, parler de responsabilité individuelle n'est pas cohérent lorsque, faute de mesures pour réduire la fracture digitale (cf. plus haut), tous n'ont pas accès aux prestations et innovations proposées par la révolution numérique.

Art. 7 Cst. Dignité humaine

Sans tomber dans la crainte de la « guerre contre les machines », voire de la singularité, c'est certainement au niveau de la dignité humaine que les conséquences de la révolution numérique peuvent être le plus importantes. La plupart de ces questions méritent un débat éthique approfondi, auquel nous n'avons pas la prétention de contribuer. Toutefois, en fonction des résultats de ce débat, la protection constitutionnelle de la dignité humaine devra être précisée. On pense notamment aux thèmes suivants :

Humanité augmentée

La révolution numérique est propice à la réalisation du rêve du cyborg, de l'humain connecté, augmenté. Les progrès technologiques sont tels qu'implanter des puces[146] et des prothèses intelligentes ne fait désormais plus partie de la science-fiction. La première question sera celle du droit à bénéficier de ces innovations : Feront-elles par exemple partie du catalogue des prestations remboursées par les assurances sociales ? Ou au contraire, doit-on les interdire afin d'éviter un creusement des inégalités ? Ou plutôt pour des raisons éthiques ?
Puis, viendra la question de l'obligation. Dans certains métiers ou activités, sera-t-il obligatoire de porter une prothèse rendant possible ou facilitant certaines tâches, une puce de localisation ou contenant des informations cruciales, notamment pour la sécurité de leur porteur ou de tiers ? Sera-t-il possible pour des parents de l'imposer à leurs enfants ou à des tiers à qui ils les confient ? A l'Etat de l'imposer à des personnes qu'il est en droit de surveiller (détenus) ou à qui il confie des tâches dangereuses, complexes (chirurgien, technicien de sécurité nucléaire), ou tout simplement pénibles (exosquelette pour travailleurs de la construction) ? Ou lorsqu'il a besoin d'obtenir des statistiques p. ex. en matière de santé publique[147] ?

Quelle interaction des humains avec les machines « intelligentes » ?

L'essor des nouvelles technologies fait que, dans de nombreuses situations de la vie courante, ce n'est plus à un interlocuteur humain à qui nous avons affaire, mais à une IA ou un robot. Une question à débattre sera celle d'un **droit de ne pas avoir à faire à une IA qui se fait passer pour un humain, ou en tout cas de savoir à qui on a affaire**[148]. Il faudra aussi discuter d'un **droit de ne pas être soigné par des robots**, par nature incapable de détenir des qualités purement humaines indispensables aux soins (empathie, créativité, relations sociales), mais qui, en raison de la pénurie de personnel qualifié et de l'augmentation de l'espérance de vie, risquent de prendre de plus en plus d'importance dans les soins et le travail de *care*[149]. Cela dit, au Japon, se faire câliner par un robot (situation devenue courante) ne pose de

problème à personne étant donné d'une part que les gens ont été habitués à vivre avec eux depuis longtemps et d'autre part la perception positive des machines que transmet le Shintoïsme[150].
Dans tous les cas, il est indispensable **d'instituer un cadre éthique pour la conception, la fabrication et l'utilisation des robots et des IA**, à l'instar de ce qui est proposé au niveau de l'UE[151].

Des humains aux ordres des robots/ des IA ?

De plus en plus souvent, des humains devront se conformer à des algorithmes. Cela peut arriver de manière non-explicite, par exemple lorsque la présence d'une IA force les humains à se comporter d'une manière dont ils pensent que l'IA jugera positive ou acceptable (cf. p. 12 à propos des logiciels de « détection des comportements suspects » des aéroports). Mais cela peut aussi arriver de manière explicite, p. ex. lorsqu'un robot est habilité à donner des directives aux travailleurs avec qui il « collabore » (c'est le cas de l'entreprise japonaise Hitachi ou d'Amazon, dont les algorithmes dictent pratiquement chaque étape du processus de travail[152]) ou lorsque c'est un algorithme qui décide d'engager ou de licencier du personnel[153]. Certes, ni un robot ni une IA ne sont des personnalités juridiques capables de prendre des décisions entraînant des effets juridiques, mais il arrivera souvent que des employeurs ordonnent à leur personnel d'obéir à ces « directives », respectivement suivent aveuglément la « recommandation » d'engager ou de licencier faite par l'algorithme. Cela équivaudra dans les faits à mettre certains humains aux ordres de machines, lesquelles pourraient prendre des décisions non pas ponctuelles et limitées à un processus de travail, mais ayant un impact majeur sur la vie des personnes concernées.
Quoi qu'il en soit, il conviendrait de compléter l'article 7 Cst. afin de créer un nouveau droit fondamental, découlant de la dignité humaine, à ce **qu'aucun humain ne devienne l'objet ou le sujet d'un algorithme[154]** et que **toute décision importante[155] doit uniquement être prise par des humains**[156]**, respectivement de donner le droit aux humains de refuser toute décision prise par ou à l'aide d'un algorithme qui serait contraire à la dignité humaine**. Par ailleurs, en cas de décision prise par ou à l'aide d'une IA, une personne (physique ou morale), doit en assumer la responsabilité.

Que reste-t-il des qualités et défauts purement humains ?

Le droit à la dignité humaine comporte aussi celui à subir les défauts ou jouir des qualités purement humains, comme le droit d'être imprévisible[157], de changer ses plans ou d'avis, d'agir selon son instinct ou ses émotions. S'il aboutir à une tentative de tout modéliser, mesure, prévoir et calculer, l'usage des nouvelles technologies n'est certainement pas compatible avec la notion de dignité humaine.

Nouveau droit fondamental au travail décent (pas uniquement en ligne)

En raison de l'importance du travail dans nos vies, le droit à un travail décent devrait découler de la dignité humaine. Il est décrit plus bas en p. 35.

Art. 8 Cst. Egalité

Il est indispensable de veiller à ce que le principe d'égalité s'applique aussi aux décisions automatisées, lesquelles présentent un risque élevé de discrimination (cf. plus haut p. 13). Pour cela, il conviendrait d'appliquer les principes suivants à l'art. 5 Cst., complété par une **inversion du fardeau de la preuve : Quiconque utilise un processus de décision automatisé doit prouver qu'il n'est pas discriminatoire**[158]. En effet, il risque d'être

impossible pour les victimes de discriminations de prouver qu'elles en ont été victimes, car il faudrait notamment pour cela connaître quelles sont les données sur lesquelles s'appuient la décision, leur qualité et les éventuels biais qu'elles contiennent.

Art. 9 Cst. Interdiction de l'arbitraire

L'interdiction de l'arbitraire, un des éléments centraux de notre Etat de droit, doit être précisée afin de garantir qu'elle s'applique aussi aux décisions automatisées, notamment pour que ces dernières tiennent compte du contexte et des situations individuelles, qui ne sont pas forcément modélisables ou traduisibles sous forme de données. On se reportera pour cela aux principes évoqués plus haut.
Il faut ici relever que la question des décisions automatisées ne doit pas être abordée, comme c'est malheureusement le cas actuellement, sous le seul angle de la protection des données (cf. l'art. 15 P-LPD), ne serait-ce que parce que la législation sur la protection des données ne traite que des données à caractère personnel (cf. plus bas p. 30 à propos du droit collectif des données).

Art. 10 Cst. Droit à la vie et à la liberté personnelle

L'art. 10 Cst. doit être complété afin de mieux garantir le droit à la vie et à la liberté individuelle malgré la révolution numérique.

Des mesures pour protéger le droit à la vie « physique »

La révolution numérique génère de nouveaux risques pour l'intégrité physique et la santé : dangers causés par les robots (pas uniquement « tueurs ») et autres engins autonomes, atteintes à la santé physique et psychique en raison de l'hyperconnectivité permanente, nouveaux risques environnementaux. Le droit à la vie est suffisamment clair et n'a pas besoin d'être complété au niveau de la Constitution. Cependant, sa mise en application doit être précisée au niveau de la loi.
En particulier, il convient de prendre des mesures contre l'impunité pénale, que la révolution numérique favorise pour les raisons évoquées plus haut. En effet, le droit à la vie (art. 10 Cst. et 2 CEDH) inclut le droit de la victime à une poursuite pénale, y compris contre la violence privée, mais aussi un devoir de protection contre les technologies dangereuses[159].
Il faut en outre préciser le droit à l'intégrité physique et psychique par des mesures contre l'hyperconnectivité, la disponibilité permanente et la surveillance constante, pas uniquement sur le lieu de travail.

Des mesures contre la « mort sociale »

Le droit à la vie doit être complété pour inclure celui d'être protégé contre la mort sociale (cf. plus haut p. 18), qui peut d'ailleurs être une étape vers la mort « réelle » (suite à une agression ou un suicide). On pense notamment au cyberharcèlement de masse par « raids numériques » organisé soit dans le but de nuire à la victime[160], soit par la mise en scène de la vie privée d'autrui sans son autorisation[161], mais aussi en tant que privatisation de la Justice (et d'une suppression totale des droits de procédure comme la présomption d'innocence ou le droit d'être entendu), lorsqu'une personne coupable ou prétendument coupable d'un délit est jetée en pâture à la vindicte des réseaux sociaux et des moyens de communications de masse (p. ex. avec : #balancetonporc). Parmi ces mesures, il convient notamment d'instaurer une **responsabilité « chapeau » du réseau social qui ne prend pas de mesure pour identifier et stopper, voire tolère ce genre d'agissement**, à plus forte raison lorsqu'il n'est pas

possible d'identifier et d'appréhender les auteurs en raison de leur grand nombre. Il convient aussi de **préciser les délits pénaux en matière de harcèlement, de menaces ou de contrainte** afin que la participation à un raide numérique, même s'il s'agit, en soi, d'une action isolée ne relevant pas du droit pénal, puisse être punissable du moment qu'il est clair que l'action est massive[162].

