Comité directeur sur les médias et la société de l'information

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CDMSI(2015)023

9e réunion

8-11 décembre 2015
(Strasbourg, Palais de l'Europe, salle 08)

Rapport de réunion

1. Ouverture de la réunion

Le Comité directeur sur les médias et la société de l'information (CDMSI) tient sa 9e réunion du 8 au 11 décembre 2015 à Strasbourg sous la présidence de Mme Maja Raković (Serbie). La répartition hommes/femmes des 60 participants est la suivante : 20 femmes (33 %) et 40 hommes (67 %).

M. Jan Kleijssen, directeur de la Direction de la société de l'information et de l'action contre la criminalité, ouvre la réunion, dernière à être organisée dans le cadre du mandat 2014-2015 du CSMSI, et souhaite la bienvenue à tous les participants. Il informe la plénière que les deux comités d'experts, à savoir le Comité d'experts sur la circulation transfrontière d'internet et la liberté d'internet (MSI-INT) et le Comité d'experts sur la sécurité des journalistes et des autres acteurs des médias (MSI-JO), ont finalisé la dernière version de leurs projets de recommandations sur « La liberté d'internet » et sur « La sécurité des journalistes et des autres acteurs des médias » respectivement, qui peuvent désormais être examinés par le CDMSI pour approbation. Il informe aussi le CDMSI du nouveau projet de stratégie 2016-2019 sur la gouvernance de l'internet qui doit être examiné et approuvé lors de cette 9e réunion, soulignant qu'il prévoit enre autres aspects la création d'une plateforme de coopération avec les entreprises. Il encourage donc le CDMSI à envisager cette plateforme également comme un outil de coordination des activités transversales du CdE avec d'autres comités directeurs et conventionnels compétents du Conseil de l'Europe (CDPC, CDCJ, TC-Y et TP-D). Mr Kleijssen informe aussi le comité de la tenue, les 13 et 14 octobre 2015 à Strasbourg, de la conférence du Conseil de l'Europe intitulée « La liberté d'expression est-elle encore une condition nécessaire à la démocratie ? » et met l'accent également sur la nouvelle mission fixée pour 2016-2017, en particulier l'adoption des mandats du CDMSI et des deux sous-comités d'experts, le Comité d'experts sur la transparence de la propriété des médias et le pluralisme des médias (MSI-MED) et le Comité d'experts sur les intermédiaires d'internet (MSI-NET). Pour finir, il donne au comité des informations sur d'autres domaines de travail et d'activité du CdE à la suite des récents attentats terroristes de Paris notamment, et remercie les membres du Bureau de leurs contributions et Mme Maja Raković (Serbie) de sa présidence.

2. Adoption de l'ordre du jour

Le CDMSI adopte l'ordre du jour qui figure à l'annexe I avec un ajout, à savoir sous le point 14 Points divers, Les lignes directrices relatives aux droits e l'homme à l'intention

des fournisseurs de services internet ; la liste des participants est reproduite à l'annexe II.

3. Informations de la présidente et du Secrétariat

Projet de Recommandation CM/Rec(2014)… du Comité des Ministres aux Etats membres sur la protection et la promotion du droit à la liberté d'expression et du droit au respect de la vie privée en lien avec la neutralité du réseau

Le CDMSI prend note des informations communiquées par le Secrétariat sur l'état actuel de la Recommandation CM/Rec(2015)xxx sur la protection du droit à la liberté d'expression et du droit au respect de la vie privée en lien avec la neutralité du réseau présentée au GR-H le 3 décembre et qui devrait être soumise au Comité des Ministres en janvier 2016.

Conférence du Conseil de l'Europe sur « La liberté d'expression est-elle encore une condition nécessaire à la démocratie ? » – Strasbourg, 13-14 octobre 2015

Le CDMSI prend note des informations communiquées par le Secrétariat sur les résultats de la Conférence du Conseil de l'Europe intitulée « La liberté d'expression est-elle encore une condition nécessaire à la démocratie ? », tenue les 13 et 14 octobre 2015 à Strasbourg et félicite le Secrétariat de l'excellente organisation.

Nouveau mandat du CDMSI 2016-2017

Le CDMSI prend note de l'adoption, par le Comité des Ministres, de son nouveau mandat pour 2016-2017 ainsi que de ceux des deux comités d'experts subordonnés, à savoir le Comité sur le pluralisme des médias et la transparence de la propriété des médias (MSI-MED) et celui sur les intermédiaires d'internet (MSI-NET), qui lui permettront d'atteindre les résultats attendus. Le CDMSI examine les propositions de candidatures au MSI-MED et au MSI-NET des Etats membres et procède à un vote. Il note que conformément aux mandats des comités, les experts indépendants seront nommés par le Secrétaire Général. La composition des deux comités d'experts fait l'objet des annexes IX et X respectivement.

4. Mise en œuvre des normes adoptées par le Conseil de l'Europe

A sa 8e réunion (16-19 juin 2015), le CDMSI a pris note des réponses des Etats membres au questionnaire sur la sécurité des journalistes en espérant que tous les Etats membres répondront. De ce fait, il a décidé d'étendre le délai de réponse à la fin du mois de juillet. Il a aussi pris note de la suite que le Secrétariat donnerait à cet exercice, à savoir une compilation et une analyse qui lui seront présentées à sa prochaine réunion en décembre 2015.

Au 3 décembre, le Secrétariat avait reçu des contributions de 21 Etats membres, à savoir la Grèce, la Slovaquie, la République tchèque, l'Autriche, l'Italie, la Norvège, l'Irlande, la Suède, l'Islande, l'Allemagne, la Lettonie, le Danemark, la Fédération de Russie, la Pologne, la Slovénie, Saint-Marin, la Bosnie-Herzégovine, les Pays-Bas, le Monténégro, l'Arménie et la Croatie.

Le CDMSI prend note des 21 réponses des Etats membres au questionnaire sur la sécurité des journalistes et d'une analyse prépée par le Secrétariat. Il décide que les réponses manquantes devront être envoyées au Secrétariat avant le 29 février 2016. Il convient d'organiser, à sa 10e réunion en juin 2016, une audition sur le sujet qui devrait se doubler d'une présentation et d'un examen de la plateforme en ligne sur la sécurité des journalistes un an après son lancement et d'une première réflexion sur les modalités d'application du projet de recommandation sur la protection du journalisme et la sécurité

des journalistes et des autres acteurs des médias qui sera soumis au CM pour adoption éventuelle.
Les Etats membres sont encouragés à traduire les textes adoptés dans leur langue respective, ce qui constituerait une première étape pour faciliter leur mise en œuvre.

La présidente propose en outre que les Etats membres favorisent la mise en œuvre du Guide des droits de l'homme pour les utilisateurs d'internet en consacrant une journée à une manifestation particulière, par exemple une conférence.

5. Travaux normatifs dans le domaine des médias

Projet de recommandation sur la protection du journalisme et la sécurité des journalistes et des autres acteurs des médias

Le CDMSI prend note du rapport de la dernière réunion du Comité d'experts sur la protection du journalisme et la sécurité des journalistes (MSI-JO), tenue les 17 et 18 septembre et félicite le Comité de son travail.

Le Secrétariat rappelle les diverses étapes du processus de rédaction et de consultation du projet de Recommandation CM/Rec… du Comité des Ministres aux Etats membres sur la sécurité des journalistes et des autres acteurs des médias. Le comité finalise le projet et décide de le transmettre au Comité des Ministres pour adoption éventuelle (annexe III).

La Fédération de Russie ne souhaite pas soutenir ce projet de recommandation et fait une déclaration reproduite à l'annexe IV du présent rapport.

6. Travaux normatifs dans le domaine d'internet

Projet de Recommandation CM/Rec… du Comité des Ministres aux Etats membres sur la liberté d'internet

Le CDMSI prend note du rapport de la dernière réunion du Comité d'experts sur la circulation transfrontière d'internet et la liberté d'internet (MSI-INT), tenue les 7 et 8 septembre 2015 ; il félicite le MSI-INT des travaux accomplis.

Le Secrétariat rappelle les étapes successives du processus de rédaction et de consultation du projet de Recommandation CM/Rec… du Comité des Ministres aux Etats membres sur la liberté d'internet. Le comité finalise le projet et décide de le transmettre au Comité des Ministres pour adoption éventuelle (annexe V). Il examine aussi le projet d'exposé des motifs du projet de recommandation et y apporte certains changements. Le texte sera transmis au Comité des Ministres pour qu'il en prenne note.

La Fédération de Russie ne souhaite pas soutenir ce projet de recommandation et fait une déclaration reproduite à l'annexe VI du présent rapport.

Projet de rapport sur la liberté de réunion et d'association sur internet

Le CDMSI examine le projet de rapport sur la liberté de réunion et d'association sur internet qui est l'un des résultats attendus du Comité d'experts sur la circulation transfrontière d'internet (MSI-INT). Il approuve certaines modifications et décide d'en prendre note, voyant dans le rapport une bonne base de réflexion future sur le sujet.

7. Gouvernance de l'internet

7.1. Stratégie du Conseil de l'Europe sur la gouvernance de l'internet 2012-2015

Le Secrétariat donne un aperçu de la Stratégie 2012-2015 du Conseil de l'Europe sur la gouvernance de l'internet en attirant l'attention sur la liste des activités jointe en annexe et sur l'état de mise en œuvre.

Le CDMSI prend note des informations et en discute. Il se félicite des travaux accomplis et attend avec intérêt le rapport final du Secrétaire Général.

7.2. Stratégie 2016-2019 du Conseil de l'Europe sur la gouvernance de l'internet

Le Secrétariat présente le projet de stratégie 2016-2019 du Conseil de l'Europe sur la gouvernance de l'internet et décrit dans le détail le processus de consultation et d'élaboration suivi.

Le CDMSI examine le projet, le révise et le soumet au vote. Il décide de le transmettre au Comité des Ministres pour adoption éventuelle (annexe VII).

La Fédération de Russie n'approuve pas le projet de stratégie 2016-2019 du Conseil de l'Europe sur la gouvernance de l'internet sous sa forme actuelle et fait une déclaration reproduite à l'annexe VIII du présent rapport.

7.3. Dialogue européen sur la gouvernance de l'internet et Forum sur la gouvernance de l'internet (João Pessoa, Brésil, 10-13 novembre 2015)

Le CDMSI prend note des informations relatives au prochain Dialogue européen sur la gouvernance de l'internet (EuroDIG) qui aura lieu à Bruxelles (9-10 juin 2016).

Il prend note des activités prévues du Conseil de l'Europe et encourage les Etats membres à y participer.

Il prend aussi note des informations communiquées par le Secrétariat et les membres ayant participé au Forum 2015 sur la gouvernance de l'internet à Joao Pessoa, Brésil (10-13/11/2015).

7.4. Comité consultatif gouvernemental (GAC) de l'Internet Corporation for Assigned Names and Numbers (ICANN)

Le CDMSI prend note des informations communiquées par le délégué du Royaume-Uni concernant la 54^{e} réunion de l'ICANN (8-22 octobre 2015) et de l'examen des résultats du Sommet mondial sur la société de l'information (SMSI). Il examine une proposition du délégué du Royaume-Uni tendant à encourager le Conseil de l'Europe à étudier et à analyser les questions des droits de l'homme liées à la liberté d'expression que traite le Comité consultatif gouvernemental de l'ICANN.

7.5 Examen des conclusions du Sommet mondial sur la société de l'information (SMSI)

Le CDMSI prend note des informations communiquées par le Secrétariat.

8. Protection des données

En ce qui concerne la protection des données, le CDMSI prend note des informations communiquées par le Secrétariat sur la modernisation de la Convention n^{o} 108. La promotion de cette convention s'est poursuivie en 2015 et a conduit à la ratification du Protocole additionnel à la Convention par le Danemark, à la ratification de la Convention par Saint-Marin, à l'invitation faite à l'Ile Maurice d'adhérer à la Convention et à son Protocole additionnel ainsi qu'à la demande du Sénégal d'être invité à y adhérer.

Le CDMSI prend aussi note d'autres travaux du T-PD sur les mégadonnées, le secteur de la police, les données médicales, le dossier passager (PNR) et l'échange automatique de données. Le Secrétariat l'informe aussi de la révision de la Recommandation R(97) 5 sur la protection des données médicales que le T-PD doit adopter à sa 33e réunion plénière (29 juin-1er juillet 2016).

9. Activités de coopération

Le CDMSI prend note des informations communiquées par le Secrétariat sur les activités de coopération en cours et futures qui représentent une partie considérable du travail de la Division médias et gouvernance de l'internet. Actuellement, plusieurs projets d'un montant total de 5,5 millions d'euros sont en cours et doivent être menés à bien sur une période d'environ deux ans et demi. Ils concernent l'Arménie, l'Azerbaïdjan, le Bélarus, la Géorgie, l'Albanie, la Bosnie-Herzégovine, « l'ex-République yougoslave de Macédoine », le Kosovo[1], le Monténégro, la Serbie, la République de Moldova et l'Ukraine. Les projets sont pour l'essentiel financés par des programmes conjoints avec la Commission européenne et par certains pays, dont le Canada, le Liechtenstein et la Norvège. De plus, dans le cadre de la politique de voisinage, des projets ont été lancés au Maroc et en Tunisie. Toutes les activités sont organisées et menées par des bureaux de projets créés à cet effet ou des bureaux décentralisés du Conseil de l'Europe.

De plus, des conseils d'experts ont été donnés à la demande de pays, dont l'Ukraine en ce qui concerne la loi relative à la réforme de la presse écrite communautaire, la loi sur la télévision et la radiodiffusion publiques et la loi sur la transparence de la propriété des médias et l'Albanie pour ce qui est de la loi sur les médias audiovisuels.

10. Programme et méthodes de travail du CDMSI

Le CDMSI est d'avis que les principaux faits survenus dans les Etats membres, en particulier en relation avec l'internet, doivent être portés à la connaissance des membres et des participants et communiqués au Secrétariat. Il est en outre décidé de demander aux membres et aux participants d'envoyer leurs observations et leurs propositions d'amendements relatives aux projets d'instruments normatifs le plus tôt possible afin de faciliter l'établissement de la version définitive des textes lors des réunions plénières.

10.1. Comités de rédaction

Le CDMSI est informé des travaux effectués par le Comité de rédaction sur les médias de service public créé lors de la dernière réunion plénière de juin 2015 et décide, au vu de son nouveau mandat pour 2016-2017, de poursuivre les discussions au sein du MSI-MED.

10.2. Evaluation de la participation des ONG aux comités directeurs

Le CDMSI prend note des informations communiquées par le Secrétariat au sujet de l'évaluation de la participation des ONG aux comités directeurs entreprise par la Direction de l'audit interne et de l'évaluation du Conseil de l'Europe. Il souligne l'importance de la présence et de la contribution des ONG et de la société civile à ses travaux.

Un rapport est en cours de rédaction et sera présenté au Comité à sa prochaine réunion.

[1] « Toute référence au Kosovo dans le présent document, qu'il s'agisse de son territoire, de ses institutions ou de sa population, doit être entendue dans le plein respect de la Résolution 1244 du Conseil de sécurité de l'Organisation des Nations Unies, sans préjuger du statut du Kosovo ».

11. Informations sur les travaux d'autres organisations et d'autres organes du Conseil de l'Europe

Le CDMSI note que le représentant permanent de la Belgique auprès du Conseil de l'Europe, l'ambassadeur Dirk Van Eeckhout, a été nommé coordinateur thématique sur la politique d'information (TC-INF) et décide de l'inviter à un échange de vues à la prochaine réunion plénière.

11.1. Assemblée parlementaire du Conseil de l'Europe (APCE)

Le CDMSI prend note des informations communiquées par M. Rüdiger Dossow, secrétaire de la commission de la culture, de la science, de l'éducation et des médias de l'APCE.

Il prend aussi note de la communication, au Comité des Ministres, de ses observations sur les recommandations suivantes de l'APCE : Recommandation 2073 (2015) intitulée « Améliorer la protection des donneurs d'alerte », Recommandation 2074 (2015) intitulée « Accroître la transparence de la propriété des médias », Recommandation 2075 (2015) intitulée « La responsabilité et la déontologie des médias dans un environnement médiatique changeant » et Recommandation 2077 (2015) intitulée « Accroître la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur internet ».

11.2. Commissaire aux droits de l'homme

Le CDMSI prend note du document thématique du Commissaire aux droits de l'homme du Conseil de l'Europe sur la surveillance démocratique et effective des services de sécurité nationale et des informations données par Mme Alessandra Ricci, conseillère du Commissaire.

11.3. Autres comités directeurs et conventionnels

Comité sur les combattants terroristes étrangers et les questions connexes (COD-CTE) et CODEXTER

Le CDMSI prend note des informations du Secrétariat sur l'invitation que lui a faite le CODEXTER de prendre part à ses travaux sur les techniques spéciales d'enquête. Il charge Mme Maja Raković de participer au groupe de rédaction du CODEXTER sur ce sujet.

12. Représentation du CDMSI aux réunions d'autres comités et à d'autres manifestations

Le CDMSI prend note des informations communiquées par les membres de son Bureau et par le Secrétariat sur les réunions suivantes : réunion du « Projet internet et juridiction », Berlin, 8-9/10/2015, « Atelier d'experts sur la liberté et les responsabilités des médias dans le contexte des politiques de lutte contre le terrorisme », Bucarest, 7-8/10/2015, « Forum sur la gouvernance de l'internet », Bosnie-Herzégovine, « Comité d'experts ad hoc sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (CAHVE) », Strasbourg, 28-29/10/2015, « Les parlements et les médias de service public dans les pays de l'élargissement », 24-25 septembre 2015, Zagreb, « Conférence internationale sur l'impunité pour les crimes commis contre des journalistes », Costa Rica, 9-10 octobre 2015.

