



Conseil de
l'Union européenne

Bruxelles, le 9 novembre 2015
(OR. en)

13744/15

JAI 821
FREMP 243

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents/Conseil
Objet:	Assurer le respect de l'État de droit - Dialogue et échange de vues

Dans la perspective de la réunion que le Coreper tiendra le 11 novembre 2015 et de la session que le Conseil des affaires générales tiendra le 17 novembre 2015, les délégations trouveront, à l'annexe I, un document de réflexion de la présidence sur le thème "Assurer le respect de l'État de droit" et, à l'annexe II, un document de réflexion de la présidence sur le thème "L'État de droit à l'ère de la numérisation".

Conseil des affaires générales

17 novembre 2015

Document de réflexion

Assurer le respect de l'État de droit

ASSURER LE RESPECT DE L'ÉTAT DE DROIT

L'Union européenne est fondée sur l'État de droit: toute action qu'elle entreprend est fondée sur les traités, approuvés volontairement et démocratiquement par tous les États membres de l'UE. En décembre 2014, le Conseil et les États membres, réunis au sein du Conseil, ont adopté des conclusions sur la garantie du respect de l'État de droit.

Ils se sont engagés à établir un dialogue entre tous les États membres au sein du Conseil en vue de défendre et de sauvegarder l'État de droit dans le cadre des traités et ont souligné que ce dialogue serait fondé sur les principes d'objectivité, de non-discrimination et d'égalité de traitement entre tous les États membres.

Par ailleurs, ils sont convenus que ce dialogue s'appuierait sur une approche non partisane et fondée sur des éléments probants et ont souligné que cette approche serait sans préjudice du principe d'attribution des compétences, ainsi que du respect de l'identité nationale des États membres, qui est inhérente à leurs structures fondamentales politiques et constitutionnelles, y compris en ce qui concerne l'autonomie locale et régionale, et des fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale, et qu'elle devrait être mise en œuvre à la lumière du principe de coopération loyale.

Ils sont également convenus que ce dialogue serait développé d'une manière complémentaire avec d'autres institutions de l'UE et organisations internationales, sans doubles emplois et compte tenu des instruments et compétences existant dans ce domaine.

Tout en veillant au plein respect des principes susmentionnés, la présidence luxembourgeoise entend organiser ce premier dialogue politique dans le cadre d'une approche inclusive.

- Dans la partie introductive de ce premier dialogue, la Commission présentera les résultats de son **colloque annuel sur les droits fondamentaux, consacré au thème "La tolérance et le respect: prévenir et combattre l'antisémitisme et l'islamophobie en Europe", qui a eu lieu les 1^{er} et 2 octobre 2015.**

- À l'issue de cette présentation, tous les États membres sont invités à donner **un exemple d'une bonne pratique** et **un exemple d'un défi** auquel ils ont été confrontés au niveau national dans le cadre du respect de l'État de droit, et à préciser **l'approche suivie pour répondre à ce défi**.
 - Enfin, les délégations auront la possibilité de réagir au document officieux de la présidence intitulé "L'État de droit à l'ère de la numérisation" en indiquant quels sont, selon eux, les domaines dans lesquels l'UE doit agir pour renforcer davantage l'État de droit.
-

Conseil des affaires générales

17 novembre 2015

Document de réflexion

L'État de droit

à l'ère de la numérisation

L'ÉTAT DE DROIT À L'ÈRE DE LA NUMÉRISATION

Un nombre de plus en plus important de citoyens de l'Union européenne font appel aux technologies de l'information et de la communication (TIC) et à Internet, qui constituent des outils essentiels pour leurs activités quotidiennes. Ils s'attendent donc à ce que les infrastructures et les services d'Internet et des TIC soient ouverts, accessibles, abordables, sûrs et fiables. En outre, ils s'attendent à ce que les valeurs fondamentales de l'Union européenne et l'État de droit soient pleinement préservées et protégées.

Pour la présidence luxembourgeoise, **le dialogue que tous les États membres doivent mener sur l'État de droit et le développement du marché unique numérique** figurent parmi les principales priorités du deuxième semestre de 2015¹. Le document de réflexion intitulé "L'État de droit à l'ère de la numérisation" associe deux thèmes, le but étant de tenter de recenser les domaines de l'environnement numérique dans lesquels l'État de droit pourrait être renforcé de manière utile et durable.

