Quelques réflexions d'avant-propos

Poullet, Yves

Published in:
L'Europe des droits de l'homme à l'heure d'Internet

Publication date:
2019

Document Version
le PDF de l'éditeur

QUELQUES RÉFLEXIONS D'AVANT-PROPOS

Yves POULLET
Professeur émérite de la Faculté de droit de Namur
Professeur associé à l'Université catholique de Lille
Membre de l'Académie royale de Belgique

Considérations liminaires

1. Le propos de cette introduction est double. Notre premier souci est de mettre en exergue ce qui nous est apparu comme la démarche suivie dans les écrits des nombreux contributeurs. Le lecteur y trouvera notre lecture de ces écrits, elle n'épuise pas – loin s'en faut – l'apport d'experts de leurs auteurs mais cherche à mettre en relief chaque apport dans ce compendium dont les éditeurs, mes collègues Cécile de Terwangne et Quentin Van Enis, ont conçu la logique de façon plus qu'heureuse. Mes commentaires suivent strictement le plan qu'ils avaient assigné à l'ouvrage. Dans un premier temps, trois contributions introduisent le débat « Droits de l'homme à l'heure d'Internet » par quelques propos transversaux. Ensuite, dans un second temps, les éditeurs ont eu soin d'ordonner les seize autres apports autour de thématiques liées à chacun de ces droits de l'homme traditionnels ou prétendument nouveaux. Sans doute, les considérations soumises au lecteur croisent parfois les regards de leurs auteurs à propos des mêmes jugements ou des mêmes événements mais comment ne pas apprécier l'enrichissement que cette confrontation apporte ?

2. Le second propos est plus personnel et nous espérons que les auteurs et éditeurs ne nous en tiendront pas rigueur. Au terme de la lecture, quelques réflexions nous sont venues sur ce paysage des droits de l'homme à l'heure d'Internet, il nous est apparu que si cette question des droits de l'homme est chaque jour plus cruciale dans notre monde numérique, ce monde multiplie les conflits entre ces droits, oblige à préciser ces droits, peut-être à les compléter et certainement à les hiérarchiser et

en tout cas à en chercher l'équilibre. Tout cela ne peut se faire qu'avec « juris-prudence », celle d'abord de nos deux cours européennes au fur et à mesure des cas qui se présentent à elles. Elles nous incitent à nous exprimer sans dogme ni *a priori*. Nous souhaitions faire part aux lecteurs de cet ouvrage de ces réflexions certes inchoatives et peut-être menées sans le recul suffisant. Nous avons voulu ces dernières brèves, sachant l'impatience du lecteur à découvrir l'essentiel de l'ouvrage.

I. Aperçu commenté des propos tenus dans l'ouvrage

Les questions « transversales »

3. Trois contributions alimentent le propos. La « gouvernance » d'Internet ou plus précisément des droits de l'homme sur la toile fait l'objet des réflexions de Mme Husson. Avec raison, elle souligne l'élargissement que la notion de gouvernance introduit par rapport à celle de réglementation voire celle de régulation. Reprenant la formule du Groupe de travail institué par le Sommet Mondial de la Société de l'Information (« SMSI ») : « Il faut entendre par gouvernance d'Internet l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leur rôle respectif, de principes, normes, règles, procédures de prise de décisions et programmes communs, propres à modeler l'évolution et l'utilisation d'Internet, évolution dans le sens technologique, utilisation au sens des pratiques », elle souligne deux points essentiels : le besoin de coordination des acteurs publics et privés et, par ailleurs, la nécessité d'un regard socio-politique, seul capable de comprendre en quoi cette gouvernance est le reflet des rapports de force entre acteurs.

La réalité globale d'Internet, son a-territorialité remet en cause la souveraineté des États et justifie la volonté de certains de développer ce qu'elle appelle une diplomatie du numérique ayant pour objet la domination sur Internet. A cet égard, l'auteur examine la manière dont l'Europe, en matière tant de liberté d'expression (affaire *Yahoo !*) que de protection des données (affaire *Schrems* et RGDP), tente d'exporter un modèle européen de développement d'un Internet promouvant les droits de l'homme. A cette « politique » des États, doit répondre l'expression collective des citoyens qui doit être entendue dans ce vaste *multistakeholder partnership* appelé de ses vœux par le SMSI. Peut-être considérera-t-on comme utopique son appel, à la suite de HARDT et NEGRI pour une « révolution démocratique », le règne de la « multitude » des cultures, des

opinions, des projets, des pouvoirs contre celui de « l'Empire » caractérisé par l'unicité d'un modèle imposé par les puissances du Net ? À cette unicité de modèle, doit répondre une « multitude » de réseaux citoyens, capable de construire *bottom up* un ordre mondial fondé sur les libertés, la justice et la paix.

4. Le rappel de la recommandation du Rapporteur spécial des Nations unies sur le rôle des entreprises privées dans la promotion des droits de l'homme sur Internet introduit la contribution de P. Fr. Docquir, consacrée à la confrontation entre droits fondamentaux et puissances privées… c'est-à-dire, soyons clairs, les GAFAM. Que dit cette recommandation ? « Les réseaux appartenant à des acteurs privés étant aujourd'hui des outils indispensables à l'exercice de la liberté d'expression, leurs opérateurs ont une fonction sociale et publique éminemment importante. Qu'elles répondent à une demande des pouvoirs publics ou à des intérêts commerciaux, les décisions prises par les acteurs du secteur peuvent avoir un effet direct, positif ou négatif, sur la liberté d'expression et les droits qui y sont associés ». Qu'en déduire ? L'auteur rappelle l'effet horizontal de la Convention européenne des droits de l'homme. Gardiens de la protection des droits de l'homme tant en matière de liberté d'expression que de vie privée, ces acteurs privés se réfugient derrière les conditions générales d'accès aux services pour prétendre que les règles du jeu ont été acceptées par les utilisateurs de leurs plateformes et services. Or, comme le montre l'auteur, ces acceptations sont fictives et les règles sont à ce point imprécises qu'elles manquent aux conditions de transparence et de prévisibilité exigées par le Conseil de l'Europe.

L'auteur voit dès lors dans l'obligation positive faite aux États d'assurer la protection des droits de l'homme dans les relations entre personnes privées, le devoir, eu égard aux risques encourus par nos libertés du fait de ces puissances privées, d'intervenir et de mettre en place une réglementation contraignante. Il s'agit d'obliger ces puissances du Net à développer un système qui permette efficacement de lutter contre les « *fake news* », à lutter contre les violations de la propriété intellectuelle par des logiciels de vérification des contenus diffusés… On pourrait étendre cette liste de devoirs dans le domaine des autres libertés, celle de la vie privée en particulier, mais également de la non-discrimination… [1]

[1] À noter en ce sens, la déclaration adressée par le Conseil de l'Europe à l'ICANN, rappelée par une autre auteure, Mme Turgis : « ces droits devraient primer sur les conditions générales d'utilisation des services de sociétés internet du secteur privé et sur les activités d'organismes spécialisés dans des missions techniques, comme l'Internet Corporation for Assigned Names and Numbers (ICANN) ».

À l'appui de cette thèse que l'auteur malheureusement esquisse à peine, on notera que, dans d'autres domaines jugés également essentiels pour le développement des citoyens, l'État n'a pas hésité à imposer aux opérateurs de tels services pourtant privés des devoirs et obligations, tel le service universel minimum ou le recours à des *ombusdmen*. Dans le cas des GAFAM, dans la mesure où ces entreprises offrent des services essentiels d'accès à des contenus et à la communication sociale, ne faut-il pas au nom des droits fondamentaux rappelés ci-dessus recourir à la même technique ? Le fait que les services qui aujourd'hui sont réglementés, étaient autrefois des services publics relevant de l'autorité publique et que les services des Google, Amazon, Facebook, … ne l'ont jamais été, ne modifie en rien notre propos.

5. De l'exposé de Mme Turgis : « Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité », nous retenons d'abord ce beau principe de neutralité que l'auteur énonce sur base de nombre de déclarations : « les libertés doivent être protégées sur le Net comme ailleurs, ni plus, ni moins ». Ce principe de base n'empêche pas que la réalité d'Internet force à la reconnaissance de nouveaux aspects de ces droits de l'homme et à la création de nouveaux droits subjectifs. Ainsi, la liberté d'expression oblige dans notre monde du numérique à la reconnaissance d'un droit d'accès à la toile (arrêt *Yildirim*) et le secret des correspondances signifie bien le secret des communications électroniques (arrêt *Copland*). La liberté d'expression connaît également des besoins d'adaptation : le blogueur doit être reconnu dans la même fonction de « chien de garde » que le journaliste. De manière plus générale, c'est à une nouvelle compréhension de la notion de média que la considération de la réalité d'Internet conduit. Comme le note le Conseil de l'Europe, « dans le cadre d'une approche différenciée et graduelle, chaque acteur dont les services sont considérés comme un média ou une activité intermédiaire ou auxiliaire bénéficie à la fois de la forme (différenciée) et du niveau (graduel) appropriés de protection, et les responsabilités sont également délimitées suivant le même schéma ».