13. Elections au Bureau du CDMSI

Conformément à la Résolution (2011)24 du Comité des Ministres concernant les comités intergouvernementaux et les organes subordonnés, leur mandat et leurs méthodes de travail, le CDMSI élit son Bureau comme suit : Mme Elfa Ýr Gylfadóttir, présidente

(Islande), M. Emir Povlakić, vice-président (Bosnie-Herzégovine) pour un premier mandat expirant le 31 décembre 2016, Mme Joanna Chansel (France), Mme Pien van den Eijnden (Pays-Bas), M. Matthias Traimer (Autriche), Mme Maja Raković (Serbie) pour un premier mandat de deux ans expirant le 31 décembre 2017 et M. Christopher Lärkner (Suède) pour un premier mandat d'un an expirant le 31 décembre 2016. Il confirme aussi que Mme Maja Zarić (Serbie) a été nommée rapporteure pour l'égalité entre les femmes et les hommes.

14. Questions diverses

Le CDMSI discute aussi de l'intérêt d'une mise à jour des lignes directrices de 2008 relatives aux droits de l'homme à l'intention des fournisseurs de services internet, qu'il souligne, et propose d'inscrire ce point à l'ordre du jour de la première réunion du MSI-NET aux fins d'une discussion plus approfondie.

15. Adoption du rapport abrégé

Le CDMSI examine le rapport abrégé de sa 9e réunion et l'adopte avec quelques modification mineures.

Annexe I

Ordre du jour de la réunion

1. Ouverture de la réunion

2. Adoption de l'ordre du jour

3. Information par la Présidente et le Secrétariat

3.1 Projet de Recommandation CM/Rec(2014)___du Comité des Ministres aux Etats membres 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
3.2 Conférence du Conseil de l'Europe « La liberté d'expression est-elle encore une condition nécessaire à la démocratie ? » Strasbourg, 13-14 octobre 2015
3.3 New mandate of the CDMSI

4. Mise en œuvre des normes adoptées par le Conseil de l'Europe

5. Travaux normatifs dans le domaine des médias

5.1 Comité d'experts sur la protection du journalisme et la sécurité des journalistes – MSI-JO

6. Travaux normatifs dans le domaine d'internet

6.1 Comité d'experts sur la circulation transfrontière d'Internet et la liberté d'Internet (MSI-INT)

7. Gouvernance de l'internet

7.1 Stratégie du Conseil de l'Europe pour la gouvernance de l'internet 2012-2015
7.2 Stratégie du Conseil de l'Europe pour la gouvernance de l'internet 2016-2019
7.3 Dialogue européen sur la Gouvernance d'Internet (9-10 juin 2016, Bruxelles) et Forum sur la gouvernance d'internet (João Pessoa, Brésil, on 10-13 novembre 2015)
7.4 7.4. Governmental Advisory Committee (GAC) de l'Internet Corporation for Assigned Names and Numbers (ICANN)
7.5 7.5. Revue des conclusions du Sommet mondial sur la société de l'information (SMSI)

8. Protection des données

9. Activités de coopération

10. Méthodes de travail du CDMSI

10.1 Comités de rédaction
10.2 Evaluation de la participation des ONGs dans les comités directeurs

11. Information sur les travaux d'autres organisations et d'autres organes du Conseil de l'Europe

11.1 Assemblée parlementaire du Conseil de l'Europe (APCE)
11.2 Commissaire aux droits de l'homme

11.3. CODEXTER

12. Représentation du CDMSI dans les réunions d'autres comités et dans des manifestations

13. Elections

14. Points divers

15. Adoption du rapport de réunion abrégé

Annexe II
LIST OF PARTICIPANTS / LISTE DES PARTICIPANTS

9TH MEETING OF THE STEERING COMMITTEE ON MEDIA AND INFORMATION SOCIETY
9EME REUNION DU COMITE DIRECTEUR SUR LES MEDIAS ET LA SOCIETE DE L'INFORMATION
(CDMSI)

8 – 11 DECEMBER / *DECEMBRE 2015*
ROOM/SALLE 8 (PALAIS DE L'EUROPE)

ALBANIA / ALBANIE
Mr Glevin Dervishi
Adviser on Media to the Albanian Minister of Foreign Affairs, Ministry of Foreign Affairs

ARMENIA / ARMENIE
Ms Shahane Hakobyan
Department for Relations with European Court of Human Rights, Ministry of Justice of the Republic of Armenia

AUSTRIA / AUTRICHE
Mr Matthias Traimer
Federal Chancellery, Media Affairs and Information Society, Federal Chancellery, Constitutional Service

AZERBAIJAN
Ms Jeyran Amiraslanova
Senior Adviser of the Administration of the President

BOSNIA AND HERZEGOVINA / BOSNIE-HERZEGOVINE
Mr Emir Povlakić
Head of Division for Licensing, Digitalization and Coordination in Broadcasting, Communications Regulatory

CROATIA / CROATIE
Mr Milan F. Zivković
Head Advisor for Communication Policy, Ministry of Culture

DENMARK / DANEMARK
Ms Katja Just Maarbjerg
Ministry of Culture

ESTONIA / ESTONIE
Dr. Indrek Ibrus
Associate Professor, Tallinn University, Baltic Film and Media School

FRANCE
Ms Joanna Chansel
Bureau des affaires européennes et internationales, Direction Générale des Médias et des Industries Culturelles
Ministère de la Culture et de la Communication

M. Julien Plubel
Rédacteur
Ministère des Affaires étrangères, Direction de la coopération culturelle, universitaire et de la recherche, Pôle de l'audiovisuel extérieur

GEORGIA / GEORGIE
Ms Irine Bartaia
Deputy Director, Department of International Law, Ministry of Foreign Affairs of Georgia
GERMANY / ALLEMAGNE
Mr Gajus Köhr (8, 9, 10, 11 December)
Division K 31, International Media Cooperation, Federal Government Commissioner for Culture and the Media

Mr Jan Wiegandt (8-9 Dec)
Representation of the State of Rhineland-Palatinate to the EU

Ms Annick Kuhl (10-11 Dec)
Representation of the Free State of Bavaria to the EU

GREECE / GRECE
Mr Evangelos Valmas
Deputy Director of the Directorate for Mass Media
Head of the Department for Audiovisual Media & Archives
Secretariat General for Information & Communication

HUNGARY / HONGRIE
Mr György Ocskó
International Legal Adviser, National Media and Infocommunications Authority

ICELAND / ISLANDE
Ms Elfa Ýr Gylfadóttir
Media Commission, Ministry of Education, Science and Education

IRELAND / IRLANDE
Mr Éanna O'Conghaile
Principal Officer, Broadcasting Policy Division, Department of Communications, Energy & Natural Resources

ITALY / ITALIE
Mr Pierluigi Mazzella
Director General, Agency for the right to university education, Professor of Information and Communication, University of Rome

LATVIA / LETTONIE
Mr Andris Mellakauls
Information Space Integration, Ministry of Culture

LIECHTENSTEIN
Mr Claudio Nardi
Officer for Foreign Affairs

MOLDOVA / MOLDOVIE
Mr Serghei Mihov
Counsellor , Global Affairs and Human Rights Division , General Directorate for Multilateral Cooperation, Ministry of Foreign Affairs and European Integration of the Republic of Moldova

MONACO
M. Serge Robillard
Chef de Division, Direction des Communications Électroniques, Principauté de Monaco

MONTENEGRO

Mr Ranko Vujović
Executive Director, UNEM

THE NETHERLANDS / PAYS-BAS
Mr Nol Reijnders
Senior Adviser for Media Policy
Ms Pien van den Eijnden
Senior legal adviser
Ministry of the Interior and Kingdom Relations, Constitutional Affairs and Legislation, Constitutional Affairs

NORWAY / NORVEGE
Mr Olav Guntvedt
Assistant Director General, Department of Media Policy and Copyright, Ministry of Culture

POLAND / POLOGNE
Ms Małgorzata Pek
Deputy director, Strategy Department, National Broadcasting Council of Poland

ROMANIA / ROUMAIE
Ms Delia Mucica
Professor, University of Theatre and Film
Senior Advisor, Unit for Project Management, Ministry of Culture and National Heritage

RUSSIAN FEDERATION / FEDERATION RUSSIE
Mr Alexander Surikov
Deputy Director Department of Information and Press, Ministry of Foreign Affairs

Mr.Arseny Nedyak

Mr.Nadzhaf Abdullaev

SAN MARINO / SAINT MARIN
Mme Chiara Cardogna
Agent de presse - Département des Affaires Etrangères

SERBIA / SERBIE
Ms Maja Raković (Chair / Président)
First Counselor, Serbian Embassy, France

Ms Maja Zarić
Adviser, Sector for International Relations, EU integration and projects, Ministry of Culture and Information

SLOVENIA / SLOVENIE
Mr Skender Adem
Undersecretary, Ministry of Culture of Republic of Slovenia

SLOVAKIA / SLOVAQUIE
Ms Ivana Maláková
Head of Unit Media Law and Audiovisual Unit Media, Audiovisual and Copyright Department Ministry of Cultura of Slovak Republic

SWEDEN
Mr Christoffer Lärkner
Department of Culture

SWITZERLAND / SUISSE
Mr Thomas Schneider
International Affairs, Federal Office of Communication, Federal Department for the environment, transport, energy and communication

Mr Frédéric Riehl
Federal Office of Communication, Federal Department for the environment, transport, energy and communication

„FORMER YUGOSLAV REPUBLIC OF MACEDONIA „/ „EX-REPUBLIQUE YOUGOSLAVE DE MACEDOINE"
Ms Vesna Poposka
Head of International PR Department, Government of the Republic of Macedonia, PR Department

TURKEY / TURQUIE
Mr Mehmet Bora Sönmez
Media Expert, Radio and Television Supreme Council of Turkey

Mr Ahmet Yanik
Assistant Expert

Mr Ahmet Kilic
Head of Department, Information and Communication Technology Authority

Mr Lufti Gunenez
Expert, Information and Communication Technology Authority

UKRAINE
Ms Olha Herasymiuk
First Deputy Chair of the National Council of Ukraine for Television and Radio Broadcasting

UNITED KINGDOM / ROYAUME-UNI
Mr Mark Carvell
Media Team, Department for Culture, Media and Sport

* * *

OBSERVERS and PARTICIPANTS / *OBSERVATEURS et PARTICIPANTS*

BELARUS
Mr Dimintry Mironchik
Head of Media Department of MFA Belarus, Press-Secretary of MFA

EUROPEAN BROADCASTING UNION (EBU)
Ms Anne-Catherine Berg

EAVI
Mr Paolo Celo
Director and Secretary General, European Association for Viewers Interests

EUROPEAN AUDIOVISUAL OBSERVATORY / OBSERVATOIRE EUROPPENNE DE L'AUDIOVISUAL
Ms Susanne Nikoltchev
Executive Director

EuroISPA
Mr Michael Rotert
Honorary Spokesman

ASSOCIATION OF EUROPEAN JOURNALISTS (AEJ) / MEDIA FREEDOM REPRESENTATIVE
Mr William Horsley
Media Freedom Representative

CONFERENCE OF INTERNATIONAL NON-GOVERNMENTAL ORGANISATIONS OF THE COUNCIL OF EUROPE / CONFÉRENCE DES ORGANISATIONS INTERNATIONALES NON GOUVERNEMENTALES DU CONSEIL DE L'EUROPE
Mr Didier Schretter
Member of the Standing Committee, Vice-chair Education and Culture Committee

HOLY SEE / SAINT SIEGE
Dr Michael Lukas
Episcopal Press Office

INTERNET WATCH FOUNDATION
Mr Kristof Claesen
Press and Public Affairs Manager

ICANN
Mr Nigel Hickson (Weds)
VP, UN and IGO Engagement

EUROPEAN COMMISSION
Mr Maciej TOMASZEWSKI
European Commission / DG-CONNECT

OFFICE OF THE COMMISSIONER FOR HUMAN RIGHTS
Ms Alessandra Ricci
Adviser to the Commissioner

PARLIAMENTARY ASSEMBLY OF THE COUNCI OF EUROPE / ASSEMBLEE PARLEMENTAIRE DU CONSEIL DE L'EUROPE
Mr Rüdiger Dossow
Secretary of the Committee on Culture, Science and Education

COUNCIL OF EUROPE EUROPEANCOMMITTEE ON LEGAL CO-OPERATION (CDCJ)
M. Maciej Lewandowski
Member

ADVISORY COUNCIL ON YOUTH OF THE COUNCIL OF EUROPE
Mr Gian Piero Carlo Milani
Member of the Advisory Council on Youth of the Council of Europe

PERMANENT REPRESENTATION OF BELGIUM TO THE COUNCIL OF EUROPE
M Jean Zamani
Research Assistant, Information Society

PERMANENT REPRESENTATION OF LUXEMBOURG TO THE COUNCIL OF EUROPE
Mr Mattia Leveghi
Interne

PERMANENT REPRESENTATION OF LUXEMBOURG TO THE COUNCIL OF EUROPE
Ms Stéphanie Toschi

Interne

PERMANENT MISSION OF MEXICO TO THE COUNCIL OF EUROPE
M. Diego Sandova Pimentel
Adjoint à l'Observateur Permanent du Mexique

* * *

INTERPRETERS / INTERPRETES
Ms Amanda Beddows
Ms Martine Caraly
M Nicolas Guittonneau
Ms Gillian Wakenhut

* * *

SECRETARIAT

Mr Jan Kleijssen, Director of Information Society and Action against Crime, Directorate General Human Rights and Rule of Law
Mr Patrick Penninckx, Head of Information Society Department, Directorate General Human Rights and Rule of Law
Ms Silvia Grundmann, Head of Media and Internet Division, Directorate General of Human Rights and Rule of Law, Secretary to the CDMSI
Ms Onur Andreotti, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Lejla Dervisagic, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Ana Gascón Marcén, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Mr Lee Hibbard, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Elvana Thaçi, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Anne Boyer-Donard, Principal Administrative Assistant, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Julia Whitham, Assistant, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Saskia De Vos, Intern, Media and Internet Division, Directorate General Human Rights and Rule of Law

Annexe III

Projet de recommandation CM/Rec(2015)__ du Comité des Ministres aux Etats membres sur la protection du journalisme et la sécurité des journalistes et autres acteurs des médias

(adopté par le Comité des Ministres le _____ 2015 lors de la __e réunion des Délégués des Ministres)

1. Il est inquiétant et inacceptable de constater que les journalistes et autres acteurs des médias en Europe sont de plus en plus souvent menacés, victimes de harcèlement et d'intimidation, mis sous surveillance, arbitrairement privés de leur liberté, agressés physiquement, torturés et parfois même tués en raison de leur travail d'investigation, de leurs opinions ou de leurs reportages, notamment lorsque leur travail porte sur les abus de pouvoir, la corruption, les violations des droits de l'homme, les activités criminelles, le terrorisme et le fondamentalisme. Ces crimes et abus ont été largement relatés dans des rapports dignes de foi publiés par des médias, des organisations non gouvernementales et des défenseurs des droits de l'homme.

2. Les journalistes et les autres acteurs des médias sont souvent spécifiquement visés en raison de leur sexe, de leur identité de genre, de leur orientation sexuelle, de leur identité ethnique, de leur appartenance à un groupe minoritaire, de leur religion ou d'autres caractéristiques pouvant motiver des discriminations ou des agressions dans le cadre de leur travail. Les femmes journalistes et les autres femmes acteurs des médias sont confrontées à des dangers spécifiques liés à leur qualité de femme, notamment à des insultes dégradantes, sexistes ou misogynes, à des menaces, des intimidations, au harcèlement et à des agressions ou violences sexuelles. Ces violations sont de plus en plus souvent commises en ligne. Elles appellent des réponses urgentes, résolues et structurelles.

3. Les violations et les crimes décrits plus haut, qui dans la pratique sont commis par des acteurs étatiques et non étatiques, ont un effet dissuasif grave sur la liberté d'expression telle qu'elle est garantie par l'article 10 de la Convention européenne des droits de l'homme, y compris sur l'accès à l'information, sur le rôle de « chien de garde » que jouent les journalistes et les autres acteurs des médias ainsi que sur la vitalité et la liberté du débat public, qui sont autant d'éléments essentiels d'une société démocratique. Souvent, les autorités publiques ne font pas d'efforts suffisants pour traduire en justice les auteurs de crimes à l'encontre des journalistes ; cela engendre une culture de l'impunité, peut alimenter d'autres menaces et violences, et peut affaiblir la confiance des citoyens dans l'Etat de droit.

4. Cette situation alarmante ne se limite pas exclusivement aux journalistes professionnels ni aux autres acteurs traditionnels des médias. Ainsi que l'ont reconnu la Cour européenne des droits de l'homme et de nombreux organismes intergouvernementaux, y compris les Nations Unies dans leur Plan d'action sur la sécurité des journalistes et la question de l'impunité ou le Comité des droits de l'homme dans son Observation générale n° 34, l'éventail des acteurs des médias s'est élargi avec l'apparition de nouvelles formes de médias à l'ère numérique. C'est pourquoi la notion d'acteur des médias comprend aussi toute personne qui contribue à alimenter le débat public, pratique des activités journalistiques ou joue un rôle de « chien de garde » dans la sphère publique.

5. L'ampleur et la gravité des menaces et des attaques contre les journalistes et autres acteurs des médias en Europe et leurs effets néfastes sur le fonctionnement des sociétés démocratiques appellent des mesures de grande envergure aux niveaux international et national pour renforcer la protection du journalisme et la sécurité des journalistes et autres acteurs des médias, et pour mettre fin à l'impunité. La

communauté internationale a maintes fois affirmé la nécessité d'une mise en œuvre plus efficace des normes internationales ou régionales en vigueur et d'un respect accru des initiatives et des mécanismes de suivi existants. La protection des journalistes et autres acteurs des médias, ainsi que la lutte contre l'impunité des auteurs de crimes contre eux, sont des priorités politiques majeures pour tous les Etats membres du Conseil de l'Europe, ainsi que l'a souligné le Comité des Ministres dans sa Déclaration relative à la protection du journalisme et à la sécurité des journalistes et des autres acteurs des médias.