(Ré)instaurer la liberté individuelle dans le Monde numérique

Comme précédemment expliqué, la révolution numérique a tendance à restreindre massivement la liberté individuelle, que ce soit en rendant les utilisateurs de services numériques captifs (d'un seul service bénéficiant d'un monopole ou d'un bouquet de services liés entre eux), en leur ôtant toute liberté de choix et pouvoir de négociation au moment de commencer une relation contractuelle sans alternative. Cela passe notamment par des mesures (décrites par ailleurs) pour limiter le pouvoir des GAFA, mais aussi un renforcement du service public numérique et le développement de nouveaux droits pour les utilisateurs, notamment en matière de portabilité des données, de droit à l'anonymat en ligne, de renforcement de la règle du consentement éclairé ou de contestation des conditions générales.

Nouveau droit fondamental à ne pas devoir utiliser les nouvelles technologies

La liberté en ligne comporte aussi la liberté… de ne pas être en ligne, de ne pas être connecté et de ne pas se servir de prestations en ligne. Peu importent les raisons : pas ou trop peu de connaissances du fonctionnement des réseaux et des services, pas d'accès aux technologies (quelle qu'en soit la raison), pas envie de se soumettre aux conditions des prestataires, pas envie de voir son comportement traqué, analysé, décortiqué, droit de protéger ses données et de rester anonyme, etc. **Il convient donc de compléter la notion de liberté personnelle pour que chacun ait droit à un Monde analogique[163].** Ce droit doit notamment inclure celui de pouvoir bénéficier de toutes les prestations publiques (et des entreprises du service public) sans passer par un moyen de communication en particulier[164].

Art. 11 Cst. Protection des enfants et des jeunes

La protection de l'enfance est certainement un des droits fondamentaux qui méritent d'être complétés et précisés en raison de la révolution numérique. Dans bien des cas, il s'agira de protéger les enfants malgré leurs parents (ou contre les négligences de ceux-ci), qui, en général par confort ou inconscience, livrent en pâture aux GAFA (et à d'autres entités publiques ou privées) la vie de leurs enfants, tant numérique que réelle. En effet, la révolution numérique pousse de nombreuses familles à livrer les données personnelles de leurs enfants via des objets connectés (pas forcément pour les surveiller) comme les peluches connectées CloudPets, facilement piratables, ou la lolette connectée Pacifi-i. Les enfants sont aussi exposés au pouvoir des géants du numérique lorsque c'est tout un foyer qui passe sous le contrôle et la surveillance d'un assistant comme Alexa (Amazon) ou Home (Google).
L'art. 11 devrait donc être complété afin que l'intégrité numérique des enfants et des jeunes soit spécifiquement protégée, en particulier pour éviter que des tiers ne s'emparent non seulement de leurs données personnelles, mais surtout du contrôle d'une partie de leur existence « réelle » (même si c'est à cause de la négligence de leurs parents) aussi longtemps qu'ils ne sont pas en mesure de faire valoir eux-mêmes leurs droits fondamentaux (cf. art. 11 al. 2 « Ils exercent eux-mêmes leurs droits dans la mesure où ils sont capables de discernement. »). Il faudrait par ailleurs faire un vrai droit fondamental du but social à l'art. 41 Cst. qui recommande que « les enfants et les jeunes soient encouragés à

devenir des personnes indépendantes et socialement responsables et soient soutenus dans leur intégration sociale, culturelle et politique ».
Les droits des enfants et des jeunes devront aussi être complétés par un **nouveau droit constitutionnel à l'éducation numérique** (pas uniquement en faveur des enfants), qui sera décrit plus bas.
Enfin, les règles en vigueur de protection de l'enfance, notamment en matière d'interdiction et de limitation du travail des enfants doivent être appliquées plus strictement, en particulier pour protéger les jeunes youtubeurs mis en scène à l'instigation de leurs parents, ou intégrés contre leur gré par ceux-ci dans des vidéos à but lucratif, quand ils ne sont carrément pas molestés ou humiliés pour faire de l'audience[165]. Il faudrait enfin envisager une application de ces règles pour éviter que les enfants, y compris très jeunes, ne soient exposés à des « tunnels » de vidéo abrutissantes et/ou publicitaires[166].

Art. 12 Cst. Aide en situation de détresse

L'accès aux réseaux et services numériques de base doit être considéré comme faisant partie du minimum vital permettant de mener une existence conforme à la dignité humaine. Si nécessaire, il faudra compléter l'art. 12 Cst. de même que les normes en matière d'aide sociale et de prestations complémentaires.

Art. 13 Cst. Protection de la sphère privée

La protection des données est certainement le thème de la révolution numérique le plus débattu et qui fait l'objet du plus grand nombre de propositions, dont certaines sont actuellement en discussion dans le cadre de la révision de la LPD (*privacy by design, by default, control by design, privacy impact assessement*, droit à l'oubli numérique, etc.). Nous n'allons donc en aborder que quelques aspects moins souvent discutés.

La portabilité au lieu de la propriété des données

Instaurer un droit (individuel) de propriété des données personnelles est une mauvaise idée. Certains postulent la création d'une sorte de « revenu de base numérique », financé par la vente (le cas échéant au plus offrant) de ses données personnelles. Sans aller jusque-là, l'idée de faire de ses données une monnaie d'échange est largement discutée et déjà expérimentée, notamment par des personnes en situation de précarité poussées à abandonner leur vie privée pour gagner un peu d'argent, p. ex. en répondant à des sondages rémunérés quelques francs. Or, la propriété de ses données, et donc la possibilité de les vendre, ne va pas sans risques. En premier, celui d'une accaparation de toutes les données (y compris les donnes non-personnelles) et donc des informations brutes[167]. Ensuite, une propriété des données donnerait un pouvoir important à celui qui détient le capteur (la source), mais aussi les capacités de stockage (Amazon est notamment leader mondial du *cloud*). En outre, la frontière entre données personnelles et non-personnelles peut être difficile à définir, ce qui serait une source d'insécurité juridique. Enfin, la propriété des données ne rééquilibrerait pas forcément le déséquilibre des forces en présence qui perturbe les échanges contractuels de données, ne serait-ce qu'en raison de la dépossession qui est la conséquence de toute vente, alors qu'aujourd'hui, les données personnelles restent « protégées » même une fois transmises.
Garantir le droit à la portabilité des données personnelles est donc beaucoup plus indiqué, à condition de donner aux individus un pouvoir de négociation au moment de conclure une nouvelle relation contractuelle, afin d'éviter que, si l'on veut bénéficier d'un nouveau service numérique ou changer de fournisseur, l'on ne soit obligé de « venir avec ses données ».

Garantir la portabilité des données pourrait aussi inciter les citoyens à partager leurs données dans le cadre de démarches d'intérêt public[168].

Un droit à la sécurité des données

C'est une chose de traiter des données en respectant les droits fondamentaux des personnes concernées. C'est une autre chose de les conserver de manière à ce que tiers ne s'en emparent pas, réduisant à néant la protection garantie jusqu'à lors. Récemment, une enceinte connectée Echo (Amazon) a par exemple enregistré les conversations privées d'un couple à son insu et les a transmises à un employé du mari[169]. Les conséquences de vol ou de perte de données sont d'autant plus importantes que les technologies gagnent en puissance et en importance. **Il convient donc de garantir un droit fondamental à ce que les données soient conservées en sécurité[170]**, assorti de sanctions dissuasives pour ceux qui ne feraient pas tout ce que l'on peut raisonnablement exiger pour garantir cette sécurité.

Un droit constitutionnel clair à l'autodétermination informationnelle

L'art. 13 Cst. est mal rédigé, car, même si le droit à l'autodétermination a été consacré par la jurisprudence, une interprétation littérale[171] ne protège que l'utilisation abusive et pas l'utilisation ordinaire des données personnelles. **Le droit à la sphère privée doit donc être un vrai droit à l'autodétermination informationnelle (ou intégrité numérique), c'est-à-dire le droit de chacun d'autoriser si et dans quel but ses données peuvent être traitées**[172].

Pour un droit clair à l'anonymat, à la cryptographie et au chiffrement

Nous ne nous comportons pas de la même façon quand nous sommes des anonymes pris dans la masse que lorsque nous savons que nous sommes identifiés individuellement. L'anonymat est donc un moyen de préserver les libertés. La Déclaration du Conseil de l'Europe du 28 mai 2003 sur la liberté de la communication sur Internet consacre d'ailleurs l'anonymat à son principe 7. « Afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées, les États membres devraient respecter la volonté des usagers de l'Internet de ne pas révéler leur identité. Cela n'empêche pas les États membres de prendre des mesures et de coopérer pour retrouver la trace de ceux qui sont responsables d'actes délictueux, conformément à la législation nationale, à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales et aux autres traités internationaux dans le domaine de la justice et de la police. » Comme le relèvent les notes explicatives de la Déclaration, « [...] les utilisateurs peuvent avoir une raison valable de ne pas révéler leur identité lorsqu'ils font des déclarations sur l'Internet. Leur imposer cela pourrait restreindre de manière excessive leur liberté d'expression. Ceci priverait également la société d'idées ou d'informations potentiellement de qualité. [...] les utilisateurs doivent être protégés contre toute surveillance en ligne non autorisée par des entités publiques ou privées. »
Le droit à l'anonymat (mais aussi : droit au chiffrement et à la cryptographie, interdiction des trappes, promotion de la cryptographie et du chiffrement de bout en bout) est certes déjà inclus dans le droit à la sphère privée en tant que droit dérivé, mais il convient de le renforcer, en l'inscrivant explicitement dans la Constitution[173].