Ceci dit, l'auteure met en garde contre la tentation de l'efflorescence de nouveaux droits de l'homme liés à Internet, tant en matière de liberté d'expression (droit d'accès à Internet, droit à la culture, droit à la transparence, ...) que de protection de la vie privée (droit à l'anonymat, droit à l'oubli, droit à la portabilité, …). Très justement, si elle reconnaît que ces droits, qu'elle qualifie de simples droits subjectifs « gigognes », s'articulent et dérivent des droits fondamentaux, elle s'inquiète comme nous

de la propension des législateurs et de certains auteurs de doctrine à les qualifier de droits fondamentaux, au risque d'un affaiblissement de la notion : « Envisager une modification de la liste des droits de l'homme, en y consacrant de nouveaux droits pose la question de l'utilité, voire du caractère contreproductif d'une telle démarche : lorsque tout devient fondamental, rien ne l'est plus vraiment ». Ainsi, par exemple, l'auteure analyse le droit d'accès à Internet non comme un droit de l'homme mais comme une conséquence de l'obligation positive de l'État de favoriser la liberté d'expression de chacun, obligation traduite par la création d'un service universel. Une telle précaution est sage et nous paraît, comme nous le dirons plus loin à propos d'autres contributions, mettre en question la reconnaissance, par la Charte des droits fondamentaux de l'Union européenne, des droits de propriété intellectuelle et de protection des données à caractère personnel comme « droits de l'homme ».

Les questions thématiques

6. Quatre thèmes ont été retenus : le premier : la liberté d'expression, le deuxième : la vie privée, le troisième rassemble une analyse des « autres » droits. Ce thème s'interroge sur l'impact d'Internet sur les droits à la culture, à la propriété intellectuelle ou à des élections libres et ensuite aborde le « sort » des droits des enfants et des détenus du fait d'Internet. Enfin, le dernier thème s'interroge sur les moyens d'action mis en place pour garantir le respect des droits de l'homme tant par le renforcement du rôle des autorités de protection des données que par les balises mises aux procédures d'investigation en cas de recherche d'infractions sur la toile.

Liberté d'expression

7. La contribution de Quentin Van Enis examine de manière générale la compatibilité de toutes mesures de filtrage et de blocage de contenus avec le droit à la liberté d'expression. On sait que ces mesures peuvent se justifier par la protection des jeunes, par la défense de la propriété littéraire et artistique mais également par l'illégalité de propos racistes ou diffamatoires ou des jeux proposés en ligne. L'auteur rappelle la différence entre filtrage et blocage, « le blocage d'un contenu spécifique n'implique pas nécessairement un filtrage préalable », concepts qu'il distingue du concept de retrait qui vise à supprimer ou effacer un

contenu à la source. L'auteur rappelle que la mise en cause de la liberté d'expression ne concerne pas uniquement l'auteur ou l'éditeur mais également l'intermédiaire qui gère l'infrastructure d'accès. Ce dernier, privé du droit de recevoir des informations, pourrait-il invoquer directement la liberté d'expression pour s'opposer à une mesure de blocage ou de filtrage ?

Au-delà de cette question, l'auteur s'interroge sur la possibilité cette fois pour un utilisateur de mettre en cause la mesure de blocage ou de filtrage. Peut-il se prévaloir de sa qualité de « victime » ? Au-delà d'apparentes contradictions entre les dispositifs de la Cour strasbourgeoise dans les affaires turques *Akdeniz*, et *Cengiz,* l'auteur montre de manière fine la cohérence du propos nuancé de la Cour strasbourgeoise en soulignant les critères utilisés : intérêt général du contenu et impact de la mesure, alors que la Cour luxembourgeoise reconnaît volontiers la qualité de victime à l'internaute privé d'accès à l'information, dans tous les cas de blocage ou de filtrage.

Le second point analyse la portée des trois conditions posées par l'article 10, paragraphe 2, de la Convention, à l'intervention des autorités publiques pour limiter la liberté d'expression. On appréciera les conclusions que l'auteur tire de cette analyse serrée, ainsi « la fermeture d'un site entier pourrait être considérée comme équivalente à la fermeture d'un journal, que la Cour européenne a eu l'occasion de qualifier d'ingérence préventive disproportionnée à la prévention du crime et à la défense de l'ordre ». « À nos yeux, pourrait encore être qualifié de restriction préalable le blocage d'accès d'un utilisateur à son compte de réseau social en raison de la présence d'un contenu problématique sur le site concerné ». L'auteur pose ainsi l'interdiction, à défaut de loi, de toutes mesures de filtrage ou de blocage par un intermédiaire sur la base d'un accord pris par ce dernier avec le détenteur de droits de propriété intellectuelle. Par ailleurs, la condition de légitimité exigée par l'article 10, paragraphe 2 impose que le motif invoqué par l'auteur de l'ingérence soit sérieux. Enfin, M. Van Enis opère cette déduction de l'exigence de proportionnalité : « la volonté d'empêcher l'accès à un contenu précis n'est pas suffisante pour justifier le blocage de l'ensemble d'une plate-forme d'expression », reprenant à cet égard notamment l'examen de l'affaire *Scarlet*. *Quid* cependant si le blocage est partiel ? Une recommandation du Conseil de l'Europe semble distinguer le blocage d'une « partie importante », qu'il estime devoir interdire, des autres hypothèses où l'interdiction est sujette à caution. Certes cette notion de

« partie importante » elle-même reste à définir et la condition de légitimité renvoie de même à celle d'adéquation et d'efficacité de la mesure, condition appréciée de manière large dans l'affaire belge *The Pirate Bay,* ainsi qu'à celle de nécessité qui exige la prudence de celui qui ordonne le blocage ou le filtrage.

Au terme de cette analyse serrée des textes du Conseil de l'Europe et des autorités européennes, au-delà des hésitations voire contradictions – souvent plus apparentes que réelles – de la jurisprudence européenne, l'auteur dessine une approche restrictive de la légalité des mesures de filtrage et de blocage. Sans doute aurait-on souhaité voir appliquer sa réflexion au projet de directive actuellement en discussion sur le droit d'auteur dans la société de l'information dont une disposition permet aux intermédiaires de filtrer les œuvres à diffuser dans la mesure où elles seraient contraires aux droits d'auteur, et ce à la demande des auteurs ou à celle de leurs ayant droits.

8. Mme Ruet résume comme suit l'approche du discours de haine : elle « est évolutive, diversifiée, et casuistique ainsi que le montre la jurisprudence de la Cour européenne » et cette approche diffère profondément de celle tenue sur d'autres continents. L'objet de la première partie de ses réflexions, consiste à analyser cette approche, en particulier à l'heure d'Internet. La seconde partie invite à réfléchir aux défis nouveaux posés en la matière par le futur du réseau mondial.

La comparaison des approches américaine et européenne est rappelée : alors que les États-Unis proclament la liberté d'expression de manière neutre sans référence au contenu, sauf lorsque le discours est directement lié à un appel à la violence, l'Europe rappelle la valeur importante de la liberté de parole pour la vitalité de notre démocratie et insiste sur la responsabilité de ceux qui investissent l'espace public. L'article 17 de la CEDH qui exclut les discours de haine est, dans cet esprit de tolérance, à appliquer de manière « exceptionnelle », comme le rappelle la Cour de Strasbourg : « dans les affaires relatives à l'article 10 de la Convention il ne doit être employé que s'il est tout à fait clair que les propos incriminés visaient à faire dévier cette disposition de sa finalité réelle par un usage du droit à la liberté d'expression à des fins manifestement contraires aux valeurs de la Convention ». C'est à la lumière de ce principe que l'auteure étudie deux textes dont elle affirme l'étroite parenté, le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, initié par le Conseil de l'Europe,

et la décision-cadre 2008/913/JAI sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal adoptée le 28 novembre 2008 par le Conseil de l'Union européenne. Elle passe également en revue les nombreux arrêts de la Cour de Strasbourg et attire l'attention sur la variété des critères utilisés (impact supposé des propos, interprétation possible du contenu, etc.) et l'extrême prudence des juges lorsqu'ils appliquent le § 2 de l'article 10 ou l'article 17 de la CEDH.

Quant aux défis suscités par Internet, le premier souligné est celui de l'effectivité des législations : « L'effectivité de la protection et des recours contre le discours de haine rencontre de multiples obstacles qui tiennent au caractère transnational d'Internet, à la diversité des législations et à la divergence des conceptions sur un plan international, à l'importance de l'anonymat, à la propagation rapide des contenus haineux dans l'univers numérique ». A ce défi, répondent un certain nombre d'initiatives législatives européennes et la volonté de la CJUE dans les affaires *Shevill* et *e-Date Advertising* de favoriser les recours des personnes lésées, en reconnaissant la compétence du juge de ces dernières comme applicable. L'affaire *Yahoo !* montre cependant que l'exécution des décisions en terre étrangère (en l'occurrence aux États-Unis) reste délicate. Sans doute, serait-il utile sur ce plan de reprendre l'exemple du RGPD qui déclare applicable suivant le critère de la cible, le droit des citoyens visés par les plateformes ou prestataires d'Internet non situés sur le territoire européen, et oblige ces derniers à nommer un représentant qui répondra de l'exécution des condamnations prononcées contre ces prestataires. Quant à la façon dont Internet modifie les critères de prise en considération des discours racistes et haineux, l'analyse des arrêts *Perinçek* et *Vejdeland* témoigne de l'importance que l'Europe aurait de se doter, comme le Canada, de critères qui permettraient de guider les juges. Ainsi que l'affirme la Cour suprême canadienne, il faut « se concentrer sur le groupe plutôt que sur une seule personne et chercher à démontrer que c'est le groupe, et pas seulement la personne qui pourrait subir un préjudice […]. L'accent doit […] porter sur l'effet que peuvent avoir les propos haineux sur la façon dont les personnes qui ne font pas partie du groupe vont percevoir le statut social de ce groupe. En dernière analyse les dispositions législatives qui limitent l'expression de propos haineux visent à protéger le statut social des groupes vulnérables ».