L'ÉTAT DE DROIT DANS L'UNION

Le terme "État de droit" désigne le principe de gouvernance en vertu duquel l'ensemble des individus, des institutions et des entités publiques et privées, y compris l'État lui-même, ont à répondre de l'observation de lois promulguées publiquement, appliquées de façon identique pour tous et administrées de manière indépendante, et compatibles avec les règles et normes internationales en matière de droits de l'homme. En outre, il implique le respect d'un certain nombre de principes: primauté du droit, égalité devant la loi, responsabilité au regard de la loi, équité dans l'application de la loi, séparation des pouvoirs, participation à la prise de décisions, sécurité juridique, refus de l'arbitraire et transparence des procédures et des processus législatifs².

¹ Présidence luxembourgeoise, Une Union pour les citoyens - Les priorités de la présidence luxembourgeoise, p. 16 et 19.

² Rapport du Secrétaire général, "Rétablissement de l'état de droit et administration de la justice pendant la période de transition dans les sociétés en proie à un conflit ou sortant d'un conflit", 23 août 2004, p.6. Consultable à l'adresse suivante:
http://www.un.org/fr/documents/view_doc.asp?symbol=S/2004/616.

Dans le préambule du traité sur l'Union européenne (TUE), les États signataires ont souligné la nécessité de s'inspirer des héritages culturels, religieux et humanistes de l'Europe, à partir desquels se sont développées les valeurs universelles que constituent les droits inviolables et inaliénables de la personne humaine, ainsi que la liberté, la démocratie, l'égalité et l'**État de droit**.

L'article 2 du TUE précise les valeurs sur lesquelles l'UE est fondée: le respect de la dignité humaine, la liberté, la démocratie, l'égalité, l'**État de droit**, ainsi que le respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Le traité indique en outre que "ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes."³

L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007. En conséquence, elle a la même valeur juridique que les traités.⁴ La charte constitue un recueil de droits civils, politiques, économiques et sociaux qui sont juridiquement contraignants non seulement pour l'Union et ses institutions, mais aussi pour les États membres, dans le cadre de la mise en œuvre du droit de l'UE. Le préambule de la charte indique que l'Union se fonde sur les valeurs indivisibles et universelles de dignité humaine, de liberté, d'égalité et de solidarité. Surtout, elle place la personne au cœur de son action en instituant la citoyenneté de l'Union et en créant un espace de liberté, de sécurité et de justice.⁵

³ Article 2 du TUE.

⁴ Article 6, paragraphe 1, du TUE.

⁵ Charte des droits fondamentaux de l'Union européenne, préambule.

LA STRATÉGIE DE L'UNION POUR UN MARCHÉ UNIQUE NUMÉRIQUE

À plusieurs occasions, le Conseil européen a insisté sur le caractère stratégique du **marché unique numérique** et sur la nécessité de mettre pleinement à profit d'ici 2015 le potentiel de l'économie numérique et des technologies numériques. Le nouveau président de la Commission européenne a inscrit l'achèvement du **marché unique numérique** parmi les dix priorités politiques de celle-ci⁶. L'objectif général consiste à œuvrer à un marché sur lequel les particuliers et les entreprises puissent sans problème, quels que soient leur nationalité et leur lieu de résidence, accéder et se livrer à des activités transfrontières en ligne dans un cadre garantissant une concurrence loyale et un niveau élevé de protection des consommateurs et des données à caractère personnel. La stratégie pour un marché unique numérique⁷ adoptée le 6 mai 2015 comprend seize initiatives à mettre en œuvre avant la fin de 2016. Le marché unique numérique s'appuiera sur trois piliers: premièrement, améliorer l'accès aux biens et services numériques pour les consommateurs et les entreprises; deuxièmement, créer des conditions propices au développement des réseaux et services numériques; et enfin et surtout, maximiser le potentiel de croissance. Afin d'atteindre ces trois objectifs dans le cadre du marché unique numérique, il sera important de garantir le respect de l'État de droit dans l'environnement numérique.

