Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 14789
04 janvier 2019

Gouvernance de l'internet et droits de l'homme

Rapport[1]
Commission de la culture, de la science, de l'éducation et des médias
Rapporteur: M. Andres HERKEL, Estonie, Groupe du Parti populaire européen

Résumé

L'internet est un bien commun et sa gouvernance doit être au cœur des politiques publiques tant au niveau national que dans le cadre des relations multilatérales régionales et globales.

Il est essentiel que les pouvoirs publics, le secteur privé, la société civile, les milieux universitaires et la communauté technique des internautes et les médias entretiennent un dialogue ouvert et inclusif afin de définir et de concrétiser une vision commune d'une société numérique fondée sur la démocratie, l'État de droit et les libertés et droits fondamentaux.

Les États membres sont invités à donner pleine application aux recommandations du Comité des Ministres dans ce domaine. Le rapport prône des politiques nationales d'investissement public cohérentes avec l'objectif d'un accès universel à internet, l'engagement des États membres pour soutenir la neutralité du Net, des politiques globales de lutte contre la criminalité informatique et contre les abus du droit à la liberté d'expression et d'information sur l'internet, ainsi qu'une mise en œuvre effective du principe de la «sécurité de la conception».

Les États membres devraient mieux utiliser la Convention sur la cybercriminalité pour améliorer la collaboration interétatique et ils devraient s'engager avec le Groupe de haut niveau des Nations Unies sur la coopération numérique et contribuer à ses travaux, en promouvant une gouvernance de l'internet qui soit multipartite, décentralisée, transparente, responsable, collaborative et participative.

1. Renvoi en commission: Doc. 13280, Renvoi 4000 du 30 septembre 2013.

Sommaire **Page**

A. Projet de résolution[2]

1. L'internet est un bien commun, dont les utilisations influencent de nombreux aspects de la vie au quotidien et touchent aussi la jouissance effective des droits de l'homme et des libertés fondamentales. L'importance de l'internet est telle que le futur de nos sociétés dépend désormais aussi du futur de l'internet. Il est essentiel que l'évolution de l'internet conduise nos sociétés vers plus d'information et de connaissance, d'innovation et de développement durable, de justice sociale et de bien-être collectif, de liberté et de démocratie. Pour atteindre cet objectif, il est impératif d'assurer une protection plus effective des droits de l'homme sur l'internet.

2. Les nombreux textes mûrement réfléchis adoptés en la matière par le Comité des Ministres du Conseil de l'Europe témoignent très clairement de l'importance cruciale que revêtent ces questions. L'Assemblée parlementaire rappelle, entre autres, la Déclaration sur des principes de la gouvernance de l'internet de 2011 et les recommandations suivantes: CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche; CM/Rec(2012)4 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux; CM/Rec(2013)1 sur l'égalité entre les femmes et les hommes et les médias; CM/Rec(2014)6 sur un Guide des droits de l'homme pour les utilisateurs d'internet; CM/Rec(2015)6 sur la libre circulation transfrontière des informations sur internet; CM/Rec(2016)1 sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau; CM/Rec(2016)5 sur la liberté d'internet; CM/Rec(2018)2 sur les rôles et les responsabilités des intermédiaires d'internet; et CM/Rec(2018)7 sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique.

3. L'Assemblée reconnaît l'accès universel à internet en tant que principe clé de la gouvernance de l'internet et considère que le droit d'accès sans discrimination à internet est une composante essentielle de toute politique solide visant à promouvoir l'inclusion et à soutenir la cohésion sociale, ainsi qu'un facteur essentiel du développement durable démocratique et socio-économique.

4. L'Assemblée souligne l'importance de garantir le droit à un internet ouvert et de bâtir un écosystème qui sauvegarde la neutralité du Net. Elle note que les acteurs économiques qui contrôlent les systèmes d'exploitation et leurs magasins d'applications peuvent imposer des limitations non justifiées à la liberté d'accès des utilisateurs aux contenus et aux services disponibles en ligne, et que le risque de telles limitations s'accroît avec l'évolution vers des terminaux toujours plus intelligents.

5. L'Assemblée rappelle la nécessité d'assurer une protection effective du droit à la liberté d'expression et d'information, en ligne et hors ligne, ainsi que l'obligation pour les États membres du Conseil de l'Europe de veiller à ce que ce droit, pilier de toute société démocratique, ne soit menacé ni par les pouvoirs publics ni par les opérateurs du secteur privé ou non gouvernemental. En même temps, il faut faire plus pour contrer les dangers que les abus du droit à la liberté d'expression et d'information sur l'internet engendrent, tels que l'incitation à la discrimination, à la haine et à la violence, ciblant en particulier les femmes ou contre les minorités ethniques, religieuses, sexuelles ou autres, le contenu concernant l'abus sexuel d'enfants, le cyberharcèlement, la manipulation de l'information et la propagande, ainsi que l'incitation au terrorisme.

6. Cette exigence se lie aussi à la nécessité de garantir que l'internet soit un environnement sécurisé, où les usagers sont à l'abri de l'arbitraire, des menaces, des attentes à l'intégrité physique et psychique et des violations de leurs droits. Il faut renforcer la sécurité des bases de données que les institutions publiques ou privées gèrent; des échanges et transactions sur le réseau; des usagers vulnérables, victimes de propos racistes et haineux, de cyberharcèlement ou de toute autre atteinte à leur dignité; des infrastructures stratégiques et des services essentiels qui s'appuient sur l'internet pour leur fonctionnement; de nos sociétés démocratiques menacées par le cyberterrorisme et la guerre cybernétique.

7. Il faut également renforcer la protection de la vie privée et des données personnelles dans le cyberespace, pour éviter que les technologies qui font désormais partie de notre quotidien deviennent des outils de manipulation des opinions et de contrôle sournois de notre vie privée. À cet égard, l'Assemblée souligne à nouveau la menace que représentent pour les droits de l'homme les systèmes d'envergure mis en place par les services de renseignement en vue de collecter, de conserver et d'analyser à une grande échelle les données des communications, et condamne sans réserves les dérives et les abus de pouvoir qui, sous des prétextes sécuritaires, sapent les fondements de la démocratie et de l'État de droit. Par ailleurs, l'Assemblée est préoccupée par le fait que l'intérêt des entreprises privées à avoir un accès aisé au plus grand nombre de données personnelles et de les utiliser librement l'emporte encore sur la protection des utilisateurs d'internet, malgré les avancées significatives dans ce domaine.

---

2. Projet de résolution adopté à l'unanimité par la commission le 6 décembre 2018.

8. Pour faire face à ces défis avec succès, il faut œuvrer ensemble plus efficacement. Ainsi, l'Assemblée prône une réflexion critique sur la gouvernance de l'internet et souligne l'importance cruciale de cette question, qui doit être au cœur des politiques publiques tant au niveau national que dans le cadre des relations multilatérales régionales et globales. Il est essentiel que les gouvernements, le secteur privé, la société civile, la communauté universitaire et technique des internautes et les médias continuent d'entretenir un dialogue ouvert et inclusif afin de définir et de concrétiser une vision commune d'une société numérique fondée sur la démocratie, l'État de droit et les libertés et droits fondamentaux. Les plates-formes de dialogue telles que le Forum des Nations Unies sur la gouvernance de l'internet (FGI), de portée mondiale, le Dialogue paneuropéen sur la gouvernance de l'internet (EuroDIG) et le Dialogue européen du Sud-Est sur la gouvernance de l'internet (SEEDIG), ainsi que les diverses initiatives nationales, contribuent à favoriser une telle vision commune et une meilleure compréhension des responsabilités et rôles respectifs des parties prenantes, et elles peuvent jouer le rôle de catalyseur de coopération dans le monde numérique. À cet égard, l'Assemblée salue également la décision prise le 12 juillet 2018 par le Secrétaire général des Nations Unies de créer un Groupe de haut niveau sur la coopération numérique, chargé de présenter les tendances de l'évolution des technologies numériques, de recenser les carences et les perspectives qu'elles recèlent et de proposer des moyens de renforcer la coopération internationale.

9. Dès lors, l'Assemblée recommande aux États membres du Conseil de l'Europe de mieux centrer la gouvernance de l'internet sur la protection des droits de l'homme, en donnant pleinement application aux recommandations du Comité des Ministres dans ce domaine et, dans ce contexte:

9.1. de mettre en œuvre des politiques nationales d'investissement public cohérentes avec l'objectif d'un accès universel à internet; ces politiques devraient viser en particulier à corriger les déséquilibres géographiques (par exemple entre les zones urbaines et les zones rurales ou isolées), à aplanir le fossé numérique entre les générations et à éradiquer les inégalités de genre, ainsi que d'autres inégalités dues aux différences socio-économiques et culturelles ou à des handicaps;

9.2. d'être actifs dans les instances internationales pour garantir la neutralité du Net et sauvegarder ce principe dans le cadre de la législation nationale, qui devrait, entre autres:

9.2.1. établir clairement le principe de liberté de choix des contenus et applications quel que soit le terminal;

9.2.2. prévoir le droit des utilisateurs de supprimer des applications préinstallées et d'accéder aisément aux applications proposées par des magasins d'applications alternatifs, avec l'obligation pour les acteurs économiques concernés d'offrir des solutions techniques adéquates à cette fin;

9.2.3. imposer la transparence des critères de référencement et de classement employés par les magasins d'applications et, à cet égard, prévoir la collecte de l'information pertinente auprès des fabricants de terminaux;

9.2.4. prévoir l'enregistrement et le suivi des signalements des utilisateurs finals, ainsi que le développement d'outils de comparaison entre les pratiques des acteurs économiques concernés;

9.3. de réfléchir à des politiques globales de lutte contre la criminalité informatique et contre les abus du droit à la liberté d'expression et d'information sur internet; ces politiques devraient s'appuyer non seulement sur une législation pénale à jour, mais aussi sur le renforcement des moyens de prévention, y compris l'établissement de forces de police spécialisées dans le dépistage et l'identification des criminels informatiques et dotées de moyens techniques adéquats, la sensibilisation et une meilleure éducation des utilisateurs, ainsi qu'une collaboration accrue avec les opérateurs de l'internet et leur responsabilisation;

9.4. d'assurer, en même temps, que toute décision ou action nationale entraînant une restriction du droit à la liberté d'expression et d'information soit conforme à l'article 10 de la Convention européenne des droits de l'homme (STE n° 5) et éviter que la protection des utilisateurs et les exigences sécuritaires ne deviennent un prétexte pour museler les opinions dissidentes et pour porter atteinte à la liberté des médias;

9.5. de reconnaître et mettre en œuvre efficacement le principe de la «sécurité dès la conception» et, à cet égard:

9.5.1. assurer que la sécurité soit un trait fondamental dans la conception de l'architecture principale de l'internet et des infrastructures informatiques des services essentiels, afin de renforcer la résilience vis-à-vis des diverses formes d'attaques terroristes ou criminelles et de réduire le risque et les conséquences potentielles des pannes;

9.5.2. prévoir des obligations de gestion des risques et de signalement des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques;

9.5.3. prôner une coopération européenne et internationale accrue visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information;

9.5.4. promouvoir le développement des normes de sécurité internationales harmonisées concernant «l'internet des objets», y compris la mise en place d'un mécanisme de certification;

9.5.5. prévoir la responsabilité des entreprises privées (mais aussi, le cas échéant, des autorités publiques) en cas de dommages dus à une sécurité insuffisante des objets connectés qu'elles produisent et commercialisent, et introduire des régimes d'assurance obligatoire (entièrement financés par le secteur privé) afin de mutualiser les risques.

10. L'Assemblée souligne que les enfants nécessitent une protection spécifique en ligne et doivent être éduqués sur la manière d'éviter les dangers et de bénéficier au maximum d'internet. Les États membres du Conseil de l'Europe, avec les autres parties prenantes, doivent tirer entièrement parti de la Recommandation CM/Rec(2018)7 du Comité des Ministres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique.

11. L'Assemblée considère que la Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185, «Convention de Budapest») devrait être mieux utilisée pour améliorer la collaboration interétatique visant à renforcer la cybersécurité. Par conséquent, l'Assemblée appelle les États membres:

11.1. à ratifier la Convention de Budapest, s'ils ne l'ont pas encore fait, et à garantir sa pleine mise en œuvre, en tenant dûment compte des notes d'orientation sur les attaques visant les infrastructures d'information critiques, sur les attaques par déni de service distribué, sur le terrorisme et sur d'autres questions;

11.2. à encourager l'achèvement des négociations du deuxième protocole additionnel à la Convention de Budapest sur une coopération internationale renforcée et l'accès aux preuves d'activités criminelles stockées dans le nuage («cloud»);

11.3. à renforcer les synergies entre la Convention de Budapest, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201, «Convention de Lanzarote» et la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE n° 210, «Convention d'Istanbul») pour remédier à la cyberviolence, en suivant les recommandations figurant dans l'étude cartographique sur la cyberviolence adoptée par le Comité de la Convention Cybercriminalité (T-CY) le 9 juillet 2018;

11.4. à soutenir, et à utiliser au mieux, les programmes de renforcement des capacités menés par le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC).