Enfin, l'article étudie la façon dont la lutte contre les discours haineux et racistes doit être l'affaire à la fois des autorités publiques (voir

notamment le code de conduite publié par la Commission européenne en 2016 sur les discours haineux) mais également des acteurs privés et donc d'une co-régulation. L'auteure signale les difficultés d'une telle entreprise au regard de la crainte de censure excessive et du besoin de veiller à l'absence de surveillance généralisée du Net. Les engagements pris par Facebook, Twitter, YouTube et Microsoft constituent-ils la solution ou au moins une solution partielle ? Sans doute faut-il, comme conclut l'auteure, que ce soit le juge et non l'opérateur privé qui en définitive règle la question du délicat équilibre entre liberté d'expression et lutte contre la haine et le racisme.

9. Qu'il s'agisse des *LuxLeaks*, de l'affaire *Snowden*, des *Panama Papers* et autres, la question de la légitimité des lanceurs d'alerte, de l'objet et des conditions de leurs révélations interroge la matière des droits de l'homme. La contribution de Mme Lachapelle sur la protection des lanceurs d'alerte contient une analyse précise et remarquablement documentée sur la proposition de directive européenne récente, comme d'autres textes internationaux en la matière. La réflexion de l'auteure ne s'arrête pas là, la dualité d'approche de la légitimité du lanceur d'alerte est mise en évidence de manière heureuse. D'une part, le lanceur apparaît à la fois comme le héros de la liberté d'expression et donc de la démocratie (approche du Conseil de l'Europe). À ce titre, il a le devoir de parler, sans doute en ayant pris certaines précautions, et toutes représailles à son égard méritent, au regard de l'article 10 de la CEDH, d'être sanctionnées (arrêts *Guja*). D'autre part, il peut être considéré comme l'auxiliaire de l'autorité dans la poursuite d'une mise en œuvre effective de sa politique, en particulier fiscale, économique voire de protection des données. Cette seconde attitude transparaît dans certains textes européens et justifie la « rétribution » des « délateurs ».

Certes la liberté d'expression permet de justifier le lancement d'alerte mais également certaines limites à la divulgation d'informations. Certes, la même liberté exige la protection de la révélation lorsqu'elle est le fait d'un journaliste ou rapportée par ce dernier. À ces considérations, la protection de la vie privée ajoute d'autres éléments à la protection du lanceur d'alerte (secret des correspondances, droit au suivi du signalement…) mais également entend protéger les personnes qui, le cas échéant, se voient dénoncées. À cet égard, l'auteure s'interroge, au-delà du devoir de confidentialité du signalement et de son auteur, sur l'existence d'un « droit au chiffrement et à l'anonymat » du lanceur d'alerte, non consacré à l'heure actuelle. Son plaidoyer s'appuie sur le fait que

l'anonymat représente sans doute la meilleure garantie pour la liberté d'expression et que par ailleurs, il découle de la volonté des lois « vie privée » de protéger le citoyen contre les conséquences de sa légitime révélation.

10. Avec Koen Lemmens, nous suivons les tâtonnements de la jurisprudence de Strasbourg cherchant à intégrer la réalité de la presse électronique. Ainsi, l'affaire *Times Newspapers*, dès 2009, est pour lui l'occasion de rappeler que la Cour strasbourgeoise met en avant comme principe la contribution d'Internet au développement de la liberté d'expression mais elle reconnaît également les risques nouveaux liés à ce mode de diffusion, en particulier pour la protection de la vie privée. Le placement d'hyperliens vers des sites illégaux ou diffusant de fausses informations ou la publication dans un journal d'un contenu tiré d'un site Internet, en cause dans l'affaire *Pravoye*, promeuvent de même la circulation de l'information. Ils n'entraineront la responsabilité de l'internaute que si ce dernier pouvait connaître l'illégalité, la fausseté de l'information. Sans doute, cette possibilité sera appréciée différemment en fonction de la qualité de l'auteur du placement et de la finalité de sa présence sur le site. Ces nuances conduiront à une plus grande sévérité vis-à-vis des journalistes professionnels dont le devoir de vérification des sources doit être rappelé, de même que la conscience de leur mission vis-à-vis de l'information du public. La vente d'informations obtenues légitimement par un journal dans le cadre de l'accès aux informations détenues par l'autorité publique et portant sur les revenus des contribuables finnois est l'objet de la décision *Satamedia* jugée par la Cour de Luxembourg. L'auteur approuve la décision de la Cour condamnant la société venderesse sur la base de la directive de protection des données sans égard au caractère prétendument journalistique de l'activité : « pour que l'exception de journalisme puisse s'appliquer, il suffisait que ces activités aient pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées ». L'affaire *Delfi*, où un portail s'était vu condamné pour avoir publié des messages haineux, est l'occasion pour l'auteur de suggérer de lier la responsabilité du portail au caractère anonyme des messages postés, appliquant ainsi le droit de la presse traditionnelle. Nous reviendrons avec d'autres contributions sur la délicate question des plateformes en ligne et la diversité des situations, diversité qui interdit une réponse unique. Avec l'affaire *Węgrzynowski*, la Cour strasbourgeoise a confirmé le principe déjà établi par l'affaire *Times Newspaper* en 2009 de l'obligation des éditeurs de journaux qui archivent électroniquement

leurs articles de signaler les recours mais jamais de retirer ou bloquer les articles incriminés quand bien même ces derniers auraient été jugés diffamatoires. Dernier point analysé par K. Lemmens, celui du blocage de sites, où nonobstant l'apparente contradiction de jugements, tous concernant la Turquie, l'auteur note que cette contradiction se résout à partir du moment où l'on constate que la Cour, si elle rejette les recours contre des blocages où les requérants n'ont pas d'intérêt direct à l'accès, les admet dès qu'il s'agit d'un site dont l'accès pour eux est précieux soit parce qu'il les concerne directement soit parce que, comme dans le cas d'un blocage de YouTube, il s'agit d'une « plateforme unique », en d'autres termes, un réel « *gatekeeper* » de l'accès à Internet. L'article s'achève par des commentaires « à chaud » sur la position européenne en matière de lutte contre les « *fake news* ».

11. Le titre choisi par M. Tréguer pour sa contribution : « Anonymat et chiffrement, composantes essentielles de la liberté de communication » révèle l'option de l'auteur. L'histoire lui donne raison, même si, dès la Révolution française, certaines sourdines « pour raison d'État » témoignent du difficile équilibre entre liberté et sécurité. Le droit à l'anonymat est proclamé ici et outre-Atlantique : droit à l'anonymat des auteurs d'articles compensé certes par une responsabilité de l'éditeur, droit des journalistes au secret des sources. La technologie, en la matière s'avère un allié précieux. L'affaire *Lacambre*, poursuivi et condamné pour avoir « hébergé » sur son site et diffusé un contenu posté anonymement et constituant une atteinte au droit à l'image d'une actrice, oblige à devoir chercher « un point d'équilibre » entre préservation de l'anonymat et possibilité de retrouver l'auteur de l'infraction. On connaît la solution proposée par la directive sur le commerce électronique quant à la responsabilité allégée des intermédiaires techniques et leur devoir de coopération avec la Justice, pour aider à l'identification des auteurs. M. Tréguer rappelle à cet égard l'arrêt de Strasbourg dans l'affaire *KU c. Finlande*, qui consacre le principe suivant lequel « l'anonymat et la confidentialité des communications Internet – préoccupations primordiales associées aux articles 8 et 10 de la Convention –, devaient être mis en balance avec d'autres droits et intérêts ». Avec inquiétude, l'auteur note la dérive actuelle qui tente, au nom des risques accrus liés aux caractéristiques du réseau Internet, à faire pencher la balance en faveur des intérêts de la sécurité publique ou des droits des tiers, en particulier le droit d'auteur. Sans doute, note-t-il, sur la base des réglementations de protection des données à caractère personnel, la résistance opposée

par les juges de Luxembourg à la conservation généralisée des données de connexion (arrêt *Digital Rights*) qu'une directive de 2006 imposait à l'ensemble des opérateurs télécoms, de même qu'à la surveillance secrète massive et exploratoire opérée aux États-Unis (arrêt *Schrems*) mais il ne peut s'empêcher, faits à l'appui, de constater l'utilisation de technologies de *Big Data* capables de repérer à la volée et en temps réel des mots-clés, des identifiants, des signatures numériques, etc. et la volonté des services de renseignements d'affaiblir les algorithmes de chiffrement ou de contourner leur existence. L'anonymat et son corollaire le chiffrement ont certes les droits de l'homme, articles 8 et 10 de la Convention, pour eux mais que pèsent et pèseront ces droits de l'homme au regard d'autres préoccupations tant privées que publiques ?

Vie privée et protection des données à caractère personnel

12. C'est avec raison, analyse fine de la jurisprudence de la Cour de Justice européenne aidant, que Mme de Terwangne s'attache à démontrer le lien étroit de filiation entre la protection de la vie privée et celle des données, deux droits fondamentaux pourtant dissociés par la Charte des droits fondamentaux de l'Union européenne. C'est avec la même justesse que l'auteure souligne que la protection de la vie privée est la condition même d'autres libertés comme celle d'association, d'expression mais également de se déplacer et, plus fondamentalement, de la dignité humaine. L'auteure procède alors à une analyse des dispositions centrales des textes en matière de protection des données et des éclairages que les jurisprudences de Luxembourg ou de Strasbourg ont pu apporter à certaines de ces dispositions. Sont particulièrement bienvenues ses remarques fondées sur l'étude du texte récemment modifié de la Convention n° 108, ainsi le rappel des limites du consentement, la signification de l'extension du principe de proportionnalité au traitement et non à son seul objet, les données. Quant aux apports jurisprudentiels, sont notables en particulier les décisions européennes à propos de la compatibilité des finalités et de l'étendue du droit d'accès. L'examen du droit des personnes à la portabilité de leurs données retiendra l'attention du lecteur.