6. Pour créer et maintenir un environnement favorable à la liberté d'expression garantie par l'article 10 de la CEDH, les Etats doivent respecter un ensemble d'obligations positives établies et développées par la Cour européenne des droits de l'homme, et énoncées dans les principes figurant dans l'annexe à la présente recommandation. Ces obligations doivent être remplies par les pouvoirs exécutif, législatif et judiciaire ainsi que par tous les autres services de l'Etat, y compris ceux responsables du maintien de l'ordre et de la sécurité nationale, aussi bien au niveau fédéral et national que régional et local.

7. En vertu de l'article 15.*b* du Statut du Conseil de l'Europe, le Comité des Ministres recommande aux gouvernements des Etats membres, avec toute la célérité requise et en tenant dûment compte des principes énoncés dans l'annexe à la présente recommandation :

(i) de respecter la lettre et l'esprit des obligations, positives et négatives, qui leur incombent ;

(ii) de mettre en œuvre, par le biais de tous les organes des autorités de l'Etat, les principes directeurs énoncés ci-après ;

(iii) de réexaminer les lois et les pratiques nationales pertinentes et le cas échéant de les réviser afin de les mettre en conformité avec les obligations qui incombent aux Etats en vertu de la Convention européenne des droits de l'homme ;

(iv) de promouvoir les objectifs de la présente recommandation au niveau national et de nouer le dialogue et de coopérer avec toutes les parties prenantes pour les atteindre.

LIGNES DIRECTRICES

Ces principes directeurs visent à répondre au défi complexe que représentent la protection effective du journalisme et la sécurité des journalistes et des autres acteurs des médias ; ce défi requiert des stratégies cohérentes et complémentaires de la part des Etats membres. Ils se fondent sur les principes qui sont énoncés dans l'annexe et qui font partie intégrante de la recommandation. Ces principes s'articulent autour de quatre piliers : la prévention, la protection, les poursuites (avec une attention particulière à l'impunité) et la promotion des mesures d'information, d'éducation et de sensibilisation. Pour chacun de ces piliers, des orientations détaillées sont proposées aux Etats membres concernant les meilleures manières de s'acquitter de leurs obligations pertinentes en associant des mesures juridiques, administratives et pratiques.

Prévention

1. Les Etats membres devraient, en accord avec leurs traditions législatives et constitutionnelles, assurer l'indépendance des médias et protéger le pluralisme des médias, en veillant notamment à l'indépendance et la pérennité des médias de service public et des médias associatifs qui sont des composantes essentielles d'un environnement favorable à la liberté d'expression.

2. Les Etats membres devraient mettre en place un cadre législatif complet qui permette aux journalistes et aux autres acteurs des médias de contribuer au débat public de manière effective et sans crainte. Ce cadre devrait tenir compte des principes énoncés dans l'annexe à la présente recommandation et garantir ainsi l'accès public à l'information, le respect de la vie privée et la protection des données, la confidentialité et la sécurité des communications ainsi que la protection des sources journalistiques et des donneurs d'alerte. Le cadre législatif, comprenant notamment des dispositions de droit pénal relatives à la protection de l'intégrité physique et morale des personnes, devrait être mis en œuvre de manière effective, y compris au moyen de mécanismes administratifs, en reconnaissant le rôle particulier que jouent les journalistes et autres acteurs des médias dans une société démocratique. Le cadre et sa mise en œuvre devraient garantir une protection efficace des femmes journalistes et des autres femmes acteurs des médias contre les dangers liés à leur qualité de femme dans le cadre de leur travail. Une attention particulière devrait être apportée à l'élaboration de lois sur le travail et l'emploi à même de protéger les journalistes et les autres acteurs des médias contre les licenciements arbitraires ou les représailles et contre des conditions de travail précaires qui peuvent les rendre vulnérables aux pressions et les amener à dévier des normes et de l'éthique journalistiques reconnues.

3. Ce cadre législatif devrait être soumis à un examen substantiel et indépendant pour s'assurer que les garanties permettant l'exercice du droit à la liberté d'expression sont solides et effectives dans la pratique et que la législation se double d'un dispositif de mise en œuvre efficace. Après un examen initial, des révisions supplémentaires devraient être menées à des intervalles réguliers. Portant sur la législation et les pratiques, ils devraient évaluer la conformité du cadre législatif et de sa mise en œuvre avec les normes européennes et internationales en matière de droits de l'homme, y compris les obligations positives correspondantes des Etats, et formuler des recommandations sur la base des principales observations réalisées. Les examens devraient porter sur les lois en vigueur et sur les projets de loi, y compris ceux qui concernent le terrorisme, l'extrémisme et la sécurité nationale, et sur tout autre texte de loi touchant le droit à la liberté d'expression des journalistes et autres acteurs des médias ou les autres droits essentiels pour en garantir l'exercice effectif.

4. Les examens peuvent être menés par un ou plusieurs organismes indépendants, nouveaux ou existants, ayant un mandat officiel et disposant de ressources suffisantes. Les autorités nationales sont instamment invitées à établir des conditions favorables à

leur réalisation, rendant possible un contrôle détaillé de l'opinion public et permettant à des organisations et des experts de formuler des recommandations indépendamment des influences gouvernementales, politiques, religieuses, commerciales ou d'autres groupes d'intérêt. Le ou les organismes de contrôle pourrai(en)t être une commission nationale des droits de l'homme, un médiateur et/ou un autre organisme indépendant créé spécifiquement dans ce but. Il est recommandé que le ou les organismes de contrôle ai(en)t un mandat clair pour collecter, recevoir et utiliser les informations de n'importe quelle source et qu'il(s) bénéficie(nt) d'un accès optimal aux documents et aux fonctionnaires de tous les services de l'Etat. Le processus de contrôle devrait être transparent et inclure des auditions publiques pour faciliter une participation pleine et active de la société civile, y compris des représentants des organisations de journalistes, des médias et d'autres parties prenantes.

5. Les rapports établis à l'issue des examens devraient être formellement transmis aux services de l'Etat concernés, en particulier les ministères, ceux-ci devant prendre sans tarder les mesures correctrices ou autres dispositions jugées nécessaires pour donner suite aux observations et recommandations formulées. Les observations et recommandations devraient également être intégrées systématiquement aux processus de rapports, de suivi ou de partage d'informations du Conseil de l'Europe, tels que le Comité des Ministres, l'Assemblée parlementaire et le Commissaire aux droits de l'homme. Elles pourront aussi, aux mêmes fins, être mises à la disposition d'autres organisations intergouvernementales, notamment le Comité des droits de l'homme, l'Examen périodique universel du Conseil des droits de l'homme de l'ONU, l'Unesco, le Haut-Commissaire aux droits de l'homme de l'ONU et le Représentant de l'OSCE pour la liberté des médias.

6. Dans le cadre des examens de leur législation et de leur pratique, les Etats membres dont la législation comporte des lois sur la diffamation devraient s'assurer que ces lois prévoient des garanties pour la liberté d'expression conformes aux normes européennes et internationales en matière de droits de l'homme, et notamment les moyens de défense comme l'exception de vérité, l'intérêt général ou le commentaire acceptable, ainsi que des garanties conformes au principe de proportionnalité contre les abus et les détournements, tel qu'il a été développé par la Cour européenne des droits de l'homme. En outre, étant donné l'effet dissuasif sur l'exercice des libertés et sur le débat public d'une législation incriminant certains types d'expression, les Etats devraient faire preuve de retenue dans l'application de cette législation, lorsqu'elle existe. A cet égard, ils devraient être guidés par la conclusion de la Cour européenne des droits de l'homme selon laquelle une peine de prison pour délit de presse ne peut être infligée que dans des circonstances exceptionnelles, notamment en cas d'atteinte grave à d'autres droits fondamentaux, par exemple dans le cas d'un discours de haine ou d'une incitation à la violence. Cette législation devrait être soumise à un examen critique similaire dans le contexte des révisions de la législation et des pratiques.

7. Les Etats membres devraient clarifier le cadre juridique de la surveillance et de l'interception des données de communication par l'Etat et les garanties procédurales permettant de prévenir son abus ou son détournement, par exemple la possibilité de contrôle d'une décision par une autorité judiciaire compétente, les garanties d'une procédure régulière et la notification à l'utilisateur. Les Etats membres devraient garantir le fonctionnement efficace de mécanismes de contrôle sur la surveillance des communications par l'Etat, afin d'assurer la transparence de la nature et de l'étendue de ces pratiques, ainsi que leur justification. Ces organismes de contrôle devraient être réellement représentatifs des diverses parties prenantes, notamment des journalistes et de leurs organisations, ainsi que des experts juridiques et techniques.

Protection

8. Les textes législatifs incriminant la violence contre les journalistes doivent se doubler d'un dispositif d'application de la loi et de mécanismes de recours pour les victimes (et leurs familles) qui soient effectifs dans la pratique. Des dispositions claires et adaptées devraient être prises afin de mettre en place des formes injonctives et préventives efficaces de protection temporaire pour les personnes faisant l'objet de menaces de violences.

9. Les autorités nationales ont le devoir de prévenir ou de réprimer les infractions à l'encontre d'individus quand elles ont, ou auraient dû avoir, connaissance d'un risque réel et immédiat pour la vie ou l'intégrité physique de ces personnes, du fait des actes criminels d'un tiers, en prenant les mesures qui sont en leur pouvoir et qui, d'un point de vue raisonnable, auraient pallié ce risque. Pour y parvenir, les Etats membres devraient recourir aux mesures opérationnelles préventives nécessaires, comme une protection policière, notamment quand elle est demandée par les journalistes et autres acteurs des médias, ou comme une évacuation volontaire vers un endroit sûr. Ces mesures devraient être efficaces, mises en œuvre à temps et adaptées aux risques spécifiques au genre auxquels les femmes journalistes et les autres femmes acteurs des médias doivent faire face.

10. Les Etats membres devraient promouvoir la création et la gestion, par les organisations de médias ou la société civile, de dispositifs d'alerte précoce et d'intervention rapide (permanences téléphoniques, plateformes en ligne ou points de contact en cas d'urgence disponibles 24 heures sur 24, par exemple) pour que les journalistes et autres acteurs des médias, lorsqu'ils sont menacés, aient un accès immédiat à des mesures de protection. S'ils sont créés et administrés par l'Etat, ces mécanismes devraient faire l'objet d'une supervision effective par la société civile et assurer la protection des lanceurs d'alerte et des sources qui souhaiteraient rester anonymes. Les Etats membres sont instamment invités à soutenir sans réserve la plateforme du Conseil de l'Europe pour promouvoir la protection du journalisme et la sécurité des journalistes, à coopérer avec la plateforme, et à contribuer ainsi au renforcement des capacités des organes du Conseil de l'Europe pour donner l'alerte et réagir efficacement aux menaces et aux violences contre les journalistes et autres acteurs des médias.

11. Dans tous les cas de privation de liberté de journalistes ou d'autres acteurs des médias par la police ou d'autres représentants des forces de l'ordre, des garanties procédurales adéquates doivent être respectées afin d'empêcher les détentions arbitraires et les mauvais traitements. Ces garanties doivent inclure : le droit pour la personne détenue d'informer ou de faire informer un tiers de son choix de la privation de liberté dont elle fait l'objet, de son lieu de détention et d'éventuels transfèrements, le droit de consulter un avocat, d'être examiné par un médecin et de contester la légalité de la détention devant une instance juridictionnelle. Les personnes arrêtées ou détenues pour une infraction doivent être aussitôt traduites devant un juge et ont le droit d'être jugées dans un délai raisonnable ou d'être libérées pendant la procédure, conformément à l'article 5 de la CEDH (Droit à la liberté et à la sûreté) tel que l'interprète la Cour européenne des droits de l'homme dans sa jurisprudence.

12. Les Etats membres sont instamment invités à concevoir des protocoles et des programmes de formation pour tous leurs services chargés d'honorer leurs obligations en matière de protection des journalistes et des autres acteurs des médias. Ces protocoles devraient être adaptés à la nature et au mandat des agents de la fonction publique concernés, par exemple, les juges, les procureurs, les policiers, le personnel militaire, le personnel pénitentiaire, les fonctionnaires de l'immigration ou d'autres services de l'Etat. Ils devraient viser à faire en sorte que tous ces personnels soient pleinement conscients des obligations de l'Etat en vertu du droit international des droits de l'homme et du droit humanitaire, ainsi que des implications concrètes de ces obligations pour chaque service. Les protocoles et les programmes de formation devraient prendre en compte la

reconnaissance du rôle important que jouent les journalistes et autres acteurs des médias dans une société démocratique, et des aspects spécifiques liés aux questions de genre.

13. Les Etats membres doivent faire preuve de vigilance pour empêcher toute application discriminatoire ou arbitraire de la législation et des sanctions contre les journalistes et les autres acteurs des médias. Ils devraient également prendre les mesures législatives et autres nécessaires pour empêcher le recours abusif, vexatoire ou malveillant à la loi et aux procédures judiciaires dans le but d'intimider ou de les faire taire. Les Etats membres devraient veiller avec autant de vigilance à ce que les mesures administratives comme les dispositifs d'enregistrement, d'accréditation et de taxation ne soient pas détournés pour harceler les journalistes et autres acteurs des médias, ou pour frustrer leur aptitude à contribuer efficacement au débat public.

14. Les Etats membres devraient prendre en compte la nature spécifique et la valeur démocratique du rôle joué par les journalistes et autres acteurs des médias dans certains contextes particuliers, notamment en temps de crise, pendant les périodes électorales, dans les manifestations publiques et dans les zones de conflit. Dans ces contextes, il est particulièrement important que les autorités répressives respectent le rôle des journalistes et autres acteurs des médias qui assurent la couverture des manifestations et autres événements. Les cartes de presse, les cartes syndicales, les accréditations pertinentes et les insignes de journaliste devraient être acceptés par les autorités de l'Etat comme documents d'accréditation des journalistes et, quand des journalistes ou autres acteurs des médias sont dans l'impossibilité de produire des documents professionnels, les autorités devraient faire tout leur possible pour établir leur statut. En outre, le dialogue entre les autorités et les organisations de journalistes est encouragé afin d'éviter les frictions ou les affrontements entre la police et les membres des médias.

15. Les représentants de l'Etat et les personnalités publiques devraient s'abstenir de mettre en cause ou d'attaquer l'intégrité des journalistes et autres acteurs des médias, notamment par des propos sexistes, en se référant à leur appartenance ethnique ou en les accusant de diffuser de la propagande, au risque de compromettre leur sécurité. De même, ils devraient se garder de soumettre des journalistes ou d'autres acteurs des médias à des exigences, des contraintes ou des pressions, au moyen de violences, de menaces, de sanctions ou incitations financières ou d'autres mesures, pour les amener à dévier des normes et de l'éthique journalistiques reconnues et à diffuser de la propagande ou de fausses informations. Les représentants de l'Etat et les personnalités publiques devraient condamner publiquement et sans équivoque toutes menaces et violences contre les journalistes et les autres acteurs des médias, quelle qu'en soit la source.

16. Les Etats membres devraient encourager les organes de presse, sans empiéter sur leur indépendance éditoriale ou opérationnelle, à s'acquitter de leurs responsabilités institutionnelles envers tous les journalistes et autres acteurs des médias qui travaillent pour eux comme salariés, pigistes ou sous tout autre statut. Cela peut passer par l'adoption de lignes directrices et de procédures internes applicables à l'affectation de journalistes et d'autres acteurs des médias à des missions difficiles ou dangereuses, par exemple dans des zones de conflit. La participation à de telles missions devrait être volontaire et informée. Les entreprises sont également responsables de fournir des informations adéquates aux journalistes et autres acteurs des médias, de les sensibiliser aux risques encourus, de les former aux questions de sécurité – y compris de sécurité numérique – et de protection des données personnelles, et de faire le nécessaire pour qu'ils disposent d'une assurance-vie, d'une couverture d'assurance maladie et d'une assurance voyage, dans le cadre global de conditions de travail équitables. Elles comprennent également, s'il y a lieu, la mise à disposition d'une assistance juridique, d'une représentation en justice et d'une aide psychologique au retour de mission.

Poursuites

17. Toute personne impliquée dans des violences, des agressions ou des homicides commis sur des journalistes ou d'autres acteurs des médias doit impérativement être traduite en justice. A cet effet, les enquêtes sur ces crimes et la poursuite de leurs auteurs doivent satisfaire à un certain nombre d'exigences générales. Lorsque les responsables de tels crimes ne sont pas traduits en justice, une culture de l'impunité peut s'installer ; des mesures particulières sont alors nécessaires.

Exigences générales

18. Les enquêtes sur les meurtres, les agressions et les mauvais traitements doivent être effectives et donc respecter les impératifs de rigueur, d'exhaustivité, d'impartialité et d'indépendance, de promptitude et de soumission au contrôle public.

19. Les enquêtes doivent être effectives en ce sens qu'elles doivent permettre d'établir les faits, d'identifier les responsables et enfin, le cas échéant, de les sanctionner. Les autorités doivent prendre toutes les mesures raisonnables pour recueillir l'ensemble des éléments de preuve relatifs à l'incident. Les conclusions des enquêtes doivent reposer sur une analyse approfondie, objective et impartiale de tous les éléments pertinents, et notamment déterminer s'il existe un lien entre les menaces ou la violence contre des journalistes et d'autres acteurs des médias et l'exercice de leurs activités journalistiques ou toute autre contribution de nature similaire au débat public. Les autorités de l'Etat sont aussi tenues d'enquêter sur l'existence d'un éventuel lien entre des positions racistes et un acte de violence de même qu'avec un éventuel lien avec les questions de genre.