12. L'Assemblée encourage les États membres du Conseil de l'Europe à s'engager avec le Groupe de haut niveau sur la coopération numérique créé par le Secrétaire général des Nations Unies et de contribuer à ses travaux. L'Assemblée recommande aux États membres du Conseil de l'Europe d'œuvrer ensemble pour améliorer, tant au niveau interne qu'au niveau international, les processus de prise de décision sur les questions concernant l'internet, en prônant une gouvernance de l'internet qui soit multipartite et décentralisée, transparente et responsable, collaborative et participative. À cet égard, ils devraient:

12.1. participer activement, y compris avec leurs parlementaires, au FGI, à l'EuroDIG et à d'autres plateformes de dialogue régionales et nationales sur la gouvernance de l'internet;

12.2. promouvoir le caractère ouvert du processus de prise de décision, afin d'assurer une participation équilibrée des parties qui y ont intérêt, selon des modalités variables en fonction du rôle qui est le leur par rapport aux questions traitées, et rechercher, dans la mesure du possible, des solutions consensuelles, tout en évitant les situations de blocage;

12.3. permettre que les différents groupes d'acteurs puissent administrer eux-mêmes les processus de désignation de leurs représentants, mais exiger que les procédures établies à cette fin soient ouvertes, démocratiques et transparentes;

12.4. encourager une dynamique de recomposition des intérêts au sein des divers groupes de parties prenantes, par exemple par le biais de structures associatives/fédératives devant respecter les critères d'une démocratie interne; concernant la représentation des usagers, encourager une représentation équilibrée selon les sexes, l'âge ainsi que l'origine ethnique;

12.5. développer, au niveau national, des mécanismes multipartites qui devraient servir de lien entre les discussions menées à l'échelle locale et les instances intervenant à l'échelle régionale et mondiale; assurer une bonne coordination et une communication fluide entre ces différents niveaux et favoriser une dynamique qui soit à la fois ascendante (du niveau local au niveau multilatéral) et descendante (du niveau multilatéral au niveau local);

12.6. éviter de concentrer les pouvoirs décisionnels dans les mains des autorités publiques et préserver le rôle des organisations chargées des aspects techniques et des aspects de gestion de l'internet, ainsi que le rôle du secteur privé;

12.7. viser à identifier les centres de décision les plus appropriés en termes d'efficacité, en raison de la connaissance des problèmes à traiter et de la capacité d'adapter les solutions aux spécificités des communautés qui doivent assurer leur mise en œuvre, en ayant égard également à une répartition horizontale des compétences décisionnelles entre acteurs de nature différente;

12.8. exiger que tous ceux qui participent à la gouvernance de l'internet assurent la transparence de leur action, celle-ci étant une condition sine qua non d'une gouvernance responsable. À cette fin:

12.8.1. il faut pouvoir identifier quelle responsabilité chacune des parties prenantes assume par rapport à la décision finale et à sa mise en œuvre;

12.8.2. au niveau multilatéral, la communauté des États devrait définir des procédures décisionnelles plus claires, en consultation avec les autres parties prenantes;

12.8.3. le sens des décisions prises doit être compréhensible pour leurs destinataires et ces décisions doivent être publiques, donc documentées, classifiées et publiées de manière à être aisément accessibles à tous;

12.9. maintenir une attitude proactive pour soutenir les caractères participatif et collaboratif du processus de décision; à cet égard, donner aux partenaires concernées les moyens de participer utilement à la prise de décision et inclure dans ces processus des experts d'autres domaines, au-delà du cercle des professionnels du métier, afin qu'ils puissent également contribuer au développement de l'internet.

B. Projet de recommandation[3]

1. L'Assemblée parlementaire, rappelant sa Résolution … (2019) «Gouvernance de l'internet et droits de l'homme», apprécie hautement les travaux que mène le Conseil de l'Europe dans le domaine de la société de l'information et souligne le rôle majeur que joue l'Organisation dans la défense d'une meilleure reconnaissance des droits de l'homme des internautes et leur protection efficace sur le web, ainsi que la contribution qu'elle apporte au renforcement du processus décisionnel sur les questions relatives à la gouvernance de l'internet. Les nombreux textes mûrement réfléchis adoptés en la matière par le Comité des Ministres témoignent très clairement de l'importance cruciale que revêtent ces questions.

2. La gouvernance de l'internet est un sujet qui doit rester prioritaire, étant donné que les décisions prises dans ce domaine ont une incidence directe sur la vie de tous les Européens et sur l'avenir de nos sociétés, y compris la stabilité de leurs fondements démocratiques et de leur développement socio-économique.

3. À cet égard, l'Assemblée considère que des efforts supplémentaires devraient être accomplis pour promouvoir une meilleure gouvernance de l'internet et aider les États membres du Conseil de l'Europe à relever ensemble les défis auxquels ils doivent faire face dans ce domaine.

4. La gouvernance de l'internet nécessite des procédures plus claires fondées sur la transparence et l'obligation de rendre compte. Ces procédures devraient être définies par la communauté des États, en consultation avec les autres parties prenantes, dans le respect d'une approche multipartite. Au niveau européen, le Conseil de l'Europe et l'Union européenne devraient œuvrer ensemble dans ce but.

5. Un premier pas dans cette direction pourrait être le renforcement de l'impact politique du dialogue paneuropéen sur la gouvernance de l'internet (EuroDIG), afin qu'il puisse jouer un rôle plus significatif dans l'établissement des objectifs et la structuration du débat sur la gouvernance de l'internet à l'échelle du continent européen. Le Conseil de l'Europe devrait adopter une attitude plus proactive vis-à-vis des pays européens qui n'ont pas d'initiatives nationales, en encourageant de telles initiatives et en veillant à leur caractère inclusif. Un engagement actif et le soutien du Conseil de l'Europe sont de grande importance pour garantir un niveau minimum de participation de toutes les régions de l'Europe dans le dialogue au sein de l'EuroDIG.

6. L'Assemblée s'inquiète de la sécurité insuffisante des réseaux et des systèmes d'information. À cet égard, elle salue l'approche qui est préconisée par l'Union européenne dans sa Directive (EU) 2016/1148 concernant des mesures destinées à assurer un niveau commun de sécurité des réseaux et des systèmes d'information dans l'Union, à savoir: des possibilités améliorées de cybersécurité au niveau national; une coopération accrue au niveau dans l'Union européenne; et des obligations de gestion des risques et de signalement des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques. L'Assemblée estime que cette approche devrait être encouragée dans tous les États membres du Conseil de l'Europe et, si possible, l'expertise acquise par l'Union européenne et ses membres devrait être partagée au sein d'un cadre européen élargi et au-delà.

7. Dès lors, l'Assemblée recommande au Comité des Ministres:

   7.1. de charger le Comité directeur sur les médias et la société de l'information (CDMSI) de suivre la mise en œuvre des recommandations adoptées par le Comité des Ministres dans le domaine de la gouvernance de l'internet, en faisant bonne usage du dialogue multipartite et des résultats des forums sur la gouvernance de l'internet, tels que le Forum sur la Gouvernance de l'Internet des Nations Unies (FGI), le Dialogue paneuropéen sur la gouvernance de l'internet (EuroDIG), ainsi que d'autres initiatives nationales et régionales;

   7.2. de lancer une étude sur comment renforcer les formes de coopération existantes en matière de prévention des attaques informatiques et sur l'opportunité de créer un mécanisme spécifique de surveillance, gestion des crises et analyse post-crise, en mutualisant les ressources existantes dans les divers pays, par exemple sur le modèle de l'Accord EUR-OPA Risques majeurs.

3. Projet de recommandation adopté à l'unanimité par la commission le 6 décembre 2018.

C. Exposé des motifs, par M. Andres Herkel, rapporteur

1. Introduction: justification et portée du rapport

1.1. Pourquoi la gouvernance de l'internet est importante

1. Internet est un «phénomène porteur de transformations, qui a la capacité de toucher pratiquement tous les aspects de la vie»[4]; c'est une sorte de superstructure centrale pour le fonctionnement de toutes les autres qui sont essentielles pour nos sociétés. Les usagers d'internet seraient plus de 4,15 milliards, soit plus de 54 % de la population mondiale[5]. Selon Eurostat, en 2017, les internautes représentaient 84 % de la population de l'Union européenne âgée de 16 à 74 ans[6]. Nous communiquons entre nous, accédons à du contenu (y compris des nouvelles et des informations qui sont cruciales afin que les citoyens puissent faire des choix éclairés et pour le fonctionnement de nos démocraties), des biens et des services commerciaux et en consommons, gérons nos comptes bancaires, dialoguons avec nos administrations locales et nationales, avons accès à des services (santé, services sociaux, justice, entre autres), payons nos impôts et participons à des processus politiques par l'intermédiaire d'internet.

2. Il apparaît donc évident que la gouvernance de l'internet est une question de politiques publiques mondiales cruciale et sensible. Sensible, en raison de la complexité inhérente aux problèmes d'ordre technique et juridique qui se posent, résultant également de la nature transnationale des flux de communication sur internet, qui outrepassent les frontières souveraines des États nations. Cruciale, aussi, car l'internet doit être considéré aujourd'hui comme un bien commun, qui a des conséquences sur de nombreux aspects de nos vies et touche aussi nos droits fondamentaux.

3. Notre futur est étroitement lié à la manière dont internet se développera. Le rapport intitulé *One Internet* de la Commission mondiale sur la gouvernance de l'internet (2016) présente les principaux risques et espoirs selon trois scénarios possibles. Il en existe certainement de nombreux autres qui pourraient résulter de tendances moins radicales et d'une combinaison des principaux éléments caractérisant chacun de ces trois scénarios. Mais je pense que cette vision quelque peu simplifiée est très utile à des fins opérationnelles.

4. Le premier scénario, effrayant, est celui d'un «cyberspace dangereux et fragmenté» où, entre autres, une collecte de données privées sans précédent et une surveillance massive par les gouvernements détruisent la vie privée des internautes, où des restrictions dictées par le pouvoir fragmentent l'internet et violent les droits de l'homme, où des actions malveillantes de cybercriminels multiplient les atteintes à la sécurité des usagers et où le risque de cyberguerre augmente, notamment les menaces au fonctionnement des infrastructures civiles, comme les réseaux électriques ou les systèmes de distribution de l'eau.

5. Le deuxième scénario est celui qui entraîne des «profits irréguliers et inégaux», où certains usagers s'emparent d'une part disproportionnée de «dividendes numériques» tandis que d'autres sont en permanence exclus. Les gouvernements ne préservent pas l'ouverture d'internet, ne permettent pas la concurrence et n'encouragent pas le secteur privé à étendre l'accès à haut débit. Ils choisissent d'assurer leur contrôle souverain en imposant des barrières commerciales, la localisation des données et la censure et en adoptant d'autres techniques qui fragmentent le réseau de façon à limiter la libre circulation des biens, des services, du capital et des données.

6. Le troisième scénario, plus optimiste, est celui d'un internet solide entraînant «de vastes progrès sans précédent» et offrant des possibilités de justice sociale, de droits de l'homme, d'accès à l'information et à la connaissance, de croissance, de développement et d'innovation.

7. À cet égard, notre tâche en tant que dirigeants politiques semble clairement de veiller à ce que la gouvernance de l'internet permette de proposer le meilleur scénario possible, en évitant les attitudes et comportements inconsidérés et autocentrés qui détourneraient le processus vers des évolutions alternatives inquiétantes[7].

---

4. Voir l'introduction de la version finale du rapport One Internet de la Commission mondiale sur la gouvernance d'internet (2016), publié par le Centre pour l'innovation dans la gouvernance internationale (CIGI) et Chatham House.
5. Voir: Internet World Stats, internet usage statistics, www.internetworldstats.com.
6. http://ec.europa.eu/eurostat/web/products-datasets/product?code=tin00028.
7. Des préoccupations concernant les risques d'un internet futur qui ne serait plus ni libre ni ouvert naissent aussi au sein de la communauté des fondateurs de l'internet. Voir, par exemple, les déclarations de Sir Tim Berners-Lee au Sommet de l'internet à Lisbonne (4-7 novembre 2018) ou les analyses dans le moz://a Internet Health report 2018.