Cette jurisprudence illustre en outre les conflits entre libertés fondamentales. L'auteure relève combien si la protection de la vie privée, dans son principe, entend soutenir ces autres droits fondamentaux, elle peut, dans certains cas, mettre en cause l'affirmation d'autres libertés

ou droits prétendus fondamentaux : conflit avec les droits de propriété intellectuelle (affaire *Promusicae*) avec la liberté d'expression (accès à l'information : affaire *Google Spain*) et en particulier journalistique (affaire *Satamedia*). Les conflits également avec des impératifs de sécurité, parfois présentés comme condition même de la survie de nos libertés, sont également étudiés. À cet égard, la position des cours est ferme, l'article 8, paragraphe 2, de la CEDH tout comme l'article 52 de la Charte des droits fondamentaux de l'UE, ne voient ces « impératifs » que comme une exception soumise aux conditions de légalité, de clarté, de proportionnalité et de nécessité dans une société démocratique. C'est ainsi que, si elles acceptent des mesures peu attentatoires à la vie privée, y compris pour des infractions légères (affaire *Ministerio fiscal*), elles refusent la surveillance de masse (notamment, affaires *Szabo* et *Tele2 Sverige*, avec les nuances que l'auteure apporte en confrontant les arrêts de la CJUE et ceux de la CEDH). La conclusion est optimiste : l'auteure salue cette année 2018 et l'affirmation toujours plus forte de la nécessité d'une protection des personnes dans une société numérique.

13. La thèse de Mme Gayrel est claire. Elle entend démontrer comment l'Europe, avec le RGPD de l'Union européenne ou la modification de la Convention n° 108 relative à la protection des données du Conseil de l'Europe, souhaite mener une politique d'expansion de ses standards en matière de protection des données dans le monde entier. L'article débute par un panorama des législations de pays, des initiatives de groupes de pays ou d'instances internationales (APEC, OCDE). En particulier, Mme Gayrel développe les *Cross-Border Privacy Rules* (CBPR) promues par l'APEC dès 2011. Revenant à l'Europe, elle souligne la portée extraterritoriale du RGPD qui dorénavant ne conditionne plus l'application du texte à l'existence d'équipements de traitements des données sur son territoire mais l'étend à toute entreprise ayant pour marché cible un territoire européen ou le suivi du comportement de citoyens européens. Les dispositions du RGPD sur les flux transfrontières participent de la même volonté, en multipliant les mécanismes d'adéquation tout en renforçant les critères d'appréciation de cette adéquation. On saura gré à l'auteure d'avoir également analysé comment la modification de la Convention n° 108 permettait par son mécanisme d'adhésion de promouvoir hors Europe les standards européens. L'auteure note cependant quelques faiblesses d'un texte qui n'admet plus de réserves, prévoit un contrôle des mesures d'application de la réglementation nationale prise en conformité avec la Convention n° 108 et, *last but not least*, apparaît trop proche du texte de l'Union européenne.

14. La protection de l'e-réputation est une nécessité pour le droit, au vu des risques liés aux caractéristiques d'Internet, à la fois par la facilité d'introduction des messages, leur diffusion sans limites et la permanence de leur mémoire. L'article de M. Cruysmans s'attache donc à analyser les divers droits qui pourraient être évoqués par la personne blessée dans son honneur mais également les confronte à la réalité d'Internet. Le droit de réponse peut tout à la fois se raccrocher au droit à la vie privée et se présenter comme une exception à l'article 10 de la CEDH. Il s'impose comme une obligation positive des États même si cette obligation à charge des États est « minimale » et n'a pas pour conséquence d'octroyer un droit absolu d'accès aux médias. L'auteur analyse la façon dont tant le Conseil de l'Europe que l'Union européenne ont consacré l'extension de ce droit à Internet sans toutefois réfléchir aux contours précis de cette transposition (ainsi, faut-il réserver, comme en matière de presse écrite ou audiovisuelle, le droit de réponse aux seules publications périodiques sur Internet ? *Quid* du droit de réponse en cas de sites participatifs ? ...).

Le droit de rectification des informations à caractère personnel est une prérogative consacrée certes par la déontologie des journalistes mais surtout depuis de nombreuses années par les législations de protection des données en cas de traitements ne répondant pas aux conditions de licéité imposées par ces législations : inexactitude des données, non pertinence de ces dernières au regard de la finalité du traitement. L'auteur se montre sceptique sur la consécration d'un véritable droit à l'oubli que nombre d'auteurs croient trouver dans la décision *Google Spain* ou l'article 17 du RGPD : « Tout au plus, *note l'auteur*, il doit être conçu comme un dessein devant être atteint par l'application d'autres droits, ceux-ci ayant d'ores et déjà été consacrés, pour la plupart, par des textes internationaux ». Il revient notamment sur l'affaire *Rotaru* pour montrer combien on est loin de la consécration d'un droit subjectif mais au contraire proche de la recherche d'un équilibre d'intérêts chaque fois lié au contexte de l'affaire. L'analyse de la décision *Google Spain* lui permet de montrer combien l'intérêt de l'entreprise à une publication ne peut l'emporter sur la protection des intérêts de la personne concernée par la publication sauf lorsque ce premier intérêt peut se prévaloir de l'intérêt du public à connaître l'information relative à des personnages publics ou, comme dans l'affaire plus récente (2017) *Camera di commercio* jugée également par la CJUE, à connaître un fait de faillite. L'auteur note très justement que l'arrêt ne consacre point un droit à l'oubli mais un simple droit au « déréférencement ». Avec M. Cruysmans, nous sommes curieux de connaître les réponses que la Cour de Justice donnera aux questions préjudicielles

posées par le Conseil d'État français et le suivons lorsqu'il insiste sur les autres dispositions du RGPD, comme le droit d'opposition et le droit de suite imposant aux responsables de traitement de données qui doivent procéder à une rectification d'alerter les tiers de cette dernière.

15. Depuis l'arrêt *Niemietz* de la Cour européenne des droits de l'homme, on sait que la vie privée ne s'arrête pas aux portes de l'entreprise. La contribution de Mme Rosier entend faire le point sur la manière dont les travailleurs, y compris à domicile, bénévoles ou à temps partiel, se trouvent protégés à la fois par l'article 8 de la CEDH et par les règles nouvelles introduites par le RGPD ou la directive *e-Privacy*. Elle cherche à distinguer la portée de l'article 8 de la CEDH consacrant la vie privée et celle des réglementations européennes qui seraient fondées, elles, sur l'article 8 de la Charte de l'Union européenne affirmant le droit quasi constitutionnel de la protection des données distingué cette fois du droit à la vie privée. Cette tentative, à l'autopsie, c'est-à-dire après lecture de cet article fouillé et plein d'enseignements, s'avère vaine. Les deux concepts de protection de la vie privée et de protection des données ne peuvent être distingués. On retrouve en effet les mêmes analyses et conséquences que l'on se base sur l'un ou l'autre droit fondamental. Ainsi faut-il ranger le secret des communications du côté de l'un ou de l'autre ? L'analyse de la proportionnalité de l'ingérence, qu'on la fonde sur l'article 8 de la Convention ou sur l'application de l'article 6 du RGPD fondé sur la protection des données suit le même raisonnement et aboutit aux mêmes résultats. Le fondement de la distinction ne trouve pas de justification dans l'écrit de l'auteure, nonobstant sa volonté de donner un sens à la distinction opérée par la Charte européenne entre « vie privée » et « protection des données ». N'eût-il pas été plus intéressant de montrer comment la jurisprudence de l'article 8 de la Convention permet de comprendre les solutions données par les réglementations de protection des données ou en vertu de celles-ci, plutôt que de séparer les deux analyses ? Le droit à la protection des données n'est jamais qu'un droit dérivé, un « droit-gigogne », dirait Mme Turgis, et doit se comprendre en fonction de celui-ci. Le récent arrêt *Barbulescu* (2017) précisément à propos de la surveillance des communications d'un employé, en donne par ailleurs le sens, qui déborde de loin le droit à l'intimité auquel on souhaiterait parfois réduire le concept de vie privée. « Des restrictions apportées à la vie professionnelle peuvent tomber sous le coup de l'article 8 lorsqu'elles se répercutent sur la façon dont l'individu forge son identité sociale par le développement de relations avec autrui ».

C'est avec minutie et avec un rare sens critique, que Mme Rosier analyse les arrêts de la Cour européenne des droits de l'homme et répond aux questions que la surveillance des employés pose. Ainsi, l'exigence de la légalité de la surveillance, imposée pour justifier l'ingérence, oblige-t-elle les pouvoirs publics à réglementer cette surveillance et ce, en fonction tant de l'obligation positive des États que de l'effet horizontal des prescrits en matière de droit de l'homme. L'arrêt déjà cité semble se contenter des règles internes de l'entreprise, ce qui m'apparaît se justifier en fonction du fait que les lois de protection des données y font référence et que ces lois ont été prises précisément en vertu de l'obligation positive imposée par l'article 8 aux États de protéger la vie privée. Reste à vérifier que la teneur des dispositions de ces règles internes respecte le principe de proportionnalité tant dans la finalité que dans le contenu des traitements, dans les moyens utilisés pour la collecte des données, et enfin dans la sanction appliquée à l'employé indélicat. Dans tous les cas, il faut ménager « un juste équilibre des intérêts en jeu ». À propos de la proportionnalité de la finalité de ces traitements, Mme Rosier souligne à la suite de la Cour dans l'affaire *Kopke* : « L'intérêt de l'employeur à la protection de ses droits de propriété ne peut être efficacement sauvegardé que s'il peut recueillir des preuves permettant de prouver le comportement fautif (et en l'occurrence infractionnel) de la travailleuse devant les juridictions du travail et conserver lesdites preuves jusqu'à ce qu'une décision judiciaire définitive intervienne. La Cour souligne également que cette possibilité peut servir un intérêt public, à avoir une bonne administration de la justice par les tribunaux nationaux ». Le Groupe de l'Article 29 insiste sur le fait que d'autres solutions permettent d'éviter l'ingérence de l'employeur, ainsi, le verrouillage de l'accès à certains sites ou le rappel par messages électroniques réguliers de la priorité de l'utilisation à des fins professionnelles. Ce même groupe exclut que la légitimité de surveillance puisse se satisfaire du consentement du travailleur et le RGPD semble l'exclure de même. Quant aux techniques de contrôle utilisées, l'article analyse le danger lié à l'utilisation de certaines technologies de *screening* déployées sous le prétexte d'assurer la sécurité du réseau et utilisées en réalité pour surveiller les communications des employés. Enfin, l'exigence de la transparence des règles qui fondent l'ingérence implique une information détaillée sur le traitement comme le recommande le Groupe de l'Article 29, même s'il faut admettre de manière exceptionnelle des surveillances secrètes.