20. Pour qu'une enquête puisse être efficace, les personnes qui en sont chargées doivent être indépendantes et impartiales, en droit et en fait. Toute personne ou institution impliquée d'une quelconque manière dans une affaire doit être exclue de toute fonction dans l'enquête. En outre, les enquêtes devraient être menées par des unités spécialisées au sein des services de l'Etat compétents, dont le personnel doit avoir correctement formé aux normes et garanties internationales relatives aux droits de l'homme. Les enquêtes devraient être effectives pour préserver la confiance du public dans la capacité des autorités à maintenir la primauté du droit, pour éviter tout sentiment de collusion ou de tolérance des agissements illicites et, dans les affaires où des agents ou organes de l'Etat sont impliqués, pour garantir que ceux-ci aient à rendre des comptes au sujet des morts survenues sous leur responsabilité. Les enquêtes devraient aussi être soumises au contrôle public et, dans tous les cas, les proches de la victime doivent être associés à la procédure dans la mesure où cela est nécessaire à la sauvegarde de ses intérêts légitimes.

21. Les Etats membres ont l'obligation de prendre toutes les mesures nécessaires pour traduire en justice les auteurs de crimes contre les journalistes et les autres acteurs des médias, que ces auteurs soient des protagonistes étatiques ou non. Les enquêtes et les poursuites devraient prendre en compte l'ensemble des différents rôles – réels et potentiels – joués dans ces crimes, comme les auteurs, les instigateurs, les exécutants et les complices, ainsi que la responsabilité pénale associée à chacun de ces rôles.

22. Les Etats membres sont tenus de s'assurer de l'intégrité des procédures judiciaires ; ils doivent garantir l'indépendance et l'impartialité du pouvoir judiciaire. Ils doivent également garantir la sécurité des juges, des procureurs, des avocats et des témoins prenant part aux poursuites pour crimes contre des journalistes et d'autres acteurs des médias.

23. Les Etats membres doivent veiller à ce que les victimes et, s'il y a lieu, leur famille disposent de moyens effectifs et adaptés d'obtenir réparation, notamment de

voies de recours et d'indemnisation financière, d'une prise en charge médicale et psychologique, d'une aide à la réinstallation et d'un hébergement. Ces dispositifs devraient tenir dûment compte des aspects culturels, ethniques, religieux ou liés au genre, et de tout autre aspect particulier. Le fait qu'une action pénale soit en cours ou dans l'attente d'un jugement ne devrait pas empêcher les victimes d'exercer des recours au civil.

Impunité

24. Lorsque des poursuites pour crimes contre des journalistes ou d'autres acteurs des médias ne sont pas engagées ou font l'objet de diverses obstructions, cela provoque des retards inadmissibles dans l'administration de la justice, ce qui aboutit à l'impunité des auteurs des crimes. Par conséquent, lorsqu'un agent de l'Etat est accusé de crimes impliquant des mauvais traitements, il est de la plus haute importance qu'aucune prescription n'affecte les procédures pénales et les peines. Afin de ne pas compromettre la confiance des citoyens dans le système judiciaire, des mesures comme l'amnistie ou la grâce ne devraient pas être envisagées ni acceptées en l'absence de raisons convaincantes. La loi devrait prévoir des peines complémentaires ou une aggravation de peine pour les fonctionnaires qui, délibérément, par négligence ou complicité, agissent de manière à empêcher ou à faire obstruction aux enquêtes, poursuites ou sanctions à l'égard des responsables de crimes perpétrés contre des journalistes ou d'autres acteurs des médias en raison de leur travail ou de leur contribution au débat public.

25. Lorsque les enquêtes et poursuites n'aboutissent pas à la traduction en justice des auteurs d'actes d'homicide ou d'autres crimes graves contre des journalistes ou d'autres acteurs des médias, les Etats membres peuvent envisager la conduite d'enquêtes judiciaires spéciales ou d'enquêtes non judiciaires sur des affaires précises ou la mise en place d'organes indépendants et spécialisés chargés de mener ce type d'enquêtes de façon continue. Ces derniers peuvent être dotés d'une autorité spéciale et comprendre en leur sein ou avoir à leur tête des personnalités respectées des médias et/ou de la société civile, et avoir pour objectif de faire progresser l'établissement des faits, sans pour autant réduire la responsabilité des services de l'Etat chargés des poursuites et des enquêtes de traduire en justice les auteurs de crimes.

26. Les Etats membres devraient améliorer la coopération et l'échange d'informations, d'expertise et de bonnes pratiques avec d'autres Etats chaque fois que des crimes contre des journalistes et autres acteurs des médias ont une dimension transfrontalière ou impliquent le cyberespace, sous réserve de garanties concernant le droit à la vie privée, la protection des données et la présomption d'innocence.

27. Les Etats membres sont invités à défendre de manière proactive et vigoureuse les priorités de la protection des journalistes et des autres acteurs des médias et de la lutte contre l'impunité dans tous les forums intergouvernementaux régionaux et internationaux et, plus généralement, dans leur politique étrangère et leurs relations extérieures. Cela peut comprendre une coopération pleine et entière avec des initiatives de collecte d'informations, de sensibilisation ou autres actions coordonnées par les organisations intergouvernementales régionales et internationales concernant la sécurité des journalistes et des autres acteurs des médias, notamment les processus d'établissement de rapports périodiques par les Etats, par exemple pour le Comité des droits de l'homme des Nations Unies, dans le cadre de l'Examen périodique universel du Conseil des droits de l'homme de l'ONU et pour la présentation d'informations au Directeur général de l'Unesco sur les mesures prises pour mettre fin à l'impunité des auteurs de crimes et sur l'état d'avancement des enquêtes judiciaires relatives aux meurtres de journalistes. Cela engloberait également le rôle et la responsabilité des Etats membres dans la supervision de l'exécution des arrêts de la Cour européenne des droits de l'homme par le Comité des Ministres du Conseil de l'Europe, et la fourniture rapide de réponses complètes à toutes les demandes ponctuelles émanant du

Commissaire aux droits de l'homme du Conseil de l'Europe ou du Représentant de l'OSCE sur la liberté des médias.

Promotion de l'information, formation et sensibilisation

28. Les Etats membres devraient promouvoir la traduction (dans la ou les langues nationales et minoritaires de leur pays) et la diffusion la plus large possible de la présente recommandation ainsi que la sensibilisation à son contenu au moyen de documents d'information variés. Les stratégies d'information et de sensibilisation devraient inclure des campagnes spécifiques conçues pour profiter de la visibilité qu'offrent les événements internationaux tels que la Journée mondiale de la liberté de la presse (3 mai), la Journée internationale de la fin de l'impunité pour les crimes commis contre des journalistes (2 novembre) ou la Journée internationale du droit de savoir (28 septembre). Les Etats membres devraient coopérer pleinement avec les initiatives de collecte d'informations, de sensibilisation et autres actions coordonnées par des organisations intergouvernementales régionales et internationales concernant la sécurité des journalistes et des autres acteurs des médias. Ce faisant, ils devraient prendre l'initiative de signaler, selon les besoins, les problèmes spécifiques aux questions de genre ou relatifs à d'autres motifs de discrimination inadmissibles.

29. Les Etats membres devraient encourager les organes compétents à mettre en avant la présente recommandation – ainsi que les supports pédagogiques traitant de toutes les questions qu'elle aborde, y compris les aspects spécifiques aux questions de genre – dans les programmes de formation des écoles de journalisme, dans la formation continue des journalistes ainsi que dans le cadre de programmes d'initiation aux médias et de maitrise de l'information.

30. Les Etats membres devraient développer un partenariat avec la société civile et les médias pour promouvoir les bonnes pratiques en matière de protection des journalistes et autres acteurs des médias et de lutte contre l'impunité. Cela devrait comprendre la mise en pratique des principes de transparence de la justice et du gouvernement et l'adoption d'une attitude constructive et responsable envers la société civile et le travail des médias sur les menaces et les violences contre les journalistes et les autres acteurs des médias, mettant en lumière les questions de genre ou d'autres questions, le cas échéant. Cela devrait également impliquer une coopération active dans l'information et l'éducation concernant les problèmes et les normes pertinents.

Annexe

PRINCIPES

La recommandation qui précède repose sur un vaste ensemble de principes ancrés dans la Convention européenne des droits de l'homme et développés par la Cour européenne des droits de l'homme dans sa jurisprudence. Les paragraphes suivants présentent et mettent en contexte une sélection des principes à prendre en compte dans le domaine qui nous intéresse ici. Les principes ont été répartis selon les catégories suivantes : liberté d'expression ; environnement propice ; sûreté, sécurité, protection ; contribution au débat public, et effet dissuasif.

Liberté d'expression

1. Le droit à la liberté d'expression, tel qu'il est consacré par l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), l'article 19 de la Déclaration universelle des droits de l'homme, l'article 19 du Pacte international relatif aux droits civils et politiques, ainsi que par d'autres instruments internationaux et régionaux, est un droit de l'homme fondamental dont jouit toute personne sans discrimination aucune, en ligne et hors ligne. C'est un

droit mixte comprenant la liberté d'opinion et la liberté de chercher, de recevoir et de communiquer des informations et des idées de tout type, sans ingérence et sans considération de frontière.

2. Le droit à la liberté d'expression et d'information, tel que garanti par l'article 10 de la CEDH, constitue l'un des fondements essentiels d'une société démocratique et l'une des conditions primordiales de son progrès et de l'épanouissement de chacun. La liberté d'expression vaut non seulement pour les « informations » ou les « idées » accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui offensent, choquent ou dérangent l'Etat ou une fraction quelconque de la population. C'est de cette façon que la liberté d'expression permet l'émergence d'un débat public solide, qui constitue un autre prérequis pour une société démocratique pluraliste, tolérante et ouverte d'esprit. Toute ingérence dans le droit à la liberté d'expression des journalistes et autres acteurs des médias a donc des répercussions sociétales car c'est aussi une ingérence dans le droit d'autrui de recevoir des informations et des idées, et une ingérence dans le débat public.

3. L'exercice du droit à la liberté d'expression comporte des devoirs et des responsabilités, comme l'énonce l'article 10(2). Dans le contexte du journalisme, les devoirs et responsabilités pertinents incluent notamment l'obligation d'agir de bonne foi pour fournir des informations précises et fiables, dans le respect de l'éthique journalistique.

4. Même si le droit à la liberté d'expression n'est pas absolu, une ingérence dans celui-ci n'est admissible que si elle est prévue par la loi, poursuit l'un des buts légitimes énoncés à l'article 10(2) de la CEDH, s'avère nécessaire dans une société démocratique, ce qui implique qu'elle correspond à un besoin social impérieux et est proportionnée au(x) but(s) légitime(s) poursuivi(s). Ces buts légitimes sont les suivants : la sécurité nationale, l'intégrité territoriale ou la sûreté publique, la défense de l'ordre et la prévention du crime, la protection de la santé ou de la morale, la protection de la réputation ou des droits d'autrui, la prévention de la divulgation d'informations confidentielles et la garantie de l'autorité et de l'impartialité du pouvoir judiciaire.

5. En outre, certains types de discours incitant à la violence ou à la haine peuvent tomber sous le coup de l'article 17 de la CEDH (Interdiction de l'abus de droit) et ne sont donc pas protégés par la Convention car ils visent à détruire certains droits et libertés reconnus dans celle-ci.

6. Tous les droits de l'homme sont universels, indissociables, interdépendants et intimement liés, et le droit à la liberté d'expression en particulier fonctionne ainsi en corrélation avec d'autres droits de l'homme comme les droits à la liberté de pensée, de conscience et de religion, à la liberté de réunion et d'association, et le droit de voter dans le cadre d'élections libres et équitables.

7. Parmi les autres droits de l'homme liés aux questions relatives à la sécurité des journalistes et autres acteurs des médias et à la lutte contre l'impunité figurent le droit à la vie (article 2) ; l'interdiction de la torture (article 3) ; le droit à la liberté et à la sûreté (article 5) ; le droit à un procès équitable (article 6) ; pas de peine sans loi (article 7) ; le droit au respect de la vie privée et familiale (article 8) et le droit à un recours effectif (article 13).

8. La CEDH est un instrument vivant qui doit être interprété à la lumière des conditions actuelles et d'une manière garantissant que tous les droits qu'elle protège soient concrets et effectifs et non pas théoriques ou illusoires, tant sur le plan de leur substance que de celui des voies de recours disponibles en cas de violation.

9. L'évolution constante de la technologie transforme l'environnement médiatique traditionnel, comme l'expose notamment la Recommandation CM/Rec (2011)7 sur une nouvelle conception des médias ; l'évolution conduit à de nouvelles conceptions des médias et à une nouvelle perception de l'écosystème médiatique en mutation. Les progrès des technologies de l'information et de la communication facilitent la participation au débat public d'un éventail d'acteurs toujours plus large et varié. C'est pourquoi la Cour européenne des droits de l'homme a maintes fois reconnu qu'outre les médias et les journalistes professionnels, les citoyens ordinaires, les organisations de la société civile, les lanceurs d'alerte et les chercheurs peuvent tous apporter des contributions utiles au débat public, jouant ainsi un rôle similaire ou équivalent à celui des médias institutionnels et des journalistes professionnels.

10. Le Comité des droits de l'homme des Nations Unies a de même affirmé que « le journalisme est une fonction exercée par des personnes de tous horizons, notamment des reporters et analystes professionnels à plein temps ainsi que des blogueurs et autres particuliers qui publient eux-mêmes le produit de leur travail, sous forme imprimée, sur l'Internet ou d'autre manière ». L'Assemblée générale des Nations Unies a également reconnu que « le journalisme est en perpétuelle évolution car il se nourrit de l'ensemble des contributions des organismes de médias, de particuliers et de diverses organisations qui cherchent, reçoivent et transmettent des informations et des idées de toute nature, sur Internet ou ailleurs […] concourant ainsi à façonner le débat public ». D'après le Plan d'action des Nations Unies sur la sécurité des journalistes et la question de l'impunité, « la protection des journalistes ne doit pas se limiter à ceux qui sont officiellement reconnus comme tels mais aussi bénéficier à d'autres personnes, dont les travailleurs des médias communautaires et les journalistes citoyens et autres personnes qui peuvent se servir des nouveaux médias pour atteindre leurs publics ».

11. L'obligation faite aux Etats de garantir l'exercice effectif des droits de l'homme suppose non seulement des obligations négatives de non-ingérence, mais aussi des obligations positives de garantir ces droits à toute personne relevant de leur juridiction.

12. Un exercice réel et efficace de la liberté d'expression peut nécessiter diverses mesures positives de protection jusque dans les relations entre individus. Ces obligations positives comprennent notamment : la création d'un environnement favorable à la participation au débat public de tous, permettant d'exprimer sans crainte opinions et idées ; la mise en place d'un système efficace de protection des auteurs et des journalistes ; la protection contre la violence physique et l'intimidation ; la protection de la vie ; le devoir d'enquêter sur les homicides et de prévenir la torture et les mauvais traitements.

Un environnement propice

13. Un environnement favorable ou propice à la liberté d'expression comporte un certain nombre de caractéristiques essentielles qui, collectivement, créent les conditions dans lesquelles la liberté d'expression et d'information et un débat public vigoureux peuvent s'épanouir. Le droit de recevoir des informations comprend le droit d'accéder à l'information et le droit pour le public de recevoir des informations ainsi que d'entendre des idées sur des questions d'intérêt public que les journalistes et autres acteurs des médias ont pour fonction de diffuser. La collecte d'informations est une étape de préparation essentielle de l'activité journalistique, dont elle fait partie intégrante ; elle est à ce titre protégée au titre de la liberté de la presse. Il faut éviter de décourager la participation de journalistes et d'autres acteurs des médias au débat sur des questions d'intérêt public légitime, par exemple par des mesures qui rendraient l'accès à l'information plus difficile ou par des restrictions arbitraires pouvant devenir une forme de censure indirecte.

14. L'écosystème médiatique est façonné par l'interaction entre des influences juridiques, politiques, socioculturelles, économiques, technologiques et autres, et sa vitalité est essentielle à un environnement propice à la liberté d'expression et d'information dans une société démocratique. L'une de ses caractéristiques est que les particuliers ont aujourd'hui la possibilité d'intervenir grâce aux nouvelles technologies qui facilitent leur participation au débat public. Une autre caractéristique réside dans le fait que des intermédiaires en ligne peuvent remplir une importante fonction de surveillance des débats publics menés sur leurs plates-formes privées, comme les réseaux sociaux. Il convient de rappeler que les intermédiaires en ligne sont indirectement liés par le respect du droit à la liberté d'expression et les autres droits de l'homme de leurs utilisateurs.

15. Le pluralisme des médias et la diversité de leur contenu sont essentiels pour le bon fonctionnement d'une société démocratique et sont les corollaires du droit fondamental à la liberté d'expression et d'information tel qu'il est garanti par l'article 10 de la CEDH. Les Etats ont l'obligation positive de garantir le pluralisme dans le secteur des médias, ce qui implique de veiller à ce que tout un éventail de points de vue, y compris les opinions critiques, puissent se faire entendre. Les autorités indépendantes de régulation des médias peuvent jouer un rôle important dans la défense de la liberté et du pluralisme des médias et, à ce titre, les Etats devraient garantir leur indépendance. L'adoption et la mise en œuvre effective d'une réglementation sur la propriété des médias peuvent également jouer un rôle important à cet égard. Une telle réglementation devrait garantir la transparence de la propriété des médias et empêcher sa concentration ; elle devrait couvrir des aspects tels que la propriété croisée ou indirecte des médias et les restrictions appropriées en matière de propriété de médias par les personnes exerçant une fonction publique.