Empêcher la ré-identification

Un pendant du droit à l'anonymat est **d'empêcher la ré-identification** là où des données anonymisées sont utilisées[174]. Il convient donc d'imposer, lors de tout traitement de données, une **analyse préalable** du risque de ré-identification et, si nécessaire, la prise de **mesures**

préventives pour l'éviter. Par ailleurs, l'utilisation de données anonymisées (ou censées l'être) ne doit pas suffire à immuniser les responsables de traitement de toute responsabilité.

Un droit à la libre circulation des données ?

Les tenants du libre marché et de la suppression des entraves à ce denier prônent de plus en plus une libre circulation des données à l'instar des 4 libertés fondamentales de l'UE. La Commission européenne élabore actuellement des propositions allant dans ce sens. Un tel mécanisme, qui favoriserait à n'en pas douter les GAFA et autres grandes entreprises multinationales, doit à notre avis être rejeté, en tout cas en l'absence de standards internationaux garantissant la protection des données dans tous les pays et empêchant une sous-enchère en matière de protection contre les désagréments causés par la révolution numérique. Nous nous rallions à l'attitude prudente du CNNum, qui prend ainsi position : « L'introduction, à ce stade, d'un principe de libre circulation des données pourrait entraîner des conséquences encore mal évaluées compte-tenu des réalités extrêmement diverses recouvertes par le terme de donnée et de la multitude des usages et des marchés que les données pourraient encore faire émerger. Il paraît essentiel de s'interroger davantage sur les actions concrètes à mener pour permettre à l'Europe de bénéficier des retombées économiques et sociales de la révolution des données, plutôt que de consacrer un nouveau principe. Par ailleurs, le Conseil considère que les barrières à la circulation des données se situent moins au niveau des frontières nationales qu'au niveau des stratégies de lock-in et de rétention de données entre acteurs économiques. C'est donc au moins autant les barrières "trans-plateformes" que "transfrontalières" à la circulation des données que la Commission doit chercher à lever. Enfin, le fait de reconnaître un principe de circulation des données au niveau européen pourrait constituer un argument pour le consacrer dans les accords de libre-échange à venir. Cela conduirait à faciliter le transfert de donnée sans contrôle (…). »

Un droit collectif des données

La protection des données souffre actuellement d'un grave défaut : elle ne protège que les données « personnelles ». Or, de nombreux usage de données en soi non liées à des individus permettent tout de même de les identifier ou peuvent avoir ont un impact discriminant sur ces derniers (cf. plus haut p. 13 à propos des décisions automatisées et des discriminations qu'elles peuvent générer). C'est par exemple le cas des données non-personnelles récoltées par un opérateur de télécommunication lorsqu'il aide une commune à devenir une « smart city ». Pour faire face à cet « angle mort » Villani préconise à juste titre la création d'un **droit collectif de la protection des données, afin de permettre aux individus de se protéger contre l'impact sur leur situation individuelle de l'usage de données non-personnelles**[175]. En outre, il convient d'introduire la possibilité **d'action civile collective en matière de protection des données**, d'une part pour donner aux personnes concernées la possibilité de se défendre en groupe contre un usage de données qui les désavantage en tant que groupe, mais aussi en raison de la faible valeur litigieuse d'un différend en matière de données personnelles, laquelle rend le « rapport qualité-prix » d'engager une action en justice déraisonnable, à moins de disposer du temps, des ressources et de la volonté nécessaires pour obtenir une décision de principe, comme l'a fait par exemple Max Schrems contre FB.
Par ailleurs, lorsque partager ses données de manière anonyme (et non ré-identifiable, cf. ci-dessus !) est dans l'intérêt public (p. ex. en matière de santé publique, de gestion des transports, des ressources naturelles, de consommation d'énergie, d'utilisation des sols et des bâtiments, etc.)[176], **l'obligation (aux personnes physiques et aux entreprises) de partager leurs données** devrait être envisagée. La solution pourrait être un mécanisme similaire aux licences obligatoires en matière de propriété intellectuelle ou à l'utilisation d'« *essential*

facility », c'est-à-dire la mise à disposition à un prix raisonnable par son propriétaire d'une infrastructure indispensable qu'il ne serait pas pertinent de dupliquer.
Cela dit, le droit collectif des données ne doit pas se limiter à protéger les utilisateurs lorsque d'une utilisation abusive de données collectives. La question qui doit se poser est plutôt de **faire des données un bien collectif**, un bien public géré de manière démocratique, comme le préconise notamment Morosov[177]. **Les données sont, depuis longtemps, un bien essentiel, une infrastructure du service public dont la propriété ne saurait être que collective.** Au lieu d'en laisser la possession à des entreprises privées qui imposent aux utilisateurs un droit d'accès aux données qu'ils ont pourtant eux-mêmes produites, il conviendrait d'inverser le cours de choses et de confier aux institutions publiques le soin et le choix de décider de qui peut utiliser quelles données, dans quels buts et à quel tarif[178].

Art. 16 et 17 Cst. Liberté d'opinion, d'information et des médias

La question du soutien aux médias et de la lutte contre les fausses informations (*fake news*)[179] sont des sujets qui sont largement débattus par ailleurs et font l'objet de nombreuses propositions, notamment de la part du PS.
Il convient toutefois d'insister sur les problèmes que posent l'hégémonie de certains sites comme Google ou les réseaux sociaux en matière de diffusion des contenus médiatiques. Cela est dangereux pour la diversité : la fermeture de BuzzFeed France (le 7.6.18) a montré que le changement d'algorithme de FB (privilégier les publications des « amis » au détriment de celles des médias, fussent-ils sérieux) a mis en difficultés plusieurs « *pure players* » comme brut.fr, qui sont désormais moins visibles et donc moins partagés, jusqu'à mettre en péril leur modèle d'affaire[180].

Art. 26 Cst. Droit à la propriété privée

Même si le droit à la propriété privée n'est pas le droit fondamental préféré des socialistes, il n'en demeure pas moins qu'il est de plus en plus limité par l'essor des objets connectés. En effet, il est difficile de se considérer comme le propriétaire d'un objet connecté dont on ne peut pas piloter à sa guise la connectivité. L'objet peut être inutilisable, voire devenir dangereux s'il est piraté[181], ou, plus simplement, s'il n'y a pas le bon réseau comme l'a récemment montré l'exemple d'une voiture Tesla indévérouillable… à cause d'absence de réseau dans le parking où elle était garée, inaccessibilité qui aurait pu causer un grave dommage à la santé du bébé qui se trouvait à l'intérieur[182]. Mais, au-delà de la simple connexion au réseau, les propriétaires d'un objet connecté sont en général tributaires du logiciel d'exploitation, de ses options, de ses API, des mises à jour, de la compatibilité de celles-ci avec le hardware, etc. **Il est donc nécessaire de préciser l'art. 26 Cst. afin que celui-ci inclue, dans tous les cas, le droit du propriétaire de contrôler si et comment l'objet en question est connecté (*control by design*)**.
En matière de propriété privée, la question de la garantie de la propriété foncière par l'Etat risque aussi de se poser avec l'essor du blockchain, qui pourrait mener à une privatisation de cette garantie hors de tout contrôle et légitimité publics[183].

Art. 27, 94 et 96 Cst. Liberté économique

La révolution numérique encourage une tendance bien connue du capitalisme : s'appuyer sur les règles de la libre concurrence pour mieux la supprimer une fois que l'on est devenu un monopole privé. Si la concurrence et le libre marché ne sont pas souhaitables dans tous les domaines, il convient de veiller, là où ils le sont, à ce qu'ils fonctionnent[184]. Le droit des cartels est l'instrument de l'Etat pour éviter que le marché ne se torpille lui-même. Or, en

Suisse, ce droit, en privilégiant le critère de l'efficience, tend à avantager les grandes entreprises[185], ce qui est particulièrement dommageable pour l'économie face à la montée en puissance des GAFA. Par ailleurs, ces dernières profitent de définition obsolète de l'abus de position dominante : on ne peut avoir qu'une part de marché de 5% dans plusieurs pays et avoir tout de même une position dominante au niveau mondial[186]. Cela dit, la sanction record infligée à Alphabet (Google) le 18 juillet 2018 par la Commission européenne[187] montre à la foi les possibilités d'intervention des pouvoirs publics fondées sur le droit de la concurrence et les défauts de ce droit : même si l'amande paraît colossale (plus de 4,3 milliards d'Euros), elle n'est que broutille comparée aux quelques 90 milliards USD de liquidités qu'Alphabet détient. Par ailleurs, il a fallu 7 ans de procédure pour faire condamner Google, qui a, entre-temps, pu établir sans problèmes sa position dominante (85% des parts du marché des applications mobiles). Ce cas n'est pas sans rappeler celui qui, il y a vingt ans, a opposé Internet explorer (Microsoft) au navigateur Netscape, qui s'est fait exclure d'un marché dont il était pionnier et qui avait disparu au moment où la condamnation des pratiques abusives de Microsoft est entrée en force.
La montée en puissance des GAFA n'est toutefois pas nuisible pour la collectivité uniquement parce qu'elle entrave le bon fonctionnement des marchés. C'est surtout en raison des menaces précédemment décrites que ces entreprises font peser sur le service public, sur la crédibilité et le financement de l'Etat, sur le respect des droits fondamentaux et, partant, sur la cohésion sociale que leur existence en tant que telle ne doit plus être tolérée par les démocraties. **Les GAFA sont devenues un risque systémique. Leur démantèlement serait souhaitable, pour ne pas dire nécessaire. Il convient donc de modifier l'art. 96 de la Cst. dans le but de ségmenter leurs activités en Suisse en séparant la source des données – le moteur de recherche, des services qui utilisent ces données.**
Il faut toutefois éviter de s'appuyer sur les précédents démantèlements spectaculaires d'entreprises monopolisitiques comme la Standard Oil ou AT&T, appliqués à des entreprises dont les monopoles étaient concentrés sur un territoire étatique défini et dont la relation avec l'Etat, les clients, fournisseurs et travailleurs était empreinte de ces limites territoriales[188]. Il ne faut par ailleurs pas se contenter de sanctions – théoriquement possibles en Suisse au titre de l'art. 49a LCart – comme dans le récent cas Google (cf. ci-dessus), non seulement parce que les entreprises sont suffisamment grosses pour les payer rubis sur l'ongle et sans douleur, mais surtout parce que ce ne sont pas seulement leurs pratiques anticoncurrentielles qui les rendent dangereuses, mais bien leur taille et leur modèle d'affaire.