⁶ Jean-Claude Juncker, Un nouvel élan pour l'Europe: mon programme pour l'emploi, la croissance, l'équité et le changement démocratique, 15 juillet 2014. Consultable à l'adresse suivante: http://ec.europa.eu/priorities/docs/pg_fr.pdf

⁷ Commission européenne, Stratégie pour un marché unique numérique en Europe, 6 mai 2015. Consultable à l'adresse suivante: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_fr.pdf

L'ÉTAT DE DROIT À L'ÈRE NUMÉRIQUE

Il est essentiel de garantir l'État de droit pour édifier dans l'Union européenne et au-delà une société numérique inclusive et ouverte. Les principes de base de l'État de droit doivent s'appliquer de la même manière aussi bien en ligne que hors ligne. Afin de définir un cadre pour le présent document de réflexion, en faisant fond sur les travaux entrepris par le Conseil de l'Europe⁸, la présidence propose d'examiner plus en détail les thèmes suivants:

- la liberté d'expression
- la gouvernance de l'internet
- la protection des données
- la cyber-sécurité

Ces thèmes, qui sont au cœur du renforcement de l'État de droit à l'ère numérique, sont extrêmement complexes et étroitement interdépendants.

⁸ Conseil de l'Europe, commissaire aux droits de l'homme, "La prééminence du droit sur l'internet et dans le monde numérique en général", décembre 2014. Consultable à l'adresse suivante:
<https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2>

LIBERTÉ D'EXPRESSION

Selon la déclaration universelle des droits de l'homme, la liberté d'expression désigne le droit de tout individu de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit⁹.

La convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales¹⁰ dispose également que toute personne a droit à la liberté d'expression. Elle précise que ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières. La convention dispose en outre, en son article 10, que l'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire.

Dans le même ordre d'idées, la charte des droits fondamentaux de l'Union européenne mentionne la liberté d'expression et d'information et dispose que toute personne a droit à la liberté d'expression. En outre, elle précise que "ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières."¹¹

Toutefois, il peut arriver dans la pratique que, dans certaines circonstances, la liberté d'expression soit restreinte, notamment sous l'effet de la censure, d'une législation restrictive en matière de presse ou encore du harcèlement subi par les journalistes, les lanceurs d'alerte, les blogueurs et autres personnes qui expriment leurs opinions, ainsi que la répression dont font l'objet des minorités religieuses et d'autres formes de suppression de la liberté de culte. La liberté d'expression et son articulation avec la législation nationale régissant les activités en ligne, par exemple en ce qui concerne la responsabilité des intermédiaires internet, représentent un défi permanent.

⁹ Nations unies, déclaration universelle des droits de l'homme, 10 décembre 1948. Consultable à l'adresse suivante: <http://www.un.org/Overview/rights.html>

¹⁰ Conseil de l'Europe, convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Consultable à l'adresse suivante: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention_ENG.pdf

¹¹ Charte des droits fondamentaux de l'Union européenne, article 11, paragraphe 1.

En ligne, la liberté d'expression est souvent remise en cause, parce qu'il peut se révéler nécessaire de supprimer des contenus, que ce soit pour des raisons liées à la protection de la vie privée ou des droits de propriété intellectuelle, entre autres. Cela place les intermédiaires de l'internet dans une situation conflictuelle, notamment pour ce qui est de leur responsabilité, dans la mesure où ils doivent trouver un équilibre entre différents droits fondamentaux.

La possibilité de limiter la liberté d'expression trouve également sa source dans deux autres instruments de droit international, à savoir la convention internationale sur l'élimination de toutes les formes de discrimination raciale¹² et le pacte international relatif aux droits civils et politiques.¹³ L'article 4, point a), de la première impose aux signataires de "déclarer délits punissables par la loi toute diffusion d'idées fondées sur la supériorité ou la haine raciale", et l'article 20 du second prévoit que "tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence (soit) interdit par la loi".

Les États membres ont mis en place une législation destinée à endiguer les discours incitant à la haine raciale et religieuse qui, à l'ère numérique, sont de plus en plus fréquemment diffusés au moyen des TIC et sur l'internet. Sauf pour ce qui est des infractions relevant du champs d'application de la décision-cadre sur le racisme et la xénophobie¹⁴, des différences existent quant à ce qui constitue un discours de haine.