16. Dans le cadre de leur travail, les journalistes et autres acteurs des médias sont souvent confrontés à des risques, des dangers et des discriminations liés au sexe, l'identité de genre, l'orientation sexuelle, la race, la couleur, la langue, la religion, l'opinion politique ou autre, l'origine nationale ou sociale, l'association avec une minorité nationale, le patrimoine, la naissance ou d'autres aspects. En outre, le fait d'enquêter sur certaines affaires ou de couvrir certaines questions (comme des sujets politiques, religieux, économiques ou sociétaux sensibles, y compris les abus de pouvoir, la corruption ou des activités criminelles) peuvent les exposer à un risque de menaces, d'agressions, de violences et de harcèlement de la part d'acteurs étatiques ou non étatiques. Les acteurs non étatiques peuvent être, par exemple, des organisations terroristes ou criminelles. Ces situations spécifiques devraient être prises en compte lors de la mise en place de mesures de prévention ou de protection efficaces.

17. Les femmes journalistes et les autres femmes acteurs des médias sont confrontées dans le cadre de leur travail à des dangers spécifiques liés à leur qualité de femme : menaces, agressions et violences (sexuelles), qui peuvent commises de manière ciblée, dans le contexte d'émeutes ou en détention. Ces risques sont souvent amplifiés par plusieurs facteurs : en effet, seule une partie des victimes porte plainte, les incidents sont insuffisamment documentés, les victimes ont un accès limité à la justice, autant de problèmes auxquels s'ajoutent les barrières sociales et les contraintes associées aux violences à motivation sexuelle et notamment la stigmatisation, le manque de reconnaissance de la gravité des problèmes et les attitudes discriminatoires d'éléments extrémistes de la société. Une approche systématique adaptée à la dimension du genre est requise pour prévenir et combattre ces dangers spécifiques, de même que pour contrer les coutumes et pratiques sociétales, les clichés sexistes, les préjugés et la discrimination dont ils s'alimentent. L'Etat a la responsabilité première de concevoir de telles stratégies, mais il ne faudrait pas oublier les médias, la société civile et les entreprises : la prise en compte des risques spécifiques auxquels les femmes sont exposées devrait occuper une place prépondérante dans toutes les mesures et

programmes traitant de la protection des journalistes et autres acteurs des médias et de la lutte contre l'impunité.

18. La possibilité d'exercer le droit à la liberté d'expression sans crainte suppose qu'au minimum la sûreté, la sécurité et la protection de tout un chacun, et en particulier des journalistes et des autres acteurs des médias, soient réellement garanties dans la pratique et que chacun puisse s'attendre à pouvoir contribuer au débat public sans crainte et sans avoir à modifier sa conduite sous l'effet de la peur. Cette peur peut résulter d'un harcèlement en ligne, de menaces, de cyber-attaques et d'autres agissements illégaux, dont le trolling, le cyber-harcèlement, le piratage des comptes e-mail ou de médias sociaux, des dispositifs de stockage d'information, de sites internet et de téléphones mobiles ou d'autres appareils électroniques. Parmi les journalistes et autres acteurs des médias, les femmes sont plus fréquemment la cible de harcèlement en ligne, de menaces, d'agressions et de violations de la sécurité numérique, ce qui appelle des réponses tenant compte des aspects liés au genre. Cependant, les menaces et la violence ne sont pas les seules causes de peur. Elle peut aussi résulter de (la menace ou l'anticipation raisonnable de) diverses pressions juridiques, politiques, socioculturelles et économiques qui peuvent être exacerbées en période de crise économique et d'austérité financière.

19. Les menaces et les manœuvres d'intimidation contre des journalistes et autres acteurs des médias signalent ou annoncent souvent une aggravation ou une intensification des atteintes à la liberté d'expression au sein de la société. Elles sont donc révélatrices d'une détérioration plus générale des droits de l'homme, de la démocratie et de l'Etat de droit.

Sûreté, sécurité, protection

20. L'Etat doit garantir la sécurité et l'intégrité physique de toute personne relevant de sa juridiction, ce qui suppose non seulement l'obligation négative de s'abstenir d'infliger la mort intentionnellement et illégalement mais aussi l'obligation positive de prendre les mesures nécessaires à la protection de la vie des personnes. Cette obligation positive a deux dimensions, de fond et de procédure.

21. La dimension de fond implique que l'Etat a l'obligation primaire d'assurer le droit à la vie en mettant en place une législation pénale efficace qui dissuade de commettre des atteintes contre la personne appuyée par un mécanisme d'application conçu pour en prévenir, réprimer et sanctionner les violations. Elle implique aussi, dans certaines circonstances, l'obligation positive pour les autorités de prendre préventivement des mesures pratiques pour protéger un individu ou un groupe d'individus dont la vie est menacée par des agissements criminels d'autrui. Eu égard aux difficultés pour la police d'exercer ses fonctions dans les sociétés contemporaines, à l'imprévisibilité du comportement humain et aux choix opérationnels à faire en termes de priorités et de ressources, il faut interpréter l'étendue de cette obligation positive de manière à ne pas imposer aux autorités un fardeau insupportable. Les autorités devraient toutefois faire attention à la vulnérabilité d'un journaliste qui couvre des sujets politiquement sensibles, face au pouvoir.

22. Le non-encadrement et l'abandon à l'arbitraire de l'action des agents de l'Etat sont incompatibles avec un respect effectif des droits de l'homme. Cela signifie qu'en plus d'être autorisées par la législation nationale, les opérations de police, y compris la gestion policière des manifestations publiques, doivent être suffisamment encadrées par la loi, à travers un système de garanties adéquates et effectives contre l'arbitraire et le recours abusif à la force, et même contre les accidents évitables. Cela suppose qu'il faut non seulement prendre en compte les actes des agents de l'Etat qui recourent directement à la force, mais aussi toutes les circonstances, y compris la planification et le contrôle des actes examinés. Un cadre juridique et administratif devrait définir les

conditions limitées dans lesquelles les services répressifs peuvent recourir à la force et aux armes à feu à la lumière des normes internationales élaborées en la matière. De ce point de vue, une chaîne de commandement claire, assortie de lignes directrices et de critères clairs, est indispensable ; une formation spécifique aux droits de l'homme peut aider à les formuler. Quoi qu'il en soit, les difficultés que suppose indéniablement la lutte contre la criminalité ne sauraient justifier des restrictions de la protection de l'intégrité physique des personnes, et l'article 3 de la CEDH n'autorise pas la recherche d'un compromis entre cette intégrité physique et l'objectif du maintien de l'ordre.

23. La dimension procédurale implique premièrement l'obligation positive, pour l'Etat de mener une enquête effective, indépendante et rapide sur toute allégation de mauvais traitements ou d'homicide commis illégalement par des acteurs étatiques ou non étatiques, afin de poursuivre en justice les auteurs de telles infractions. L'article 13 de la CEDH demande également aux Etats de garantir un recours effectif dès lors qu'il y a violation de l'un quelconque des droits substantiels consacrés par la Convention.

24. L'absence de telles mesures efficaces engendre une culture de l'impunité, qui conduit à tolérer les violences et les crimes contre les journalistes et les autres acteurs des médias. Lorsque les risques de poursuites sont nuls ou quasi nuls, les auteurs de tels actes ne craignent pas les sanctions. Cela inflige des souffrances supplémentaires aux victimes et peut mener à une répétition des violences et des crimes.

25. L'Etat a l'obligation de garantir la liberté fondamentale de toute personne relevant de sa juridiction et doit pour cela veiller à ce que les journalistes et autres acteurs des médias ne fassent pas l'objet d'arrestations arbitraires, d'une détention illégale ou d'une disparition forcée.

26. L'Etat ne devrait pas imposer de restriction abusive de la liberté de circulation, y compris transfrontalière, des journalistes et autres acteurs des médias, ni l'accès à certains secteurs, sites et forums, vu l'importance que revêtent cette mobilité et cet accès pour la collecte d'informations.

27. Des facteurs contextuels, comme les situations de crise ou de conflit, peuvent influer sur l'efficacité d'un système de protection en raison des risques accrus pour la sécurité et l'indépendance des journalistes et autres acteurs des médias, dans des contextes où les pouvoirs publics peinent à maintenir un contrôle de facto sur le territoire. Pourtant, les obligations de l'Etat restent valables, mutatis mutandis, dans ces contextes spécifiques, qui sont toujours soumis au droit international des droits de l'homme et au droit international humanitaire.

28. Assurer la sécurité et la sûreté des journalistes et des autres acteurs des médias est une condition préalable sans laquelle ils ne peuvent participer efficacement au débat public. La persistance d'intimidations, de menaces ou de violences contre les journalistes et les autres acteurs des médias, ajoutée à un échec à en traduire les auteurs en justice alimente la peur et a un effet dissuasif sur la liberté d'expression et la participation au débat public. Les Etats ont l'obligation positive de protéger les journalistes et les autres acteurs des médias contre toute intimidation, menace ou violence, quelle qu'en soit la source – gouvernementale, judiciaire, religieuse, économique ou criminelle.

Contribution au débat public

29. Les journalistes et autres acteurs des médias apportent une contribution essentielle au débat public et aux processus de formation de l'opinion dans une société démocratique en jouant le rôle de « chiens de garde » publics ou sociaux et en créant des espaces partagés qui permettent l'échange d'informations et d'idées et une interaction discursive. Le rôle de « chiens de garde » implique notamment d'informer le public sur des questions d'intérêt public, de les commenter, de faire rendre des comptes

aux autorités publiques et à d'autres milieux de pouvoir dans la société, et de dénoncer la corruption et les abus de pouvoir.

30. La Cour européenne des droits de l'homme a reconnu que pour que les journalistes et autres acteurs des médias puissent remplir les fonctions qui leur sont assignées dans une société démocratique, leur droit à la liberté d'expression devrait être protégé de manière très large. Cette protection comprend un ensemble de libertés qui leur sont concrètement nécessaires pour mener à bien leurs activités, comme la protection des méthodes de collecte de l'information et de la confidentialité des sources, la protection contre les perquisitions des locaux professionnels et des domiciles privés et contre la saisie de matériel ainsi que l'autonomie éditoriale et de présentation.

31. Les libertés opérationnelles ou fonctionnelles dont jouissent les journalistes et autres acteurs des médias, qui couvrent la collecte, le traitement et la diffusion de nouvelles et d'informations, sont nécessaires à l'exercice concret et effectif de leur droit à la liberté d'expression en ligne et hors ligne.

32. Outre la substance des idées et informations exprimées, l'article 10 de la CEDH protège aussi leur mode d'expression. Cela implique que les journalistes et autres acteurs des médias sont libres de choisir leur propre technique ou style dans les reportages d'information sur les questions d'intérêt public, ce qui comprend le recours possible à une certaine dose d'exagération, voire de provocation. Outre les reportages, d'autres genres contribuent de diverses manières au débat public et méritent à ce titre d'être protégés, comme la satire, qui est une forme d'expression artistique et de commentaire de la société visant tout naturellement, par l'exagération et la distorsion des faits qui lui sont caractéristiques, à provoquer et à susciter le débat.

Effet dissuasif

33. L'effet dissuasif sur la liberté d'expression apparaît lorsqu'une ingérence dans ce droit provoque la peur, conduit à l'autocensure et, en définitive, appauvrit le débat public, au détriment de la société tout entière. Les autorités étatiques devraient donc éviter de prendre des mesures ou d'imposer des sanctions ayant pour effet de décourager la participation au débat public.

34. La législation et son application concrète peuvent avoir un effet dissuasif sur la liberté d'expression et le débat public. Les ingérences ont un effet dissuasif plus marqué si elles prennent la forme de sanctions pénales plutôt que de sanctions civiles. Etant donné la position dominante des institutions de l'Etat, il convient que les autorités fassent preuve de retenue dans le recours aux poursuites pénales. Un effet dissuasif sur la liberté d'expression peut naître de toute sanction, disproportionnée ou non, mais aussi de la crainte d'une sanction, même dans l'éventualité d'un acquittement, compte tenu de la probabilité qu'une telle crainte décourage une personne de tenir des propos similaires à l'avenir.

35. Si la fixation des peines est en principe l'apanage des juridictions nationales, une peine de prison infligée pour une infraction commise dans le domaine de la presse n'est compatible avec la liberté d'expression journalistique garantie par l'article 10 de la CEDH que dans des circonstances exceptionnelles, notamment lorsque d'autres droits fondamentaux ont été gravement atteints, comme ce serait le cas, par exemple, en cas de diffusion d'un discours de haine ou d'incitation à la violence.

36. La menace de recours ou le recours effectif, abusif ou inconsidéré à différents types de textes législatifs – notamment les lois sur la diffamation, sur la lutte contre le terrorisme, sur la sécurité nationale et l'ordre public, sur le discours de haine, sur le blasphème ainsi que les lois mémorielles est un moyen efficace pour intimider et faire taire les journalistes et autres acteurs des médias qui enquêtent sur des questions

d'intérêt public. Les poursuites judiciaires abusives, vexatoires ou malveillantes, dans le contexte du coût élevé de tels procès peuvent constituer un outil de pression et de harcèlement, surtout quand elles se multiplient. L'effet du harcèlement peut être particulièrement rude lorsqu'il est exercé contre les journalistes et autres acteurs des médias qui ne bénéficient pas de la protection juridique ou du soutien financier et institutionnel offert par les grands médias. A cet égard, il convient de rappeler qu'un aspect central de la notion de procès équitable, dans les affaires civiles comme dans les affaires pénales, requiert que les Etats doivent prendre les mesures qui s'imposent, y compris la mise en place d'un dispositif d'aide juridictionnelle, pour garantir que chacune des parties dispose d'une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à son adversaire.

37. L'effet dissuasif peut aussi résulter du recours (abusif) à des mesures administratives telles que les régimes d'enregistrement et d'accréditation des journalistes, des bloggeurs, des usagers d'internet, des correspondants étrangers, des ONG, etc., ainsi que de dispositifs fiscaux, afin de harceler les journalistes et autres acteurs des médias ou de les priver des moyens de nourrir efficacement le débat public. La discrimination dans l'octroi de subventions destinées aux médias publics ou à la presse, ou de recettes publicitaires de l'Etat, peuvent aussi dissuader les divers acteurs des médias d'adopter des positions critiques, surtout pour les organisations de petite envergure ou exposées à une situation économique précaire.

38. La surveillance des journalistes et autres acteurs des médias et le suivi de leurs activités en ligne peuvent entraver l'exercice légitime du droit à la liberté d'expression si elles sont menées sans les garanties nécessaires. Ces pratiques peuvent également menacer la sécurité des personnes concernées et nuire à la protection des sources journalistiques. La surveillance et le suivi sont facilités lorsque l'intégrité des communications et des systèmes est compromise, par exemple lorsque des fournisseurs d'accès ou des fabricants de matériel informatique ou de logiciels intègrent des moyens de surveillance ou des portes dérobées dans leurs services ou leurs systèmes, ou lorsque des fournisseurs d'accès sont impliqués dans la surveillance exercée par l'Etat. Pour être compatibles avec l'article 8 de la CEDH, les mécanismes de surveillance secrète doivent être assortis de garanties suffisantes et efficaces contre les abus, et notamment un contrôle indépendant, car de tels systèmes destinés à protéger la sécurité nationale présentent le risque de fragiliser la démocratie, voire de la détruire, au motif de la défendre.

39. Les agressions et les manœuvres d'intimidation à l'endroit de journalistes et d'autres acteurs des médias ont inévitablement un grave effet dissuasif sur la liberté d'expression, qui s'amplifie encore lorsque la prévalence des agressions et des manœuvres d'intimidation se double d'une culture d'impunité juridique à l'égard des auteurs de ces actes. Cette culture d'impunité juridique est le symptôme de violations endémiques des droits de l'homme.

Annexe IV

Déclaration interprétative du Représentant de la Fédération de Russie (RF) concernant le projet de recommandation du Comité des Ministres aux Etats membres sur la protection du journalisme et la sécurité des journalistes et autres acteurs des médias

Le représentant de la Fédération de Russie s'est abstenu de soutenir le projet de recommandation du Comité des Ministres aux Etats membres sur la protection du journalisme et la sécurité des journalistes et autres acteurs des médias et fait la déclaration suivante.

La Fédération de Russie soutient l'approche globale de la recommandation, mais est forcé d'émettre une réserve pour la recommandation, en niant expressément son application aux «autres acteurs des médias", étant donné que la Fédération de Russie considère ce terme indéfini, dépourvu de précision et non inscrite dans les instruments juridiques contraignants internationaux. La Fédération de Russie affirme que seules les obligations des États applicables en vertu du droit international, ainsi qu'en vertu de la législation nationale constituent le cadre juridique pour l'application future de la présente recommandation.

Cette approche prévoit que la recommandation peut être applicable seuls aux journalistes professionnels conformément à la législation de la Fédération de Russie et ses dispositions peuvent être mises en œuvre à condition qu'elles ne contredisent pas la législation de la Fédération de Russie.

Annexe V

Projet de Recommandation CM/Rec(2015)__ du Comité des Ministres aux Etats membres sur la liberté d'internet

(adopté par le Comité des Ministres le _____ 2015 lors de la __e réunion des Délégués des Ministres)

1. La Convention européenne des droits de l'homme (ci-après « CEDH ») s'applique aussi bien en ligne qu'hors ligne. Les Etats membres du Conseil de l'Europe sont soumis à des obligations positives et négatives qui leur imposent de respecter, protéger et promouvoir les droits de l'homme et les libertés fondamentales sur internet.

2. La liberté d'internet s'entend comme l'exercice et la jouissance, sur internet, des droits de l'homme et des libertés fondamentales et leur protection, conformément à la CEDH et au Pacte international relatif aux droits civils et politiques. Les Etats membres du Conseil de l'Europe devraient adopter une approche volontariste de la mise en œuvre de la CEDH et d'autres normes du Conseil de l'Europe relatives à internet. La définition de la liberté d'internet devrait être complète et s'appuyer fermement sur ces normes.