Art. 34 Cst. Droits politiques

Les récents événements rendent nécessaire **une précision de l'art. 34 pour une meilleure protection du processus de création de l'opinion publique ainsi que contre l'influence électorale en ligne[189]**. Dans ce contexte, il semble hasardeux, pour ne pas dire déraisonnable, de faire basculer tout ou partie du processus démocratique vers des outils en ligne (*e-voting, e-collecting, civic software*, « profils électoraux » smartvote ou vimentis). Par ailleurs, si l'émergence de nouveaux outils doit être saluée lorsqu'elle permet d'augmenter la participation et la mobilisation citoyenne, il ne faut pas perdre de vue que ce n'est en général pas la technologie qui génère la participation, mais la volonté des autorités de faire participer la population, de tenir compte de son avis ainsi que leur capacité à l'intégrer sérieusement au processus de prise de décision. La problématique de la fracture digitale risque d'être encore plus aigüe, car il va de soi que multiplier les formes de participation en ligne exclut de facto les victimes de la fracture.
La révolution numérique accroit par ailleurs le risque de « politique dictée par les données et les algorithmes (*data-driven policy*) » (qui est souvent les nouveaux habits de l'expertocratie

néolibérale). Il convient donc de **veiller d'abord à la bonne application, voire au renforcement des règles protégeant les décideurs désignés démocratiquement contre les influences extérieures** (cf. p. ex. art. 161 al. 2 Cst. « Les membres de l'Assemblée fédérale votent sans instructions. »). Mais il s'agit aussi, là où la population détient un pouvoir de contrôle de l'action publique qui n'est pas conditionné à des connaissances particulières (notamment en matière de droits politiques, p. ex. le dépouillement d'un scrutin), **d'éviter que ce pouvoir ne soit transféré à des experts parce qu'il faut désormais des connaissances pointues en informatiques pour en comprendre le fonctionnement**[190].

Art. 35 Cst. Réalisation des droits fondamentaux

Il convient de compléter l'al. 1 ainsi : « Les droits fondamentaux doivent être réalisés dans l'ensemble de l'ordre juridique, *y compris en ligne*. » Cette modification n'aurait certes qu'une portée symbolique étant donné, car la version actuelle suffit probablement à réaliser cet objectif. Il nous semble néanmoins qu'il ne serait pas inutile d'insister sur ce fait, en particulier après la récente votation sur la Loi sur les jeux d'argent (qui ne portait certes pas sur un droit fondamental, mais sur l'application d'un principe constitutionnel), dont certains opposants ont tenté de nier l'application à des entreprises non-suisses proposant des offres accessibles dans notre pays.

Art. 38 Cst. Nationalité / Identité

Même si l'art. 38 aborde la question de la nationalité sous l'angle de l'appartenance à un pays et des conditions de son octroi, il devrait aussi poser les bases de comment l'Etat reconnaît l'identité de ses citoyens et habitants. Il conviendrait toutefois d'examiner plus en profondeur si l'art. 38 est le bon siège de la matière pour cette question.
La question de l'identité digitale[191] est devenue cruciale. Cela va de l'obligation d'identifier ses clients (p. ex. pour des raisons d'âge légal), mais aussi de risque d'usurpation d'identité et donc de sécurité du droit[192]. Or, certifier l'identité de ses citoyens et habitants est l'une des prérogatives de l'Etat que la révolution digitale met à mal[193]. En effet, l'identité numérique (e-ID) pourrait être confiée en partie à des acteurs privés, voir s'autogérer hors de tout contrôle étatique (p. ex. un modèle « *self-sovereign* » via le blockchain)[194]. Il faut aussi veiller à ce que l'Etat conserve aussi le monopole de l'identification des personnes morales, ainsi que leur ayant-droit économiques.
La mésaventure d'un conseiller communal lausannois nommé Xavier Company, que FB a longtemps refusé d'identifier sous son vrai nom (arguant que « company » pouvait prêter à confusion avec une entreprise…) montre à quel point il est indispensable de ne pas laisser les questions d'identification au privé.

Art. 43a Cst. Prestations de base du service public

L'art. 43a doit être complété afin d'introduire de nouvelles prestations et infrastructures de service public et de réaffirmer les monopoles publics sur ces derniers. Ce nouveau service public numérique doit garantir :

- **l'accès universel aux réseaux et leur bon fonctionnement ;**
- **les prestations en ligne devenues indispensable et l'accès à celles-ci.**

Définir les nouvelles prestations du service public numérique

Parmi les nouvelles prestations et infrastructures de service public rendues nécessaires par la révolution numérique, on trouve :

- La **neutralité du net**[195] ;
- La **neutralité des terminaux** : un accès égal et universel de toutes les données à tous les réseaux ne suffit pas si les terminaux et plateformes qui permettent d'accéder aux réseaux privilégient certains contenus. Ainsi, les GAFA tentent de plus en plus de lier la consultation d'Internet à l'utilisation de leur matériel/*hardware* (ou de leur plateforme), dont le logiciel d'exploitation est verrouillé, quitte à offrir cet accès gratuitement pour attirer des clients qui deviennent captifs (« Kindelisation » du nom de la liseuse d'Amazon « Kindle »). Aux USA, les gens qui ont de tels accès bridés sont… les classes sociales défavorisées !
- **Droit d'accès Internet**, afin de supprimer la fracture digitale. En France, ce droit existe déjà à un niveau constitutionnel comme une condition nécessaire de l'exercice du droit à *« la libre communication des pensées et des opinions »,* protégé par la déclaration des droits de l'homme[196].
- **Droit à un accès à Internet performant, sur tout le territoire.**
- La gestion des **noms de domaine et TLD** doit relever du service public.

Par ailleurs, l'accès aux prestations du service public, y compris celles des entreprises publiques externalisées, doit être véritablement universel et pas réservé aux seuls détenteurs d'une certaine technologie comme le montre le récent exemple des clients des CFF, qui, pour recevoir une indemnisation en raison des travaux sur la ligne Lausanne-Berne en été 2018, devaient disposer d'un smartphone très récent, ce qui discrimine notamment les usagers d'un certain âge[197] ou dont les revenus sont faibles.

Défendre les prérogatives de l'Etat dans le service public « classique »

Mais les GAFA ne font que pas proposer de nouveaux services qui deviennent si essentiels qu'on doit désormais les considérer comme devant relever du service public. Elles s'implantent aussi massivement dans des secteurs qui relèvent traditionnellement du service public, tant au niveau des prestations (p. ex. la cartographie, naguère une compétence relevant de la défense nationale !) que des infrastructures. Ainsi, FB, Google etc. posent leur propres câbles sous-marins[198]. Or, de planification de telles infrastructures ne peut être efficiente et juste que si elle est le pilotée par les collectivités publiques. Par exemple, dans certains pays, il y a redondance de câbles. Dans d'autres, notamment en Afrique, il y en a trop peu pour assurer le débit aux heures de pointes… et en cas de coupure, tout le trafic est interrompu. **L'Etat devra donc veiller à rester maître des infrastructures de service public (à tout le moins de leur planification)**.

Nouveaux droits fondamentaux :

Notre Constitution ne reconnaît pas certains droits pour lesquels les socialistes se battent depuis des décennies, si ce n'est depuis leurs débuts. Aucun n'est nouveau et leur nécessité ne date pas d'hier. Mais la révolution numérique rend leur adoption d'autant plus urgente.

Droit à la formation numérique

Les défis posés à la population par la révolution numérique rendent plus indispensable que jamais l'instauration d'un droit à la formation, en particulier au numérique et à la culture du numérique (digital literacy). Cela inclut le **droit à des connaissances de base sur le fonctionnement des réseaux, sur la compréhension de leur contenus** (*fake news*, arnaques, canulars/*hoax*, satire, etc.), **sur l'impact d'une activité en ligne sur les individus et l'environnement** (p. ex. la participation à un cyber-harcèlement de masse) **ainsi que sur les intérêts en jeu** (p. ex. à qui appartient quel service). Il est aussi indispensable de renforcer **la**

formation des utilisateurs sur leurs droits (et devoirs, p. ex. la netiquette). Cette formation doit commencer dès le plus jeune âge (école obligatoire), et contrairement à ce que beaucoup pensent, les jeunes générations prétendument omniscientes en matière d'Internet (les « *millenials* » et autres « génération Y ou Z ») en ont aussi urgemment besoin.

Droit à la formation continue

Le droit à la formation doit aussi inclure un droit à une **formation continue au numérique**. D'abord, pour pouvoir continuer à en comprendre les enjeux et risques malgré la rapidité de l'évolution technologique. Ensuite, la transformation du monde du travail exige la création d'un vrai **droit à la formation professionnelle continue et, le cas échéant, au reclassement professionnel**, pas seulement en cas de suppression d'emploi due à la digitalisation. Ce reclassement professionnel doit pouvoir aussi être choisi, planifié (et non pas seulement subi en raison d'une évolution technologique ayant un impact sur sa place de travail) et doit être (co-)financé par les assurances sociales et les employeurs.