¹² Convention internationale sur l'élimination de toutes les formes de discrimination raciale, 21 décembre 1965. Consultable à l'adresse suivante:

<http://www.ohchr.org/Documents/ProfessionalInterest/cerd.pdf>

¹³ Pacte international relatif aux droits civils et politiques, 16 décembre 1966. Consultable à l'adresse suivante: <http://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx>

¹⁴ Décision-cadre 2008/913/JAI du Conseil sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, JO L 328 du 6.12.2008.

Pour ce qui est des principaux moyens de prévenir l'antisémitisme et l'islamophobie et de lutter contre ces phénomènes, il est proposé, à la suite du premier colloque annuel sur les droits fondamentaux, de lutter contre les discours de haine en coopérant avec les entreprises de technologies de l'information, la société civile et les médias et de veiller à ce que soient mises en œuvre les législations sanctionnant les crimes de haine et les nouvelles dispositions de l'UE relatives à la protection des droits des victimes de ces infractions et à l'amélioration de la collecte et de l'enregistrement des données relatives aux crimes de haine¹⁵. La première réunion de coordination avec les plateformes internet et les réseaux sociaux, qui sera préparée par le groupe d'experts de la Commission sur la mise en œuvre de la décision-cadre sur le racisme et la xénophobie, se tiendra à Bruxelles le 23 novembre 2015.

GOUVERNANCE DE L'INTERNET

Lors du sommet mondial sur la société de l'information organisé à l'initiative des Nations unies, il a été proposé de retenir la définition de la gouvernance de l'internet figurant dans le rapport de juin 2005 du groupe de travail sur la gouvernance de l'internet: "Il faut entendre par "gouvernance de l'Internet" l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet."¹⁶

L'approche multipartite adoptée concernant la gouvernance de l'internet tient compte des intérêts des États, du secteur privé, de la communauté technique, des milieux universitaires et de la société civile. Ce modèle favorise l'inclusivité et la responsabilisation. Les principes régissant la gouvernance de l'internet soulignent la nécessité d'appliquer le droit international public et le droit international relatif aux droits de l'homme tant en ligne que hors ligne. Ils rappellent également la nécessité de respecter l'État de droit et la démocratie sur l'internet. Ces principes reconnaissent et encouragent le caractère multipartite de la gouvernance de l'internet et, ce qui est plus important encore, ils engagent tous les acteurs publics et privés à respecter les droits de l'homme dans le cadre de toutes leurs opérations et activités, y compris la conception de nouvelles technologies, de nouveaux services et de nouvelles applications. Enfin, ils appellent les États à respecter la souveraineté nationale des autres États et à s'abstenir de toute action qui porterait préjudice à des personnes ou à des entités établies en dehors de leur juridiction territoriale.

¹⁵ Commission européenne, "Joining forces against anti-Semitic and anti-Muslim hatred in the EU: outcomes of the first annual colloquium on fundamental rights", 9 octobre 2015. Consultable à l'adresse suivante: http://ec.europa.eu/justice/events/colloquium-fundamental-rights-2015/files/fundamental_rights_colloquium_conclusions_en.pdf

¹⁶ Groupe de travail sur la gouvernance de l'Internet, Rapport du Groupe de travail sur la gouvernance de l'Internet, Château de Bossey, juin 2005. Consultable à l'adresse suivante: <http://www.wgig.org/docs/WGIGREPORT.pdf>

Il va sans dire que pour certains, ces principes sont encore essentiellement déclaratoires: en effet, les mécanismes de gouvernance de l'internet qui visent à en garantir l'application pratique sont encore insuffisants. Les États devraient veiller à ce que toute limitation de l'accès à des contenus internet affectant les utilisateurs relevant de leur compétence soit fondée sur un cadre juridique rigoureux et prévisible. Ce cadre devrait être de nature à régir l'ampleur de toute limitation de ce type et à garantir un contrôle juridictionnel afin de prévenir tout abus. Lorsqu'elle se révèle nécessaire, la suppression de contenus doit être effective et proportionnée, et elle doit en particulier être suffisamment ciblée pour n'affecter que le contenu spécifique qui doit être supprimé. En outre, les juridictions nationales doivent examiner si une mesure de blocage est nécessaire, effective et proportionnée, et notamment si elle est suffisamment ciblée pour n'affecter que le contenu spécifique qui doit être bloqué.

