Préface

Lettre d'Amérique : le grand écart transatlantique

Il ne faut pas se laisser prendre au mythe : non, même à l'*ère du numérique*, abandonner toute vie privée n'est pas inéluctable ! Avec un peu d'ambition et de réflexion, nous pourrions probablement reprendre la main sur notre identité et sur notre *image numérique*, à condition toutefois de nous sortir des griffes des soi-disant spécialistes et de la technocratie. Il suffirait pour cela de remettre la vie privée à la mode et d'ouvrir à ce propos un débat public entre des citoyens informés et majeurs. C'est pourquoi je propose de mettre nos idées en ordre sur cette question qui fut souvent dévoyée.

Cessons tout d'abord d'accuser la technologie d'un travers qui n'est pas de son fait : ni le progrès technique ni la généralisation d'Internet ne doivent être blâmés pour les multiples indiscrétions qui nous dérangent chaque jour. La technique n'explique pas tout. S'il est aujourd'hui facile de troubler notre intimité, c'est à des entreprises et à des administrations très puissantes que nous le devons : ce sont elles qui saisissent, conservent et exploitent des données nominatives qui décrivent notre personne et nos comportements.

En Amérique, l'ordre juridique n'impose pas, comme cela semble être le cas en Europe, de protéger les données nominatives en fonction d'un véritable « impératif catégorique » semblable à celui qu'exprimaient déjà les lois allemandes et françaises des années 1970[1].

1. Bundesdatenschutz Gezetz, du 27 janvier 1977, et loi Informatique et libertés, du 6 janvier 1978.

On ne doit pas en déduire que le droit américain est indifférent à la vie privée ; ni que les lois fédérales, celles des États de l'Union et la jurisprudence négligent l'intimité des individus, la protection de leurs croyances, de leur domicile, de leurs biens et leur réputation. Le quatrième amendement de la Constitution garantit, par exemple, le citoyen contre toute perquisition et toute saisie abusives ; la jurisprudence a restreint la diffusion indue de faits diffamatoires ; et dans plusieurs secteurs précis comme la santé, la banque, la location de cassettes vidéo, etc., les données nominatives sont encadrées et au moins autant protégées en Amérique qu'en Europe.

Il est vrai qu'il faut être bien informé pour connaître et pour identifier ces diverses protections, et pour savoir comment, dans quelles circonstances et pourquoi certaines informations personnelles bénéficient d'une protection explicite alors que d'autres données nominatives peuvent être rassemblées, exploitées et disséminées presque sans limites. Ce système juridique ne découle pas d'un unique principe général fondateur. De très grandes organisations peuvent donc multiplier les traitements de données personnelles sans que les sujets fichés puissent s'y opposer ; personne ne sait en vérité et avec certitude ce qui est enregistré ni par qui ni pourquoi. Bref, il est difficile et compliqué de se prémunir contre un fichage dont on ne veut pas.

Renverser la pratique actuelle est pourtant tout à fait concevable : il suffit de jeter un coup d'œil vers l'Europe communautaire pour découvrir un monde autrement policé que le nôtre à ce propos. Face aux mêmes techniques que celles qui fonctionnent en Amérique, les options ouvertes aux Européens sont différentes. Nous pourrions donc non seulement nous inspirer de ce qui se passe actuellement en Europe, aller parfois plus loin afin que les gens puissent disposer de véritables *droits positifs* sur l'information qui les représente.

La réponse institutionnelle actuelle se résume à deux affirmations : 1) restreindre le traitement de l'information nominative dans l'entreprise privée entraverait la *libre expression* des affaires[2] ; 2) limiter la surveillance généralisée de la population par l'État, dit-on aussi, pourrait gravement menacer la sécurité nationale. Il en résulte que l'État fédéral peut rassembler à sa guise de l'information nominative sur les individus, dès que la sécurité nationale l'exige[3]. Il n'existe pour le moment aux États-Unis aucun

2. NDLR : on connaît la très grande importance des textes constitutionnels en Amérique. Parmi la dizaine d'amendements apportés à la Constitution américaine par le Bill of Rights (rédigé en 1789 mais ratifié deux ans plus tard, le 15 décembre 1791), le *premier amendement* instaure des règles beaucoup plus libérales que celles des autres démocraties occidentales : « Le Congrès ne prendra aucune loi limitant la liberté d'expression ou de presse » (notre traduction).

3. NDLR : en 2001 le Patriot Act a brutalement étendu les pouvoirs de l'exécutif au détriment des garanties judiciaires pour toute affaire qui relève d'une présomption de « terrorisme » (voir chapitre 6).

principe qui définirait « par défaut » ce que les bureaucraties publiques et privées peuvent – ou ne peuvent pas – faire avec les données personnelles qu'elles détiennent. Une situation très différente de celle qui prévaut en Europe et que Wolfgang Kilian[4] résume ainsi : « Contrairement au droit européen, le système américain suppose que tout ce qui n'est pas interdit est licite ! » Ceux qui déplorent cette situation aimeraient retrouver un vrai respect de la vie privée et de l'intimité, et restaurer des droits et des pratiques qui impliqueraient une vraie protection *omnibus* de la vie privée et de l'intimité, et que la technologie se mette au service de ce droit au lieu de le saper, comme c'est actuellement le cas.