Droit au travail décent (y compris liberté syndicale selon art. 28)

La révolution numérique n'est certes pas l'unique raison qui rend indispensable l'instauration d'un **droit au travail décent**[199], mais elle génère de nouvelles dégradations des conditions de travail qui accentuent encore cette nécessité, ne serait-ce qu'en raison de l'émergence d'un nouveau prolétariat de « galériens du numérique » ou d'une planification du travail ordonnée par des IA. La technologie doit être l'exécutante du travailleur, et non l'inverse !
Le droit au travail décent doit notamment garantir :

- Que tout travailleur bénéficie des droits (même minimaux) que lui accorde le droit du travail, même s'il travaille pour une plate-forme qui ne se considère pas comme son employeuse.
- Que tout travailleur soit protégé contre les conséquences d'un travail qui le met en contact avec des contenus insoutenables (p. ex. les modérateurs de vidéos contenant des images de violence extrême, pédopornographiques, etc.).
- Que tout travailleur soit protégé contre un retour la précarité extrême qu'est travail à la journée[200] sur appel au bon vouloir des employeurs, pas uniquement dans le numérique.
- Que tout travailleur bénéficie d'un revenu décent et que, même en cas de travail à la tâche, il soit possible d'obtenir un tel revenu en consacrant à son travail une durée ordinaire (donc : chaque tâche, même minime et insignifiante comme celles proposées par Amazon mecanical turk, doit être correctement rémunérée afin que les tâches effectuables en une journée de travail permettent d'atteindre un revenu convenable).
- Que tout travailleur soit protégé contre la sous-enchère et une mise en concurrence à outrance, y compris contre les travailleurs employés au sein d'une même entreprise (y c. plate-forme).
- Que la collaboration avec les robots et les IA au travail respecte les droits fondamentaux des travailleurs, en particulier celui de ne pas soumis à leurs ordres ou en cas d'entretien d'embauche mené par un robot, une IA ou un avatar (comme Digital Room de Manpower).
- Qu'un travailleur qui collabore avec une machine intelligente ne soit pas rendu responsable des erreurs de celle-ci[201].
- Qu'il n'y ait pas d'obligation de se faire « augmenter », même pour effectuer pour certains travaux dangereux.

- Que tout travailleur puisse bénéficier de sa liberté syndicale et d'un contrôle (par l'Etat ou les partenaires sociaux) de ses conditions de travail, même lorsque les lieux de travail sont très décentralisés (p. ex. en cas de télétravail).
- Que le droit à la déconnexion et à ne pas être submergé par l'emploi des nouvelles technologies (p. ex. le flot de courriels[202]) soit précisé. A contrario, les employeurs doivent être forcés d'utiliser les nouvelles technologies lorsque cela permet de mieux protéger la personnalité de leurs travailleurs (p. ex. gestion des courriels ou des requêtes clients).
- Que les travailleurs soient protégés des conséquences négatives de la tendance à évaluer toutes les prestations[203].

La Suisse doit enfin initier (et collaborer à) **un renforcement des conventions de l'OIT là où la révolution numérique le rend nécessaire**, et, bien sûr, ratifier d'éventuelles nouvelles conventions.

* * *

Abréviations

ARCEP	Autorité de régulation des communications électroniques et des postes (France)
CC	Code Civil, RS 210.
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales (Convention Européenne des Droits de l'Homme), RS 0.101
CF	Conseil fédéral
CNNum	Conseil National du Numérique (France)
Cst.	Constitution fédérale, RS 101
DDPS	Département fédéral de la défense, de la protection de la population et des sports.
FB	Facebook
GAFA	Google (Alphabet), Apple, Facebook, Amazon. Cet acronyme (parfois complété d'un M pour Microsoft) désigne, dans le présent document, tous les « géants du Net » de la Silicon Valley, y compris d'autres entreprises dominantes comme PayPal, tripadvisor, AirBnB, booking.com, Uber, etc. et en incluant leurs concurrents chinois comme Alibaba, Baidu, Tencent ou WeChat.
IA	Intelligence artificielle
LCart	Loi fédérale sur les cartels et autres restrictions à la concurrence, RS 251.
LPD	Loi fédérale sur la protection des données (P-PLD = projet de nouvelle LPD, actuellemet en traitement aux chambres fédérales)
m2m	*machine to machine* : objets connectés et échangeant des informations entre eux.
MIT	*Massachusset Institute of Technology*
OCDE	Organisation pour la Coopération et le Développement Economique
OIT	Organisation Internationale du Travail
P2P	*peer to peer* : pair à pair

QS	*quantified self* : mesure de soi
R&D	recherche et développement
RGPD	Règlement général (de l'UE) sur la protection des données (2018)
RS	Recueil systématique des lois fédérales
TF	Tribunal fédéral
TLD	*Top level domain* : domaine de premier niveau. Ex. : « .ch », « .biz », « .swiss ».
USS	Union Syndicale Suisse

Bibliographie

Sauf indication contraire, les sources sont citées avec le seul nom du premier auteur indiqué. Les sites internet cités ont tous été consulté aux mois de juin et juillet 2018.

- Acemoglu, Daron/Restrepo, Pascual, (MIT) Robots and Jobs: Evidence from US Labor Markets, Boston, mars 2017, sur : http://www.nber.org/papers/w23285
- Article 19, Le droit à l'anonymat en ligne, document d'orientation, Londres, 2015.
- Attali, Jacques (éd.), L'avenir du travail, Paris 2007.
- Autorité de régulation des communications électroniques et des postes (ARCEP), Smartphones, tablettes, assistants vocaux… Les maillons faibles de l'ouverture d'internet, Paris, février 2018.
- Avenir.Suisse (éd.), Quand les robots arrivent, Préparer le marché du travail à la numérisation, Zurich, Octobre 2017.
- Bradley, Joseph/Barbier, Joel/Handler, Doug, L'internet of everything, un potentiel de 14,4 trillions de Dollars, livre blanc édité par Cisco, 2013. https://www.cisco.com/web/FR/tomorrow-starts-here/pdf/ioe_economy_report_fr.pdf
- Brundage Miles (et al.), The malicious use of artificial intelligence : Forecasting, prevention and mitigation, Oxford, février 2018.
- Conseil fédéral, Conséquences de la numérisation sur l'emploi et les conditions de travail : opportunités et risques, Rapport en réponses à diverses interventions parlementaires, Berne, 8 novembre 2017.
- Conseil National du Numérique (CNNum), La libre circulation des données dans l'Union Européenne, Paris, Avril 2017.
- Crawford, Kate, Artificial Intelligence's White Guy Problem, New York Times du 25 juin 2016
- Cuvelliez, Charles, Légiférer contre les « fake news » ne sert à rien, Le Monde du 4 avril 2018.
- DDPS, Stratégie nationale de protection de la Suisse contre les cyberrisques, Berne 2012.
- Degryse, Christophe, Les impacts sociaux de la digitalisation de l'économie, working paper 2016.02 de l'ETUI, Bruxelles.
- Diakopoulos, Nicholas, Friedler, Sorelle, How to Hold Algorithms Accountable : Algorithmic systems have a way of making mistakes or leading to undesired consequences. Here are five principles to help technologists deal with that, MIT Technology Review, 17.11.2016.
- Doueihi, Milad, Le numérique, un nouveau processus civilisateur, Le Monde du 24 janvier 2018.

- Dowek, Gilles, Réseaux sociaux : « Les téléphones, les tablettes, les ordinateurs sont devenus des armes létales », Le Monde du 29 mai 2018, sur https://abonnes.lemonde.fr/idees/article/2018/05/29/reseaux-sociaux-les-telephones-les-tablettes-les-ordinateurs-sont-devenus-des-armes-letales_5306266_3232.html
- Ehrenzeller/Schindler/Schweizer/Vallender, Die Schweizerische Bundesverfassung, St. Galler Kommentar, Zurich/St. Gall 2014.
- Fichter, Adrienne, Rausgewunden, Stammtischpolterer in elegant: Wie Entscheidungsträger sich mit allerlei Floskeln um eine sinnvolle Debatte über Digitalisierung drücken – ein Erfahrungsbericht, publié sur republik.ch le 18.1.2018 : https://www.republik.ch/2018/01/18/altfuersten (consulté le 14.6.18)
- Flückiger, Alexandre, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ? AJP/PJA 2013, p. 837ss.
- Forteza, Paula/Frassa Christophe-André, Proposition de « Charte du numérique » à l'attention des présidents de l'Assemblée nationale et du Sénat français, Paris, 21 juin 2018.
- Gallusser, Martin / Ringger, Beat (Denknetz), Cyborgs, Blockchains, künstliche Intelligenz : Was kommt da auf uns zu ? Das Denknetz, 003/ Avril 2018, p. 14ss.
- Gencer, Adem Efe (et al.), Decentralization in Bitcoin and Ethereum, Cornell University Library, mars 2018 (résumé sur : http://hackingdistributed.com/2018/01/15/decentralization-bitcoin-ethereum/)
- Honsell, Heinrich/Isenring, Bernhard/Kessler, Martin, Schweizerisches Haftpflichtrecht, Zürich/Bâle/Genève, 2013
- Ito, Joichi, Resisting Reduction, Designing our Complex Future with Machines, a manifesto, 14.11.2017 sur https://jods.mitpress.mit.edu/pub/resisting-reduction
- Jaccard, Gabriel, Partie I : L'identité digitale et la création du surhomme 2.0, Jusletter du 30 avril 2018.
- Kerdellant, Christine, Dans la Google du Loup, Paris (Plon), 2017
- Kitano, Naho, Animism, Rinri, Modernization : the Base of Japanese Robotics, sur : http://www.roboethics.org/icra2007/contributions/KITANO%20Animism%20Rinri%20Modernization%20the%20Base%20of%20Japanese%20Robo.pdf
- Lampart, Daniel/Cirigliano, Luca, La numériation doit servir aux salarié(e)s : analyse et mesures requises, Dossier de l'USS, octobre 2017.
- Lohmann, Melinda, Ein europäisches Roboterrecht – überfällig oder überflüssig ? ZRP 6/2017, p. 168ss.
- Lohr, Steve, Data-ism ,The revolution transforming decision making, consumer behavior, and almost everything else, New York, 2015.
- Lorenzi, Jean-Hervé/Berrebi, Mickaël, L'avenir de notre liberté. Faut-il démanteler Google ?, Paris (Eyrolles) 2017.
- Maas, Heiko, Internet-Charta : Unsere digitale Grundrechte, Die Zeit, 10 décembre 2015.
- Morin-Desailly, Catherine, L'Union européenne, colonie numérique ? Rapport d'information fait au nom de la commission des affaires européennes, 2013.
- Morozov, Evgeny, silicon circus, blog sur : https://blog.mondediplo.net/-Silicon-circus-
- Nevejans, Nathalie, Règles européennes de droit civil en robotique, étude pour la commission juridique du Parlement européen, Bruxelles 2016.
- OCDE, Automation, Skills use and Training, Social – Employment and Migration Working Paper no 202, Paris, 2018, sur : https://www.oecd-