.

1.2. Ce que l'on entend par «gouvernance de l'internet»

8. L'Agenda de Tunis, adopté lors de la deuxième phase du Sommet mondial sur la société de l'information en novembre 2005, donne une «définition pratique» de la gouvernance de l'internet comme étant l'élaboration et l'application par les gouvernements, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'internet[8].

9. Cette définition (que le Comité des Ministres du Conseil de l'Europe reprend dans sa Recommandation CM/Rec(2007)16 sur des mesures visant à promouvoir la valeur de service public de l'Internet) n'est pas forcément parfaite et a d'ailleurs ses détracteurs. Elle a toutefois à mon sens le mérite d'offrir un bon point de départ à notre analyse:

– elle fait état de la pluralité d'acteurs aux fonctions distinctes (mais néanmoins corrélées) qui prennent part à la gouvernance de l'internet – et devraient continuer à le faire – même s'il conviendrait selon moi d'inclure les organisations internationales (intervenant aux niveaux mondial et régional) dans la liste;

– elle souligne la nécessité de bâtir l'internet et de réglementer son utilisation à partir de fondations idéalement «communes», en commençant par arrêter d'un commun accord un ensemble de principes de base;

– de manière plus implicite, elle reconnaît que «la gouvernance de l'internet porte non seulement sur la conception et l'administration de l'internet, mais aussi sur son évolution et son utilisation; elle est donc axée par essence sur l'avenir et sur l'incidence de l'internet sur la société»[9].

10. La définition de l'Agenda de Tunis envisage la gouvernance de l'internet, semble-t-il, comme une sorte de système monolithique, masquant par là même une réalité d'une complexité extrême – comme le fait, par exemple, que les dispositifs de gouvernance peuvent varier d'un domaine à un autre[10]. Pour surmonter cette complexité, le rapport *One Internet* de la Commission mondiale sur la gouvernance de l'internet suggère «[qu']il peut être utile de se représenter internet en termes de couches. Il existe de multiples taxinomies possibles pour classifier ces couches, mais un cadre simple (...) propose de décomposer internet en quatre couches: infrastructures, logiciels, applications et contenu»[11]. Il ressort de ce même rapport que des questions politiques importantes imprègnent chacune de ces couches.

11. Dans ce rapport, j'aborderai surtout des questions politiques qui sont plus étroitement liées à la couche applicative (qui englobe par exemple les applications mobiles, les moteurs de recherche, les réseaux sociaux et les plateformes d'échange de contenus générés par les utilisateurs) et à la couche de contenu (qui inclut textes, audio, images, vidéos, musique et des contenus multimédia de toutes sortes). On pourrait synthétiser ces questions comme suit: Il est impératif d'assurer une protection plus effective des droits de l'homme sur internet. Même si je parlerai de la «gouvernance de l'internet», je souhaite noter ici que le terme «gouvernance digitale» est utilisé de plus en plus fréquemment pour comprendre tous les aspects de gouvernance qui accompagnent la transformation digitale de nos vies sociales, économiques et politiques fondée sur la diffusion des services digitaux et des applications qui utilisent l'internet et d'autres technologies et infrastructures digitales.

1.3. Thèmes principaux et fond du rapport

12. Il ressort très clairement des différents textes du Conseil de l'Europe[12] et d'autres parties prenantes[13] que les droits de l'homme, la démocratie et l'État de droit sont – et doivent rester – les objectifs clés de la gouvernance de l'internet. Je me limiterais ici à citer la Déclaration sur des principes de la gouvernance de l'internet, que le Comité des Ministres du Conseil de l'Europe a adopté le 21 septembre 2011. Le premier principe porte sur «Droits de l'homme, démocratie et État de droit»:

> *«Les dispositions pour la gouvernance de l'internet doivent assurer la protection de tous les droits et libertés fondamentaux et affirmer leur universalité, leur indivisibilité, leur interdépendance et leur corrélation, conformément au droit international des droits de l'homme. Elles doivent également veiller*

---

8. www.itu.int/net/wsis/docs2/tunis/off/6rev1-fr.html.
9. Voir l'introduction de la version finale du rapport *One Internet*, *op. cit.*
10. Voir à ce propos Mark Raymond et Laura DeNardis, Multistakeholderism: Anatomy of an Inchoate Global Institution, Paper Series n° 41, septembre 2016, publié par le Centre pour l'innovation dans la gouvernance internationale et Chatham House. D'après ses auteurs, la formulation de cette définition, même si elle affirme la nature multipartite de la gouvernance de l'internet, ne serait pas elle-même le fruit d'un effort multipartite.
11. Une taxinomie plus élaborée est proposée par Mark Raymond et Laura DeNardis dans leur publication «Multistakeholderism: Anatomy of an Inchoate Global Institution».

au respect plein et entier de la démocratie et de l'État de droit et elles devraient promouvoir le développement durable. Tous les acteurs publics et privés devraient reconnaître et respecter les droits de l'homme et les libertés fondamentales dans leur fonctionnement et leurs activités ainsi que dans la conception de nouveaux services, technologies et applications. Ils devraient être au fait des évolutions qui conduisent à l'amélioration des droits et libertés fondamentaux, mais également de celles qui constituent des menaces pour ces mêmes droits et libertés fondamentaux, et participer pleinement aux efforts visant à reconnaître de nouveaux droits.»

13. Dans les chapitres qui suivent, je m'intéresserai tout d'abord à une courte liste de droits fondamentaux que nous devons préserver ensemble, en tenant compte des dangers spécifiques qui les menacent. Dans cette analyse, je me fonderai sur les travaux du secteur intergouvernemental du Conseil de l'Europe ainsi que sur nos précédents travaux très fructueux.

14. Il n'est pas suffisant de réaffirmer que les droits de l'homme doivent être placés au cœur de la gouvernance de l'internet; ce point semble déjà plus ou moins convenu. Dès lors, j'examinerai comment nous pourrions améliorer la prise de décision sur les questions concernant la gouvernance de l'internet, et dans quelle mesure le Conseil de l'Europe et ses États membres peuvent agir avec plus d'efficacité au sein de l'écosystème de la gouvernance de l'internet pour faire respecter ces droits et en assurer une mise en œuvre effective.

15. La portée de ce rapport englobe des problèmes qui ont déjà été examinés ou sont en cours de discussion par notre commission, ainsi que par le secteur intergouvernemental du Conseil de l'Europe. Par conséquent, tout en cherchant à donner une vue globale et à apporter des mises à jour, je n'ai pas l'intention de refaire les analyses que nous avons déjà effectuées et je ne discuterai pas des questions clés qui sont couvertes par les travaux ciblés en cours de notre commission.

2. Les droits de l'homme en cause

16. Lorsque nous parlons de l'internet, le premier droit qui vient à l'esprit est celui de la liberté d'expression et d'information, qui est aujourd'hui intimement lié à l'internet: il faut garantir la liberté de s'exprimer et d'accéder aux contenus diffusés par d'autres sur le Net. L'on peut aussi rappeler les libertés de pensée, de conscience et de religion, et les libertés de réunion et d'association; mais, au fond, l'exercice de ces libertés dans le cyberespace se confond avec la liberté d'expression et d'information.

17. Pour que toute personne puisse bénéficier pleinement de ce(s) droit(s), il faut commencer par garantir l'accès à internet. Il faut aussi assurer que l'internet reste un écosystème ouvert; à cet égard, la «neutralité du Net» s'appuie sur deux piliers: l'obligation pour les fournisseurs d'accès à internet (FAI) de ne pas discriminer les contenus transmis sur le réseau et la possibilité pour les internautes de consulter et diffuser librement des contenus sur le réseau. En même temps, il faut assurer le droit à la sécurité des utilisateurs et leur droit au respect de leur vie privée, notamment sous l'angle de la protection des données personnelles.

2.1. Le droit d'accès à internet, sans discriminations

18. Je souhaite clarifier d'entrée que, lorsque je me réfère à un «droit d'accès à internet», cela ne signifie pas un droit pour chacun d'avoir un accès à l'internet gratuit, mais plutôt un droit d'accès à un internet libre à un prix abordable. Dans sa Résolution 1987 (2014) sur le droit d'accès à internet, l'Assemblée a soutenu que l'accès à internet devrait être reconnu en tant que tel comme un droit fondamental. Le rapport de la commission de la culture, de la science, de l'éducation et des média[14] soulignait que les actions et points de vue de plusieurs gouvernements, acteurs internationaux – dont le Conseil de l'Europe – et parties prenantes sur internet allaient dans cette direction, et il mentionnait une large reconnaissance de l'importance d'internet pour la liberté d'expression[15] (mais aussi pour d'autres droits), la promotion de la valeur de service public

12. J'ai repris les textes pertinents du Comité des Ministres dans le document AS/Cult/Inf (2018) 08 rev.
13. Voir, parmi d'autres: la Charte des Droits de l'Homme et Principes pour Internet et les 10 Droits et Principes d'Internet, publiés en 2011 par la Coalition Dynamique Droits et Principes d'Internet (IRPC); ces deux documents font partie d'un livret publié dans différentes langues; la Déclaration finale multipartite NETmundial du 24 avril 2014; l'ensemble de quatorze Principes pour l'élaboration des politiques de l'internet publiés en 2014 par l'Organisation pour la coopération et le développement économiques (OCDE).
14. Doc. 13434 (rapporteure: M^me^ Jaana Pelkonen, Finlande, PPE/DC).
15. Le rapport cite en particulier Nicola Lucchi, "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression" (6 février 2011), *Cardozo Journal of International and Comparative Law* (JICL), vol. 19, n^o^ 3, 2011. Disponible au SSRN: https://ssrn.com/abstract=1756243.

d'internet et la jurisprudence des tribunaux nationaux et internationaux. À cet égard, le Comité des Ministres, dans sa Déclaration sur des principes de la gouvernance de l'internet, a affirmé que «Les politiques relatives à l'internet devraient reconnaître le caractère mondial de l'internet et l'objectif d'accès universel»[16].

19. Dans quelques États, la loi reconnaît l'accès (abordable) à internet en tant que droit. Par exemple, depuis 2000, l'accès à internet est un droit selon la législation de l'Estonie[17]. Depuis 2007, en Suisse, la loi sur les télécommunications (LTC)[18] garantit le droit à un accès à l'internet de qualité à un prix abordable pour tous les habitants où qu'ils vivent. Depuis 2009, en Finlande, tous les individus et entreprises sont réputés avoir droit à un accès haut débit à internet dans leur lieu de résidence[19]. Plus généralement, au niveau de l'Union européenne, la Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive «service universel») vise à garantir pour l'ensemble des utilisateurs un minimum de services de communications électroniques de bonne qualité à un prix abordable.

20. Il peut être difficile pour un certain nombre de pays, y compris en Europe, d'affirmer de manière formelle que l'accès à internet est un droit en soi, compte tenu des implications que cela aurait en termes de développement des infrastructures (et de coûts liés pour le budget public) afin de garantir effectivement ce droit. J'estime cependant que non seulement nous devrions demander que l'accès universel à internet soit reconnu en tant que principe clé de la gouvernance de l'internet, mais que nous devrions aussi encourager en Europe des politiques nationales d'investissement public cohérentes avec un tel objectif, car l'atteindre me semble un facteur essentiel du développement durable démocratique et socio-économique.

21. Le droit d'accès à internet implique certainement de compenser les déséquilibres géographiques (par exemple entre les zones urbaines et les zones rurales ou isolées), mais il exige – et implique – beaucoup plus. Il existe une fracture numérique évidente entre les générations[20], ainsi que des différences socio-économiques et culturelles. Ce sont là des handicaps qui nécessitent un examen spécifique et une action ciblée afin de veiller à ce que certaines catégories d'usagers puissent disposer d'un véritable accès à internet. Il existe également des inégalités de genre qui ont un impact non négligeable sur l'accès à internet[21]. À ce propos, la proportion de femmes utilisant internet est inférieure de 12% à celle des hommes utilisant internet dans le monde; même en Europe, l'écart entre les hommes et les femmes internautes demeure d'environ 8%[22]. Il est toutefois encourageant de constater que cet écart a diminué depuis les précédentes statistiques et que, dans certains pays, le taux de pénétration est désormais le même.