La première priorité consisterait, peut-être, à formuler le principe général d'une protection des données nominatives. Cela pourrait reposer sur ce que l'on appelle en Europe une « base légale » qui impliquerait : un contrat explicite avec le sujet concerné (par exemple le contrat qui lie le client et sa banque ou le client et son fournisseur) ; on pourrait aussi imaginer que tout recueil de données personnelles résulte d'un mandat confié par le sujet à une grande organisation publique ou privée avec laquelle il est nécessairement en rapport étroit (pour les impôts, l'état civil, l'école des enfants, etc.) ; et considérer enfin que le sujet concerné doive exprimer son consentement avant d'être fiché et encarté (pour participer à un sondage ou à un panel de consommation, par exemple)[5].

Il serait aussi souhaitable que les systèmes d'informations nominatives soient bien connus par le grand public et que chacun, citoyen ou consommateur, puisse découvrir – par exemple sur un site Internet – ce qui est enregistré sur lui-même ; et que chaque individu dispose d'un *droit d'accès* aux informations personnelles qui le concernent, droit qui est admis depuis longtemps en France, en Allemagne ou en Suède notamment. Les abus ou les dissimulations devraient alors être clairement répréhensibles.

On pourrait, enfin, accorder *deux droits positifs au sujet fiché* : 1) celui de dire explicitement s'il accepte ou non que les données personnelles qui le concernent soient exploitées par un tiers ; et 2) qu'il bénéficie alors d'une contrepartie monnayable, d'une sorte de « droit de propriété » qui pourrait déboucher sur l'éventuelle exploitation commerciale des données en question[6]. Faute d'un tel accord, la règle *par*

4. NDLR : professeur émérite à la faculté de droit de Hanovre, W. Kilian est un expert respecté en matière d'informatique et de droit ; voir notre collectif auquel il fut associé ainsi que J.B. Rule et d'autres : Chamoux, J.-P. (1986). *L'appropriation de l'information*. LITEC, Paris, 99 sq.

5. NDLR : si un tel cadre existait, tout courtier de données nominatives devrait convaincre les gens d'adhérer à cette activité (cela conduirait sans doute à les rémunérer).

6. NDLR : voir à ce propos le chapitre 1 (géolocalisation), le chapitre 2 (risque algorithmique), le chapitre 7 (droit à l'oubli) et le chapitre 8 (protection des données et consumérisme).

défaut devrait être de respecter l'intimité du sujet et donc *qu'une telle exploitation soit prohibée*.

Aucune des hypothèses précédentes n'est vraiment nouvelle[7]. Plusieurs d'entre elles sont plus ou moins en vigueur en Europe. D'autres, déjà évoquées par la doctrine, n'ont jamais été appliquées en Amérique jusqu'à présent. Notre idée directrice est toute simple : nous voudrions illustrer concrètement comment *respecter sérieusement la vie privée en Amérique*, sans vouer pour autant aux gémonies ceux qui n'en ont que faire et qui livrent par conséquent leur intimité aux quatre vents, ce qui est leur affaire personnelle.

Bien des forces s'opposeraient, sans doute, à une telle évolution. Mais la cause n'est pas perdue d'avance d'autant qu'elle n'impose nullement de partir en guerre contre la technologie ; cela n'a d'ailleurs jamais été dans nos intentions, bien au contraire[8] !

James B. RULE
Université de Californie
Berkeley

7. NDLR : dédié à la mémoire de George Orwell, l'ouvrage publié par J.B. Rule *et al.* il y a quarante ans posait déjà les bases d'une analyse sociopolitique de la vie privée dans le monde moderne. Il annonçait en introduction et en substance que les gens commençaient à comprendre que certaines données d'ordre fiscal ou social pouvaient être détournées de leur finalité ; et l'indignation soulevée par de telles pratiques était le véritable objet de son livre : Rule *et al.* (1980). *The Politics of Privacy*. Mentor Books, New York, 5-6.

8. L'ouvrage à paraître : Rule, J.B. *Taking privacy seriously* (University of California Press, Berkeley), prolonge et précise les travaux entrepris par l'auteur depuis de nombreuses années sur ce vaste sujet.