ilibrary.org/docserver/2e2f4eea-en.pdf?expires=1529935558&id=id&accname=guest&checksum=FF242B48771C2257167E7936E9DBEC75
- Oftinger, Karl/Stark, Emil, Schweizerisches Haftpflichtrecht, Zürich 1995
- PSS, Politique liée à Internet, Les chances offertes par Internet doivent profiter à tous, sans privilèges : papier de position adopté à l'AD de St. Gall du 5 décembre 2015.
- Perry Barlow, John, A Declaration of the Independence of Cyberspace, 8 février 1996 et Ertzscheid, Olivier, Une nouvelle déclaration d'indépendance du cyberespace, Libération du 9 février 2018.
- Rifkin, Jeremy, La nouvelle société du coût marginal zéro, Paris 2014.
- Rossnagel, Alexander, Eine Zukunft ohne Selbstbestimmung ? in : Spektrum Kompakt, Der Digitale Mensch, 4.10.2016, p. 41ss.
- Rouvroy, Antoinette, Des données et des hommes, Droits et libertés fondamentales dans un monde de données massives, Rapport à destination du Comité Consultatif de a Convention pour la protection des personnes au regard du traitement automatisé de données personnelles du Conseil de l'Europe, Strasbourg, 11 janvier 2016 (citée: Rouvroy, données).
- Rouvroy, Antoinette, Le gouvernement algorithmique ou l'art de ne pas changer le monde, La revue nouvelle, 8/2016 et sa version remaniée sur https://www.academia.edu/28370856/Le_gouvernement_algorithmique_ou_lart_de_ne_pas_changer_le_monde (citée: Rouvroy, algorithmes)
- Rouvroy, Antoinette, La transparence des algorithmes : un leurre ? Publié le 4 mars 2016 sur https://www.linkedin.com/pulse/la-transparence-des-algorithmes-un-leurre-antoinette-rouvroy/ (citée : Rouvroy, transparence)
- Schwaab, Jean Christophe, La licéité de l'évaluation et du « forced ranking » en droit suisse du travail, in Dunand/Mahon (éd.), La protection des données dans les relations de travail, Genève/Zürich/Bâle, 2017
- von Stockar, Thomas (et al.), Sharing economy – teilen statt besitzen, TA-Swiss, Zurich 2018, disponible ici : https://vdf.ch/index.php?route=product/product/download&eoa_id=9123&product_id=2090
- Thiel, Peter, De zéro à un, Comment construire le futur, Paris (JC Lattès) 2016.
- Ulmi, Nic, L'apprentissage de l'incertitude, « Horizons » du 5 juin 2018, sur : https://www.revue-horizons.ch/2018/06/05/lapprentissage-de-lincertitude/ (consulté le 18 juin 2018).
- Villani, Cédric, Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne, rapport de mission parlementaire, mars 2018.
- Wachter-Boettcher, Sara, Technically Wrong: Sexist Apps, Biased Algorithms, and other threats of toxic tech, New York, 2017
- Widmer, Michael/Hegyi, Stefan, Ethische Normen und Werte im Zeiten von Quantified Self, Jusletter du 5 février 2018.
- Wildhaber, Isabelle, Die Roboter kommen, Konsequenzen für Arbeit und Arbeitsrecht, ZSR 2016 I p. 315ss.
- Wolfangel, Eva, Wie sichern wir unsere Unberechenbarkeit ? in : Spektrum Kompakt, Der Digitale Mensch, 4.10.2016, p. 69ss.
- Wohlmann, Herbert, Das struktur- und gesellschaftspolitische Versagen des Kartellrechts, Jusletter du 23 avril 2018.

Notes et références :

[1] Cf. le résumé historique de Gallusser/Ringger, p. 15 ou l'introduction de Degryse, p. 9.
[2] https://www.republik.ch/2018/06/25/weltweite-webkunst?utm_source=newsletter&utm_medium=email&utm_campaign=republik%2Fnewsletter-editorial-250618 . Le Larousse définit les algorithmes ainsi : « Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur. » Les algorithmes ne sont pas forcément numériques (cf. l'exemple ci-dessus du métier à tisser Jaccard) : les recettes de cuisines et les jugements cliniques sont aussi des algorithmes.
[3] Rouvroy, données, p. 5ss.
[4] Gallusser/Ringger, p. 19, Degryse, p. 9
[5] https://www.lemonde.fr/europe/article/2011/08/08/emeutes-a-londres-la-presse-britannique-dramatise-et-tente-de-comprendre_1557250_3214.html
[6] Fichter
[7] Villani, p. 105
[8] CF, p. 105
[9] Degryse, p. 12
[10] No 380 juin 2018, p. 43
[11] Cf, p. 104
[12] Villani, p. 124, avec de nombreux exemples. Villani insiste toutefois sur le risque d'« effet rebond ».
[13] Voir l'exemple de la gestion de l'eau et l'optimisation de l'arrosage dans une oliveraie tunisienne sur https://abonnes.lemonde.fr/afrique/article/2018/06/22/en-tunisie-un-algorithme-met-de-l-huile-dans-les-systemes-d-irrigation_5319533_3212.html
[14] Villani, p. 130s. avec de nombreux exemples
[15] Villani, p. 127-128. Sur les lois, ou conjecture de Moore : https://fr.wikipedia.org/wiki/Loi_de_Moore
[16] Widmer/Hegi, Rz 5
[17] Villani, p. 195
[18] Denknetz 003/avril 2018, p. 26s
[19] Villani, p. 173
[20] Jaccard, N 70-71, 76. Voir aussi « L'Estonie, première cybervictime de Moscou » https://abonnes.lemonde.fr/international/article/2017/03/14/l-estonie-premiere-cybervictime-de-moscou_5093948_3210.html
[21] Références citées par Degryse, p. 9s., CF, p. 104
[22] Le progrès technique est-il toujours source de croissance ? Alternatives Economiques no 376, février 2018, p. 78s.
[23] Qui existe depuis la nuit des temps, comme le rappellent à juste titre Gallusser/Ringger, p. 19… Lire à ce sujet l'étude très détaillée de von Stockar, p. 137ss. et les références citées
[24] Même si l'effet de l'économie du partage sur l'environnement est incertain, cf. von Stockar, p. 148ss.
[25] Cf. l'interview de Hugues Sibille, Président du Labo de l'économie sociale et solidaire, dans le « Nouvelobs » : https://www.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE1450/l-economie-collaborative-accroit-les-inegalites-patrimoniales.html. Cf. aussi Degryse, p. 30ss et 51ss.
[26] Degryse, p. 49.
[27] Cités par Degryse, p. 49.
[28] Villani, p. 101 ; Interview de David Dorn in La vie économique 1-2/2018, p. 47ss.
[29] Alternatives Economiques no 380 juin 2018, p. 42, ainsi que : https://www.numerama.com/politique/245152-selon-le-mit-chaque-robot-introduit-sur-le-marche-du-travail-detruit-6-emplois.html et https://www.numerama.com/tech/340505-finalement-les-robots-ne-vont-pas-nous-voler-tout-notre-travail.html
[30] Cité par Degryse, p. 13 et 26
[31] Degryse, p. 13s., p. 32ss.
[32] Degryse p. 21s. et les références citées
[33] Degryse, p. 43
[34] Schwaab
[35] CF, p. 105. Voir aussi : https://abonnes.lemonde.fr/emploi/article/2018/07/01/numerique-la-nouvelle-fracture-sociale_5324053_1698637.html
[36] CF, p. 105
[37] Degryse, p. 40ss.