22. En d'autres termes, le droit d'accès à l'internet est une composante essentielle de toute politique solide visant à lutter contre la discrimination, à promouvoir l'inclusion et à soutenir la cohésion sociale. Nous sommes là au cœur des responsabilités de l'État et cela ne peut pas être simplement laissé au secteur privé.

23. Il existe aussi de bons arguments pour convaincre ceux d'entre nous qui s'intéressent davantage à la dimension économique (et aux contraintes budgétaires) des politiques publiques. Pour ne citer qu'un exemple intéressant concernant la discrimination de genre, un rapport de 2015 du McKinsey Global Institute[23] estime

---

16. Dans ce même ordre d'idées, parmi d'autres exemples, le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, dans son rapport au Conseil des droits de l'homme du 16 mai 2011, a affirmé que: «En tant que moyen par lequel le droit à la liberté d'expression peut être exercé, l'internet ne peut atteindre son but que si les États respectent leur engagement à élaborer des politiques efficaces visant à assurer l'accès universel à l'internet» (document A/HRC/17/27, paragraphe 60). NETmundial 2014 affirme que la gouvernance de l'internet devrait favoriser l'accès à un internet universel, équitable, d'un coût abordable et de qualité, de manière à constituer un outil performant d'épanouissement personnel et d'inclusion sociale.

17. L'article 33 de la loi sur l'information publique de l'Estonie (*Journal officiel de l'État*, 2000, 92, 597, adoptée le 15 novembre 2000) garantit à toute personne la possibilité d'un accès gratuit à l'information publique via internet dans les bibliothèques publiques, conformément à la procédure prévue dans la loi sur les bibliothèques publiques.

18. Voir: https://www.admin.ch/opc/fr/classified-compilation/19970160/index.html.

19. Suite à un amendement à l'article 60.c de la loi sur le marché des communications (393/2003) qui est entré en vigueur le 1er juillet 2009.

20. Selon ICT facts and Figures 2017, la proportion de jeunes âgés de 15 à 24 ans utilisant internet (71% dans le monde; 95,7% en Europe) était bien plus élevée que la proportion de la population totale utilisant internet (48% dans le monde; 79,5% en Europe).

21. Sur cette question, voir entre autres l'analyse sur Empowering women on the Internet, effectuée en 2015 par la Direction des politiques internes du Parlement européen, Département des droits des citoyens et des affaires constitutionnelles.

22. Selon *ICT facts and Figures 2017*, le taux de pénétration d'internet pour les hommes est de 50,9 % dans le monde (contre 82,9 % en Europe) et de 44,9 % pour les femmes (contre 76,3 % en Europe). L'écart entre les sexes chez les internautes est calculé comme étant la différence entre les taux de pénétration d'internet pour les hommes et les femmes par rapport au taux de pénétration d'internet pour les hommes, exprimé en pourcentage.

que l'inégalité de genre est non seulement une question morale et sociale urgente, mais aussi un défi économique crucial et considère que, selon un scénario «à plein potentiel» dans lequel les femmes et les hommes joueraient un rôle identique sur les marchés du travail, jusqu'à 28 000 milliards de dollars pourraient être ajoutés au produit intérieur brut (PIB) mondial d'ici à 2025. Naturellement, nous ne saurions envisager de réduire l'inégalité de genre au travail et dans la société sans supprimer la fracture numérique[24].

24. Le rapport *One Internet* suggère que les gouvernements doivent non seulement encourager l'amélioration permanente des infrastructures d'internet, utiliser la concurrence comme un outil pour étendre les structures d'accès à internet et investir afin de garantir la disponibilité lorsque les forces du marché s'avèrent insuffisantes, mais qu'ils doivent aussi développer les investissements publics dans des lieux comme les écoles et les bibliothèques afin de fournir un accès aux communautés qui auraient sinon des possibilités limitées en raison de facteurs comme le revenu ou la géographie; développer la culture numérique; créer des mesures incitatives pour l'adoption de normes relatives au web visant à garantir que toute personne, indépendamment de ses capacités physiques, puisse utiliser internet.

2.2. Le droit à un internet ouvert: bâtir un écosystème qui sauvegarde la neutralité du Net

25. La Déclaration sur des principes de la gouvernance de l'internet, lorsqu'elle fixe les *Principes d'architecture*, demande à préserver «[l]es normes ouvertes, l'interopérabilité et le caractère 'de bout en bout' [end-to-end] de l'internet» et affirme qu'«[i]l ne devrait pas exister de barrières déraisonnables à l'entrée de nouveaux usagers ou à de nouveaux usages légitimes de l'internet, ni de charges superflues qui pourraient affecter le potentiel d'innovation en matière de technologies et de services». À cet égard, l'acquisition, par de puissantes plates-formes internet, d'outils novateurs à un stade précoce de leur développement est un phénomène qui suscite des inquiétudes quant à la possibilité réelle que de nouveaux concurrents émergent à un niveau mondial en recourant exclusivement à des mécanismes du marché libre[25].

26. Puis, cette déclaration insiste sur le principe d'*Ouverture du réseau:* «([l]es usagers devraient avoir le plus large accès possible à tout contenu, application et service de leur choix sur l'internet, qu'ils leur soient offerts ou non à titre gratuit, en utilisant les appareils appropriés de leur choix.». Et elle ajoute ensuite que: «Toute mesure de gestion du trafic qui a un impact sur l'exercice des droits et libertés fondamentaux, et particulièrement le droit à la liberté d'expression et le droit à recevoir et transmettre des informations sans considération de frontières, (…) doit être conforme aux dispositions du droit international relatives à la protection de la liberté d'expression et d'accès à l'information».

27. Plus récemment, le Comité des Ministres, dans sa Recommandation CM/Rec(2015)6 sur la libre circulation transfrontière des informations sur internet (adoptée le 1er avril 2015), après avoir rappelé que «[l]es dispositions sur les droits et les libertés figurant dans la Convention européenne des droits de l'homme (…) et l'article 19 du Pacte international relatif aux droits civils et politiques s'appliquent de la même façon en ligne et hors ligne», note que «[l]'article 10 de la [Convention européenne des droits de l'homme] concerne non seulement le contenu des informations, mais aussi leurs moyens de diffusion ou d'hébergement, dans la mesure où toute restriction apportée à ceux-ci a nécessairement un impact sur le droit de recevoir et de communiquer des informations». Puis le Comité des Ministres ajoute: «[l]a circulation transfrontière libre des informations sur internet est une condition essentielle au plein exercice de ces droits et libertés, au maintien du pluralisme et de la diversité de l'information, au développement de la culture, de l'éducation et de l'innovation et à la croissance économique.»

28. Je tiens également à mentionner ici la Recommandation CM/Rec(2016)1 du Comité des Ministres sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau (adoptée le 13 janvier 2016). Cette recommandation contient une série de lignes directrices sur la neutralité du réseau, qui englobent l'égalité de traitement du trafic internet, le pluralisme et la diversité de l'information, la vie privée, la transparence et la responsabilisation. Elle appelle les États européens à préserver le principe de la neutralité du réseau lors du développement de leur cadre juridique national afin d'assurer la protection du droit à la liberté d'expression, à l'accès à l'information et au respect de la vie privée.

---

23. How advancing women's equality can add $12 trillion to global growth (septembre 2015).
24. Voir par exemple les *Harvard Business Reviews* suivants: Bhaskar Chakravorti, There's a Gender Gap in Internet Usage. Closing It Would Open Up Opportunities for Everyone (12 décembre 2017), et Julie Sweet, Access to Digital Technology Accelerates Global Gender Equality (17 mai 2016).
25. Voir par exemple ici une liste, mise à jour en janvier 2018, de 66 acquisitions de Facebook.

29. Le Règlement (UE) 2015/2120[26] consacre le principe de la neutralité du Net et l'accès à un internet ouvert. Il prévoit un droit individuel et exécutoire pour les utilisateurs finals en Europe d'accéder aux contenus et services internet de leur choix et de les diffuser, et un traitement égal et non discriminatoire du trafic dans le cadre de la fourniture de services d'accès à l'internet[27]. Le règlement impose aussi aux fournisseurs de services d'accès à l'internet des obligations de transparence (article 4), notamment en ce qui concerne le contenu de tout contrat incluant des services d'accès à l'internet, et il charge les autorités réglementaires nationales de surveiller l'application du règlement et de veiller à la neutralité du Net et au respect des droits des utilisateurs (article 5).

30. Cependant, le principe de la neutralité du Net a été remis en question par la US Federal Communications Commission (FCC), qui a abrogé (avec effet au 11 juin 2018) des règles fédérales visant à garantir la neutralité du Net. Ainsi, aux États-Unis, les géants de la téléphonie et du câble peuvent désormais mettre en place des «voies rapides» pour des sites et services spécifiques privilégiés (leurs propres sites et services et/ou ceux de leurs clients qui sont prêts à payer davantage pour bénéficier d'un traitement préférentiel), tous les autres se voyant attribuer des voies plus lentes. Ils pourraient également décider (en théorie) de bloquer l'accès à certains services, ceux de leurs concurrents par exemple[28].

31. Les usagers européens sont protégés par la législation de l'Union européenne et le Commissaire européen Andrus Ansip a déclaré publiquement que l'abrogation des règles de neutralité du Net par les États-Unis n'aurait aucun effet en Europe. Cependant, nous ne sommes pas «isolés» de ce qui se passe dans d'autres parties du monde – et plus particulièrement aux États-Unis – et j'ai du mal à croire que cela n'aura aucun impact quel qu'il soit, notamment en termes d'avantages et d'inconvénients pour les entreprises européennes fonctionnant au niveau mondial. L'Europe a un certain nombre de dossiers controversés à traiter avec l'Administration Trump qui pourraient sembler plus importants, mais la gouvernance de l'internet ne devrait pas être négligée et nous devrions être actifs dans toutes les instances internationales possibles pour garantir la neutralité du Net.

32. Par ailleurs, la neutralité du Net est menacée, en Europe aussi, tant par différentes formes de «censure d'État» – que certains régimes utilisent pour museler les critiques – que par certaines pratiques des opérateurs. Je traiterai brièvement des questions concernant la liberté d'expression et d'information sur le Net, y compris de la censure d'État, dans la section suivante.

33. Quant aux pratiques des opérateurs qui vont à l'encontre de la neutralité du Net, je souhaite évoquer ici un rapport qui a été publié en février 2018 par l'autorité française de régulation des communications électroniques et des postes (ARCEP) intitulé «Smartphones, tablettes, assistants vocaux: les terminaux, maillon faible de l'internet ouvert». Ce rapport fort instructif explique bien que la chaîne d'accès à internet ne s'arrête pas aux réseaux d'accès et que la capacité des utilisateurs à accéder aux contenus et services de leur choix sur internet peut être (et en effet est) limitée par d'autres intermédiaires. L'ARCEP pointe à cet égard le doigt vers les terminaux (smartphones, tablettes, ordinateurs…), leurs systèmes d'exploitation et

---

26. Règlement (UE) 2015/2120 du Parlement européen et du Conseil de l'Union européenne du 25 novembre 2015, établissant des mesures relatives à l'accès à un internet ouvert.

27. L'article 3.1 dispose que «[l]es utilisateurs finals ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet». L'article 3.3 impose aux fournisseurs de services d'accès à l'internet de traiter tout le trafic «de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés». Pour plus d'informations, voir la page de la Commission européenne sur l'Open Internet.

Néanmoins, les droits des utilisateurs finals (et les obligations correspondantes des fournisseurs de services d'accès à l'internet) ne sont pas absolus: d'une part, il y a les limites fixées par le droit de l'Union et par le droit national en ce qui concerne la légalité des contenus, des applications et des services (article 3.1, alinéa 2); d'autre part le règlement (article 3.3, alinéa 2) permet aux fournisseurs de services d'accès à l'internet «de mettre en œuvre des mesures raisonnables de gestion du trafic.». Le texte précise ensuite que, pour être réputées raisonnables, les mesures doivent être: transparentes, non discriminatoires et proportionnées, non fondées sur des considérations commerciales, mais sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic; par ailleurs, ces mesures «ne concernent pas la surveillance du contenu particulier et ne sont pas maintenues plus longtemps que nécessaire».