Introduction

Des mœurs et des usages

Je ne peux introduire ce dernier volume de notre œuvre de collaboration sans exprimer ma profonde gratitude à tous ceux qui y ont apporté leur pierre : aux contributeurs qui se sont pliés, avec abnégation, aux règles qu'impose une ambition encyclopédique et didactique ; aux professionnels que nous avons, les uns et les autres, abordés, écoutés et dérangés pour nous transmettre leur expérience et leur compréhension des techniques et des savoirs de l'ère numérique ; aux savants collègues d'origines et de disciplines diverses, grâce auxquels nous avons repéré, au fil des ans et des lectures, le neuf et le vieux, le sûr et le probable et, parfois, le vrai et le faux.

Tous ont eu la patience et la courtoisie de nous aider à décrypter la complexité transfrontière du monde au sein duquel nous baignons depuis un demi-siècle, dont les clés, parfois invisibles, peuvent être trompeuses. Entamé il y a plus de cinq ans, l'exercice pourrait ne jamais s'achever ; nous y mettons un terme sans regret, sachant la vanité que suppose ce choix que l'on nous pardonnera, je l'espère ! L'aphorisme de Frédéric Bastiat, l'un des esprits libres du XIX^e^ siècle, plus connu en terre américaine que française, comme le fut longtemps Alexis de Tocqueville, nous suggère le clap de fin[1] : pour le numérique comme pour l'économie, ne jamais oublier que « derrière ce que l'on voit, ce que l'on ne voit pas permet aussi de comprendre le monde réel ».

Des cas d'école...

Juriste spécialisé dans les nouvelles techniques de communication et de l'Internet, Paul Salaün balise, dans le chapitre 1, les questions que posent les multiples objets connectés qui envahissent notre quotidien et les savoir-faire correspondants. Il porte

Introduction rédigée par Jean-Pierre CHAMOUX.

1. Bastiat, F. (2005 [1850]). *Ce qu'on voit et ce qu'on ne voit pas*. Romillat, Paris.

particulièrement son regard sur les libertés humaines et sur l'autonomie de la personne, sur nos rapports avec les automates et sur les options philosophiques qui guident les prosélytes du transhumanisme. Très attentif à l'évolution du droit européen sur lequel porte une partie de ce chapitre, l'auteur s'efforce toutefois d'inscrire la pratique dans le droit existant, sans pour autant exclure qu'il soit utile d'imaginer parfois des formes nouvelles dès lors qu'il est prouvé que la disruption l'exige vraiment. La *responsabilité civile* a bien intégré les questions technologiques[2]. Solidement fondé en jurisprudence, son diagnostic est circonspect : il souligne que la jurisprudence civile a relevé de nombreux défis depuis deux siècles, tant dans le droit romano-germanique qu'en droit anglo-américain de la responsabilité. Après avoir digéré des nouveautés majeures (les véhicules automobiles, les ascenseurs, l'électricité ainsi que les errements d'un objet mal identifié comme l'assistant connecté Alexa), nous devrions lui faire confiance à l'avenir. Longtemps, remarque-t-il, les robots furent cantonnés à des tâches d'exécution, programmables et répétitives : piloter une machine-outil, conduire un engin de mine, tondre une pelouse. Mais la rupture numérique, souligne-t-il, impose d'envisager que certaines tâches, conditionnées par les circonstances et par l'environnement du robot, posent à son propriétaire (et à son exploitant) des questions vraiment nouvelles : c'est le cas, très emblématique, de la conduite d'un véhicule autonome au sein de la circulation automobile, qui lui permet de poser de telles questions. La relative autonomie de la machine n'atteint pour autant pas encore les capacités mythiques qu'attribuent aux *cyborgs* (organismes cybernétiques) les auteurs de science-fiction, principalement américains. Ces *êtres*, essentiellement imaginaires, hantent le rêve éveillé de ceux qui tendent à confondre la réalité avec la fiction : les similitudes entre le robot et l'être pensant sont de pure forme et risquent d'induire une dérive romantique dont le praticien du droit doit absolument se méfier.

Le chapitre 2 est un véritable cas d'école : il s'appuie sur les travaux d'une équipe de recherche qui s'inscrit dans une tradition germanique dont le droit européen s'est assez largement inspiré, tant pour le droit de la concurrence qui régit les comportements économiques depuis plus d'un demi-siècle que pour *instaurer un équilibre* savamment calculé entre des agents économiques dont certains, les consommateurs, sont présumés faibles, tandis que d'autres, les marchands, sont présumés forts et organisés. Les trois auteurs, Florian Saürwein, Natascha Just et Michael Lätzer, abordent un aspect important de l'économie numérique : la pression qu'exercent des procédures algorithmiques, discrètes mais puissantes, sur les internautes en général, et sur les consommateurs en particulier. Alimentés par une

2. Article 1382 (nouvel art. 1240) du Code civil : « tout fait quelconque de l'homme qui cause à autrui un dommage oblige celui par la faute duquel il est arrivé à le réparer », une tradition analogue à celle du dommage en Amérique ou en Grande-Bretagne (*Tort law*).