[38] Von Stockar, p. 147 et les références citées
[39] Degryse et les références citées, p. 24, 38s.
[40] Degryse, p. 50. Voir aussi : https://abonnes.lemonde.fr/emploi/article/2018/07/01/numerique-la-nouvelle-fracture-sociale_5324053_1698637.html
[41] Cf. par exemple ce récit d'une « transcripteuse » francophone de l'assistant vocal Cortana (Microsoft) https://www.laquadrature.net/fr/temoin_cortana
[42] Degryse et les références citées, p. 9ss. et p. 50
[43] http://moralmachine.mit.edu/hl/fr
[44] Rossnagel, p. 48
[45] Cf. à titre d'exemple : Naomi Klein, La stratégie du choc, La montée d'un capitalisme du désastre, paris 2013.
[46] Et donc l'essence même du contrat de travail, à savoir la rémunération par l'employeur du temps passé à son service par le travailleur.
[47] Avenir.Suisse. Le CF, p. 104, utilise, lui, les euphémismes de « modèles d'affaires innovants, nouvelles perspectives de revenu, conditions de travail plus flexibles »
[48] Gallusser/Ringger, p. 18
[49] https://blog.mondediplo.net/2017-12-13-Le-taylorisme-a-la-mode-hippie
[50] Comme le montre l'exemple de l'indemnisation des clients CFF pour les travaux sur la ligne de Berne en été 2018 http://www.rts.ch/info/suisse/9712679-defaillante-discriminante-l-application-d-indemnisation-des-cff-critiquee.html
[51] PSS, p. 2.
[52] Villani, p. 176, von Stockar, p. 146s.
[53] Von Stockar, p. 99.
[54] Degryse, p. 48
[55] Crawford, Villani, p. 163ss. Cf. aussi https://www.tagesanzeiger.ch/sonntagszeitung/itentwickler-sind-auch-nur-maenner/story/22557041 avec de nombreux exemples.
[56] CF, p. 105
[57] ATF 143 V 21 ; Arrêts du TF 1B_185/2016, 1B_186/2016 et 1B_188/2016 du 16.11.2016 (Facebook) ainsi que 1B_142/2016 du 16.11.2016 (Google/Gmail). Cf. aussi la motion 18.3379 de la CAJ-E et les motions Levrat 16.4082 et Schwaab 16.4080 qui l'ont initiée.
[58] https://www.24heures.ch/high-tech/facebook-debloque-contacts-erreur/story/24295694
[59] Rossnagel, p. 45
[60] https://www.theguardian.com/news/2017/may/22/how-facebook-allows-users-to-post-footage-of-children-being-bullied Tous les documents collectés par « The Guardian » à propos de Facebook se trouvent ici : https://www.theguardian.com/news/series/facebook-files Voir aussi ce document révélant les règles internes de FB pour « bannir » les utilisateurs : https://motherboard.vice.com/en_us/article/ne5nxz/leaked-documents-facebook-threshold-delete-pages-groups
[61] https://www.watson.ch/!5314555
[62] C'est par exemple le cas du premier ministre indien Narendra Modi ou d'Elon Musk, propriétaire de Tesla, https://www.rts.ch/info/monde/9605595-les-fans-d-elon-musk-ne-semblent-plus-tolerer-la-moindre-critique-contre-lui.html
[63] DDPS, Stratégie cyberrisques, p. 11, Rossnagel.
[64] Ce qui ne semble pourtant pas inquiéter le Conseil fédéral dans sa réponse à l'interpellation 17.3277.
[65] Widmer/Hegyi, N 27s
[66] Rouvroy, données, p. 44, qui parle de « normativité constitutive ».
[67] Le service australien des douanes utilise notamment un système conçu par IBM analysant le « risque terroriste » des passagers étrangers en partance pour ce pays, Villani, p. 149.
[68] Rouvroy, données, p. 18ss., 30s.
[69] Honsell/Isenring/Kessler, p. 5, Oftinger/Stark, p. 12
[70] Rouvroy, algorithmes
[71] Voir p. ex. cet exemple édifiant : http://www.wired.co.uk/article/uber-employment-lawsuit-gig-economy-leigh-day
[72] Rouvroy, données, p. 45
[73] Sonntagszeitung du 14.12.2014
[74] Voire aussi l'exemple d'un jeune malade du diabète donné par Mascha Madörin in Denknetz 003/avril 2018, p. 27s.).
[75] Crawford
[76] Rouvroy, algorithmes/données, p. 45
[77] Villani, p. 150.
[78] Brundage et al.

[79] https://abonnes.lemonde.fr/idees/article/2018/05/28/parcoursup-pourquoi-un-tel-choc_5305731_3232.html
[80] https://abonnes.lemonde.fr/societe/article/2018/06/02/les-lyceens-de-banlieue-et-les-embuches-de-parcoursup_5308639_3224.html?xtmc=parcoursup&xtcr=5
[81] https://www.alternatives-economiques.fr/boursiers-parcoursup-enterine-discrimination-sociale/00085018
[82] Carnegie-Mellon citée par le The Guardian https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study
[83] https://www.srf.ch/news/schweiz/rueckfallrisiko-bei-straftaetern-die-grosse-screening-maschine
[84] Wachter-Boettcher,, voire aussi son interview dans « Watson » sur https://www.watson.ch/digital/leben/156143365-warum-siri-es-lustig-findet-wenn-du-ihr-von-deiner-vergewaltigung-erzaehlst
[85] https://www.tagesanzeiger.ch/sonntagszeitung/itentwickler-sind-auch-nur-maenner/story/22557041
[86] Wachter-Boettcher,, voire aussi son interview dans « Watson » sur https://www.watson.ch/digital/leben/156143365-warum-siri-es-lustig-findet-wenn-du-ihr-von-deiner-vergewaltigung-erzaehlst
[87] https://abonnes.lemonde.fr/pixels/article/2018/06/27/epingle-pour-biais-raciste-microsoft-modifie-son-logiciel-de-reconnaissance-faciale_5321958_4408996.html
[88] Cf. le biais raciste du logiciel de reconnaissance faciale « Face API » cité à la note précédente, biais causé par une base de données de programmation contenant surtout des visages d'hommes blancs.
[89] Gallusser/Ringger, p. 17, Degryse, p. 52, Rouvroy, algorithmes. L'effet de contagion marche aussi dans l'autre sens, certains algorithmes d'évaluation de la solvabilité ayant tendance à juger que « les gens biens se lient entre eux » : https://www.journaldunet.com/ebusiness/le-net/1127850-attention-a-vos-amis-facebook-ils-pourraient-vous-couter-votre-pret/
[90] Rouvroy, algorithmes, qui parle même de « dictatures algorithmique ».
[91] Villani, p. 28
[92] Rouvroy, données. P. 25
[93] Rouvroy, données, p. 28ss.
[94] Expérience du MIT, citée par Rouvroy, données, p. 28
[95] Rouvroy, données, p. 28
[96] Une analyse des données détenues par FB parue sur http://www.tilllate.com/fr/story/donn%C3%A9es-facebook?ref=home-story-3 montre que sa connaissance de ses utilisateurs est très précise, même lorsque ceux-ci mentent ; FB a pu p. ex. déterminer le sexe d'un homme qui se faisait passer pour une femme.
[97] Widmer/Hegyi, Rz 29
[98] Interview dans « 20 Minuten » du 19.8.14
[99] Villani, p. 123
[100] https://www.lemonde.fr/technologies/article/2009/01/12/une-recherche-google-a-un-cout-energetique_1140651_651865.html
[101] Bilan du 4 juillet 2018, p. 16s.
[102] https://www.courrierinternational.com/article/desole-la-voiture-autonome-ne-mettra-pas-fin-aux-embouteillages?utm_term=Autofeed&utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter&Echobox=1530451622 . Voir aussi cet article sur le déclin des transports en commun dans de nombreuses villes de pays développés, parce que leurs usagers utilisent de plus en plus Uber : https://www.economist.com/international/2018/06/23/public-transport-is-in-decline-in-many-wealthy-cities?fsrc=scn/tw/te/bl/ed/publictransportisindeclineinmanywealthycitiesmissingthebus
[103] Google détient p. ex. 91,6% du marché mondial de la recherche en ligne selon statcounter.com cité par Gallusser/Ringger, p. 24
[104] Gallusser/Ringger, p. 18, Rouvroy, données, p. 6
[105] von Stockar, p. 140s.
[106] Villani, p. 29, qui donne notamment l'exemple de Netflix, dont un des dirigeants avoue qu'internaliser les développeurs qui utilisent les API maisons coûterait près d'un milliard d'USD par an.
[107] Cf. « Fermeture de BuzzFeed France : quel modèle économique pour les médias en ligne ? » Sur https://abonnes.lemonde.fr/actualite-medias/live/2018/06/08/fermeture-de-buzzfeed-france-quel-modele-economique-pour-les-medias-en-ligne_5311624_3236.html.
[108] Selon Gencer et al., les 4 plus gros mineurs de bictoin, resp. les 3 plus gros mineurs d'ethereum contrôlent 50% de leur blockchain respectifs.
[109] https://www.watson.ch/!100008372
[110]Cf. le cas d'un restaurateur lucernois sur https://www.watson.ch/!833465447, mais aussi ces exemples : https://www.watson.ch/!145590740 (influenceuse qui exige des prestations gratuites en « échange » de commentaires positifs) et https://www.numerama.com/business/333246-lufc-victime-dun-review-bombing-des-