L'article se termine par des réflexions sur les incertitudes quant à la portée de l'interdiction de la surveillance et de l'interception des

communications électroniques affirmée tant par l'article 7 de la Charte européenne que par la directive *e-Privacy* : vise-t-elle uniquement les services prestés par les opérateurs de service de communication ou s'étend-elle à tout tiers non partie à la communication, ainsi l'employeur ? Le lecteur appréciera la critique adressée à la proposition de règlement *e-Privacy* actuellement en discussion, notamment sur le fait qu'un considérant du texte précise que la protection des communications ne vaut que pendant la transmission et non au-delà.

Un regret au terme de la lecture de cette contribution majeure en la matière, la question des limites à la liberté d'expression des employés, en particulier les critiques adressées à la conduite de l'entreprise ou à ses pratiques, eût également mérité une contribution particulière au regard de quelques décisions récentes.

Autres droits fondamentaux

16. Notre collègue, M. Michaux, nous entretient des prérogatives des auteurs – et surtout de leurs ayants droit– sur Internet. D'emblée, il souligne la nature de droit fondamental que désormais, Charte des droits fondamentaux de l'UE aidant, la propriété intellectuelle revêt. Sans doute, avons-nous sur ce point quelques réticences, malgré les justifications apportées par les textes, en particulier la Charte européenne, et développées par notre collègue. Par ailleurs, ces textes fondent la propriété intellectuelle sur le droit de propriété alors que notre sentiment est que le droit de propriété intellectuelle relève bien plus de la liberté d'expression de l'article 10 CEDH. La propriété intellectuelle entend en effet nourrir l'« espace public des idées » cher à Habermas et encourager son développement. Au-delà, fallait-il avec le droit fondamental de la propriété intellectuelle ajouter un droit fondamental de plus, au risque de perdre les conséquences que l'on peut déduire du rattachement de ce « droit-gigogne » ou dérivé[2] à la liberté d'expression.

Reconnaître le droit d'auteur comme un droit fondamental à part entière, c'est nécessairement, à l'heure où la réalité d'Internet multiplie les actes illégaux de copie et de diffusion d'œuvres protégées,

[2] L'auteur montre notamment comment la jurisprudence de Strasbourg a consacré indirectement la propriété intellectuelle comme droit fondamental : « Celle-ci l'a dégagée au départ du protocole n° 1 (protocole additionnel) dont l'article 1er, consacré à la protection de la propriété, porte que "Toute personne physique ou morale a droit à la protection de ses biens". Dans un premier temps, la Cour a inféré de la disposition précitée que le droit fondamental de propriété s'étend à la propriété intellectuelle (en général). Dans un deuxième temps, elle a observé que cette extension bénéficiait en particulier au droit d'auteur ».

s'interroger sur les conflits entre droits fondamentaux, comme le reconnaît le législateur européen à l'occasion de l'adoption de la directive sur le droit d'auteur.

La contribution analyse divers aspects de cet équilibre et ce, sur le plan tant du contenu du droit d'auteur que de la protection accordée à ce droit. J'en épingle quelques-uns relatifs au contenu. La question des hyperliens, déjà évoquée dans la contribution de K. Lemmens, est un premier aspect. Dans l'arrêt *GS Media,* la Cour, au nom de l'apport des hypertextes à la circulation des idées (à noter qu'il s'agit là de la justification première du droit d'auteur), exonère de toute responsabilité l'internaute privé, dans la mesure où ce dernier n'a pas connaissance de la violation du droit d'auteur, et, au contraire, présume de manière réfragable cette connaissance et donc la responsabilité du professionnel qui pratique ce lien. Cet écart par rapport aux règles classiques de la responsabilité apparaît cependant justifiable pour l'auteur. La reproduction numérique d'une œuvre et sa mise sur le Net sans l'autorisation de l'auteur ont été légitimées par la Cour de Luxembourg dans l'affaire *Eugen Ulmer,* une fois de plus au nom de l'intérêt public que représente cette mise à disposition. Quant à la protection légale accordée au droit d'auteur, le commentaire des affaires *Ashby et Neij & Sunde* est intéressant. La Cour de Strasbourg reconnaît l'applicabilité du droit d'auteur contre des plateformes de diffusion qui avaient diffusé les œuvres sans le consentement des titulaires de droit d'auteur, nonobstant l'argument de la liberté d'expression invoqué par les plateformes. Mais comme le note M. Michaux, « si la liberté d'expression cède, c'est plutôt au motif que la diffusion de l'information en question ne relève pas de l'expression et du débat politiques ». Dans les affaires portant sur le filtrage des réseaux (affaires *Scarlet* et *Netlog),* la réclamation pourtant légitime de l'auteur cède, en juge ainsi la Cour de Justice, par rapport aux exigences de non violation de la protection des données des usagers des services du fournisseur d'accès, dans le premier cas, du réseau social, dans le second cas. Le blocage de l'accès à un site internet pour violation de droit d'auteur par le propriétaire d'un site fait l'objet de sévères restrictions par la CJUE (affaire *UPC Telekabel*) destinées à limiter au strict minimum la limitation de l'accès des internautes et à garantir les droits de la personne accusée d'avoir violé le droit d'auteur. Par ailleurs, ces restrictions doivent être nécessaires.

Quelles conclusions, l'auteur tire-t-il de ces débats ? Il refuse de se laisser enfermer dans le dilemme souvent présenté : accorder d'office la

primauté soit au droit d'auteur, soit à la liberté d'expression (ou à la protection de la vie privée). Il préfère laisser aux juges le soin de déterminer *in casu* la pondération à accorder à chacun de ces droits fondamentaux. Peut-être est-il bon en conclusion de notre rapport, de rappeler cependant que le droit « fondamental » de la propriété intellectuelle partage avec la liberté d'expression l'objectif de la création d'un espace libre de discussion et la promotion du savoir et de la culture.

17. C'est précisément l'accès à la culture qui constitue l'objet de la contribution de Mmes Nennen et Pastor. Le Pacte international relatif aux droits économiques, sociaux et culturels parle même d'un « droit à la culture », c'est-à-dire un droit d'accès à tous les moyens « par lesquels des individus, des groupes d'individus et des communautés expriment leur humanité ». De ce « droit » d'accès à la culture, se distingue le « droit des cultures d'être reconnues et promues dans leur identité ». Ce droit est prôné par l'UNESCO et, ajoutons-nous, objet de quelques principes affirmés par le Sommet Mondial de la Société de l'Information (SMSI) en 2003, soit le droit « d'accéder aux moyens d'expression et de diffusion constituant des éléments importants pour mettre en valeur la diversité culturelle et encourager la compréhension mutuelle ». Certes, la contribution rappelle que l'article 4, paragraphe 2, du Traité sur l'Union européenne (TUE) impose à l'Union de respecter l'identité nationale des États membres et la Charte des droits fondamentaux de l'Union européenne (« la Charte ») consacre, quant à elle, respectivement le respect de la diversité culturelle (article 22). Toutefois, cette double reconnaissance n'a engendré aucun droit subjectif au profit des citoyens, vu les compétences limitées de l'Union européenne en la matière (article 167 du Traité sur le fonctionnement de l'UE).

Y a-t-il un droit à la culture ? Les auteures s'interrogent sur la signification d'un tel « droit » ? Leur verdict est nuancé : « La jurisprudence de la CJUE s'est donc caractérisée par une intégration négative en ce qu'elle a permis de supprimer des mesures nationales qui entravent l'accès à la culture en considérant que cela nuit à la libre circulation des biens, des services, des personnes et des capitaux ». Étonnante approche par l'économique d'une question qui, nonobstant certains aspects économiques, est d'abord une question de construction de l'identité personnelle. On conçoit dès lors, à la suite des auteures, qu'entraîné sur ce terrain, le balbutiant « droit » à la culture, cède, dans l'environnement numérique, devant un autre droit dont les aspects économiques sont prépondérants : le droit de propriété intellectuelle dont, avec B. Michaux, la contribution

souligne la nature, cette fois incontestée, de droit fondamental. À regret, l'article relève qu'à aucun moment dans des affaires où il s'agissait de conflits entre le droit d'accès et la communication d'œuvres culturelles, la Cour de Justice de l'UE (arrêts *ITV Broadcasting* et *Egeda and Others*) n'ait mentionné l'intérêt, à défaut de droit, des citoyens européens à l'accès à la culture, voire ait considéré (arrêt *Stichting Brein*) que des mesures de blocage de l'entièreté d'un site et non des seules œuvres protégées par un droit d'auteur soient légitimes.