masse considérable de données nominatives que recueillent les automates du commerce électronique, les moteurs de recherche ou les téléphones portables, les algorithmes des plates-formes numériques suggèrent des consommations, des services ou des divertissements dont ils présument que les destinataires sont friands (publicité personnalisée et ciblée, notamment). Ce chapitre décrit et compare diverses formes d'encadrement (réglementaire ou contractuel) qui pourraient neutraliser la crainte exprimée par une partie de la population qui se sent démunie face à la surveillance algorithmique. Prolongeant l'ordolibéralisme allemand, l'école de la régulation suggère souvent, depuis un siècle, qu'une régulation publique encadre le comportement des services publics, des réseaux, les marchés agricoles, l'énergie, les matières premières, etc. Protéger le consommateur contre la sollicitation des commerçants est l'un de ses soucis classiques. Il en est de même des locataires face aux bailleurs et les travailleurs de l'industrie face à leur employeur, etc. Les auteurs proposent une palette de remèdes pour contrer la défiance qu'exprime une partie du public envers les algorithmes : faut-il autolimiter l'initiative des annonceurs afin d'améliorer la relation du producteur à ses clients ? Développer une déontologie professionnelle ? Limiter l'intrusion des automates dans la vie du consommateur et de l'internaute (pour prévenir la vente forcée, par exemple) ? L'instauration d'une réglementation contraignante dans certains domaines entraînant une « police des algorithmes » pourrait être conçue à l'échelle communautaire en prolongeant les dispositions existantes sur la *protection des données personnelles*[3]. Les auteurs concluent toutefois avec circonspection : les applications algorithmiques sont récentes ; la société européenne, dans son ensemble, n'a réellement pas encore pris la mesure des risques véritablement attentatoires à nos libertés ni des retombées positives de ces méthodes, tout particulièrement en matière de santé publique et de prévention des risques majeurs d'ordre catastrophique ou cataclysmique[4]. Ce chapitre suggère donc des recommandations mesurées : tout devrait être fait, suggèrent les chercheurs, pour mieux décrire et pour comprendre la combinaison entre divers modes d'action, partiellement politiques et partiellement comportementaux. Conserver les algorithmes sous une surveillance attentive leur paraît l'objectif

3. Dispositions complémentaires de celles qu'étudient le chapitre 7 (le droit à l'oubli) et le chapitre 8 (informatique et libertés).

4. De nombreuses méthodes algorithmiques peuvent contrôler les épidémies. On piste les individus en localisant leur téléphone portable ; sous réserve d'inventaire, cela attire l'attention du porteur sur la présence de personnes infectées. Ces contacts successifs repèrent la propagation du virus ; cette méthode peut toutefois entraîner un *contrôle social* dont l'exemple emblématique est celui de la reconnaissance faciale que pratiquent les grandes villes chinoises (témoignage de Sébastien Faletti pour *Le Point*, 27 novembre 2018). Plusieurs pays (tels que Taïwan et la Corée du Sud) ont mis en œuvre de telles applications, mais avec un succès inégal (*Le Temps*, 29 août 2020).

minimum, jusqu'à ce que la pratique – et la jurisprudence – propose une action crédible pour garantir l'avenir de notre libre arbitre.

Comme l'ont illustré les chapitres 7 et 8 du volume 1, la santé et le soin sont des activités dont l'organisation et la perspective sont mises en cause par les outils numériques. Le traitement de données médicales concerne aussi bien les patients que les praticiens et les biotechnologies. Le chapitre 3 illustre l'effet des technologies de l'information sur l'ordre des choses et sur les pratiques professionnelles. Tirant parti de la méthode prospective, Sylvaine Mercuri Chapuis et Thomas Gauthier, tous deux enseignants-chercheurs, ont exercé conjointement à la Haute école de gestion genevoise (HEG). Ils ont conçu une étude qui consistait à construire des scénarios pour illustrer l'évolution du système de santé publique helvétique sous la pression des technologies numériques. Comme dans tous les pays modernes, la santé publique romande (cinq cantons de taille inégale : Genève, Fribourg, Neuchâtel, Vaud et Valais) est submergée par une demande de soins croissante. Ni la démographie vieillissante de ces cantons ni la capacité contributive des actifs ne paraissent en mesure de garantir une prise en charge durable de cette demande explosive. Cette analyse prospective a impliqué plus de soixante collaborateurs, en grande partie étudiants de la HEG de Genève. Elle a un double intérêt documentaire : d'abord parce qu'elle porte sur l'une des populations européennes les mieux pourvues en infrastructures, en revenus et en support logistique ; et parce qu'elle souligne qu'aucune « martingale » ne peut promettre au peuple suisse – ni dans les cantons francophones ni dans les cantons alémaniques ou italianisants – de sortir de l'impasse qui condamne les pays riches de la planète (États-Unis, Europe occidentale ou Japon, principalement) à laisser le coût de la santé dériver sans contrôle. Les résultats suggèrent que les nouvelles technologies peuvent effectivement soutenir l'effort de santé et contribuer à limiter la dérive budgétaire qui touche le soin, la thérapeutique et l'hôpital d'un pays moderne. Comme à peu près partout en Europe, recettes et dépenses ne sont pas équilibrées en Suisse ; la course au diagnostic est coûteuse et le prix des thérapeutiques ciblées augmente plus vite que la capacité contributive de la population. Le système de santé helvétique révèle des rigidités et des limites que confirme sa vulnérabilité aux imprévus[5]. Malgré son très haut niveau de vie et l'excellence de ses industries pharmaceutiques et instrumentales[6], ce système de santé dépend des échanges internationaux dans plusieurs dimensions essentielles. Comme bien d'autres pays, la Suisse est fortement intégrée au commerce et à la finance internationale ; cette force pourrait poser un problème si les frontières étaient moins ouvertes aux échanges