28. Les jeux ne sont cependant pas encore faits aux États-Unis: outre les réactions publiques et les procédures légales que des groupes de défense des droits des consommateurs et certains procureurs généraux ont intentées contre la décision de la FCC, cette décision a également mobilisé une opposition au sein du Congrès américain et dans un certain nombre d'États. Ainsi, dans les États de Washington, du Vermont, de l'Oregon et de Californie, des nouvelles lois imposant de traiter les données de manière égale sont entrées en vigueur pour remplacer les règles fédérales abrogées.

leurs magasins d'applications, qui sont contrôlés par un nombre réduit d'acteurs économiques. Comme l'ARCEP l'explique: «La liberté de choix de l'utilisateur se trouve peu à peu réduite, par des limitations imposées par ces équipements. Certaines de ces limitations peuvent se justifier pour des raisons d'ergonomie, de sécurité ou d'innovation. D'autres restreignent artificiellement l'accès à internet et au foisonnement de contenus et de services disponibles pour les usagers. L'évolution vers des terminaux toujours plus intelligents – assistants vocaux à la maison, ordinateur de bord dans la voiture, objets connectés – laisse entrevoir un risque de limitation toujours plus grand, dans ces environnements parfois non compatibles entre eux[29].»

34. Pour faire face à ce risque, l'ARCEP identifie cinq pistes d'actions (reprises à la page 68 de son rapport), qui méritent d'être portées à l'attention de tous nos États membres:

– clarifier le champ de l'internet ouvert en posant un principe de liberté de choix des contenus et applications quel que soit le terminal;

– réguler «par la data» (collecter l'information auprès des fabricants de terminaux; recueillir les signalements des utilisateurs finals; promouvoir des outils de comparaison; imposer la transparence des critères de référencement et de classement employés par les magasins d'applications);

– renforcer la fluidité;

– lever certaines restrictions imposées artificiellement par les acteurs-clefs des terminaux et, à cet égard, entre autres, permettre aux utilisateurs de supprimer des applications préinstallées et d'accéder sereinement aux applications proposées par des magasins d'applications alternatifs, dès lors qu'ils sont jugés fiables;

– établir une procédure agile pour accompagner les entreprises, notamment les petites et moyennes entreprises (PME) et les start-ups, face à des pratiques discutables.

2.3. Le droit à la liberté d'expression et d'information

35. On ne compte plus le nombre de fois où notre commission et notre Assemblée parlementaire ont insisté sur l'importance fondamentale du droit à la liberté d'expression et d'information – consacré par l'article 10 de la Convention européenne des droits de l'homme et par l'article 19 du Pacte international relatif aux droits civils et politiques des Nations Unies – en tant que pilier de toute société démocratique. Nous avons insisté sur l'obligation pour les États membres du Conseil de l'Europe de veiller à ce que ce droit ne soit menacé ni par les pouvoirs publics ni par les opérateurs du secteur privé ou non gouvernemental.

36. Nous n'avons pas manqué de souligner dans nos rapports le rôle que l'internet et les médias sociaux ont assumé dans le nouveau contexte médiatique, en mettant un terme à la concentration du pouvoir d'information et en transformant le paradigme de la communication, mais aussi en modifiant en profondeur la communication institutionnelle et l'articulation des relations entre électeurs et forces politiques, ainsi qu'entre les citoyens, les élus et les administrations.

37. Nous avons également signalé les dangers nouveaux que les abus du droit à la liberté d'expression et d'information sur le réseau engendrent, tels que: l'incitation à la discrimination, à la haine, à la violence contre les minorités ethniques, religieuses ou autres; l'incitation au terrorisme; la pédopornographie; le cyberharcèlement et la violence contre les femmes sur le Net; la manipulation de l'information et la propagande à des fins de déstabilisation politique ou autre. Le présent rapport ne reviendra pas sur ces questions, d'autant qu'elles sont régulièrement reprises dans des rapports plus spécifiques, y compris ceux que notre commission prépare actuellement[30]. Nous avons fait un diagnostic complet, mais nous sommes encore à la recherche de solutions valables, car il n'est pas aisé de combattre les abus sans mettre en péril le droit à la liberté d'expression et d'information lui-même.

38. La Déclaration sur des principes de la gouvernance de l'internet affirme que «[t]oute décision ou action nationale entraînant une restriction des droits fondamentaux devrait être conforme aux obligations internationales et, en particulier, être prévue par la loi, être nécessaire dans une société démocratique et respecter pleinement le principe de proportionnalité et le droit à un recours indépendant, assorti de garanties

29. Voir le communiqué de presse de l'ARCEP du 15 février 2018.

30. Il s'agit notamment des rapports suivants: La liberté des médias en tant que condition pour des élections démocratique (Doc. 14669); Les médias de service public dans le contexte de la désinformation et de la propagande (Doc. 14780); Vers une institution d'ombudsman chargé des questions liées à l'internet; Les réseaux sociaux: créateurs de liens sociaux ou destructeurs des libertés fondamentales?; Éducation aux médias dans le nouvel environnement médiatique; Menaces sur la liberté des médias et la sécurité des journalistes en Europe.

juridiques et procédurales adéquates». Bien que la déclaration utilise le conditionnel «devrait», ce principe est clairement lié à l'article 10 de la Convention européenne des droits de l'homme; donc, il n'est pas négociable. Cependant, sa mise en œuvre effective est loin d'être assurée.

39. Les mesures de fermeture de sites internet peuvent s'avérer nécessaires pour assurer la protection des utilisateurs; mais si, par exemple, le but réel est d'empêcher la dissidence et de saper l'action de l'opposition démocratique, il s'agit d'une atteinte grave à la liberté d'expression en général et à la liberté des médias en particulier. Au-delà des violations graves et systémiques du droit à la liberté d'information et d'expression par de régimes peu ou pas démocratiques, l'étendue de ce droit (soit les limites fixées par les législations nationales à ce droit) peut varier d'un pays (démocratique) à un autre. Cela n'est pas forcément une anomalie, car il s'agit aussi de fixer les points d'équilibre entre ce droit et d'autres droits également dignes de tutelle et chaque communauté nationale exprime à cet égard des préférences qui lui sont propres. Cependant, lorsqu'il s'agit de l'internet, des différences peuvent devenir un obstacle à une régulation suffisamment harmonisée sur la licéité (ou pas) des contenus.

40. De plus, la transformation progressive de certains moteurs de recherche et médias sociaux en sélectionneurs actifs et organisés de nouvelles et d'informations pour leurs utilisateurs pourrait avoir de lourdes conséquences sur l'accès à une diversité de médias et d'opinions[31].

41. Enfin, je souhaite souligner ici le lien qui existe entre, d'une part, le droit à la liberté d'expression et d'information et, d'autre part, la possibilité de mettre en valeur la diversité culturelle et les particularismes locaux sans pour autant aboutir à une sorte de communautarisme sur le Net. À cet égard, selon la Déclaration sur des principes de la gouvernance de l'internet, «[l]a préservation de la diversité culturelle et linguistique et la promotion de la création de contenus locaux, sans considération de langue et caractères d'écriture, devraient être des objectifs essentiels des politiques, de la coopération internationale ainsi que du développement de nouvelles technologies dans le domaine de l'internet».

2.4. Gouvernance de l'internet et sécurité

42. La sécurité est un droit fondamental. Nous avons tous l'aspiration à vivre dans un environnement sécurisé, où nous sommes à l'abri de l'arbitraire, des menaces, des atteintes à notre intégrité physique et psychique, des violations de nos droits. Comme nous le rappelle le titre de l'article 5 de la Convention européenne des droits de l'homme, «liberté et sécurité» vont ensemble. Cela concerne l'internet aussi, en tant que partie intégrante de notre environnement de vie. Nous parlons de monde «virtuel», mais il ne faut pas s'y méprendre: ce qui arrive sur l'internet fait partie de notre vie réelle. Nous avons besoin de beaucoup plus de sécurité dans l'internet. Le discours du Président français Emmanuel Macron au Forum sur la gouvernance de l'internet à Paris (12-14 novembre 2018)[32] a été un cri d'alarme que nous ne devrions pas ignorer.

43. Cette question présente différents aspects, dont les suivants:

– la sécurité des bases de données que les institutions publiques ou privées gèrent et qu'il faut défendre des actions malveillantes de piratage informatique visant à voler, manipuler, rendre inaccessibles ou détruire les données en question;

– la sécurité des échanges et transactions sur le réseau et la lutte contre les fraudes informatiques;

– la sécurité personnelle d'usagers vulnérables – enfants, adolescents, femmes, mais d'autres aussi – victimes de propos racistes et haineux, de violence psychologique, d'atteintes à leur dignité, de cyberintimidation et de cyberharcèlement;

– la sécurité des infrastructures stratégiques et des services essentiels qui s'appuient sur l'internet pour leur fonctionnement, comme les réseaux de communications, les réseaux énergétiques (y compris la sécurité des centrales nucléaires), les systèmes de transport, le système des banques et de la bourse, les services de santé ou de la justice, dont les dysfonctionnements peuvent engendrer des conséquences extrêmement graves, voire dramatiques;

– plus généralement, la sécurité de nos sociétés démocratiques face à tout type d'attaque, y compris des institutions démocratiques, liées à ce que l'on nomme cyberterrorisme et cyberguerre ou guerre cybernétique.

---

31. Cette question importante est traitée par le rapport de notre commission sur «Les réseaux sociaux: créateurs de liens sociaux ou destructeurs des libertés fondamentales?»
32. Voir le texte ici.

44. La question, dans ses diverses facettes, a fait l'objet de plusieurs travaux de l'Assemblée (et de notre commission)[33]. En m'inspirant des recommandations que l'Assemblée a formulées, mais aussi des propositions avancées par nombre d'experts, je souhaite ici insister sur l'importance d'orienter notre action politique (à tous les niveaux) vers quelques résultats clé.

45. Premièrement, il faut intégrer la sécurité comme trait caractéristique essentiel dès la conception. Le principe de la «sécurité dès la conception» est crucial pour l'architecture principale d'internet et les infrastructures informatiques des services essentiels afin de renforcer la résilience vis-à-vis des diverses formes d'attaques terroristes ou criminelles, mais aussi de réduire le risque et les conséquences potentielles des pannes. À cet égard, je recommanderais l'approche qui est préconisée par l'Union européenne dans sa Directive (EU) 2016/1148 sur la sécurité des réseaux et des systèmes d'information (NIS Directive), qui vise à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne grâce à des possibilités améliorées de cybersécurité au niveau national, une coopération accrue au niveau de l'Union européenne et des obligations de gestion des risques et de signalement des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques[34]. Cette approche devrait être encouragée dans tous les États membres du Conseil de l'Europe et, si possible, l'expertise acquise par l'Union européenne et ses membres devrait être partagée au sein d'un cadre européen élargi et au-delà.

46. Le principe de la «sécurité dès la conception» est aussi crucial pour le réseau des dispositifs physiques, appareils électroménagers et autres éléments que nous appelons «l'internet des objets» (IO), qui entrent progressivement dans notre vie quotidienne. L'intérêt commercial des entreprises en vue de maximiser les bénéfices économiques (et peut-être l'intérêt pour les gouvernements de profiter des bénéfices immédiats que ce commerce apporte en termes d'opportunités d'emplois et de revenus fiscaux) ne saurait l'emporter sur la sécurité des usagers. Il incombe aux développeurs et aux vendeurs de livrer les produits les plus sûrs et cette responsabilité devrait être clairement inscrite dans les réglementations nationales même pour l'internet des objets. Pour que ces réglementations soient efficaces, elles devraient être harmonisées; il faut donc développer des normes de sécurité internationale harmonisées. La certification devrait devenir obligatoire et un mécanisme de certification devrait être adopté. De même, il en va de la responsabilité à la fois des entreprises privées et des autorités publiques de garantir une couverture des dommages; ainsi, des régimes d'assurance obligatoire (devant être entièrement financés par le secteur privé), similaires à ceux qui existent pour les accidents de voiture, devraient être introduits afin de mutualiser les risques.

47. Deuxièmement, la lutte pour la sécurité (et particulièrement la crainte d'attentats terroristes et de cyberguerre et les tentatives pour contrer ces menaces) est étroitement liée à la tendance de balkanisation du cyberespace. Si nous devons renforcer la protection au niveau national, nous devons également éviter la fragmentation de l'internet et le contrôle omniprésent de l'État sur la circulation des informations sur internet. Cela non seulement réduirait considérablement le potentiel d'internet, mais constituerait aussi une menace majeure pour les droits fondamentaux des citoyens. Cependant, quelles sont les alternatives à la balkanisation et au contrôle de l'État qui pourraient préserver un internet libre et un haut niveau de sécurité? Je n'ai pas de réponse complète à cette question, mais ce que je suggère, c'est d'explorer la possibilité de renforcer la coopération internationale, du moins au niveau régional, au lieu de nous diviser, en tenant compte aussi du fait que, dans un monde de l'internet global, des mesures qui sont simplement nationales sont très souvent inutiles.