3. Les règles applicables à la gouvernance d'internet, qu'elles soient nationales, régionales ou mondiales, doivent partir de cette définition de la liberté d'internet. Les Etats ont des droits et des responsabilités concernant les politiques internationales relatives à internet. Dans l'exercice de leur souveraineté, ils doivent, dans les conditions prévues par le droit international, s'abstenir de toute action portant directement ou indirectement préjudice à des personnes ou à des entités sur ou en dehors de leur juridiction. Toute décision ou action nationale restreignant des droits de l'homme et des droits fondamentaux sur internet doit respecter les obligations internationales et, en particulier, être prévue par la loi, être nécessaire dans une société démocratique, respecter pleinement le principe de proportionnalité et garantir l'accès aux voies de recours et le droit d'être entendu et de faire appel, assorti des garanties d'une procédure régulière.

4. Dans le cadre de leur obligation de reconnaître à toute personne relevant de leur juridiction les droits et libertés définis dans la CEDH, les Etats devraient créer un environnement favorable à la liberté d'internet. A cette fin, il est recommandé aux Etats d'évaluer régulièrement la situation de la liberté d'internet au plan national afin de veiller à ce que les conditions juridiques, économiques et politiques nécessaires à l'existence et à la progression de la liberté d'internet soient bien en place. De telles évaluations contribuent à une meilleure compréhension de l'application de la CEDH à internet dans les Etats membres et à sa meilleure mise en œuvre par les autorités nationales.

5. La CEDH et les normes du Conseil de l'Europe offrent des critères et des références pour les évaluations nationales de la liberté d'internet. Elles peuvent tenir lieu d'indicateurs pour guider les Etats membres et leur permettre de déceler les menaces qui pèsent ou pourraient peser sur la liberté d'internet, de cadre analytique pour évaluer la mise en œuvre des normes des droits de l'homme sur internet, et de référence pour élaborer les politiques et les approches internationales relatives à internet.

6. Le Conseil de l'Europe devrait jouer un rôle clé dans la promotion de la liberté d'internet en Europe et dans le monde. En s'appuyant sur les évaluations nationales de ses Etats membres, le Conseil de l'Europe peut y observer l'évolution des cadres réglementaires et autres développements et faire régulièrement le point sur les défis posés à la liberté d'internet en Europe. Cela constituerait une bonne base pour développer encore les politiques du Conseil de l'Europe dans le domaine d'internet.

7. Le Comité des Ministres recommande aux Etats membres :

- d'évaluer régulièrement le respect et la mise en œuvre des normes en matière de droits de l'homme et de libertés fondamentales en lien avec internet en utilisant les indicateurs proposés dans la présente recommandation en vue d'établir, le cas échéant, des rapports nationaux ;

- de veiller à associer tous les acteurs du secteur privé, de la société civile et des milieux universitaire et technologique, dans leur rôle respectif, à l'évaluation de la situation de la liberté d'internet et à l'élaboration des rapports nationaux ;

- d'envisager de communiquer au Conseil de l'Europe à titre volontaire des informations ou des rapports nationaux sur la liberté d'internet ;

- de s'inspirer de ces indicateurs et de les promouvoir lorsqu'ils participent au dialogue international et à l'élaboration de politiques mondiales en matière de liberté d'internet ;

- de prendre les mesures appropriées pour promouvoir les «Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence "protéger, respecter et réparer"» des Nations Unies.

8. Le Comité des Ministres invite également le Secrétaire Général du Conseil de l'Europe à aborder les questions liées à la liberté d'internet dans son rapport annuel sur la situation de la démocratie, des droits de l'homme et de l'Etat de droit en Europe, en insistant en particulier sur le partage de bonnes pratiques. Cette réflexion devrait également s'appuyer sur les évaluations nationales des Etats membres.

INDICATEURS DE LA LIBERTÉ D'INTERNET

La liberté d'internet s'entend comme l'exercice et la jouissance, sur internet, des droits de l'homme et des libertés fondamentales et leur protection, conformément à la CEDH. Ces indicateurs portent principalement sur les droits à la liberté d'expression, à la liberté de réunion et d'association, au respect de la vie privée et à un recours effectif. Ils s'appuient sur les normes en vigueur en matière de droits de l'homme et sur les mécanismes d'application établis. Une approche globale de la liberté d'internet prend en considération tous les indicateurs. Ils sont censés fournir des orientations pour la conduite d'une évaluation qualitative et objective de la liberté d'internet dans les Etats membres du Conseil de l'Europe et l'élaboration de rapports à ce sujet. Ils ne sont conçus ni comme un outil de notation du niveau de liberté d'internet, ni comme un moyen de comparaison entre les différents pays.

1. Un environnement favorable à la liberté d'internet

1.1. La protection des droits de l'homme et des libertés fondamentales sur internet est garantie en droit, dans le plein respect de la CEDH.

1.2. L'ingérence de l'Etat dans l'exercice des droits de l'homme et des libertés fondamentales sur internet est conforme à la CEDH.

1.3. Dès leur élaboration, les lois et les politiques relatives à internet font l'objet d'une évaluation pour déterminer l'incidence que leur mise en œuvre pourrait avoir sur l'exercice des droits de l'homme et des libertés fondamentales.

1.4. Les lois et les politiques relatives à internet sont élaborées par les autorités de l'Etat selon une approche inclusive et transparente permettant la participation de

toutes les parties intéressées, y compris le secteur privé, la société civile, les milieux universitaire et technologique.

1.5. Tout organisme public investi de compétences en matière de régulation ou autres d'internet mène ses activités sans aucune ingérence politique ou commerciale, de façon transparente, et protège et encourage la liberté d'internet.

1.6. L'Etat protège les personnes contre la cybercriminalité par des mesures effectives de justice pénale ou autres. Lorsque ces mesures risquent de porter atteinte au droit au respect de la vie privée, au droit à la liberté d'expression ou au droit à la liberté de réunion et d'association pacifiques, elles sont assorties de conditions et de garanties contre les abus. Elles sont conformes aux articles 8, 10 et 11 de la CEDH, elles sont notamment prévues par la loi - qui est claire, précise, accessible et prévisible – poursuivent un but légitime, sont nécessaires et proportionnées dans une société démocratique et permettent l'introduction d'un recours effectif.

1.7. L'Etat formule des politiques et prend des mesures pour appliquer les «Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence "protéger, respecter et réparer"» des Nations Unies.

1.8. L'Etat propose aux utilisateurs d'internet des programmes de formation aux médias et à la culture numérique afin d'accroître leur capacité à prendre des décisions éclairées et à respecter les droits et libertés d'autrui. Il favorise l'accès à des contenus éducatifs, culturels, scientifiques, universitaires et autres ainsi que leur utilisation.

2. Le droit à la liberté d'expression

2.1. Liberté d'accès à internet

2.1.1. Internet est disponible, accessible et d'un coût abordable pour toutes les catégories de population sans discrimination.

2.1.2. Le public a accès à internet dans des locaux financés par l'administration publique (points d'accès à internet), des établissements d'enseignement ou des acteurs privés (service universel communautaire).

2.1.3. L'Etat prend des mesures raisonnables pour garantir l'accès à internet aux personnes à faibles revenus, vivant dans des zones rurales ou enclavées ou présentant des besoins particuliers, comme les personnes handicapées.

2.1.4. L'accès à internet ne fait l'objet d'aucune restriction générale à l'échelle nationale, excepté en cas de mise en œuvre d'une mesure de restriction pleinement conforme à l'article 10 de la CEDH.

2.1.5. L'Etat reconnaît, en droit et en pratique, que le fait de couper la connexion d'un utilisateur à internet constitue, en règle générale, une restriction disproportionnée au droit à la liberté d'expression.

2.1.6. Toute restriction d'accès à internet, y compris au sein d'établissements pénitentiaires, satisfait aux conditions énoncées à l'article 10 de la CEDH quant à la légalité, la légitimité et la proportionnalité des restrictions à la liberté d'expression, et à l'obligation positive qui incombe à l'Etat de protéger le droit à la liberté d'expression.

2.1.7. Avant l'application de mesures restreignant l'accès à internet, un tribunal ou une autorité administrative indépendante décide que la coupure de la connexion à

internet constitue la mesure la moins restrictive pour atteindre l'objectif légitime poursuivi. La nécessité de maintenir la mesure de restriction est évaluée en permanence par les autorités susmentionnées. Ces conditions ne s'appliquent pas aux affaires de non-paiement par les utilisateurs de leurs services internet.

2.1.8. En cas d'application de mesures restrictives, l'intéressé a droit à une procédure régulière devant un tribunal ou une autorité administrative indépendante dont les décisions sont soumises à un contrôle juridictionnel, comprenant le droit d'être entendu et de faire appel, conformément à l'article 6 de la CEDH.

2.2. Liberté d'opinion et droit de recevoir et de communiquer des informations

2.2.1. Toute mesure prise par les autorités de l'Etat ou des acteurs du secteur privé pour bloquer ou restreindre l'accès à la totalité d'une plate-forme internet (médias et réseaux sociaux, blogs et tout autre site internet) ou à des outils TIC (messagerie instantanée et autres applications) ou toute demande en ce sens formulée par les autorités de l'Etat, satisfait aux conditions énoncées à l'article 10 de la CEDH quant à la légalité, légitimité et proportionnalité des restrictions.

2.2.2. Toute mesure prise par les autorités de l'Etat ou des acteurs du secteur privé pour bloquer, filtrer ou supprimer un contenu internet, ou toute demande en ce sens formulée par les autorités de l'Etat, satisfait aux conditions énoncées à l'article 10 de la CEDH quant à la légalité, légitimité et proportionnalité des restrictions.

2.2.3. Les fournisseurs de services internet ont pour règle générale de traiter le trafic internet à égalité et sans discrimination, quels que soient l'émetteur, le destinataire, le contenu, l'application, le service ou le dispositif. Les mesures de gestion du trafic internet sont transparentes, nécessaires et proportionnées à la satisfaction d'un intérêt public supérieur, conformément à l'article 10 de la CEDH.

2.2.4. Les utilisateurs d'internet ou les autres parties intéressées ont accès à une procédure de recours conforme à l'article 6 de la CEDH devant toute mesure prise pour limiter leur accès à internet ou leur capacité à consulter et à publier des contenus ou à recevoir et communiquer des informations.

2.2.5. L'Etat fournit au public, à temps et de manière appropriée, des informations sur les restrictions appliquées à la liberté de recevoir ou de communiquer des informations, expliquant quel site a été bloqué ou quelle information supprimée, notamment en précisant en détail les raisons, le fondement juridique, la nécessité et la justification de telles restrictions, la décision de justice les autorisant et le droit de recours.

2.3. Liberté des médias

2.3.1. L'indépendance éditoriale des médias opérant sur internet est garantie par la loi, par les politiques et dans la pratique. Ils ne subissent aucune pression visant à leur faire mentionner ou exclure certaines informations dans leurs reportages ou suivre une ligne éditoriale particulière.

2.3.2. Les médias ne sont pas tenus d'obtenir une autorisation ou une licence auprès du gouvernement ou d'autorités publiques en dehors de la déclaration de leur activité pour opérer sur internet ou créer des blogs.

2.3.3. Les journalistes et les autres acteurs des médias utilisant internet ne font l'objet d'aucune menace ou harcèlement de la part de l'Etat. Ils ne pratiquent pas l'autocensure par crainte de sanction, de harcèlement ou d'agression.

2.3.4. La confidentialité des sources des journalistes et des autres acteurs des médias est protégée par la loi et respectée dans la pratique.

2.3.5. Les sites internet des médias et des acteurs des nouveaux médias ne sont pas la cible de cyberattaques ou d'autres actes qui perturbent leur fonctionnement (par exemple, des attaques par déni de service).

2.3.6. Les crimes perpétrés contre des journalistes et des acteurs de nouveaux médias font l'objet d'enquêtes promptes et efficaces. Il n'existe aucun climat d'impunité.

2.4. Légalité, légitimité et proportionnalité des restrictions

2.4.1. Toute restriction au droit à la liberté d'expression sur internet respecte les exigences de l'article 10 de la CEDH telles que l'interprète la Cour européenne des droits de l'homme, à savoir qu'elle :

- est prévue par la loi, laquelle est accessible, claire, sans ambiguïté et suffisamment précise pour permettre aux personnes de régler leur conduite en conséquence. La loi garantit un contrôle rigoureux de la portée de la restriction et un contrôle juridictionnel effectif afin de prévenir tout abus de pouvoir. La loi définit de manière suffisamment claire l'étendue du pouvoir de discrétion accordé aux autorités publiques eu égard à la mise en œuvre des restrictions et aux modalités d'exercice de ce pouvoir.

- poursuit un des buts légitimes énumérés de façon exhaustive à l'article 10 de la CEDH ;

- est nécessaire dans une société démocratique et proportionnée au but légitime poursuivi. La restriction répond à un besoin social impérieux et fait suite à une décision prise par un tribunal ou une autorité administrative indépendante soumise à un contrôle juridictionnel. La décision devrait être ciblée et spécifique. Elle devrait également reposer sur une évaluation de l'efficacité de la mesure et des risques de blocage excessif. Cette évaluation devrait déterminer si la restriction est susceptible de conduire à une interdiction d'accès disproportionnée à un contenu ou à des types spécifiques de contenu internet et s'il s'agit du moyen disponible le moins restrictif pour atteindre le but légitime poursuivi.

2.4.2. L'Etat n'impose aucune restriction indue à la liberté d'expression sur internet au moyen de la loi. Les lois sur la diffamation sont spécifiques et leur champ d'application est étroitement défini. Elles n'empêchent ni le débat public, ni les critiques à l'encontre des organes de l'Etat et n'imposent ni amendes excessives, ni dommages-intérêts ou frais de justice d'un montant disproportionné. Des sanctions sévères, notamment des peines d'emprisonnement, ne sont prononcées qu'en cas d'atteinte grave aux droits fondamentaux d'autrui, par exemple en cas d'incitation à la violence ou à la haine.

2.4.3. Les lois visant à lutter contre le discours de haine ou à protéger l'ordre public, la morale publique, les mineurs, la sécurité nationale ou le secret d'Etat et les lois sur la protection des données ne sont pas appliquées d'une manière qui empêche

un débat public. Elles n'imposent de restriction à la liberté d'expression qu'en réponse à un intérêt public impérieux, sont définies aussi étroitement que possible pour répondre à cet intérêt et prévoient des sanctions proportionnées.

3. Le droit à la liberté de réunion et d'association pacifiques

3.1. Chacun est libre d'utiliser des plates-formes internet, telles que les médias sociaux et d'autres TIC, pour s'associer ou créer des associations, en déterminer les objectifs, constituer des syndicats et mener des activités dans les limites prévues par une législation conforme aux normes internationales.

3.2. Les associations sont libres d'utiliser internet pour exercer leur droit à la liberté d'expression et pour participer à des débats publics et politiques.

3.3. Chacun est libre d'utiliser des plates-formes internet, telles que les médias sociaux et d'autres TIC, pour organiser des réunions pacifiques.

3.3. Les mesures appliquées par l'Etat dans le contexte de l'exercice du droit de réunion pacifique, et qui constituent un blocage ou une restriction de plates-formes internet telles que les médias sociaux et d'autres TIC, sont conformes à l'article 11 de la CEDH.

3.4. Toute restriction à l'exercice des droits à la liberté de réunion pacifique et à la liberté d'association sur internet respecte les exigences de l'article 11 de la CEDH, à savoir qu'elle :

- est prévue par la loi, laquelle est accessible, claire, sans ambiguïté et suffisamment précise pour permettre aux personnes de régler leur conduite en conséquence ;

- poursuit un but légitime figurant parmi ceux énumérés de façon exhaustive à l'article 11 de la CEDH ;

- est nécessaire dans une société démocratique et proportionnée au but légitime poursuivi. La restriction répond à un besoin social impérieux. Il existe un juste équilibre entre l'exercice du droit à la liberté de réunion et d'association et les intérêts de la société dans son ensemble. Si une mesure moins intrusive permet d'atteindre le même but, c'est cette mesure qui est appliquée. La restriction est interprétée et appliquée stricto sensu et ne met pas en cause l'essence du droit à la liberté de réunion et d'association.

4. Le droit au respect de la vie privée et familiale

4.1. Protection des données à caractère personnel

4.1.1. Le droit au respect de la vie privée et familiale est garanti conformément à l'article 8 de la CEDH, tel que l'interprète la Cour européenne des droits de l'homme. Toute restriction à ce droit poursuit un des buts légitimes énumérés de façon exhaustive à l'article 8 de la CEDH, est nécessaire dans une société démocratique et proportionnée au but légitime poursuivi.

4.1.2. La loi garantit la protection de toutes les données à caractère personnel, conformément à l'article 8 de la CEDH tel que l'interprète la Cour européenne des droits de l'homme, et à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) dans les Etats qui l'ont ratifiée.

4.1.3. Les données personnelles sont traitées licitement (avec le consentement non-équivoque de la personne concernée ou sur la base de la loi) à des fins légitimes et sans excès au regard des finalités poursuivies, de façon précise et sûre. Ces conditions s'appliquent également au profilage (technique de traitement automatisé des données à caractère personnel qui consiste à collecter et utiliser des informations relatives à une personne donnée en vue de déterminer, d'analyser ou de prévoir ses préférences, comportements et attitudes personnels).

4.1.4. Les personnes ne sont pas soumises à une décision les affectant de manière significative qui serait uniquement fondée sur un traitement automatisé de données, sans que leurs points de vue soient pris en compte. Des procédures efficaces permettent à quiconque d'obtenir, sur demande, des informations sur le traitement de ses données à caractère personnel et la raison de ce traitement, de s'y opposer; d'en obtenir, sur demande, la rectification ou leur effacement, et de consentir au traitement de ses données à caractère personnel ou au profilage, de le refuser ou de retirer son consentement. En cas de non-respect de ces droits, les personnes concernées disposent d'un recours effectif. Les cadres juridiques de protection des données à caractère personnel offrent des garanties suffisantes concernant l'accès à l'information et la liberté d'expression.