5. La pandémie de COVID-19 qui n'était pas inscrite dans les hypothèses de cette recherche, confirme ce diagnostic.

6. Industries concentrées autour de la capitale de la « pharma suisse », les cantons alémaniques de Bâle.

qu'elles ne l'ont été ces trente dernières années. La Suisse, d'autre part, manque de main d'œuvre dans les métiers de la santé (médecins, infirmiers, pharmaciens, thérapeutes, personnels de services, etc.) ; construits autour d'un mécanisme complexe d'assurances, de mutuelles et de coopératives, le soin et la médecine recherchent le Graal de l'équilibre financier sans l'atteindre. À travers les scénarios que résume ce chapitre, rien ne permet d'affirmer que la numérisation du diagnostic, du traitement et des prestations stabilise la demande de soin, le prix de la dépendance, celui de la gestion hospitalière et celui des actes médicaux. Les appareils connectés pourraient, certes, transférer aux patients une partie des tâches qu'effectuent les professionnels, tâches que des machines sont déjà en mesure de prendre en charge (simples analyses ou diagnostics, par exemple). Pour autant, la technologie n'est gratuite ni pour les professionnels ni pour les patients ; il conviendrait, au surplus, d'équiper des lieux pour cela. L'approche prospective atteint malheureusement ses limites quand le système établi (qui repose sur un flux tendu de services et de soins) bute sur l'imprévu : c'est donc (peut-être ?) à la gestion de crise que pourrait se consacrer la prochaine analyse prospective de la santé helvétique !

Le chapitre 4 aborde enfin un vaste sujet, fondamentalement international et de portée générale, celui de la *disruption numérique du secteur financier*, qui comprend les banques, les bourses, l'assurance et les intermédiaires non bancaires (fonds de pension et fonds d'investissement), ainsi que des instruments financiers typiquement numériques, tels que les *marchés de devises*, les *produits dérivés* ainsi que les *cybermonnaies* dont les volumes précédents ont évoqué le rôle novateur mais perturbateur pour la finance traditionnelle[7]. Résultat d'une longue coopération entre le coordinateur de l'ouvrage et deux contributeurs d'expérience, de formation et de perspectives différentes – Gérard Dréan, auteur de trois chapitres parus dans les volumes précédents et l'économiste Henri Lepage, observateur informé et critique du système financier international –, ce chapitre tente de repérer les éléments de convergence ou de fracture que provoque le numérique au sein des institutions monétaires que nous avons héritées de l'histoire. Cet héritage, l'économie contemporaine le remodèle constamment grâce à des technologies qui assurent l'ubiquité, le fonctionnement et la sécurité des marchés financiers et de la monnaie. Par contraste, les institutions monétaires proprement dites comme les banques centrales, la Banque mondiale, le Fonds monétaire international et le Trésor des grands pays modernes, dans leur dimension purement politique, s'avèrent prudentes. Écrit à plusieurs mains, ce chapitre poursuit les développements consacrés aux cybermonnaies dans les volumes précédents : il rappelle que la crise financière qui a perturbé la finance mondiale de 2007 à 2009 a provoqué la naissance du *Bitcoin*, première cybermonnaie conçue hors de tout impératif politique ou social. Malgré de vives critiques,

7. Voir les chapitres 5 et 6 du volume 1 et le chapitre 7 du volume 2.

le succès de nombreux jetons monétaires électroniques est indubitable. L'argent, le crédit et la monnaie ne sont pas sortis indemnes de cette crise et de la disruption induite par Bitcoin : des fissures ont perturbé l'ensemble (apparemment solide) de la finance mondiale. Quant aux institutions monétaires, établies il y a soixante-quinze ans, elles reposaient sur des principes que la société contemporaine n'admet plus : la convertibilité du dollar en or fut abandonnée en 1971 ; l'équilibre économique et politique de la planète n'est plus celui d'après la conflagration mondiale de 1939-1945. Les crises financières qui ont secoué le monde depuis 1950 ont posé des questions qui restent irrésolues à ce jour, bien que vivement débattues par moment[8]. L'époque est donc propice pour ressortir des bibliothèques les analyses subtiles (parfois visionnaires) d'auteurs dont les essais sont trop oubliés aujourd'hui !