PROTECTION DES DONNÉES

Le traité sur le fonctionnement de l'Union européenne (TFUE) rappelle que toute personne a droit à la protection des données à caractère personnel la concernant et que le Parlement européen et le Conseil fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.¹⁷

La présidence luxembourgeoise a pour objectif de finaliser la réforme en matière de protection des données dans l'UE d'ici la fin de l'année. L'achèvement et la réussite du marché unique numérique dépendra grandement de la confiance accordée par les citoyens et les entreprises aux flux transfrontaliers de données. L'UE peut être considérée comme un modèle en termes de protection élevée des données. Cet acquis doit être renforcé par l'adoption du nouveau cadre réglementaire. Les droits des citoyens, tout comme la compétitivité de l'économie européenne, doivent être protégés.¹⁸

¹⁷ Article 16 du TFUE.

¹⁸ Présidence luxembourgeoise, Une Union pour les citoyens - Les priorités de la présidence luxembourgeoise, p. 16 et 17.

Dans son arrêt du 8 avril 2014 invalidant la directive 2006/24/CE¹⁹ relative à la conservation de données,²⁰ la Cour de justice de l'Union européenne (CJUE) a souligné l'importance des droits fondamentaux que constituent le droit à la vie privée et le droit à la protection des données à caractère personnel, tels que consacrés dans la charte. Une réponse adéquate qui tienne compte des principes dégagés par la jurisprudence est nécessaire et doit être insérée dans le cadre juridique rénové régissant la protection des données. Dans son arrêt du 6 octobre 2015, la CJUE déclare invalide la décision de la Commission constatant que les États-Unis assurent un niveau de protection adéquat aux données à caractère personnel transférées²¹. Ces décisions de la CJUE témoignent de l'importance accordée à la protection élevée des données dans l'Union européenne.

La protection des données est le premier et le plus important pilier de l'État de droit à l'ère de la numérisation. La spécification et la limitation de la finalité, ainsi que l'équité, sont des principes clés de la protection des données. Le respect des principes et des règles de protection des données doit être suivi de près et étroitement contrôlé par des autorités indépendantes. Les États ne doivent pas imposer la conservation obligatoire de données par des tiers, y compris des entités privées, sauf si le principe de proportionnalité est pleinement respecté.²² La conservation de données de communication doit être licite et des paramètres équilibrés sont nécessaires pour examiner par exemple l'étendue des données collectées, les critères d'accès, les durées de conservation et la surveillance, conformément au principe de proportionnalité tel qu'interprété par la CJUE dans les affaires susmentionnées.

¹⁹ Directive 2006/24/CE. Consultable à l'adresse suivante:
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:FR:PDF>

²⁰ Cour de justice de l'Union européenne, communiqué de presse n° 54/14, 8 avril 2014.
Consultable à l'adresse suivante:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf>

²¹ Cour de justice de l'Union européenne, communiqué de presse n° 117/15, 6 octobre 2015.
Consultable à l'adresse suivante:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fr.pdf>

²² Charte des droits fondamentaux de l'Union européenne, article 52.

CYBERSÉCURITÉ

La cybersécurité est une condition préalable essentielle dans un environnement propice au développement des réseaux et des services numériques. Les États ont reconnu relativement tardivement l'importance de l'internet en ce qui concerne leur rôles traditionnels et leurs responsabilités. Ce n'est qu'en coopérant étroitement avec l'ensemble des parties prenantes que l'environnement en ligne pourra être efficacement préservé pour les générations futures. Les récents cas de cyber-détournement²³ et les cyberattaques constantes contre les gouvernements et les entreprises privées dans le monde entier montrent que les cyberopérations sont devenues un outil de manipulation et de coercition politique pour les États comme pour les acteurs non étatiques.

La cybercriminalité consiste en des actes criminels commis en ligne en utilisant les TIC ou l'internet. Il s'agit d'un problème qui ne connaît pas de frontières et qui peut être classé dans différentes catégories: les crimes propres à l'internet (les attaques contre les systèmes d'information ou le filoutage), la fraude en ligne et la falsification (l'usurpation d'identité, les pourriels et les codes malveillants) et les contenus en ligne illicites (y compris le matériel pédopornographique, l'incitation à la haine raciale, l'incitation à commettre des actes de terrorisme et l'apologie de la violence, du terrorisme, du racisme et de la xénophobie).