48. Il y a, je crois, deux raisons principales et interdépendantes qui entravent le renforcement de la collaboration au niveau international (et même une discussion sur les structures et mécanismes nécessaires): le désir de rester ou de devenir prédominant ou pour le moins suffisamment influent (en termes de pouvoirs politique, militaire et économique), et le manque de confiance dans la bonne volonté et les intentions de l'autre. Le défi consiste donc à trouver la voie qui renforcera la solidarité et la confiance mutuelle, y compris la volonté de mutualiser (au moins dans une certaine mesure) les technologies nationales mises au point pour améliorer la sécurité. L'objectif de toute tentative de renforcement de la coopération internationale ne saurait

---

33. Voir par exemple les rapports et textes adoptés sur: La pornographie violente et extrême; La protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne; Violence véhiculée dans et par les médias; Mettre fin à la cyberdiscrimination et aux propos haineux en ligne.

Concernant la cybercriminalité, le cyberterrorisme et la cyberguerre, je rappelle les travaux de l'Assemblée sur Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet; Améliorer la protection et la sécurité des utilisateurs dans le cyberespace; Problèmes juridiques posés par la guerre hybride et obligations en matière de droits de l'homme.

34. Pour d'autres renseignements, voir la Fact Sheet de la Commission européenne (en anglais).

être la mise en place d'une superstructure qui aurait un contrôle total à la place des États individuels: cela risquerait d'être le début d'un monde orwellien. J'y reviendrai lorsque nous discuterons des processus de prise de décision en matière de gouvernance de l'internet.

49. Troisièmement, la sécurité de l'internet est certainement une responsabilité du secteur privé et des pouvoirs publics, mais les usagers ont aussi un rôle crucial à jouer. La communauté des internautes est non seulement une victime potentielle, mais aussi une armée potentielle contre les menaces à la sécurité individuelle et collective. Ainsi, leur conscience des divers risques, leur compréhension de ce qu'ils devraient faire pour les réduire et leur capacité à réagir lorsqu'ils deviennent des cibles d'attentats ou décèlent des attaques contre d'autres personnes sont capitales pour toute stratégie de défense effective. Les autorités publiques et les médias sociaux devraient être actifs pour éduquer et former cette armée. C'est le sujet du travail en cours de la commission sur «L'éducation aux médias dans le nouvel environnement médiatique» auquel je fais référence. Cependant, je souhaite souligner ici que les enfants nécessitent une éducation sur comment éviter les dangers et bénéficier au maximum de l'internet. Les États membres du Conseil de l'Europe, avec les autres parties prenantes, doivent tirer entièrement parti de la Recommandation CM/Rec(2018)7 du Comité des Ministres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique.

50. Quatrièmement, j'estime que la Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185, «Convention de Budapest») devrait être mieux utilisée pour améliorer la collaboration interétatique visant à renforcer la cybersécurité. À cet égard, nous devrions appeler les États membres du Conseil de l'Europe:

– à ratifier la Convention de Budapest, s'ils ne l'ont pas encore fait, et à garantir sa pleine mise en œuvre, en tenant dûment compte des notes d'orientation sur les attaques visant les infrastructures d'information critiques, sur les attaques par déni de service distribué, sur le terrorisme et sur d'autres questions;

– à encourager l'achèvement des négociations du deuxième protocole additionnel à la Convention de Budapest sur une coopération internationale renforcée et l'accès aux preuves d'activités criminelles stockées dans le nuage («cloud»);

– à renforcer les synergies entre la Convention de Budapest, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201, «Convention de Lanzarote» et la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE n° 210, «Convention d'Istanbul») pour remédier à la cyberviolence, en suivant les recommandations figurant dans l'étude cartographique sur la cyberviolence adoptée par le Comité de la Convention Cybercriminalité (T-CY) le 9 juillet 2018;

– à soutenir, et à utiliser au mieux, les programmes de renforcement des capacités menés par le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC).

51. Dernier point et non des moindres, l'intelligence artificielle (IA) est déjà sur le champ de bataille. Les progrès dans le développement de l'intelligence artificielle et de sa capacité d'«apprentissage profond» pourraient nous fournir de nouveaux outils de défense solides. Mais dans le même temps, cela fournira aux délinquants potentiels de nouvelles armes puissantes. En outre, la possibilité que, dans un certain nombre d'années, il existe des formes d'intelligence artificielle capables d'une certaine forme d'«autodétermination» soulève – entre autres – un nouveau type de problèmes de sécurité. Notre avenir en cohabitation avec l'intelligence artificielle est une question sensible et très complexe qui, selon moi, mérite un nouveau rapport spécifique.

2.5. La protection de la vie privée et des données personnelles dans le cyberespace

52. Les technologies qui font désormais partie de notre quotidien au point d'être devenues incontournables, que nous utilisons aussi pour construire nos relations interpersonnelles et à qui nous confions sans trop y penser, peu à peu, les éléments les plus intimes de notre identité, deviennent des outils pour la manipulation des opinions et qui rendent possible le contrôle insidieux de notre vie privée[35]. Cette question aussi a fait l'objet de travaux antérieurs de l'Assemblée[36], qui a exprimé ses inquiétudes concernant la collecte massive de données à caractère personnel par les entreprises privées, a mis en exergue la problématique liée à l'établissement de profils d'utilisateurs de l'internet, mais aussi les risques résultant des actions des hackers

35. Voir, par exemple, Résolution 1970 (2014) «Internet et la politique: les effets des nouvelles technologies de l'information et de la communication sur la démocratie».
36. Voir, par exemple, les rapports et textes adoptés sur La protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne et sur Les opérations de surveillance massive.

qui s'infiltrent dans les systèmes informatiques dans le but d'obtenir des données détenues par les sociétés commerciales, les institutions financières, les instituts de recherche et les pouvoirs publics. L'Assemblée a également souligné la menace que représentent pour les droits de l'homme les systèmes d'envergure mis en place par les services de renseignement en vue de collecter, de conserver et d'analyser à une grande échelle les données des communications.

53. Je pense qu'il s'agit d'un domaine où les intérêts des entreprises privées l'emportent encore sur la protection des utilisateurs d'internet, en dépit de la protection renforcée des données à caractère personnel au sein de l'Union européenne, grâce au Règlement général sur la protection des données (RGPD) désormais en vigueur[37], et aux améliorations dans le cadre de l'Europe élargie, avec l'adoption récente de la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («Convention 108 modernisée»), qui est maintenant ouverte à la signature et à la ratification[38].

54. L'avant-propos du nouveau manuel Handbook on European data protection law[39] déclare que «l'Europe est à la pointe de la protection des données au niveau mondial». Cependant, en réalité, le modèle économique actuel des plus grands opérateurs d'internet est basé sur les données, le nouveau «pétrole» de la société numérique et (conformément à leur intérêt réel) ils agissent tous pour obtenir le «consentement de l'usager» nécessaire pour recueillir et utiliser comme ils le jugent approprié le plus grand nombre possible de données (personnelles). Cette question est traitée aussi dans le cadre du rapport de notre commission sur «Les réseaux sociaux: créateurs de liens sociaux ou destructeurs des libertés fondamentales?», auquel je renvoie.

3. Améliorer la prise de décision sur les questions concernant l'internet

55. La question du processus décisionnel concernant l'internet se pose tant au niveau multilatéral (global ou régional) qu'au niveau national, dans le cadre de l'ordre juridique interne. Les grands principes qui reviennent constamment dans les prises de position des organes du Conseil de l'Europe et dans celles d'autres partenaires sont applicables à tous les niveaux décisionnels, encore que leur mise en œuvre doit être adaptée au contexte. J'ajoute que, comme je l'ai indiqué dans l'introduction, il ne s'agit pas de définir un modèle universel: la gouvernance de l'internet n'est pas monolithique, mais complexe, avec différents rôles et responsabilités pour les diverses parties prenantes dans les différents domaines[40]. Dès lors, mes considérations doivent être comprises comme une tentative d'identifier des orientations pour une gouvernance dont le but est la sauvegarde effective des droits précédemment identifiés.

56. La Déclaration du Comité des Ministres sur des principes de la gouvernance de l'internet inclut trois principes concernant le processus décisionnel qu'il convient de souligner: «gouvernance multiacteurs», «autonomisation des usagers de l'internet» et «gestion décentralisée».

57. La Déclaration finale multipartite NETmundial de 2014 recense, elle aussi, un certain nombre de «principes relatifs aux processus de gouvernance de l'internet», qui portent sur les processus décisionnels et sur la structure des organes décisionnels. Certains de ces principes se recoupent ou se complètent réciproquement; d'autres portent davantage sur les finalités du processus décisionnel que sur le processus lui-même; mais en substance, les trois principes évoqués ci-avant sont confirmés.

58. Selon cette Déclaration, la gouvernance de l'internet devrait être:

– «multipartite», «axée sur l'ouverture, la participation et le consensus», «inclusive et équitable»;

---

37. Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données). Pour plus d'informations sur ce règlement, voir la page officielle du site de la CE sur la Réforme des règles de l'UE en matière de protection des données 2018 et le Portail du RGPD.

38. La Convention 108 modernisée a été adoptée lors de la 128e session du Comité des Ministres du Conseil de l'Europe (Elsinore, Danemark, 17-18 mai 2018). Pour plus d'informations, voir la page web du Conseil de l'Europe sur la modernisation de la Convention 108 et le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE no 223).

39. Le manuel (édition 2018, disponible actuellement en anglais seulement) a été préparé par l'Agence des droits fondamentaux de l'Union européenne (FRA), avec le Conseil de l'Europe (y compris le Greffe de la Cour européenne des droits de l'homme) et le Contrôleur européen de la protection des données.

40. Dans certains domaines tels que l'élaboration de normes internet de base et la gestion du système de noms de domaines, les États ne sont pas responsables au premier chef et la gouvernance repose sur une approche multipartite, les chefs de file étant des acteurs privés (IETF, ICANN, etc.).

– «distribuée», c'est-à-dire «menée dans le cadre d'un écosystème distribué, décentralisé et multipartite»;

– «génératrice d'une participation significative» (ce qui demande de soutenir le renforcement des capacités des parties prenantes avec moins d'expérience ou sous-représentées).

59. La Déclaration NETmundial souligne que la gouvernance de l'internet doit être aussi «transparente», «responsable» et «collaborative». Transparence et responsabilité sont des mots-clés qui se retrouvent dans la Déclaration sur des principes de la gouvernance de l'internet dans les textes explicatifs qui accompagnent le principe de la gouvernance multiacteurs et de la gestion décentralisée. Néanmoins il me semble utile de les mettre davantage en valeur.

60. Dès lors, une bonne gouvernance de l'internet serait (entre autres) multipartite et décentralisée, transparente et responsable, collaborative et participative. Dans une certaine mesure, ces principes sont interconnectés et se soutiennent mutuellement. Par exemple: pour avoir un processus inclusif et ouvert aussi aux usagers, il est nécessaire de soutenir leur autonomisation; afin que chaque partie prenante puisse jouer pleinement son rôle dans le cadre d'une gouvernance multipartite, il faut aussi garder une gestion décentralisée; une telle gestion ne saurait cependant garantir les droits fondamentaux sans la transparence et la responsabilité. Ainsi, même s'il convient d'analyser ces principes séparément, il ne faut pas perdre de vue les liens qui les tiennent ensemble.

3.1. Gouvernance multipartite et décentralisée, et dialogue politique sur la gouvernance de l'internet

61. Il n'y a pas de définition commune de ce qu'une approche multipartite à la gouvernance de l'internet pourrait ou devrait être.

62. Pour expliquer la «gouvernance multiacteurs», la Déclaration du Comité des Ministres du Conseil de l'Europe sur des principes de la gouvernance de l'internet parle de la pleine participation des gouvernements, du secteur privé, de la société civile, des milieux techniques et des utilisateurs, compte tenu de leurs rôles et de leurs responsabilités spécifiques; et elle ajoute que l'élaboration des politiques publiques internationales relatives à l'internet et des mécanismes de gouvernance de l'internet devrait permettre la pleine participation égale de toutes les parties prenantes de tous les pays.

63. La Déclaration NETmundial préconise une gouvernance ouverte à tous les acteurs qui souhaitent y participer et garantissant leur participation significative et responsable; elle explique que les rôles et les responsabilités respectives des parties prenantes devraient être interprétés de manière à pouvoir les adapter aux questions discutées, puis elle ajoute que l'élaboration de politiques publiques et d'arrangements internationaux relatifs à la gouvernance de l'internet devrait permettre à l'ensemble des parties prenantes d'y prendre part pleinement et de manière équilibrée, et émaner d'un consensus, dans la mesure du possible.