Le salut viendrait-il du Conseil de l'Europe ? Les auteures y croient, elles rappellent la déclaration du Comité des Ministres, exigeant un filtrage à contenu spécifique et clairement identifiable, soumis au contrôle d'une autorité indépendante. À la suite de la jurisprudence de Strasbourg, elles concluent : « Le droit de recevoir des informations tel que protégé par l'article 10 engloberait donc le droit d'accès du public à des expressions culturelles, le cas échéant, dans la langue de l'individu ». Leur satisfaction n'est cependant pas complète : le droit de recevoir des informations, même dans sa langue, privilégie un certain type d'informations, à savoir celles qui entrent dans la discussion politique. Ce droit ne peut être, selon elles, assimilé au droit d'accès à la culture et à ses expressions culturelles. Par contre, ce droit, elles le lisent en filigrane d'une décision récente (arrêt *Akdas)* dans une affaire où l'autorité turque s'était opposée à la publication d'un poème d'Apollinaire considéré comme obscène. La Cour conclut sur la base de l'article 10 et souligne à l'évidence le droit d'accès aux œuvres culturelles : « la reconnaissance accordée aux singularités culturelles, historiques et religieuses des pays membres du Conseil de l'Europe, ne saurait aller jusqu'à empêcher l'accès du public d'une langue donnée, en l'occurrence le turc, à une œuvre figurant dans le patrimoine littéraire européen ». Si nous ne pouvons que nous réjouir de cette décision, faut-il pour autant ajouter à l'arsenal des droits de l'homme un droit nouveau ou simplement inciter à une meilleure compréhension d'un droit aussi solide que celui de la liberté d'expression ?

18. Le « droit » à des élections libres est-il bouleversé par Internet ? M. Bouhon rappelle les fondements de ce droit. Son propos évoque deux questions : la campagne électorale, d'une part ; le déroulement des opérations électorales, d'autre part. Sans doute, aurait-il été intéressant d'analyser d'autres questions au moment où les sondages permis par Internet, les dialogues directs entre l'élu et les citoyens, le contrôle des parlementaires et plus généralement des autorités publiques, désormais

facilités par le média, soulèvent d'autres questions de démocratie ! Au-delà, on songe à la parcellisation du débat public autour de thèmes qui transcendent les partis politiques et rendent obsolètes selon certains les clivages traditionnels qui fondent nos partis politiques.

Le scandale récent *Cambridge Analytica* révèle les biais que l'intelligence artificielle peut entraîner dans les campagnes électorales et, comme le souligne l'auteur dans ses conclusions, « la capacité des grandes entreprises à influencer les processus de transmission de l'information politique… ». De manière plus pointue, le propos de l'auteur se concentre sur la façon dont le message électoral passe désormais par les réseaux sociaux ou les blogs, sans aucune régulation de l'État et prend dès lors une autre tournure. Ses réflexions sur les sondages en ligne via le media d'Internet et les sites d'information sur les candidats attirent l'attention sur les dangers que recèle cette médiation, par l'analyse de l'électorat et du discours publicitaire « adéquat », c'est-à-dire de plus en plus profilé en fonction de chaque citoyen. Autre point, la possibilité pour chaque candidat d'avoir accès à Internet permet à la Cour européenne des droits de l'homme (*arrêt TV Vest AS,* 2008) de considérer que cet accès peut suppléer à des restrictions d'accès aux médias traditionnels. L'absence de contrôle de la façon dont chaque candidat utilise, à la veille des élections, le média qu'offre Internet et notamment les contenus qu'il diffuse, d'une part et les risques de certains dérapages liés à cette utilisation, d'autre part, sont analysés de façon critique par la même Cour, au motif que cette utilisation peut mettre en danger l'égalité des candidats voire le pluralisme des opinions et détériorer le climat préélectoral. La Cour est alors amenée « à juger nécessaire, avant ou pendant une élection, de prévoir certaines restrictions à la liberté d'expression, alors qu'elles ne seraient habituellement pas admissibles » (affaire *Bowman*, 1998).

On connaît les débats non seulement politiques mais également juridictionnels sur l'utilisation d'Internet comme instrument de vote. À la réticence de nos juges et d'une partie de l'opinion publique, s'oppose la volonté de certains gouvernements de le rendre possible. La Cour de Strasbourg sera amenée à trancher à court terme ce débat. La pratique des *Stemfies,* par lesquels les électeurs révèlent leur vote, fait de même l'objet de débats, la Commission européenne pour la démocratie par le droit rappelant que : « le secret du vote est non seulement un droit, mais aussi une obligation pour l'électeur ». L'auteur termine par quelques réflexions à propos de la publication via Internet des résultats d'élections avant la date réglementaire.

19. En exergue de sa contribution sur « Les droits de l'enfant et Internet : entre autonomie et protection », Mme Mathieu tient ces propos : « Toute réflexion sur les droits de l'enfant demande à trouver un subtil équilibre entre, d'une part, le droit de l'enfant à l'autonomie et à l'autodétermination, d'autre part, son besoin fondamental de protection. L'utilisation d'Internet cristallise parfaitement cette tension entre la nécessité de reconnaître à l'enfant son besoin crucial d'autonomisation, notamment par l'éducation et la maîtrise du numérique, et celle d'une vigilance accrue des adultes pour le protéger, notamment des contenus préjudiciables et des comportements illégaux présents sur la Toile ». Que les enfants puissent sans discrimination participer pleinement à la vie de la Toile, qu'ils soient même encouragés en ce sens, ressort de nombre de déclarations internationales, en particulier du Comité créé par la Convention onusienne relative aux droits de l'enfant. Qu'ils bénéficient du même droit que les adultes à disposer de leur image est de même affirmé, même si ici l'autorisation parentale est requise pour protéger le mineur, étant entendu que les parents ont le devoir d'associer l'enfant de manière graduelle à cette décision, voire d'obtenir son consentement propre, en fonction de son âge. À cela s'ajoute, RGPD oblige, le droit à l'oubli, c'est-à-dire à l'effacement des images prises à son insu ou dont la publication a été autorisée par les parents.

La question de la protection des mineurs, utilisateurs d'Internet est une autre question : on connaît les législations pénales sur la pédopornographie (au niveau européen, voir la directive 2011/92 relative à la lutte contre les abus et l'exploitation sexuelle des enfants ainsi que la pédopornographie) étendue à la diffusion d'images « fabriquées » d'enfants, sur l'usurpation d'identité où un adulte se fait passer pour un mineur pour mieux approcher d'autres mineurs. Plus spécifiques à Internet, les labels, filtres et autres mesures techniques de vérification d'âge constituent des remparts efficaces vis-à-vis des contenus illicites, violents, à caractère pornographique, etc., qui polluent la Toile. L'appel à l'autorégulation dans l'élaboration et la mise en place de ces mesures techniques provient à la fois de l'Union européenne (voir, notamment, le programme *Safer Internet)* et du Conseil de l'Europe (voir les multiples recommandations du Comité des Ministres, à cet égard). Ces instances plaident pour leur mise en place et le contrôle tant de leur effectivité, de leur proportionnalité que de leur légitimité, outre leur plaidoyer pour une éducation des enfants à l'utilisation d'Internet. Au-delà de cet appel, l'auteure souligne la volonté des autorités de l'UE, lors de la révision prochaine de la directive SMA, d'appliquer aux plateformes de partage de vidéos

(YouTube) les dispositions déjà en vigueur pour les médias traditionnels. Ces mesures concernent la signalisation des œuvres, les heures d'accès à certains contenus, les restrictions d'accès liées à des codes d'accès, etc.. L'article se termine par un vigoureux appel aux parents à prendre leur pleine responsabilité dans l'éducation de leurs enfants à l'utilisation d'une technologie dont les bienfaits comme les méfaits ne sont plus à énumérer, en particulier pour les mineurs.

20. À l'heure où notre conception de la prison évolue, celle-ci devant être d'abord un lieu de préparation à la réinsertion sociale, il est certain que l'accès à Internet dans les prisons doit être considéré de manière positive, c'est la conviction que partagent Messieurs Scalia et Fischmeister. Il s'agit bien de plaider pour une « liberté numérique totale dans le paysage carcéral ». Un premier argument est à rechercher selon eux dans un droit non encore reconnu pleinement : le droit d'accès à Internet. Selon ces auteurs, s'il est reconnu comme dérivant de l'article 10 de la CEDH, on n'a pas encore assisté à la reconnaissance d'un droit autonome. À cette première réflexion, les auteurs ajoutent un second contre-argument. L'accès à Internet implique une large autodétermination du détenu par la multiplicité des services offerts par le réseau (réception d'informations, participation à des fora, communication avec des tiers, etc.), largement incompatibles avec l'idée de contrôle des sujets prisonniers et de sécurité des lieux et de la société, en définitive « norme fondamentale à laquelle tout droit subjectif (du prisonnier) doit céder le pas ».

La pratique est un second argument. Les auteurs citent les expériences en particulier norvégiennes, françaises et inchoatives en Belgique, tenues dans certaines prisons. Ces expériences permettent un accès partiel des prisonniers à Internet et ce, au service de droits reconnus aux prisonniers : les droits à la formation et à l'information. MM. Scalia et Fischmeister s'interrogent sur l'appui que cette ouverture partielle pourrait trouver à Strasbourg dans la mesure où, à l'occasion d'arrêts comme l'arrêt *Yildirim*, la Cour considère en effet que la mesure litigieuse, la coupure d'accès à Internet, est « constitutive d'une ingérence d'autorités publiques dans le droit de l'intéressé à la liberté d'expression, dont fait partie intégrante la liberté de recevoir et de communiquer des informations ». Bref, un refus d'accès complet à Internet constituerait une ingérence disproportionnée dans la liberté des prisonniers de recevoir et de communiquer des informations. Cette position est confirmée par deux décisions, cette fois concernant des détenus, où les prisonniers

ont obtenu gain de cause, l'une (affaire *Kalda*) en ce qui concerne l'accès à des bases de données du Ministère de la Justice, l'autre (affaire *Jankovskis)* à un programme de formation à distance. Quant au droit de s'exprimer, affirmé par l'article 10 de la CEDH, il implique la possibilité, certes sous contrôle, de s'exprimer à travers un blog ou une plateforme de discussion.