… et des questions politiques

Quatre questions sont abordées et mises en perspective avec un détail particulier dans les chapitres suivants. Le chapitre 5, conçu par Paul Salaün déjà cité, fait le point sur une expression attrape-tout qui agite le microcosme professionnel et les régulateurs depuis plus de trente ans. Il aborde une question séminale : le management des réseaux d'Internet – qui sont les héritiers directs des infrastructures téléphoniques – peut-il se soumettre à une norme simple et générale, inspirée par l'histoire qui considérait les télécommunications comme une infrastructure universelle et lui imposait, sans biais ni privilège, de transmettre la pensée, le savoir et les échanges interpersonnels au profit des êtres humains dans leur ensemble ? On verra dans ce chapitre combien cette prétention universaliste est décalée par rapport aux réalités du XXI^e^ siècle et ce qu'une telle ambition peut avoir de réducteur. La neutralité des réseaux est une question polysémique que la littérature aborde depuis des années sans pour autant guider le lecteur, même informé, ni asseoir son jugement. Les *variations* de Paul Salaün introduisent un peu d'ordre dans ce sujet débattu d'une façon désordonnée. La croissance spectaculaire des firmes qui animent le Net mondial et leur poids financier[9] entraînent une partie de la doctrine à penser qu'il faudrait encadrer ces mastodontes que plébiscitent les internautes. Inspirés par une tradition de « service universel », on

8. Au-delà du Bitcoin évoqué *supra*, on songe au défi lancé par F. von Hayek en 1974 : imaginer la concurrence généralisée entre les monnaies *fiat*, un sujet résumé dans l'annexe A du chapitre 4 (voir (Hayek 1990)), ainsi qu'au projet Libra (renommé Diem en 2000) domicilié à Genève et soutenu par Facebook depuis 2019.

9. Il s'agit évidemment des cinq titres les plus en vue de la bourse américaine : Google (ou plutôt Alphabet), Apple, Facebook, Amazon et (en mode plus mineur à ce jour) Microsoft, firmes dont les valorisations boursières sont impressionnantes. Depuis début 2020, en pleine crise sanitaire, l'importance de ces entreprises, portées par la demande de services à distance, a encore augmenté.

pourrait, par exemple, imposer aux opérateurs du réseau des contraintes analogues à celles que supportait le téléphone d'antan. Mais l'auteur démonte plusieurs *fables* qui remontent au temps, bien antérieur à Internet, où les réseaux de communication n'avaient qu'un seul usage : depuis le XIX^e^ siècle, les fils du téléphone ne transmettaient que la voix. Sauf en Amérique du Nord, ces lignes étaient une propriété de l'État, exploitée par un service public. Peu répandu en dehors des pays industrialisés, le téléphone fournissait des prestations uniformes, une prescription liée, en France, à la *neutralité* du service public qui interdisait toute différentiation entre les bénéficiaires. Paul Salaün décline les multiples connotations d'une expression qui ressemble à une *auberge espagnole* ! Mise à toutes les sauces, la *neutralité du réseau est trop polysémique pour guider l'action*. En définitive, les querelles (politiques, doctrinales ou judiciaires) qui ont opposé depuis trente ans les multiples parties impliquées dans la croissance d'Internet, laissent un goût amer. Les arguments, souvent byzantins, avancés par les uns et par les autres pour convaincre le public, les autorités ou la justice, principalement en Amérique du Nord et en Europe, se résument en quelques mots : certains tentent de reformuler le *principe d'un service public* étendu aux réseaux actuels, avec l'espoir qu'Internet soit inspiré par une politique redistributive ; d'autres aimeraient cantonner les plates-formes et briser les plus grands (les GAFA) au profit d'agents dispersés ; d'autres, enfin, voudraient réhabiliter les institutions qui régulent la communication pays par pays, des autorités remises en cause car la globalisation d'Internet les rend ineffectives.