²³ TV5 Monde et Sony Pictures peuvent être pris pour exemples.

L'Union européenne a élaboré une stratégie de cybersécurité de l'UE²⁴ et la directive proposée relative à la sécurité des réseaux et de l'information (SRI) renforcera la coopération entre les États membres et améliorera la préparation de l'ensemble des parties prenantes, y compris les gouvernements. Plusieurs actions législatives de l'UE contribuent à la lutte contre la cybercriminalité, parmi lesquelles des directives relatives aux attaques contre les systèmes d'information²⁵ et à la lutte contre l'exploitation sexuelle des enfants en ligne ainsi que la pédopornographie²⁶, la directive "vie privée et communications électroniques"²⁷ et la décision-cadre concernant la lutte contre la fraude et la contrefaçon²⁸.

Concernant la directive relative aux attaques contre les systèmes d'information, une référence est faite au plein respect de l'État de droit lorsqu'il s'agit de favoriser et d'améliorer la coopération entre les prestataires de services, les producteurs, les organismes chargés de l'application de la loi et les autorités judiciaires.

Le Centre européen de lutte contre la cybercriminalité (EC3), qui a commencé ses activités en janvier 2013, joue le rôle de coordinateur dans le cadre de la lutte contre la cybercriminalité dans l'Union européenne, mettant en commun l'expertise européenne en matière de cybercriminalité pour soutenir les enquêtes des États membres sur la cybercriminalité et se faisant le porte-voix des enquêteurs européens sur la cybercriminalité par l'intermédiaire des autorités policières et judiciaires.

L'un des défis les plus importants consiste à concilier les pouvoirs effectifs en matière d'application de la loi et la protection des droits fondamentaux. Les États doivent respecter pleinement les obligations internationales en matière de droits de l'homme lorsqu'il s'agit de définir la cybercriminalité dans le cadre des enquêtes ou poursuites pénales, notamment en ce qui concerne l'entraide judiciaire et l'extradition.²⁹

²⁴ Parlement européen, Conseil de l'Union européenne, Comité économique et social européen, Comité des régions, Stratégie de cybersécurité de l'Union européenne: un cyberspace ouvert, sûr et sécurisé, 2013. Consultable à l'adresse suivante: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52013JC0001&from=FR>

²⁵ Directive 2013/40/UE. Consultable à l'adresse suivante: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:FR:PDF>

²⁶ Directive 2011/92/UE. Consultable à l'adresse suivante: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32011L0093&from=FR>

²⁷ Directive 2009/136/CE. Consultable à l'adresse suivante: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:fr:PDF>

²⁸ <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32001F0413&from=FR>

²⁹ Conseil de l'Europe, Commissaire aux droits de l'homme, *op. cit.*, p. 22.

Si un État prend des mesures qui touchent des individus situés hors de son territoire, il doit satisfaire aux obligations qui lui incombent tout comme il le ferait sous sa juridiction et il doit respecter les accords internationaux.³⁰ À l'exception des contenus jugés illicites au regard du droit international, les États ne peuvent exercer leur pouvoir de juridiction sur des ressources numériques étrangères que dans certaines circonstances limitées, en particulier lorsque les ressources et/ou le diffuseur et l'État en question sont clairement et étroitement liés.

CONCLUSIONS

Le monde numérique fait partie de notre quotidien. Les technologies de l'information et de la communication et l'internet peuvent soutenir l'État de droit, mais ils peuvent également encourager son non-respect. L'Union européenne est fondée sur l'État de droit: toute action qu'elle entreprend est fondée sur les traités, approuvés volontairement et démocratiquement par tous les États membres de l'UE. Par conséquent, l'Union a un rôle important à jouer et une responsabilité particulière à assumer au niveau mondial dans la définition des règles et principes généraux du monde numérique.

Le document de réflexion montre qu'il existe une large marge pour des initiatives au niveau de l'UE afin de permettre au marché unique numérique de pleinement fonctionner et de continuer à renforcer l'État de droit à l'ère de la numérisation.

³⁰ par exemple la Convention européenne d'extradition ou la Convention européenne d'entraide judiciaire en matière pénale.