La question des correspondances électroniques et de leur contrôle est un autre sujet abordé par les auteurs. Le droit à la correspondance est clairement affirmé par la jurisprudence comme nécessaire à l'épanouissement de la personne du détenu. Certes, contrôle il doit y avoir, strictement proportionné aux risques encourus du fait de la qualité du prisonnier mais, comme le note le Contrôleur général français des lieux de privation de liberté, « La mise à disposition (contrôlée) d'Internet doit être assurée dans les lieux de privation de liberté dans lesquels la durée de séjour excède quatre jours. Cette mise à disposition inclut l'accès à la messagerie (également soumis à contrôle éventuel) ». C'est sur une note mitigée qu'au terme de leur étude, les auteurs concluent que le droit d'accès à Internet en prison est encore loin d'être effectif mais que ses premiers balbutiements laissent augurer d'une reconnaissance progressive du droit des détenus à bénéficier des services de cette technologie au service de leur développement personnel et de leur (re)socialisation.

21. Qui mieux que Mme Verbruggen pouvait parler du rôle de l'autorité de protection des données (« APD ») ? Son expérience reconnue au service de la Commission belge de la protection de la vie privée justifiait amplement sa participation à l'ouvrage sur un thème dont l'enjeu est crucial pour la protection de notre vie privée face aux défis de la société numérique. Si comme le note l'auteur, le mot Internet n'apparaît que peu dans les deux textes européens nouveaux, la Convention 108 modifiée et le RGPD, il est partout en filigrane et sa maîtrise est bien l'enjeu même de ces textes nouveaux. Depuis l'arrêt *Gaskin* de la Cour européenne des droits de l'homme en 1989 qui affirme haut et fort que l'existence d'une autorité indépendante est requise pour arbitrer les multiples intérêts contradictoires que suscite la création d'un traitement de données, le rôle des APD n'a cessé de croître et leur statut s'est précisé. À propos de ce statut, le concept d'autorité indépendante a été précisé par divers arrêts de la CJUE dont les leçons ont été retenues par le RGDP, qui en outre a souhaité préciser les critères d'appréciation de cette indépendance qui s'entend également des membres de l'autorité de protection des données (APD) et de ses moyens financiers et humains. On sait que,

dans la perspective d'une meilleure cohérence de l'action des autorités, le RGPD a souhaité, chose heureuse à l'heure où les flux et traitements de données ne connaissent plus de frontières, développer à la fois la coopération entre ces autorités et la désignation d'une d'entre elles comme « chef de file », sorte de guichet unique. Enfin, c'est surtout l'analyse des compétences de ces APD européennes qui retient l'attention de l'auteure. Ces compétences se déclinent autour de cinq pôles : informer et conseiller ; protéger ; réguler et co-réguler ; contrôler (à noter sur ce point, les références de l'auteure aux actions de contrôle décidées par ces institutions) et, enfin, sanctionner. Cette liste de compétences témoigne de la volonté des autorités européennes de voir les APD jouer un rôle actif tant auprès des citoyens que de l'opinion publique, des responsables de traitement et du législateur pour rendre effectives les dispositions du RGPD voire les faire évoluer. Ajoutons trois réflexions à la contribution de Mme Verbruggen. Premièrement, cette responsabilité active a une contrepartie, la responsabilité des autorités vis-à-vis des personnes, victimes de son action. Deuxième remarque, la crainte de cette responsabilité risque de rendre les autorités plus frileuses, moins « chien de garde » et plus « juge compassé ». Troisième point, la dimension prospective sur les promesses et enjeux d'une technologie sans cesse en évolution nous amène à insister à la fois sur les besoins de la réflexion éthique et interdisciplinaire au cœur des APD et de leur nécessaire coopération avec d'autres organisations de « *Technology Assessment* » ou de bioéthique sur des questions comme le transhumanisme, les applications des NBIC (Nanotechnologies, biotechnologies, informatique et sciences cognitives) ou les risques de l'intelligence artificielle, thèmes dont on regrette que les enjeux au regard du développement des droits de l'homme n'aient pas été abordés dans l'ouvrage.

22. « Procédures et méthodes d'investigation sur Internet », voilà le titre de l'article avec lequel Mme Forget conclut l'ouvrage. Toute enquête est ingérence dans la vie privée et il est donc important de mesurer si les critères d'acceptation de l'ingérence sont rencontrés : la nécessité dans une société démocratique, la proportionnalité et la transparence de la base légale de cette ingérence. L'exposé de l'auteure est une analyse sous l'angle des exigences ainsi rappelées des différentes procédures et méthodes d'investigation.

Ainsi, on connaît le sort négatif que la CJUE a réservé à l'obligation de conservation des métadonnées de communications électroniques par les opérateurs de ces services, imposée par la directive de 2006 sur ce

thème. La conservation doit être ciblée et des garanties procédurales (intervention d'un magistrat) doivent être suivies. La préservation des données, préconisée par la Convention du Conseil de l'Europe sur la cybercriminalité de 2001, apparaît moins intrusive et donc plus acceptable. La perquisition, préalable à une saisie des données informatiques ne nécessite pas l'information préalable du suspect mais bien le respect de certaines conditions. Ainsi, pour obtenir l'autorisation de procéder à une mesure de perquisition, il faut disposer de raisons de penser que de telles données « existent dans un endroit précis et permettent de prouver qu'une infraction pénale spécifique a été commise ». L'arrêt *Vinci* de la Cour de Strasbourg étonne cependant en ne réclamant pas de cibler *a priori* les données visées par la perquisition : « Un inventaire remis aux intéressés *a posteriori* détaillant le nom des fichiers, leur extension, leur provenance, leur empreinte numérique ainsi qu'une copie des documents saisis, constituait une garantie suffisante au regard de l'article 8, § 2, de la Convention ».

D'autres auteurs ont évoqué la question du blocage de sites. Sur ce point, la contribution analysée reprend les 9 critères dégagés par le juge Pinto de Albuquerque dans l'arrêt *Yildirim*. L'obligation de coopération de certains acteurs (hébergeurs, dirigeants d'entreprise, experts informatiques…) est affirmée, en particulier lorsque les autorités judiciaires ou policières se heurtent au chiffrement de messages ou à l'anonymat de leurs auteurs. Dans l'affaire *K.U. c. Finlande* (2 décembre 2008) la Cour « déduisit du droit au respect de la vie privée une obligation positive pour les États membres de prévoir dans leur droit interne des dispositions permettant d'exiger d'un fournisseur de services de dévoiler l'identité d'un destinataire de leurs services ». Cette coopération a même été jugée (affaire *Saunders*) due par la personne suspectée d'infraction, nonobstant son « droit au silence ». La dernière mesure étudiée est l'interception des communications. Il est rappelé que ces mesures ne peuvent exister que si des précisions sont apportées quant à la nature des infractions et des personnes suspectées. L'arrêt *Schrems* de la Cour de Justice confirme par ailleurs la condamnation sans appel de toute mesure générale d'écoutes téléphoniques, même si d'autres arrêts se montrent plus laxistes en présence de menaces graves à la sécurité publique (attentats terroristes). L'arrêt *Zakharov* de la Cour européenne des droits de l'homme soumet à de sévères conditions les surveillances dites secrètes, exigeant notamment le contrôle par une autorité indépendante de l'exécutif (pas nécessairement judiciaire) des raisons de la surveillance. Sur ce point, l'auteure note une évolution

vers des exigences moins sévères certes liées aux circonstances (attentats terroristes) (arrêt *Szabo*).

II. Quelques réflexions personnelles soumises à l'indulgence du lecteur

23. Internet et, de manière plus large, la numérisation de notre société bouleversent les droits de l'homme. C'est peu dire qu'ils donnent des ailes à certains. Ainsi, pouvoir, depuis n'importe quel point du globe, adresser et recevoir un message confère une portée inédite à la liberté d'expression voire, au-delà de cette liberté et parfois contre elle, à un droit de l'homme souvent oublié de nos amoureux des libertés : le droit de propriété… « intellectuelle », s'entend. À l'inverse, dira-t-on, cette expression de soi, voire n'importe quelle utilisation d'Internet, engendre des traces dont on ne sait, sauf exceptions, qui les récupère, comment il les traite et à quelles fins il les utilise. La vie privée n'existe plus sur Internet, diront les pessimistes. L'ambiguïté d'Internet vis-à-vis des droits de l'homme est déjà bien présente dans cette première constatation.

24. À cette première ambiguïté, nous aimerions ajouter d'autres débats. Premièrement, les droits de l'homme sont nés dans l'après-guerre d'une société mondiale dominée par l'Occident et sa culture. Est-il encore possible de lire les déclarations onusiennes ou du Conseil de l'Europe de la même manière à l'heure où le monde technologiquement unifié par un réseau unique au langage commun s'avère au contraire profondément divisé culturellement et dans ses valeurs ? Pouvons-nous imposer, au nom de la liberté d'expression ou plutôt de notre conception de celle-ci, des images choquantes ou irrespectueuses des lois et de la culture d'autres pays ? Bref, curieusement, il est plus difficile de parler des droits de l'homme aujourd'hui qu'hier.