Le sujet qu'aborde Pierre Schweitzer est très différent du précédent : le chapitre 6 pose des questions clivantes, comme toutes les interrogations qui portent à la fois sur la *grande politique* et sur la *politique de l'ombre*, toutes deux chères à Machiavel, dans un rapport profondément dialectique. Entre l'utopie d'une « transparence absolue » (qui exposerait tout un chacun à la curiosité plus ou moins malsaine du passant) et l'opacité des régimes qui jouent cyniquement avec leurs semblables ou avec leurs penchants pervers, la raison espère encore qu'une société policée soit possible. Internet a dévoilé, sous diverses formes, ce qu'il y a de pire et de meilleur chez les êtres humains et dans leur vie sociale. Bien fourni, ce chapitre parcourt avec subtilité les dérives, les scandales et les pratiques qui agitent périodiquement le réseau des réseaux depuis que les *grands de ce monde* tentent d'en mettre les performances au service de leurs ambitions politiques. Nous touchons là une matière où la réalité côtoie en permanence la fiction, où les comportements réels dépassent ce que l'on peut imaginer ; bref, il s'agit d'un champ où se croisent la *real politik* et l'instinct guerrier ! Ces pages ont le grand mérite de ne guère laisser de question dans l'ombre ; et de souligner que les vingt dernières années ont été marquées par un usage débridé des technologies d'information et de communication, partout dans le monde, souvent au détriment de notre insouciance et de notre tranquillité. La série dramatique d'attentats qui a frappé l'Amérique du Nord en septembre 2001 a renversé durablement les

priorités politiques. Comme au temps de la *guerre froide*, la surveillance des hommes, de leurs actes et de leurs avoirs est redevenue prioritaire, au détriment de la liberté d'agir, de jouir de ses biens, d'aller et venir ainsi que de franchir les frontières sans obstacle. Les tolérances que nous avions fini par considérer comme des droits ont été mises en cause. La défiance remplace l'optimisme qui caractérisait la société américaine depuis très longtemps. Elle a cédé devant la raison d'État et mis la puissance technologique des industries numériques au service de la puissance tutélaire et répressive du gouvernement fédéral et de ses administrations centrales. Pierre Schweitzer s'est immergé avec mesure dans ce sujet plein de non-dits ; il décrit les faits et les circonstances, les événements remarquables et les personnages clés de cette période qui a provoqué une *révolution copernicienne* dans les mœurs politiques, un changement de perspective dont nous ne sommes pas près de sortir car les attentats du 11 septembre ont créé un climat de suspicion dont les comportements sont imprégnés. L'auteur revient sur les faits caractéristiques de ces années charnières (2001 à 2012 à peu près), sur le rôle et sur l'inspiration des « lanceurs d'alerte » qui ont défié la puissante Amérique, ainsi que sur l'effet qu'ont eu ces événements sur le reste du monde. Il décrit le revirement brutal de priorité politique qui caractérisa cette période. En s'appuyant sur le cas de la France, il montre qu'une nation impliquée depuis des siècles dans une partie du monde où la menace panislamique est très active, multiplie des dispositions coercitives, parfois liberticides. Que, sous prétexte d'ordre public, des juridictions et des procédures d'exception antinomiques avec un état de droit équitable et serein, se multiplient. Il souligne également l'interaction entre l'inflexion sécuritaire de nos institutions et la tendance inquisitoire qui encadre désormais la personne humaine et le citoyen, sa vie privée et son autonomie. Ce chapitre fait écho aux thèmes des chapitres suivants, mais sous une forme différente.

Le chapitre 7 reprend et synthétise l'étude sur le *droit d'être introuvable* qu'a réalisée Michel José Reymond, enseignant-chercheur à l'université de Genève, alors en résidence au Berkman-Klein Center for Internet & Society de l'université Harvard grâce à une bourse du Fonds national suisse. Bien circonscrite, cette étude est d'intérêt général : l'arrêt rendu par la Cour de justice européenne le 13 mai 2014 (dit « Google Spain »), a tranché une question qui conditionne l'exercice de deux droits fondamentaux pour l'*individu numérique*, l'un et l'autre définis par les textes préexistants en Europe – *droit d'accès* du sujet aux enregistrements nominatifs que conserve un tiers et *droit de faire rectifier* des enregistrements litigieux, deux questions que ni les lois nationales ni le Règlement européen sur les données personnelles (RGPD 2016) n'avaient vraiment cadrées. Michel José Reymond démonte les faits et l'argumentation des parties d'un contentieux qui est lié à la mise en œuvre du règlement pourtant postérieur à cette cause. Un arrêt plus récent (« Google CNIL » du 24 septembre 2019) insiste d'ailleurs sur le *caractère relatif de la protection des données* au regard d'autres principes que la Cour juge d'un ordre

supérieur comme la *libre expression* et l'*accès à l'information*. Il conclut que le *droit à l'oubli numérique* et le *déréférencement* par un moteur de recherche ou par une plate-forme Internet sont des notions délicates à mettre en œuvre et que la Cour de Luxembourg a pris un chemin de traverse en confiant à Google le soin de gérer des cas d'espèce par une procédure quasi arbitrale qui pourrait être considérée, si elle se prolonge, comme essentiellement discrétionnaire.