4.1.5. La loi définit les obligations des entités publiques et privées au regard du traitement des données à caractère personnel.

4.1.6. Une autorité de contrôle, agissant en totale indépendance et impartialité, veille au respect des cadres juridiques de protection des données.

4.1.7. L'Etat n'interdit pas en droit et en pratique l'anonymat, l'utilisation d'un pseudonyme et la confidentialité des communications privées ou le recours à des technologies de cryptage. Toute atteinte à l'anonymat et à la confidentialité des communications est soumise aux exigences de légalité, de légitimité et de proportionnalité prévues à l'article 8 de la CEDH.

4.2. Surveillance

4.2.1. Les mesures de surveillance prises par les autorités publiques (notamment les services de sécurité) respectent les exigences prévues à l'article 8 de la CEDH et sont soumises à un contrôle effectif, indépendant et impartial.

4.2.2. Les mesures de surveillance sont mises en œuvre dans le respect de la loi qui est claire, précise, accessible et prévisible. La loi prévoit des garanties encadrant l'exercice de pouvoirs discrétionnaires par les autorités publiques et définit donc avec suffisamment de clarté et de précision :

- la nature des infractions qui pourraient entraîner des mesures de surveillance;
- les autorités compétentes chargées d'appliquer les mesures de surveillance, l'étendue et les modalités d'exercice de tout pouvoir de discrétion accordé à ces autorités eu égard au but légitime de la mesure en question ;
- les catégories de personnes susceptibles de faire l'objet de mesures de surveillance ;
- les limitations de durée applicables à ces mesures de surveillance ;
- les procédures applicables à l'examen, à l'utilisation et à la conservation des données collectées dans le cadre de mesures de surveillance ;

- les précautions à prendre lorsque les données collectées dans le cadre de mesures de surveillance sont communiquées à d'autres parties, et les mesures applicables pour assurer la sécurité des données durant la communication ;

- les circonstances justifiant la destruction et l'effacement des données obtenues dans le cadre de mesures de surveillance ;

- les organes chargés de superviser les mesures de surveillance.

4.2.3. Les mesures de surveillance poursuivent un des buts légitimes énumérés de façon exhaustive à l'article 8 de la CEDH, sont nécessaires dans une société démocratique et proportionnées au but légitime poursuivi.

4.2.4. Les mesures de surveillance directement mises en œuvre par des autorités publiques ou par l'intermédiaire d'entités du secteur privé ou encore en collaboration avec ces dernières, sont autorisées par un tribunal indépendant et impartial établi par la loi ou par un autre organisme public indépendant des autorités qui les mettent en œuvre et de l'exécutif.

4.2.5. Les mesures de surveillance directement mises en œuvre par des autorités publiques ou par l'intermédiaire d'entités du secteur privé ou encore en collaboration avec ces dernières n'impliquent pas d'activités susceptibles d'affaiblir les systèmes de cryptage et l'intégrité de l'infrastructure de communication (par exemple l'introduction délibérée de failles et de portes dérobées dans les systèmes de sécurité, d'information et de communication).

4.2.6. Les mesures de surveillance font l'objet d'un contrôle effectif assuré par une instance judiciaire ou sont supervisées par un autre organisme public offrant les meilleures garanties d'impartialité et d'indépendance par rapport aux autorités qui les mettent en œuvre ou à l'exécutif.

4.2.7. La loi garantit à l'organe de contrôle le droit d'accès à toutes les informations utiles à l'accomplissement de son mandat, quel que soit leur niveau de classification. L'accès à l'information par un organe de contrôle s'étend à toutes les informations pertinentes détenues par les autorités publiques, y compris celles fournies par des organes étrangers.

4.2.8. Les organes de contrôle exercent leurs pouvoirs, y compris la recherche et le traitement d'informations classifiées et de données à caractère personnel, d'une façon professionnelle et aux seules fins pour lesquelles ils y sont habilités par la loi, tout en garantissant que ces informations ne seront pas exploitées ou divulguées à des fins autres que ce qui relève de leur mandat.

4.2.9. Dans le cadre de leurs compétences, les organes de contrôle vérifient que les mesures de surveillance prises par les autorités publiques respectent les droits de l'homme, y compris celles prises en collaboration avec des organes étrangers lors de l'échange de données ou de la réalisation d'opérations conjointes.

4.2.10. Les instances judiciaires et les organes de contrôle ont le pouvoir d'annuler et de suspendre les mesures de surveillance appliquées quand elles sont considérées avoir été illégales. Ils ont également le pouvoir de demander l'effacement de toute information obtenue par le recours à ces mesures.

4.2.11. La portée de la législation sur la liberté d'information s'étend aux autorités publiques qui appliquent des mesures de surveillance ainsi qu'à leurs organes de contrôle. Les décisions de ne pas communiquer certains renseignements sont

prises au cas par cas, dument motivées et soumises au contrôle d'un commissaire aux informations/données indépendant. Les organes de contrôle publient une version informative de leurs rapports périodiques et de leurs rapports d'investigation.

5. Voies de recours

5.1. L'Etat veille à ce que les personnes aient accès à des procédures judiciaires ou administratives à même de trancher impartialement leurs réclamations concernant des allégations d'atteintes aux droits de l'homme en ligne, conformément à l'article 6 de la CEDH.

5.2. L'Etat garantit le droit à un recours effectif, conformément à l'article 13 de la CEDH. Cela inclut des mécanismes non judiciaires effectifs, des moyens administratifs ou autres de former recours, par l'intermédiaire par exemple d'institutions nationales de protection des droits de l'homme. Les personnes ne rencontrent aucun obstacle juridique, procédural, financier ou autre d'ordre pratique qui entrave leur accès à un recours effectif.

5.3. L'Etat, en tant que première entité responsable, prend des mesures appropriées pour assurer une protection contre les violations des droits de l'homme sur internet par des acteurs du secteur privé et pour garantir aux personnes concernées l'accès à un recours effectif.

5.4. L'Etat met en œuvre des politiques et des mesures pour encourager tous les acteurs du secteur privé à respecter les droits de l'homme sur internet dans leurs opérations. Pour ce faire, il met notamment en place des mécanismes de plainte efficaces permettant de traiter rapidement les réclamations de personnes dont les droits de l'homme et libertés fondamentales sur internet ont pu être lésés et d'y remédier directement. Ces mécanismes sont légitimes (ils doivent susciter la confiance et répondre du bon déroulement des procédures de réclamation), accessibles (ils sont communiqués aux personnes concernées et aucun obstacle n'entrave leur accès), prévisibles (ils prévoient une procédure clairement établie assortie d'un calendrier indicatif pour chaque étape, et un descriptif précis des types de procédures et d'issues disponibles et des moyens d'en suivre la mise en œuvre), équitables (ils assurent un accès raisonnable aux sources d'information, aux conseils et aux compétences nécessaires à une procédure de réclamation), transparents (ils tiennent les parties informées du cours de la procédure de plainte) et compatibles avec l'article 13 de la CEDH.

Projet d'exposé des motifs du projet de Recommandation CM/Rec__ (2015) ___ du Comité des Ministres aux Etats membres sur la liberté d'internet

Historique et processus

1.Les ministres des Etats participant à la Conférence des ministres du Conseil de l'Europe responsables des médias et de la société de l'information, tenue à Belgrade (Serbie) les 7 et 8 novembre 2013, ont adopté une Résolution sur la liberté de l'internet. Cette résolution invitait le Conseil de l'Europe à continuer de développer, suivant une approche multipartite, la notion de « liberté de l'internet » sur la base des normes adoptées par le Comité des Ministres sur les principes de la gouvernance de l'internet, la neutralité du réseau et l'universalité, l'intégrité et l'ouverture de l'internet.

2. Lors de sa 1185e réunion le 20 novembre 2013, le Comité des Ministres a approuvé le mandat du Comité d'experts sur la circulation transfrontière d'internet et la liberté d'internet (MSI-INT) (CM(2013)131 add final). Aux termes de ce mandat, le MSI-INT est chargé de préparer et soumettre au CDMSI un projet de recommandation sur la liberté d'internet. Par la suite, dans les Décisions du Comité des Ministres adoptées lors de sa 1187e réunion, les 11 et 12 décembre 2013, le Comité des Ministres a chargé le Comité directeur sur les médias et la société de l'information (CDMSI) « de développer, dans une approche multipartite, la notion de "liberté de l'internet" sur la base des normes adoptées par le Comité des Ministres sur les principes de la gouvernance de l'internet, la neutralité du réseau et l'universalité, l'intégrité et l'ouverture de l'internet ».

3. Le MSI-INT a tenu sa première réunion les 17 et 18 mars 2014 à Strasbourg. Tout en constatant que la notion de liberté d'internet est potentiellement vaste, le MSI-INT a décidé de concentrer sa réflexion sur la définition du concept et de l'examiner plus attentivement dans le cadre de ses discussions avec les parties prenantes, selon les besoins, dans le cadre du Dialogue européen sur la gouvernance de l'internet (EuroDIG, 12-13 juin 2014, Berlin) et du Forum sur la gouvernance de l'internet (FGI, 2-5 septembre 2014, Istanbul).
4. Les discussions menées au cours de la deuxième réunion du MSI-INT, les 3 et 4 juillet 2014 à Strasbourg, ont souligné que la valeur ajoutée de cet instrument serait qu'il recommande aux Etats de concevoir la liberté d'internet de façon globale. Le projet de recommandation pourrait être envisagé comme un outil destiné à guider les décideurs et aider les Etats membres à évaluer la situation de la liberté d'internet, ainsi qu'à organiser le débat au niveau international sur le sujet. Le MSI-INT a approuvé un avant-projet de recommandation qui visait à encourager les Etats membres à mettre en œuvre les normes des droits de l'homme en ligne et comprenait une liste d'indicateurs sur la liberté d'internet.

5. Lors de sa réunion de travail, les 23 et 24 octobre 2014 à Strasbourg, le MSI-INT a validé l'approche générale adoptée dans le projet de recommandation au sujet d'une évaluation périodique de la situation de la liberté d'internet au plan national à l'aide des indicateurs définis dans le projet de recommandation. L'objectif est de créer un environnement dans les Etats membres du Conseil de l'Europe qui soit favorable à l'exercice et à la jouissance, sur internet, des droits et des libertés fondamentales. Les indicateurs de la liberté d'internet doivent servir à la mise en œuvre effective des normes relatives aux droits de l'homme. Les participants du secteur privé ont estimé que le projet de recommandation fournira des orientations à la société civile et aux citoyens sur la manière de renforcer leur rôle d'observation de la liberté sur internet. Le CDMSI, lors de sa 7e réunion (18-21 novembre 2014), a pris note de l'avant-projet de recommandation et invité ses membres à envoyer leurs commentaires éventuels au MSI-INT.

6. Au cours de sa troisième réunion, qui a eu lieu les 5 et 6 mars 2015 à Strasbourg, le MSI-INT a discuté en détail du préambule et du dispositif du projet de recommandation. Conformément à la décision du Comité des Ministres appelant à développer la notion de liberté d'internet, suivant une approche multipartite , le MSI-INT a décidé d'organiser des consultations jusqu'à la fin avril 2015. Le MSI-INT a donc décidé de proposer au Bureau du CDMSI d'inviter le Comité directeur pour les droits de l'homme (CDDH), le Comité directeur pour les problèmes criminels (CDPC), le Comité européen de coopération juridique (CDCJ), le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) et le Comité de la Convention sur la cybercriminalité (T-CY) à fournir leurs commentaires. En outre, le projet de recommandation devait être publié sur le site internet du Conseil de l'Europe et les parties prenantes invitées à faire part de leurs commentaires.

7. Suite à l'approbation par le Bureau du CDMSI des propositions du MSI-INT, des consultations multipartites ont été organisées pendant la période du 30 avril au 14 mai 2015. Des membres du CDDH, du CDCJ, du Bureau du T-PD et du TC-Y ont soumis leurs commentaires. Par ailleurs, une trentaine de contributions ont été reçues de différentes régions du monde et de représentants du secteur privé (entreprises de télécommunication et prestataires de services d'accès à internet), d'organisations de la société civile, de la communauté technique et du monde universitaire. Elles saluaient pour la plupart les travaux du Conseil de l'Europe sur le projet de recommandation et contenaient de nombreux commentaires et propositions de changement au projet.
8. Lors de sa 8e réunion (16-19 juin 2015), le CDMSI a pris note des commentaires recueillis au cours des consultations multipartites. Il a soutenu l'approche stratégique globale du projet de recommandation visant à promouvoir la mise en œuvre des normes existantes des droits de l'homme sur internet. Il a décidé d'inviter les délégations à envoyer leurs commentaires au MSI-INT avant le 31 juillet 2015.

9. A sa dernière réunion (7-8 septembre 2015, Strasbourg), le MSI-INT a finalisé ses propositions au CDMSI pour un projet de recommandation du Comité des Ministres CM/Rec(2015)__ aux Etats membres sur la liberté d'internet.

[10. Le CDMSI, lors de sa 9e réunion (8-11 décembre 2015, Strasbourg) a finalisé le projet de recommandation du Comité des Ministres CM/Rec(2015)__ aux Etats membres sur la liberté d'internet et décidé de le transmettre au Comité des Ministres pour adoption éventuelle.]

Commentaires sur la Recommandation CM/Rec (2014)___ du Comité des Ministres aux Etats membres sur la liberté d'internet

Préambule de la Recommandation

11. Le préambule affirme le principe selon lequel les droits de l'homme et les libertés fondamentales s'appliquent à la fois en ligne et hors ligne. La norme essentielle est la CEDH. L'idée centrale du préambule est que la liberté d'internet ne doit pas être considérée comme sélective quant aux droits et aux libertés qui doivent être protégés. Il est nécessaire au contraire d'adopter une approche globale eu égard à l'ensemble des indicateurs.

12. La liberté d'internet est comprise comme l'exercice et la jouissance, sur internet, des droits de l'homme et des libertés fondamentales. Les Etats ont des obligations au regard de la protection et de la promotion des droits de l'homme, conformément à la CEDH. La participation des Etats aux dispositifs de gouvernance de l'internet est considérée nécessaire à la mise en œuvre effective des droits de l'homme et des libertés fondamentales. C'est pourquoi la recommandation mentionne au paragraphe 3 le rôle et les responsabilités des Etats en ce qui concerne les politiques internationales concernant

internet. Ce paragraphe est basé sur la Déclaration du Comité des Ministres sur des principes de la gouvernance de l'internet adoptée en 2011.

13. La recommandation repose sur l'idée que, pour assurer la liberté d'internet, certaines conditions juridiques, économiques et politiques doivent être satisfaites et il appartient aux Etats de le vérifier. C'est pourquoi il est recommandé aux Etats membres d'évaluer la situation en matière de liberté d'internet à l'aide des indicateurs définis sur la base des normes existantes du Conseil de l'Europe. Ce travail d'évaluation leur permettra de déterminer l'état de la mise en œuvre des normes et, lorsque cela est nécessaire, motivera une application meilleure et plus efficace de ces normes. La CEDH et d'autres normes du Conseil de l'Europe offrent des [points de] référence et des comparaisons pour l'évaluation de la liberté d'internet dans chaque pays. Ces normes peuvent donc être conceptualisées comme indicateurs de la liberté d'internet.

14. Dans le dispositif de la recommandation, le Comité des Ministres recommande aux Etats membres de procéder régulièrement à l'évaluation de la mise en œuvre et du respect des normes des droits de l'homme. Les Etats membres sont les mieux placés pour déterminer la fréquence ou la périodicité des exercices d'auto-évaluation et de la préparation de rapports sur la liberté d'internet, au vu de leurs capacités institutionnelles. La décision de communiquer ou non les rapports nationaux sur la liberté d'internet au Conseil de l'Europe est aussi laissée à leur appréciation. Ces rapports pourront contribuer à la réflexion du Secrétaire Général en vue de la préparation de son rapport annuel sur l'état de la démocratie, des droits de l'homme et de l'Etat de droit en Europe. L'objectif est de promouvoir la mise en œuvre des normes existantes et l'échange de bonnes pratiques.

Indicateurs de la liberté d'internet

15. Les indicateurs inclus dans la Recommandation sont conçus pour guider la conduite de l'évaluation qualitative et objective de l'existence d'un environnement favorable à la liberté d'internet dans les Etats membres du Conseil de l'Europe et la préparation de rapports. L'exposé des motifs précise comment ces indicateurs se fondent sur les normes internationales des droits de l'homme. Il suggère en outre des sources de vérification applicables, le cas échéant, aux indicateurs, dont les autorités nationales pourront se servir dans leur évaluation.

1. Un environnement favorable à la liberté d'internet

16. Un principe essentiel des normes du Conseil de l'Europe relatives à l'internet est que les droits de l'homme et les libertés fondamentales s'appliquent à la fois dans les environnements en ligne et hors ligne[2]. La Cour européenne des droits de l'homme a déclaré que « l'internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information : on y trouve des outils essentiels de participation aux activités et débats relatifs à des questions politiques ou d'intérêt public »[3]. Elle a également souligné que l'internet est un important medium où les citoyens exercent leurs droits fondamentaux et que les droits énoncés dans la CEDH s'y appliquent[4]. Le Rapporteur spécial des Nations Unies sur la liberté d'expression a déclaré qu'« en tant que catalyseur de l'exercice du droit à la liberté d'opinion et d'expression, l'internet facilite la réalisation de bien d'autres droits de l'homme »[5].