25. Le deuxième point est plus délicat encore. Internet est source de conflits entre les droits de l'homme, comme le souligne en particulier Cécile de Terwangne. Le premier point le sous-entendait déjà : s'exprimer sur Internet, c'est parfois s'exprimer à propos d'autrui voire le mettre en cause. De même, les informations reçues grâce à nos réseaux parlent parfois d'autrui. Liberté d'expression et vie privée, alors même qu'elles s'épaulent souvent et qu'il m'est arrivé de soutenir que la seconde était la condition de la première, trouvent sur Internet des terrains

d'affrontement que les juges se doivent d'arbitrer. L'arrêt *Google Spain* de la CJUE, en date du 13 mai 2014, qui institue le droit au « déréférencement », illustre bien la façon dont les juges essaient de trouver leur voie entre deux droits, en l'occurrence le droit à la vie privée et celui à la libre expression. C'est en considérant les intérêts respectifs poursuivis à travers ces deux libertés que se justifie la décision : les droits des internautes « prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche [*Ndl'A : la liberté d'entreprendre*], mais également sur l'intérêt public à trouver ladite information portant sur le nom de cette personne ». Cette prévalence vaut, insiste la Cour, en fonction des particularités de la cause et dépend « de la nature de l'information en question et de sa sensibilité pour la vie privée, ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment en fonction du rôle joué par cette personne dans la vie publique ». Le même souci de moduler l'arbitrage entre droits fondamentaux en fonction des particularités de la cause est patent dans bien d'autres décisions (voir l'affaire *Satamedia* à propos du conflit entre les deux mêmes droits) ou peut être déduit d'une analyse comparative de décisions apparemment contradictoires comme le montrent très bien MM. Michaux et Lemmens à propos des conflits entre droit de propriété intellectuelle et liberté d'expression. On note en particulier cet attendu de la CJUE dans l'affaire *SABAM* : « le juge national, en adoptant une injonction obligeant le prestataire de services d'hébergement à mettre en place un tel système de filtrage, ne respecterait pas l'exigence d'assurer un juste équilibre entre d'une part, le droit de propriété intellectuelle, et d'autre part, la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations ».

26. À lire la jurisprudence, on s'aperçoit qu'elle voit les droits de l'homme soumis à d'autres balises. La réclamation d'un éditeur contre le copiage réalisé à partir des infrastructures d'Internet est source de nombreux litiges où les juges parfois se déchirent en décisions contradictoires. À l'inverse, les « hébergeurs » et les opérateurs de plateformes se prévalent de leur neutralité, garante de la liberté d'expression, pour décliner toute responsabilité en cas de diffusion d'un contenu protégé par des droits d'auteur. À nouveau, on s'interroge : la liberté d'expression (peut-être complétée par le droit à la propriété) n'est-elle pas à la base du droit d'auteur qui permet d'enrichir l'espace public de multiples créations originales ? Et voilà le fils tout à coup se retournant contre le

père, le droit d'auteur réclame des limites à la liberté d'expression, au nom d'un autre droit de l'homme : la propriété. Cette propriété, on le rappelle, le Conseil de l'Europe l'a reconnue comme proche d'un droit fondamental par la petite porte d'un Protocole dit annexe avant que la Charte des droits fondamentaux de l'UE l'élève désormais en droit quasi-constitutionnel. Quelle solution ? Forts de la Charte, les titulaires se prévalent de ce droit de l'homme nouveau : le droit de propriété intellectuelle qu'ils opposent aux droits de l'homme traditionnels : le droit à vie privée, comme le prouve l'arrêt *Promusicae* de la CJUE ; la liberté d'expression, comme le relate l'exposé de M. Michaux. À cet égard, la tendance de l'Union européenne nous inquiète, tendance à gonfler ce droit, l'étendant au secret d'affaires voire y trouvant un fondement pour affirmer le droit de l'utilisateur d'un système informatique à la « propriété » de ses données. Sans doute, le propos est-il un peu caricatural mais la tendance est bien présente.

27. Le numérique voit s'affirmer de nouveaux droits de l'homme dont la qualité au regard des droits traditionnels pose question. Ainsi, la reconnaissance par la même Charte de l'UE du « droit à la protection des données » désormais distingué du droit à la vie privée, l'affirmation d'un droit d'accès à Internet discuté par Sandrine Turgis et d'autres auteurs, voire d'un droit d'accès à la culture prôné par Mmes Pastor et Nennen, corollaires nécessaires du droit à l'égalité et du droit de chacun à la liberté d'expression, constituent d'autres exemples. La reconnaissance du droit à la liberté d'entreprendre récemment également affirmée par la Charte apparaît également comme source potentielle de conflits avec d'autres droits de l'homme. Ici aussi, on s'interrogera, après Mme Turgis, sur les conséquences et l'intérêt de cette multiplication, dangereuse à mon sens, de droits de l'homme « nouveaux ». Dans bien des cas, on préférerait parler, à sa suite, de « droits-gigognes », de droits dérivés et donc subordonnés, même si ces droits sont désormais quasi-constitutionnels. Ainsi, le droit à la culture doit, selon nous, se réclamer du droit à la liberté d'expression ; le droit à la protection des données, du droit à la vie privée, comme nous le pensons à la lecture de la contribution de Mme Rosier.

28. Ces arbitrages et cette éventuelle hiérarchisation des droits fondamentaux se voient confiés aux juges nationaux certes mais de plus en plus aux juges européens. Sans doute, était-on habitué à entendre la seule voix des juges de Strasbourg dans ce domaine mais voilà que désormais forte des compétences nouvelles dont l'Union européenne

s'est dotée en matière de droits de l'homme, les juges de Luxembourg se font également entendre. La Cour de Justice, par les questions préjudicielles de plus en plus nombreuses qui lui sont posées en la matière, se pose désormais comme l'interprète par excellence des droits fondamentaux et, comme les décisions *Schrems* et *Digital Rights* en matière de vie privée en témoignent, n'hésite pas à remonter les bretelles des autorités européennes. On peut espérer que les acquis de Strasbourg soient repris par Luxembourg et que leurs voix ne soient pas trop discordantes et servent l'intérêt de la protection des citoyens à l'heure d'Internet.

29. Une quatrième réflexion nous vient à l'esprit, en parcourant l'ensemble des chapitres de l'ouvrage. Tous les droits de l'homme, s'ils sont fondamentaux, ne sont jamais absolus et cèdent aux intérêts prééminents de tiers mais également de l'État. En d'autres termes, il existe une marge de manœuvre que les autorités publiques peuvent invoquer au nom des tels intérêts contre des libertés, y compris ceux rattachés au droit de propriété. Les cas récents de « *fake news* » témoignent de toute la difficulté de l'exercice mené au nom de la protection d'une information loyale des citoyens contre des propos déformant la réalité. Au-delà, on songe aux messages terroristes ou d'incitation à la haine raciale. Il s'agit bien, en l'occurrence, d'une liberté d'expression débridée qui tue elle-même son principe. Au-delà, on s'inquiète non seulement de la difficulté de fixer les balises de cet équilibre mais surtout de l'effectivité des moyens sans précédents dont, grâce à Internet, la puissance publique dispose dans le contrôle de l'activité et des expressions des citoyens, à défaut de pouvoir bénéficier de cette même puissance contre les géants du net.

30. Cette remarque me permet d'avancer une dernière réflexion. Certains articles soulignent le rôle important des organisations non gouvernementales (ICANN, IETF, W3C...) dans la régulation d'Internet, voire des accords entre entreprises comme le *Data Transfer Protocol* conclu à propos de la portabilité, ou *l'Artificial Intelligence Alliance*, l'accord récent en matière de *fake news* signé par les grosses plateformes d'information. Cette montée en puissance de l'autorégulation d'Internet est à souligner au moment où Internet, originellement conçu comme une foire aux idées et donc un lieu de libertés, est devenu, au grand dam de ses créateurs, une foire commerciale marquée par des logiques d'abord économiques. Notre propos n'est pas de déplorer cette évolution mais de réclamer des États qu'ils prennent leurs responsabilités. Deux points, à cet égard. Premièrement il leur revient de consacrer, à l'heure où Internet est devenu une condition de l'exercice pour tous les

citoyens de leurs libertés fondamentales, le droit de chacun à accéder à un service universel élargi de qualité, service à la fois d'information et de communication, et à voir garantir l'exercice de ses libertés fondamentales. Secondement, il leur appartient de veiller à poser les limites dans lesquelles pourront s'exprimer les régulations privées, comme l'a fait le RGPD. Bref, il s'agit bien d'affirmer la co-régulation et le pouvoir du dernier mot de l'autorité publique. Cette autorité publique est aidée en cela par des autorités administratives indépendantes (les autorités de protection des données, les commissions d'accès à l'information, les contrôleurs des services d'information) dont le rôle crucial dans la promotion des libertés fondamentales devrait être souligné.

31. Ces quelques réflexions témoignent de l'enjeu des propos tenus par les auteurs de l'ouvrage et de l'excellence des réponses à nos interrogations. J'ai pris un vif plaisir à les relever et les souligner. Que les auteurs me pardonnent mes oublis et peut-être mes trahisons. Merci surtout à mes estimés collègues Cécile de Terwangne et Quentin Van Enis, orfèvres en droits de l'homme sur Internet, d'avoir lancé le débat, d'avoir convoqué nombre de collègues d'ici et d'outre-Quiévrain, autour de ce débat essentiel et d'avoir agencé leurs propos riches et variés, de manière structurée.

Moxhe, le 29 octobre 2018