Soigneusement préparé et documenté par Michel José Reymond, le chapitre 8 complète cette seconde partie de l'ouvrage. D'inspiration personnaliste, la doctrine élaborée en Europe au début des années 1970 reposait sur deux principes : le respect de la personne humaine et de sa vie privée ; la hiérarchie des normes qui plaçait l'individu et son autonomie à un niveau supérieur à celui de l'un quelconque de ses intérêts économiques, jugeant que la considération de la personne humaine dépasse ses intérêts matériels, quelle qu'en soit l'importance. Priorité était donc accordée à un droit personnel, d'essence supérieure à l'utilité économique, une démarche cohérente avec le mandat du Conseil de l'Europe depuis sa fondation à Strasbourg en 1949[10]. Les lois promulguées dès 1973 en Suède (pays extérieur à l'Europe communautaire), aux États-Unis (1974), en Allemagne fédérale (1976) et en France (1978) étaient donc en harmonie avec la Convention 108 du Conseil de l'Europe (1981), mais sans lien direct avec les prérogatives de la Commission européenne. Ces textes fondateurs n'avaient au demeurant pas pour objet de *protéger des données*, mais d'éviter que les données nominatives puissent *mettre une personne humaine sous la tutelle d'une machine* ou d'un processus machinal qui limiterait son autonomie, sa liberté d'agir ou celle de s'exprimer. De tels droits n'ont aucun rapport avec un quelconque *droit de propriété* comme on a pu le laisser entendre par excès de langage ; accordés à la personne fichée, ils donnent seulement au *sujet de droit* un *droit d'accès et de regard* sur les enregistrements qui le concernent nommément ; et l'autorisent à en faire rectifier la teneur s'il s'avère qu'ils comportent des inexactitudes (*droit de rectification*). La démarche communautaire suit désormais une tout autre piste : elle vise à établir une *libre circulation des données en Europe*, facilité étendue, sous réserve de réciprocité, à des pays tiers comme les États-Unis. Ce droit européen rapproche la protection des données personnelles des droits reconnus au consommateur, ce que confirme le Règlement général pour la protection des données personnelles (RGPD) entré en vigueur en mai 2018. Après avoir situé le régime des données personnelles dans sa perspective historique, ce chapitre précise la portée de ce règlement qui renforce le rôle que tient la Commission européenne pour organiser l'échange international et la conservation des données massives que rassemblent les plates-formes Internet comme Google, Facebook ou Amazon sur l'ensemble des internautes. L'effet de ce règlement

10. Qui n'avait qu'un lointain rapport avec l'objet économique et social des communautés européennes.

européen n'est pas négligeable ; plusieurs contentieux l'ont déjà mis en évidence. L'un d'eux est cité au chapitre 7 (« Google LLC contre CNIL », 24 septembre 2019). La position dominante des plates-formes américaines, très prisées par les Européens, soulève des questions délicates du seul fait que ces grands intermédiaires ont une très forte présence en Europe et que leurs fichiers nominatifs sont traités et conservés ailleurs qu'en Europe, notamment aux États-Unis où les données concernant les étrangers sont facilement accessibles aux autorités policières ou judiciaires[11].

Évolution ou rupture ?

Le chapitre 9, conçu par Ejan Mackaay, doyen honoraire de la Faculté de droit de Montréal, s'efforce de situer les thèmes précédents dans leur perspective sociétale. Les démocraties occidentales sont en effet écartelées entre deux penchants contradictoires : celui de garantir à leurs peuples les libertés positives promises par leurs institutions ; et celui de protéger ces mêmes peuples contre l'imprévu et contre des menaces extérieures qui pourraient déstabiliser ces mêmes institutions. Maintenir l'équilibre entre l'État nounou et l'État libéral n'est jamais évident : Tocqueville a déjà posé ce dilemme dans les termes suivants : « L'amour de l'ordre se confond avec le goût des tyrans ; et le culte saint de la liberté avec le mépris des lois. »[12] Comment résoudre cet apparent dilemme ? Dans ce chapitre, Mackaay compare le comportement de cinq grandes démocraties qui, confrontées aux événements dramatiques de ces dernières décennies, ont réagi bien différemment les unes des autres.

11. La Cour de justice de l'Union européenne a répondu à une question préjudicielle à ce propos (dossier C 311.18 : Data Protection commission/Facebook Ireland & Maximilien Schrems) : tout transfert de données nominatives vers des pays tiers doit être subordonné à des garanties équivalentes de celles qu'offre le droit européen (RGPD). Ce n'est actuellement pas le cas de la loi américaine ; l'exportation de données nominatives vers les États-Unis est donc restreinte. Pour un commentaire de cet arrêt, voir : Bradford, A. (2020). Broken Shield: Privacy vs Surveillance in Europe. European Council for Foreign Relations, 30 juillet [En ligne]. Disponible à l'adresse : www.ecfr.eu/article/commentary_broken_shield_privacy_versus_surveillance_in_europe.

12. Tocqueville (de), A. (1981). *De la démocratie en Amérique*, volume 1. Flammarion, Paris, 68.