opticiens-ou-comment-les-notes-sur-internet-cristallisent-les-passions.html (une association professionnelle d'opticiens qui tentent de saper la réputation d'une association de consommateurs sur FB).
[111] La Vie économique, 3/2018, p. 36
[112] https://www.journaldunet.com/ebusiness/le-net/1127850-attention-a-vos-amis-facebook-ils-pourraient-vous-couter-votre-pret/
[113] Wohlmann.
[114] Morosov, https://blog.mondediplo.net/2018-04-10-Pour-un-service-public-des-donnees
[115] Alternatives économiques no 379, mai 2018
[116] Il faut toutefois avoir à l'esprit que la gauche, les syndicats et les mouvements sociaux sont familiers de ce genre d'interventions massives sur les réseaux sociaux d' «agit-prop » ou de « *name and shame* », notamment en utilisant des outils comme « Thunderclap »…
[117] Dowek
[118] https://abonnes.lemonde.fr/pixels/article/2018/07/09/planebae-la-belle-rencontre-dans-un-avion-vire-au-cauchemar-pour-la-vie-privee_5328419_4408996.html?xtmc=planebae&xtcr=1
[119] Cf. l'exemple récent des opératrices des services d'urgence français accusées à tort d'être responsables de la mort d'une jeune femme dont l'appel à l'aide n'a pas été pris au sérieux : http://abonnes.lemonde.fr/les-decodeurs/article/2018/05/14/affaire-naomi-trois-operatrices-du-samu-mises-en-cause-a-tort-victimes-de-harcelement_5298898_4355770.html?xtmc=naomi_harcelement&xtcr=1
[120] DDPS, p. 13ss.
[121] Rouvroy, algorithmes
[122] Références citées par Degryse p. 9s.
[123] Rouvroy, données, p. 13s.
[124] Rouvroy, algorithmes
[125] Wolfangel, p. 74
[126] http://www.sciencemag.org/news/2018/05/ai-researchers-allege-machine-learning-alchemy
[127] Alternatives Economiques n 380 juin 2018
[128] Gallusser/Ringger, p.23
[129] Rossnagel
[130] Rossnagel
[131] Alternatives économiques, no377, mars 2018
[132] Lorrenzi/Berrebi
[133] Gallusser/Ringger, p. 19
[134] C'est-à-dire la capacité à observer et étudier la nature puis la reproduire – une machine sera p. ex. incapable de comprendre pourquoi une fourmi peut porter autant de fois son poids
[135] Fortezza/Frassa, cf. https://abonnes.lemonde.fr/pixels/article/2018/06/22/comment-des-parlementaires-veulent-inscrire-la-neutralite-du-net-dans-la-constitution-francaise_5319402_4408996.html
[136] Morin-Desailly, à propos de la France, mais le Constat est valable pour toute l'Europe
[137] Cf. aussi Maas, art. 12
[138] Gallusser/Ringger, p. 18
[139] Widmer/Hegyi, Rz 36ss, Rouvroy, algorithmes.
[140] Villani, p. 142s
[141] Elaborés notamment par Rouvroy, données, p. 51, Diakopoulos/Friedler et Villani, p. 146ss. (*Transparency by design, Ethics by design, Discrimination impact assessement*). Cf. aussi le postulat Marti (Schwaab) 16.4007.
[142] Lohmann, Villani, p. 140ss ; cf. aussi l'art. 15.1 RGPD
[143] http://ingenuingenieur.blog.lemonde.fr/2018/05/22/que-revele-une-premiere-analyse-du-code-source-de-parcoursup/
[144] Rouvroy, transparence
[145] Qui est responsable en cas d'accident impliquant une voiture autonome ? in Le Monde du 20 mars 2018.
[146] Jaccard, Rz 82ss.
[147] Jaccard, Rz 92ss.
[148] Cf. « Le terrifiant assistant de Google qui appelle le coiffeur à votre place » : https://abonnes.lemonde.fr/pixels/article/2018/05/16/le-terrifiant-assistant-google-qui-appelle-le-coiffeur-a-votre-place_5299701_4408996.html?xtmc=le_terrifiant_assistant_google&xtcr=1
[149] Madörin in Denknetz 003/avril 2018, p. 27
[150] Kitano
[151] Nevejans, chapitre 4 et les références citées
[152] Degryse, p. 43
[153] Wildhaber, p. 217ss.
[154] Maas, art. 4

[155] On pense notamment aux questions de vie et de mort en lien avec l'emploi des « robots tueurs ». Cf. notamment Villani, p. 152.
[156] Villani, p. 29, 152 ; cf. aussi l'art. 22 RGPD.
[157] Wolfangel, p. 70.
[158] Rouvroy, données, p. 49s.
[159] CourEDH : Huch Jordan c. UK du 4 mai 2001 24746/94, Kemalaloglu c. Turquie, 19986/06 (2012), N.34s. ; ATF 131 I 455 c. 1.2.5 et 135 I 113 c. 2.1 ; Schweizer in Ehrenzeller/Schindler/Schweizer/Vallender p. 305ss. et les références citées.
[160] Un exemple parmi tant d'autres, le tristement célèbres « forum 18-25 » de jeuxvideo.com, qui a notamment servi à organiser des raids numériques de masse contre des militantes féministes https://www.numerama.com/politique/222533-cyber-harcelement-sur-le-18-25-jeuxvideo-com-pourra-t-il-se-sauver-de-sa-communaute.html , attaques parfois couronnées de succès : https://www.numerama.com/politique/302215-le-06-anti-relous-desactive-apres-une-attaque-du-forum-18-25-de-jeuxvideo-com.html
[161] Cf. l'affaire #PlaneBae : https://abonnes.lemonde.fr/pixels/article/2018/07/09/planebae-la-belle-rencontre-dans-un-avion-vire-au-cauchemar-pour-la-vie-privee_5328419_4408996.html?xtmc=planebae&xtcr=1
[162] A propos des mesures prises en France : https://abonnes.lemonde.fr/pixels/article/2018/05/17/l-assemblee-nationale-muscle-les-sanctions-contre-le-cyberharcelement-de-groupe_5300473_4408996.html?xtmc=cyberharcelement&xtcr=1
[163] Maas, art. 13
[164] Contre-exemple : l'indemnisation des clients CFF pour les travaux sur la ligne de Berne en été 2018, pour laquelle les usagers doivent obligatoirement passer par une application qui ne fonctionne que sur certains smartphones récents : http://www.rts.ch/info/suisse/9712679-defaillante-discriminante-l-application-d-indemnisation-des-cff-critiquee.html
[165] Cf. ce cas tristement célèbre de parents youtubeurs étasuniens, qui la garde des enfants a fort heureusemen étét retirée et qui, une fois n'est pas coutume, ont été banni du réseau social : https://www.numerama.com/pop-culture/395780-aux-etats-unis-youtube-bannit-des-parents-qui-ont-piege-leurs-enfants.html
[166] Exemples sur : https://www.lemonde.fr/pixels/article/2018/05/26/ufs-surprises-deballages-et-comptines-sur-youtube-le-tunnel-des-videos-pour-enfants_5305043_4408996.html
[167] CNNum
[168] Villani, p. 37
[169] https://abonnes.lemonde.fr/pixels/article/2018/05/25/une-enceinte-connectee-d-amazon-envoie-une-conversation-privee-par-erreur_5304453_4408996.html Cf. aussi ce récit d'une transcipteuse de l'assistant vocal Cortana (Microsoft), parlant de nombreux enregistrements réalisés « par erreur » à l'insu des utilisateurs : https://www.laquadrature.net/fr/temoin_cortana
[170] Maas, art. 11
[171] minoritaire en doctrine, cf. Flückiger, p. 847s.
[172] Cf. l'initiative parlementaire Vischer 14.413. Flückiger, p. 851ss. PSS, p. 11s.
[173] PSS, p. 12s., Article 19, p. 2s.
[174] Rouvroy, données, p. 28ss.
[175] Villani, 148s
[176] CNNum, Gallusser/Ringger, p. 17, Villani, p. 30ss., 130ss. 196.
[177] https://blog.mondediplo.net/2016-12-15-Pour-un-populisme-numerique-de-gauche et https://blog.mondediplo.net/2018-04-10-Pour-un-service-public-des-donnees , mais aussi in Le Monde Diplomatique du 7 janvier 2017.
[178]Morosov : https://blog.mondediplo.net/2016-12-15-Pour-un-populisme-numerique-de-gauche (i. f.)
[179] Si tant est qu'il soit possible de les endiguer, question posée par Cuvelliez
[180] Cf. « Fermeture de BuzzFeed France : quel modèle économique pour les médias en ligne ? » Sur https://abonnes.lemonde.fr/actualite-medias/live/2018/06/08/fermeture-de-buzzfeed-france-quel-modele-economique-pour-les-medias-en-ligne_5311624_3236.html.
[181] Divers exemples de piratages de véhicules connectés sur : https://www.01net.com/actualites/voiture-connectee-voici-les-hacks-les-plus-fous-des-dernieres-annees-1043464.html
[182] « 20 minutes » du 21.6.18
[183] Gallusser/Ringger, p.23
[184] Si tant est que cela soit possible autrement qu'en théorie, mais tel n'est pas le sujet du présent document.
[185] Wohlmann.
[186] Alternatives Economiques, no 379, avril 2018, p. 43s.
[187] http://europa.eu/rapid/press-release_IP-18-4581_fr.htm
[188] Alternatives Economiques, no 379, avril 2018, p. 43s.

[189] Thomas Metzinger in https://www.watson.ch/!586642134
[190] cf. l'initiative parlementaire 18.420 (Glättli) à propos du vote électronique.
[191] Il faut distinguer l'identité digitale au sens large = toutes les données que l'on produit vs. l'identité digitale au sens étroit = ensemble des données qui permettent de s'authentifier, cf. Jaccard, Ch. 1.2. Il ne faut par ailleurs pas la confondre avec la signature électronique cf. Jaccard, Rz 48ss.
[192] Jaccard, Rz 23
[193] Jaccard, Rz 21
[194] Jaccard, Rz 32, 35 et 102
[195] Cf. l'initiative parlementaire 18.407 (Reynard)
[196] Décision du Conseil Constitutionnel 2009-580 DC du 10 juin 2009.
[197] http://www.rts.ch/info/suisse/9712679-defaillante-discriminante-l-application-d-indemnisation-des-cff-critiquee.html
[198] https://abonnes.lemonde.fr/economie-mondiale/article/2018/06/24/internet-la-bataille-du-cable-ne-fait-que-commencer_5320491_1656941.html . Google possède p. ex. déjà 4 câbles sous-marin et en possèdera 7 d'ici 2019. Les GAFA sont présent dans 22 consortiums qui exploitent de tels câbles.
[199] selon la définition de l'OIT : http://www.ilo.org/global/topics/decent-work/lang--fr/index.htm
[200] Maas, art. 7
[201] C'est ce à quoi pourrait conduire l'adoption d'une responsabilité sous la forme de « Risiko-Management », cf. Lohmann.
[202] Degryse, p. 47
[203] Cf. à ce sujet, avec beaucoup de détails et d'exemples : Schwaab