64. Sur cette base, la gouvernance multipartite implique d'abord:

– le caractère tendanciellement ouvert du processus de prise de décision, afin de pouvoir y inclure les parties qui y ont intérêt, qu'il s'agisse des gouvernements (ou plus en général des pouvoirs publics), du secteur privé, de la société civile, des milieux techniques ou des utilisateurs;

– une participation de ces parties selon des modalités variables en fonction du rôle qui est le leur par rapport aux questions traitées;

– dans le cadre multilatéral, un accès équilibré, sinon égalitaire, des parties prenantes de tous les pays et, dans la mesure du possible, la recherche de solutions consensuelles.

65. Plusieurs problèmes demeurent néanmoins. Un premier problème est que, dans plusieurs domaines de la gouvernance de l'internet, il n'y pas d'accord sur quels doivent être les rôles et les responsabilités respectifs des différentes parties prenantes. Une autre question ouverte est celle de savoir comment assurer une représentation qualitativement adéquate et quantitativement équitable des diverses catégories de parties prenantes, étant donné le nombre des partenaires potentiels et l'impossibilité en pratique d'associer tout le monde (par exemple tous les utilisateurs) et comment éviter les blocages, tout en recherchant le consensus le plus large, étant donné les divergences d'intérêts qui peuvent subsister entre ces catégories de parties prenantes, voire même en leur sein. Je n'ai pas de recette miracle à cet égard.

66. La Déclaration NETmundial souligne certaines questions auxquelles il convient d'avoir égard pour l'évolution future de la gouvernance de l'internet. Deux d'entre elles me semblent particulièrement pertinentes:

– les représentants des parties prenantes désignés pour participer à un processus de la gouvernance multipartite de l'internet devraient être choisis à l'issue d'une procédure ouverte, démocratique et transparente; les différents groupes d'acteurs devraient administrer eux-mêmes leurs processus en s'appuyant sur des mécanismes inclusifs, connus du grand public, bien définis et obligeant à rendre des comptes;

– des mécanismes multipartites devraient être élaborés au niveau national, dans la mesure où nombre des problématiques liées à la gouvernance de l'internet doivent être traitées à ce niveau; ces mécanismes devraient servir de lien entre les discussions menées à l'échelle locale et les instances intervenant à l'échelle régionale et mondiale; il est par ailleurs essentiel d'assurer une bonne coordination et une communication fluide entre ces différents niveaux.

67. Quant au premier point, nous pourrions encourager une dynamique de recomposition des intérêts au sein des divers groupes de parties prenantes, par exemple par le biais de structures associatives/fédératives devant respecter les critères d'une démocratie interne. Quant au deuxième point, il s'agit de favoriser une dynamique qui soit à la fois ascendante (du niveau local au niveau multilatéral) et descendante (du niveau multilatéral au niveau local).

68. À cet égard, je souhaiterais saluer le développement des initiatives nationales et régionales (NRI) du Forum pour la gouvernance de l'internet comme faisant partie intégrante du processus du Forum pour la gouvernance de l'internet (FGI) des Nations Unies[41]. Le FGI et les NRI ont le potentiel de défendre des approches multipartites, inclusives et collaboratives pour la conception des politiques relatives à l'internet et leur mise en œuvre effective. Ils ne prennent pas de décision; ce sont des plates-formes qui prônent un dialogue multipartite ouvert et inclusif. Ce dialogue contribue à identifier les opportunités et les défis qu'apportent les nouvelles technologies numériques et les applications de l'internet; il contribue aussi, de façon fondamentale, à apporter une compréhension commune des responsabilités et rôles respectifs des parties prenantes. Le FGI et les NRI peuvent jouer le rôle de catalyseur pour la conception de solutions pratiques et le développement de partenariats; en décidant des priorités du débat sur les questions de politique publique, ils peuvent influencer la prise de décision dans d'autres enceintes et institutions. Si l'on regarde de près l'expérience européenne, le dialogue européen sur la gouvernance de l'internet (EuroDIG)[42] est considéré comme l'un des modèles les plus novateurs d'un processus démocratique, ascendant et multipartite parmi les NRI. Le Conseil de l'Europe, la Commission européenne et d'autres institutions soutiennent le dialogue paneuropéen par leur participation au processus de planification de programme ascendante, sans «prendre le contrôle» ni compromettre le caractère multipartite d'EuroDIG. Cela étant, le potentiel que recèlent EuroDIG, le FGI et d'autres NRI n'est pas encore pleinement exploité.

69. La faiblesse du financement de ces enceintes est une question essentielle. Comme le FGI et de nombreuses NRI, EuroDIG est un mécanisme fragile, tributaire de financements volontaires, qui est piloté par des ressources essentiellement bénévoles. Une présence plus forte et un soutien plus appuyé du Conseil de l'Europe permettraient de stabiliser le processus et de garantir un niveau minimum de représentation géographique dans le mécanisme EuroDIG. Autre défi: l'attitude quelque peu contradictoire de certains États et de nombreux représentants du monde des affaires, qui insistent pour que le FGI et les NRI restent des plates-formes de dialogue qui ne soient le lieu ni de négociations ni de décisions, mais qui, dans le même temps, refusent de s'y investir davantage ou de participer à leur financement précisément parce que ces enceintes ne prennent pas de décision et ne produisent donc pas de «résultats concrets». Par conséquent, le lien entre les débats qui se déroulent dans ces enceintes et ces instances décisionnaires n'est toujours pas assez fort.

70. À l'échelon mondial, les pays organisateurs des FGI 2017 (Suisse), 2018 (France) et 2019 (Allemagne) ont conjugué leurs efforts pour produire des résultats plus concrets en prenant exemple sur EuroDIG, qui, depuis 2008, publie un ensemble de «Messages» faciles à lire, politiques mais non négociés, qui sont le reflet des conclusions majeures des débats. Par ailleurs, la Suisse et la France ont accru la visibilité politique du

41. Ce développement a également donné lieu à la création de l'Association de soutien au Forum pour la gouvernance de l'internet (IGFSA) en 2014. Le but de cette association est de promouvoir et soutenir le FGI mondial ainsi que les initiatives nationales et régionales du FGI.

42. EuroDIG est le forum régional le plus vaste et le plus ancien pour la gouvernance de l'internet. Il a été lancé avec le soutien du Conseil de l'Europe en octobre 2008 à Strasbourg. Il compte également sur le partenariat institutionnel de la Commission européenne et d'autres organisations, comme par exemple l'Union européenne de radio-télévision (UER), l'ICANN et l'Internet Society (ISOC).

FGI avec la présence de leur président au Forum. Une autre façon de renforcer l'impact politique du FGI, d'EuroDIG et des autres NRI serait d'associer davantage de parlementaires au dialogue. Si le nombre de membres du Parlement européen qui participent au FGI a augmenté ces dernières années, seul un petit nombre de députés nationaux y prennent part. Je nourris l'espoir que notre Assemblée encourage la participation de parlementaires aux FGI nationaux et régionaux afin de contribuer à ce que les discussions menées dans ces enceintes soient en lien avec les décisions à prendre au niveau national. Avec une dimension parlementaire plus forte, EuroDIG pourrait favoriser le travail entre les sessions et ainsi améliorer les résultats produits lors de l'événement annuel et poursuivre le débat tout au long de l'année. Il contribuerait en outre à renforcer les initiatives nationales qui existent dans presque tous les pays européens.

71. Le Conseil de l'Europe et d'autres parties prenantes réfléchissent aux moyens d'accroître l'efficacité du processus EuroDIG; par conséquent, il est peut-être prématuré d'avancer des propositions concrètes dans ce domaine. Cela dit, le FGI, l'EuroDIG et les autres NRI sont des catalyseurs importants pour la mise en œuvre des recommandations du Comité des Ministres en matière de gouvernance de l'internet.

72. Je souhaiterais ajouter ici que l'inclusion au niveau national mais aussi aux niveaux européen et mondial doit être comprise non seulement en termes de groupes de parties prenantes, mais aussi en termes de diversité démographique – à savoir une représentation équilibrée selon les sexes, l'âge ainsi que l'origine ethnique, le cas échéant. À cet égard, il semble qu'il y ait encore un long chemin à parcourir. Par conséquent, je suggérerais, lorsqu'on encourage la mise en place de plateformes multipartites pour discuter de la gouvernance de l'internet au niveau de l'État, d'accorder davantage d'attention à leur dimension inclusive.

73. Quant au caractère décentralisé, l'idée qui résulte de la Déclaration sur des principes de la gouvernance de l'internet est de préserver la situation actuelle, où les organisations chargées des aspects techniques et des aspects de gestion de l'internet[43], ainsi que le secteur privé, ont un rôle de premier plan dans le domaine technique et opérationnel. Il s'agit donc de ne pas concentrer les pouvoirs uniquement dans les mains des États (et des organisations intergouvernementales).

74. Cependant, je crois que le principe de décentralisation implique autre chose aussi et qu'il faut le comprendre comme étant intimement lié à l'idée de «subsidiarité» (adaptée au contexte): la gouvernance de l'internet (comme toute gouvernance des phénomènes sociaux) requiert d'identifier les centres de décision le plus appropriés en termes d'efficacité, en raison de la connaissance des problèmes à traiter et de la capacité d'adapter les solutions aux spécificités des communautés qui doivent assurer leur mise en œuvre.

75. Ainsi entendue, l'idée d'une gouvernance décentralisée d'internet n'implique pas seulement une distribution verticale des compétences (en évoquant l'existence de centres de décisions à divers niveaux) mais aussi une répartition horizontale entre acteurs de nature différente. Dans ce sens, gouvernance décentralisée et multipartite vont de pair.

3.2. Gouvernance transparente et responsable

76. La Déclaration sur des principes de la gouvernance de l'internet, lorsqu'elle encourage la gestion décentralisée d'internet, affirme aussi que «[l]es organisations chargées des aspects techniques et des aspects de gestion de l'internet et le secteur privé devraient conserver leur rôle de premier plan dans le domaine technique et opérationnel, tout en s'acquittant de leur obligation de rendre des comptes à la communauté mondiale, en toute transparence, des actions ayant une incidence sur les politiques publiques». Nous pourrions dire, plus généralement, que tous ceux qui participent à la gouvernance de l'internet doivent assurer la transparence de leur action et doivent en rendre compte.

77. Selon la Déclaration NETmundial, une gouvernance transparente d'internet requiert que les décisions prises doivent être faciles à comprendre, les processus doivent être documentés de manière claire et respecter des procédures qui ont été développées et fixées par le biais de processus multipartites.

78. La transparence demande, tout d'abord, de savoir exactement qui décide sur quoi; cet aspect n'apparaît pas directement dans la définition contenue dans la Déclaration NETmundial, peut-être au motif que le problème typique du concept même de gouvernance en général réside dans la difficulté de localiser exactement un «centre de décision», à cause de l'éclatement du pouvoir décisionnel. Il n'est pas ici le lieu où nous pouvons discuter à fond de cette problématique. Pour simplifier, ma position est que même dans un processus décisionnel complexe et multipartite, il faut pouvoir identifier quelle responsabilité chacune des

43. Par exemple: l'Internet Corporation for Assigned Names and Numbers (ICANN), les Regional Internet Registries (RIRs) ou le Internet Engineering Task Force (IETF).

parties prenantes assume par rapport à la décision finale (et à sa mise en œuvre). Il n'est pas possible d'abandonner ce principe sans abandonner en même temps toute idée de légitimité des décideurs et de contrôle démocratique, et donc ouvrir la voie aux pouvoirs occultes et à la loi du plus fort.

79. Dans une certaine mesure, la question peut être couverte par l'exigence que le processus décisionnel (et donc l'intervention de chaque partie) suive une procédure clairement établie. La Déclaration NETmundial ajoute que les procédures en question doivent être fixées par le biais de processus multipartites. Il peut être impossible en pratique de suivre cette logique jusqu'au bout, car il faut alors légitimer ces processus multipartites et leur donner des procédures à leur tour à convenir; et ainsi de suite. Dès lors, je pense qu'il faut reconnaître un rôle premier à la communauté des États (et, dans le contexte national, aux législateurs). Cette approche est sans doute justifiée lorsqu'il s'agit de processus décisionnels qui ont un impact (actuel ou potentiel) sur les droits de l'homme.

80. La gouvernance de l'internet nécessite des procédures plus claires qui doivent être définies par la communauté des États, en consultation avec les autres parties prenantes, dans le respect d'une approche multipartite. Au niveau européen, le Conseil de l'Europe et l'Union européenne sont les instances qui devraient, ensemble, relever ce défi.

81. Enfin, la transparence implique que le sens des décisions prises soit compréhensible pour leurs destinataires et que ces décisions soient publiques, donc documentées, classifiées et publiées de manière à être aisément accessibles à tous. À cet égard, la dispersion des centres de décision rend nécessaire une forme de «centralisation»: il faudrait réfléchir à un système commun d'information sur la gouvernance de l'internet.

82. La transparence est le meilleur antidote dont nous disposons pour contrer l'arbitraire et une prédominance sournoise d'intérêts particuliers (y compris étatiques) sur l'intérêt public. Elle est également la condition sine qua non d'une gouvernance responsable.

83. Concernant la «responsabilité», la Déclaration NETmundial préconise la mise en place de mécanismes de contrôle indépendant ainsi que de révision et de recours; et elle affirme que, «à cet égard, les gouvernements sont responsables au premier chef, d'un point de vue juridique et politique, de la protection des droits de l'homme».

84. Nous connaissons bien les forces et les faiblesses des mécanismes indépendants de contrôle, de révision et de recours pour assurer le respect des droits de l'homme au plan international et au plan européen. L'analyse de leur efficacité lorsqu'il s'agit de la violation des droits examinés dans la section 2 (et d'autres droits pouvant être mis en cause sur le Réseau et par l'entremise d'internet) sort du champ du présent rapport; de même, il n'est pas possible d'examiner ici la question de l'efficacité de la protection offerte au plan national, étant donné la dimension transfrontalière d'internet (avec toute sa cohorte de problématiques liées à la juridiction des tribunaux nationaux, au droit applicable et à l'exécution des décisions).

85. Je souhaite néanmoins insister sur la difficulté d'assurer une réelle transparence et un contrôle efficace de l'action des grands opérateurs privés de l'internet et rappeler aussi que parfois ce sont des gouvernements qui sont à l'origine des violations des droits de l'homme, comme par exemple dans le cas des opérations de surveillance massive ou de la cyberguerre.

86. À ce dernier égard, je me demande s'il ne serait pas possible de renforcer les formes de coopération existantes et, peut-être, de créer un mécanisme spécifique de surveillance, gestion des crises et analyse post-crise, en mutualisant les ressources existantes dans les divers pays. Dans le cadre de l'Union européenne, la Commission européenne a proposé de renforcer l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[44], qui pourrait devenir une véritable Agence européenne pour la cybersécurité. Dans le cadre du Conseil de l'Europe, un modèle pourrait être celui de l'Accord EUR-OPA Risques majeurs[45]. Je suis conscient que de telles coopérations demandent un niveau de confiance

---

44. L'ENISA est un centre d'expertise en matière de cybersécurité en Europe, qui aide l'Union européenne et ses États membres à être mieux équipés et préparés pour prévenir et détecter les problèmes de sécurité de l'information et y répondre.

45. L'Accord EUR-OPA Risques majeurs est une plate-forme de coopération entre les pays d'Europe et du Sud de la Méditerranée dans le domaine des catastrophes naturelles et technologiques majeures. Son domaine de compétence est lié à la gestion des risques de catastrophe, en particulier la connaissance, la prévention, la gestion des crises et l'analyse post-crise. Ses objectifs principaux sont de resserrer et de dynamiser la coopération entre les États membres d'un point de vue pluridisciplinaire, afin d'assurer une meilleure prévention et protection face aux risques et une meilleure préparation en cas de catastrophes naturelles et technologiques majeures.

réciproque élevé et que, parfois, c'est justement la confiance qui manque. Néanmoins, je suis aussi conscient que bâtir progressivement des formes de coopération sur des questions sensibles est vraisemblablement le moyen le plus efficace de faire grandir cette confiance réciproque dont nous avons tant besoin. Cela nous amène au point suivant.

3.3. Gouvernance collaborative et participative

87. La Déclaration NETmundial demande une gouvernance de l'internet collaborative, fondée sur des principes de coopération représentatifs des contributions et des intérêts des parties prenantes. La Déclaration sur des principes de la gouvernance de l'internet souligne qu'«[i]l est essentiel de promouvoir la coopération multi-acteurs au niveau national et international pour préserver l'intégrité et le fonctionnement continu de l'infrastructure de l'internet ainsi que la confiance que lui accordent les usagers».

88. La coopération demande une double attitude positive des parties prenantes: d'une part, la reconnaissance du rôle des autres parties et de la valeur ajoutée que la contribution de chacun comporte; d'autre part, l'engagement à mettre au service de l'intérêt commun ses propres compétences, capacités et moyens. Une gouvernance multipartite de l'internet n'a de sens que si cet esprit collaboratif anime les parties. Le danger à éviter et que la volonté de participation soit affirmée dans le seul but de sauvegarder ses intérêts particuliers, sans trop se soucier de ceux des autres.

89. Je ne suis pas naïf au point de croire que les parties prenantes renoncent à faire valoir leurs intérêts particuliers. Dans une certaine mesure, il est tout à fait normal qu'elles le fassent. Dans un contexte multipartite, il est naturel qu'il y ait une confrontation entre les intérêts des diverses instances et c'est pour cela qu'il faut se préoccuper aussi de leur représentativité. La coopération n'est pas l'abandon des intérêts propres, mais elle implique l'acceptation de la primauté des finalités communes, qu'il n'est pas toujours possible de réconcilier entièrement avec les gains recherchés individuellement.

90. Concernant la participation, la Déclaration sur des principes de la gouvernance de l'internet parle d' «autonomisation des usagers de l'internet» et affirme qu'«[i]l conviendrait de donner aux usagers les moyens d'exercer leurs droits et libertés fondamentaux, de prendre des décisions en connaissance de cause et de participer aux dispositions pour la gouvernance de l'internet, en particulier aux mécanismes de gouvernance et à l'élaboration des politiques publiques relatives à l'internet, en toute confiance et en toute liberté». La Déclaration NETmundial préconise une participation significative des diverses parties prenantes. À cette fin, «les institutions et processus relatifs à la gouvernance de l'internet devraient soutenir le renforcement des capacités des nouveaux acteurs, notamment ceux issus des pays en développement et des groupes sous-représentés».

91. Le caractère participatif est complémentaire tant au caractère collaboratif qu'au caractère multipartite: il implique non seulement l'ouverture aux partenaires concernés – et notamment aux usagers – mais également une attitude proactive et l'effort de leur donner les moyens de participer afin de les associer utilement.

92. Le thème de l'autonomisation des usagers pour qu'ils puissent participer de manière effective à la gouvernance de l'internet rentre dans le champ de deux rapports que notre commission prépare actuellement sur le rôle de l'éducation à l'ère numérique et sur l'éducation aux médias dans le nouvel environnement médiatique. Ici, je me limiterai donc à souligner qu'un des défauts des processus actuels de gouvernance de l'internet est que, *de facto,* il n'implique que des «initiés». Le défi est donc de dépasser le cercle des gens du métier et de faire en sorte que des experts d'autres domaines puissent contribuer au développement de l'internet. Cela est d'autant plus nécessaire que l'internet (comme nous l'avons souligné) a un impact sur tous les aspects de nos sociétés (politiques, juridiques, économiques, sociaux, culturels, éthiques).

4. Conclusions

93. L'internet a transformé en profondeur notre société et continue de le faire. Il a un potentiel énorme en tant qu'outil clé pour permettre aux individus d'exercer leur droit à la liberté d'opinion et d'expression ainsi que d'autres droits fondamentaux, et pour promouvoir le progrès. Cependant, il peut aussi être utilisé pour détruire les valeurs auxquelles nous sommes attachés et nous avons besoin de mieux maîtriser son développement pour éviter cela.

94. De fait, modeler l'internet revient à modeler une société mondiale en indiquant la voie de son évolution ainsi que, dans une large mesure, la voie du progrès de nos sociétés nationales. Dès lors, la gouvernance de l'internet doit être une priorité pour les décideurs politiques. Notre objectif doit être de faire en sorte que les politiques publiques relatives à internet soient centrées sur les personnes et qu'elles respectent les valeurs fondamentales de la démocratie, des droits de l'homme et de l'État de droit.

95. La réflexion menée autour des droits de l'homme doit éclairer la définition des objectifs stratégiques de la gouvernance de l'internet et le rôle et les responsabilités des différents acteurs concernés. Les arrangements institutionnels et les processus décisionnels, ainsi que le cadre réglementaire d'internet et les mécanismes établis pour contrôler la conformité aux normes et règlements applicables, doivent être conçus pour faire en sorte que les droits de l'homme soient pleinement reconnus et effectivement garantis.

96. Mon analyse pointe vers plusieurs défis auxquels la gouvernance de l'internet se heurte concernant les droits de l'homme. Nous devons parvenir à délimiter de manière concertée le périmètre des droits de l'homme dont il est question, droits qui, malgré leur «universalité» proclamée, ne sont ni perçus ni mis en œuvre de manière homogène. Nous devons renforcer la protection de ces droits face aux risques émanant des États et des acteurs privés. Nous devons aussi réduire les écarts dans la jouissance de ces droits et, pour commencer, élaborer des politiques et des plans d'action concrets pour combler la «fracture numérique». Enfin, nous devons résoudre les tensions qui peuvent exister entre les différents droits.

97. J'ai également recensé quelques défis qui concernent les processus de la gouvernance de l'internet, tels que: écarter le risque qu'internet et la communauté mondiale de l'internet ne se fragmentent; améliorer l'efficacité de la prise de décision multipartite et multiniveaux; améliorer la coordination des processus de gouvernance descendant et ascendant, en équilibrant et en réconciliant les intérêts parfois divergents des différentes parties prenantes.

98. En ce qui concerne la protection effective des droits fondamentaux, les pouvoirs publics ont un rôle essentiel et des responsabilités non transférables. Dès lors, même si je prône une gouvernance de l'internet multipartite, un modèle de gouvernance multipartite qui diluerait les responsabilités des États en matière de promotion et de sauvegarde des droits fondamentaux n'est pas, selon moi, souhaitable.

99. Les gouvernements et les législateurs nationaux restent les décideurs dans le domaine des droits (et devoirs) des citoyens et répondent de leur effectivité. Dans le domaine de la gouvernance de l'internet, tout en étant ouverts au dialogue et dans le respect du rôle des autres parties prenantes, il incombe aux pouvoirs publics de prendre les initiatives appropriées afin de définir les normes, les mécanismes de contrôle et les mesures en cas de violation. Réaffirmer ce rôle et cette responsabilité n'est pas suffisant; il faut travailler ensemble pour le remplir correctement. Pour cette raison, il me semble indispensable d'intensifier la coopération internationale.

100. À cet égard, la gouvernance de l'internet est un domaine où le Conseil de l'Europe peut apporter une «valeur ajoutée» non négligeable; j'espère ainsi que les considérations d'ordre financier à courte vue pourront être dépassées par une approche plus judicieuse, peut-être sous la forme d'un programme spécifique fondé sur des contributions volontaires ciblées, ou par le lancement d'un nouvel accord partiel élargi sur la «gouvernance de l'internet».

101. Dernier point et non des moindres, nous, parlementaires, devrions être davantage conscients de l'énorme impact potentiel et réel que les décisions prises dans le domaine de l'internet et du cyberespace peuvent avoir sur nos vies en tant qu'individus et sociétés, notamment sur l'efficacité et la résilience de notre système démocratique. Nous devrions être plus proactifs à la fois dans la sphère nationale, en tant que législateurs, pour la définition de stratégies globales de l'internet, et pour pousser nos gouvernements à agir collectivement à travers les organisations intergouvernementales dans les processus multilatéraux de prise de décision concernant la gouvernance de l'internet.

102. À cette fin, nous disposons des nombreuses recommandations pertinentes adoptées par le Comité des Ministres, dont nous devrions faire un meilleur usage. Nous disposons aussi dorénavant des «Indicateurs de l'universalité de l'internet» de l'UNESCO (publiés le 17 octobre 2018)[46] grâce auxquels nous pourrions évaluer les niveaux de réalisation dans nos pays. Pour ce faire, il conviendrait d'appliquer les quatre principes fondamentaux DOAM compris dans le concept d'«universalité de l'internet», ce qui signifie que l'internet devrait être fondé sur les droits humains (D), Ouvert (O), Accessible à tous (A) et alimenté par la participation de Multiples acteurs (M).

46. Voir: https://fr.unesco.org/internetuniversality/indicators.