[2] Voir Déclaration du Comité des Ministres sur des principes de la gouvernance de l'internet, Principe 1 « Droits de l'homme, démocratie et Etat de droit ».
[3] Cour européenne des droits de l'homme, requête n° 3111/10, *Yildirim c. Turquie*, arrêt définitif, 18 mars 2013, paragraphe 54.
[4] *Neij et Sunde Kolmisoppi c. Suède*, requête n° 40397/12, arrêt du 19 février 2013, p. 9.
[5] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, Assemblée générale des Nations Unies, 16 mai 2011, p. 22.

17. L'*Indicateur 1.1.* a pour but de vérifier que l'Etat a bien inscrit ces principes dans son système juridique. Cela peut être fait dans la constitution ou dans d'autres textes de loi portant sur la protection des droits de l'homme ; ces textes constituent par conséquent les sources de vérification pour les évaluations portant sur cet indicateur. Ce dernier n'exige pas que les textes constitutionnels ou autres mentionnent spécifiquement leur application à l'internet, il suffit qu'elle ne soit pas limitée au monde physique, ce qui exclurait la mise en œuvre des normes des droits de l'homme au regard de l'internet. Les traités internationaux des droits de l'homme reconnus par les Etats membres qui ne prévoient pas d'exemptions significatives, ainsi que toute autre forme d'intégration effective des normes internationales des droits de l'homme dans la législation ou les politiques se rapportant à l'internet, sont également des sources de vérification.

18. Les Etats membres devraient examiner la conformité de leurs actions qui portent préjudice au droit à la vie privée, au droit à la liberté d'expression et au droit à la liberté de réunion et d'association avec les articles 8, 10 et 11 de la CEDH. Les sources de vérification de l'*Indicateur 1.2.* sont constituées par les textes de loi et les mesures qui restreignent ces droits et libertés qui doivent être en conformité avec les normes de la CEDH telles qu'interprétées par la Cour européenne des droits de l'homme : toute restriction doit être motivée par l'un des objectifs légitimes envisagés dans la CEDH et être nécessaire et proportionnée dans une société démocratique. Les moyens les moins restrictifs doivent être employés pour atteindre l'objectif légitime.

19. Une autre vérification cherchera si les Etats veillent à ce que les acteurs privés sont en mesure de garantir l'exercice de ces droits et libertés, tout particulièrement les acteurs privés qui gèrent des infrastructures ou des équipements nécessaires à un tel exercice. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme fournissent des directives supplémentaires à cet égard[6]. La Cour européenne des droits de l'homme a jugé que la responsabilité des Etats était engagée pour n'avoir pas protégé leurs citoyens des incidences préjudiciables à leurs droits et libertés découlant d'actes d'entreprises privées[7].

20. Les questions relatives à l'internet sont souvent réglementées par différents instruments juridiques ou politiques. C'est pourquoi il est nécessaire non seulement de coordonner leur élaboration dans un but de cohérence mais aussi d'évaluer l'impact négatif qu'ils peuvent avoir sur l'exercice et la jouissance des droits de l'homme et des libertés fondamentales. Une telle approche, en outre, permettra aux Etats de trouver un équilibre correct entre des droits concurrents. L'*Indicateur 1.3.* demande aux Etats d'analyser l'équilibre atteint entre toute loi ou politique ayant pour effet de restreindre des droits et des libertés et d'autres droits et libertés qui sont protégés, et de vérifier que les critères juridiques appropriés ont bien été appliqués.

21. Les Etats sont aussi tenus de veiller à la prévisibilité de toute loi ou mesure mise en place conformément aux normes et principes établis par la Cour européenne des droits de l'homme dans l'interprétation de la CEDH. Pour assurer cette prévisibilité, il convient de vérifier la conformité des lois et des politiques avec la CEDH avant leur adoption, en s'assurant que les critères de conformité sont pleinement respectés par l'Etat. Tout rapport explicatif ou exposé des motifs pour un projet de législation ou de politique pourra servir ici de source de vérification.

[6] Rapport du Représentant spécial du Secrétaire Général de l'ONU pour les droits de l'homme et les sociétés transnationales et autres sociétés, John Ruggie, 21 mars 2011.

[7] *López Ostra c. Espagne*, requête n° 16798/90, par. 44 à 58 ; *Taşkin et Autres c. Turquie* ; *Fadeyeva c. Fédération de Russie*. Dans l'affaire *Khurshid Mustafa et Tarzibachi c. Suède*, requête n° 23883/06, la Cour a jugé que l'interprétation d'un acte privé (contrat) par un tribunal national engage la responsabilité de l'Etat défendeur, étendant ainsi la protection de l'article 10 aux restrictions imposées par des personnes privées.

22. L'*Indicateur 1.4.* est basé sur le principe de la gouvernance multi-acteurs inclus dans la Déclaration du Comité des Ministres sur des principes de la gouvernance de l'internet. S'appuyant sur la définition de la gouvernance de l'internet, ce principe affirme le caractère multipartite des environnements internet. Il reflète l'idée exprimée par la Déclaration de principes de Genève selon laquelle « Les gouvernements, le secteur privé, la société civile, l'Organisation des Nations Unies, ainsi que d'autres organisations internationales sont investis d'une responsabilité et d'un rôle importants dans l'édification de la société de l'information et, selon le cas, dans les processus de prise de décision. L'édification d'une société de l'information à dimension humaine est une entreprise commune qui requiert une coopération et un partenariat entre toutes les parties prenantes ». Elle souligne également que « La gestion internationale de l'Internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des Etats, du secteur privé, de la société civile et des organisations internationales ».

23. L'exigence de prévisibilité de la loi signifie que les citoyens doivent être en mesure de prévoir les conséquences de son application pour eux-mêmes en tant qu'individus, et que la loi doit être formulée de façon suffisamment claire et précise pour indiquer de manière adéquate aux citoyens les conditions et situations dans lesquelles les autorités ont le droit d'agir. Un processus d'élaboration de la législation ouvert favorise le respect de ce critère.

24. Comme sources de vérification pour cet indicateur, on pourra utiliser toute information - rapports, articles ou autres – sur les activités engagées par les autorités compétentes de l'Etat pour consulter les parties prenantes. Ces activités pourront être des conférences, réunions, séminaires, forums publics, consultations sur des projets de lois ou de politiques, ou toute autre forme de participation des agents publics aux débats publics sur les questions de fond concernant l'internet.

25. L'*Indicateur 1.5.* exige que, lorsqu'elle accorde à l'exécutif ou à un organe de régulation le pouvoir discrétionnaire d'appliquer des mesures restreignant l'exercice ou la jouissance des libertés et des droits fondamentaux, la loi doit prévoir des sauvegardes suffisantes pour assurer l'autonomie et l'indépendance à l'égard d'intérêts politiques ou commerciaux. Les membres des organes de régulation doivent être désignés de manière démocratique et transparente afin de réduire au minimum les ingérences partisanes ou commerciales. Leurs compétences et leurs responsabilités doivent être définies dans la législation et comprendre l'obligation explicite de promouvoir la liberté d'expression, la libre circulation de l'information, le respect de la vie privée et la liberté de réunion et d'association. Tout texte de loi ou autre instrument juridique définissant le rôle, la composition et les compétences de ces organes pourra servir de source de vérification pour cet indicateur.

26. Les utilisateurs d'internet en général doivent être protégés de la cybercriminalité. Cela permettra de créer un environnement sûr où chacun peut exercer ses droits et libertés en toute sécurité, contribuant ainsi à la qualité globale de l'environnement pour la liberté d'internet. La vérification de l'*Indicateur 1.6.* s'appuiera sur toute loi ou mesure pénalisant les atteintes à la confidentialité et à l'intégrité des données et systèmes informatiques, ou définissant les infractions en matière de contenu (pédopornographie, violation du droit d'auteur), d'accès illégal à l'ensemble ou aux composantes d'un système informatique (matériel informatique, éléments d'un système, données conservées, etc.), d'intrusion dans un système informatique (piratage, infiltration ou autres formes d'intrusion) pouvant donner accès à des données confidentielles, d'interférence avec des données informatiques comme les codes malveillants (virus et chevaux de Troie, par exemple), d'interférence avec le fonctionnement d'un système informatique ou de télécommunication par l'introduction, la transmission, l'endommagement, l'effacement, l'altération ou la suppression de données informatiques comme, par exemple, les programmes qui génèrent des attaques par déni de service, les

codes malveillants comme les virus qui empêchent ou entravent gravement le fonctionnement d'un système, ou les programmes qui envoient de grandes quantités de courrier électronique à un destinataire afin de bloquer les fonctions de communication d'un système (pollupostage), et de falsification informatique. Toutes mesures prises pour combattre la cybercriminalité doivent être conformes aux articles 8, 10 et 11 de la CEDH.

27. Les entreprises internet étant les principaux interlocuteurs ou instances avec lesquelles les individus sont en contact pour ce qui concerne l'exercice des droits de l'homme et des libertés fondamentales sur l'internet, leur rôle dans la protection, le respect et la réparation de ces droits est essentiel à la création d'un environnement favorable à l'existence et au développement de la liberté d'internet. C'est pourquoi l'*Indicateur 1.7.* se réfère aux *Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies*. Ces Principes directeurs requièrent des Etats : de faire appliquer des lois tendant à exiger des entreprises qu'elles respectent les droitsde l'homme, ou qui ont cet effet, et, périodiquement, d'évaluer la validité de ces lois et de combler les éventuelles lacunes ; de veiller à ce que les autres lois et politiques régissant la création et la gestion des entreprises, comme le droit des sociétés, n'entravent pas mais favorisent leur respect des droits de l'homme ; de fournir aux entreprises des orientations effectives sur la manière de respecter les droits de l'homme dans toutes leurs activités ; de les inciter à communiquer comment elles gèrent les incidences de leur activité sur les droits de l'homme, et de les y contraindre le cas échéant[8].

28. L'un des principes fondamentaux des Principes directeurs relatifs aux entreprises et aux droits de l'homme est que les entreprises doivent respecter les droits de l'homme. Cela signifie qu'elles doivent éviter de porter atteinte aux droits fondamentaux d'autrui et remédier aux incidences négatives sur ces droits dans lesquelles elles ont une part. La transparence et l'obligation des acteurs du secteur privé de rendre des comptes sont soulignées comme moyens essentiels de faire la preuve de leur responsabilité, de même qu'en faire une promotion active.

29. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme spécifient que les sociétés devraient mettre en place des mécanismes de réclamation accessibles, prévisibles (avec une procédure clairement établie communiquée eu public et assortie d'un calendrier indicatif pour chaque étape, un descriptif précis des types de procédures et de résultats disponibles et des moyens de suivre la mise en œuvre), équitables (assurant un accès aux sources d'information, aux conseils et aux compétences), transparents et en capacité d'offrir des mesures de réparation qui soient pleinement compatibles avec les droits de l'homme internationalement reconnus[9].

30. La vérification de l'Indicateur 1.7. pourra s'appuyer sur toute loi ou politique mettant en œuvre les Principes directeurs décrits ci-dessus, ou tout autre plan d'action ou document stratégique visant à promouvoir la protection des droits de l'homme et des libertés fondamentales par les entreprises.

31. La liberté d'internet comprend aussi des libertés et des droits positifs comme le droit à l'éducation qui est consacré à l'article 2 du Protocole n° 1 à la CEDH. *L'indicateur 1.8*. considère la question de la formation au numérique comme nécessaire à l'exercice des

[8] Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies (A/HRC/17/31), adoptés par le Conseil des droits de l'homme par la Résolution « Les droits de l'homme et les sociétés transnationales et autres entreprises » (A/HRC/RES/17/4).

[9] Voir Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies (A/HRC/17/31), adoptés par le Conseil des droits de l'homme par la Résolution « Les droits de l'homme et les sociétés transnationales et autres entreprises » (A/HRC/RES/17/4), chapitre III, principes 28 à 31.

autres libertés, ainsi que la promotion générale de l'accès à l'internet aux fins d'éducation et d'accès à la culture. La formation au numérique désigne la possibilité pour les citoyens d'obtenir une information de base, une éducation, des connaissances et des compétences afin d'être en mesure d'exercer leurs libertés et droits fondamentaux sur l'internet.

32. Cette idée s'inscrit dans le droit fil des normes du Comité des Ministres du Conseil de l'Europe qui promeuvent la maîtrise de l'informatique comme condition essentielle à l'accès à l'information, à l'exercice des droits culturels et au droit à l'éducation[10]. La Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public d'internet encourage la création, l'utilisation de contenus pédagogiques, culturels et scientifiques sous forme numérique et leur accès, afin de veiller à ce que toutes les cultures puissent s'exprimer et accéder à internet dans toutes les langues, y compris les langues autochtones[11]. Les citoyens doivent avoir librement accès sur internet aux œuvres culturelles et aux travaux de recherche financés sur fonds publics[12]. Il conviendrait à cet égard d'assurer, dans des limites raisonnables, un accès libre aux éléments du patrimoine numérique passés dans le domaine public. Des conditions à l'accès au savoir peuvent être établies dans des cas spécifiques afin de rémunérer les détenteurs de droits pour le travail accompli, dans les limites admissibles du droit à la protection de la propriété intellectuelle.

33. La Recommandation CM/Rec(2014)6 du Comité des Ministres aux Etats membres sur un Guide des droits de l'homme pour les utilisateurs d'internet contient également des indications utiles sur les droits de l'homme et les libertés fondamentales des utilisateurs d'internet en ligne, ainsi que sur leurs responsabilités quant au respect des droits d'autrui. La vérification de l'*Indicateur 1.8.* sera l'existence de programmes de formation au numérique financés par l'Etat, et d'autres programmes visant à promouvoir l'accès à la culture et au savoir via internet. La mise en œuvre du Guide des droits de l'homme pour les utilisateurs d'internet du Conseil de l'Europe sera un autre critère de vérification.

2. Le droit à la liberté d'expression

2.1. Liberté d'accès à internet

34. La jurisprudence de la Cour européenne des droits de l'homme affirme que l'article 10 s'applique pleinement à l'internet, puisque toute restriction qui lui est imposée porte nécessairement atteinte au droit de recevoir et de communiquer des informations[13]. Par conséquent, l'accès à l'infrastructure est une condition préalable nécessaire à la réalisation de l'objectif de garantir la liberté d'expression[14]. Le Comité des Ministres du Conseil de l'Europe a reconnu à cet égard que la protection de l'infrastructure de

[10] Déclaration du Comité des Ministres sur les droits de l'homme et l'état de droit dans la société de l'information, CM(2005)56 final, 13 mai 2005.
[11] Voir aussi ci-dessus note 8, CM/Rec(2007)16, Section IV.
[12] *Ibid*.
[13] *Yildirim c. Turquie*, requête n° 3111/10, 18 mars 2013.
[14] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, Assemblée générale des Nations Unies, 16 mai 2011, section 85 : « L'internet est devenu un outil indispensable pour la réalisation de toute une série de droits fondamentaux, pour combattre l'inégalité et pour accélérer le développement et le progrès humain. Assurer un accès universel à l'internet devrait donc devenir une priorité pour tous les Etats. Tout Etat devrait développer une politique concrète et efficace, en consultation avec tous les segments de la société, y compris le secteur privé et les ministères gouvernementaux concernés, afin de faire en sorte qu'internet soit largement disponible, accessible et abordable pour tous les groupes de la population ».
[14] Voir plus haut note 2, par. 50. Voir aussi *Autronic AG c. Suisse* (requête n° 12726/87). Dans l'affaire *Khurshid Mustafa et Tarzibachi c. Suède* (requête n° 23883/06), la Cour a jugé que l'interprétation d'un acte privé (contrat) par un tribunal national engage la responsabilité de l'Etat défendeur, étendant ainsi la protection de l'article 10 aux restrictions imposées par des personnes privées.
[14] Yildirim c. Turquie, paragraphe 53.

l'internet doit être une priorité[15]. Afin de garantir la possibilité pour tous les citoyens d'avoir accès à l'internet, l'Etat devrait mettre en œuvre des politiques infrastructurelles pour assurer qu'il est disponible, accessible et abordable à tous les groupes de la population et en promouvoir le principe d'universalité[16].

35. L'*Indicateur 2.1.1.* porte sur l'accès à internet et les modalités de connexion des abonnés. Il concerne l'universalité de l'accès dans toutes les régions et parties de l'Etat, quelle que soit la technologie utilisée pour le fournir Les actions ou mesures positives qui peuvent être prises par les pouvoirs publics pour garantir que tout un chacun soit connecté constituent un autre aspect de la question de l'accès à internet. La valeur de service public de l'internet est comprise comme « le fait pour les personnes de compter de manière significative sur l'internet comme un outil essentiel pour leurs activités quotidiennes (communication, information, savoir, transactions commerciales) et (…) l'attente légitime qui en découle que les services de l'Internet soient accessibles et abordables financièrement, sécurisés, fiables et continus »[17].

36. La vérification de cet indicateur s'appuiera sur les actions ou les mesures positives prises par les pouvoirs publics pour assurer que tous les citoyens sont en mesure d'obtenir une connexion à internet, par exemple des lois ou politiques sur l'universalité de l'accès à internet, en y incluant l'étendue géographique de l'infrastructure du réseau. Des données chiffrées pourront être recueillies à partir de rapports ou d'études sur l'accessibilité d'internet et la couverture de l'infrastructure, ou en analysant les initiatives, programmes ou investissements qui la concernent.

37. L'*Indicateur 2.1.2.* est basé sur la Recommandation CM/Rec (2007)16 du Comité des Ministres du Conseil de l'Europe aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'internet[18]. Les pouvoirs publics devraient s'efforcer raisonnablement de faciliter l'accès à l'internet de certaines catégories de personnes comme de celles vivant dans des zones isolées ou les personnes handicapées. C'est ce qui découle du principe de service universel communautaire énoncé dans la Recommandation N° R(99)14 du Comité des Ministres relative aux nouveaux services de communication et d'information[19]. En vertu de ce principe, les personnes vivant dans des régions rurales ou géographiquement isolées, les personnes à bas revenu et les personnes handicapées ou présentant des besoins particuliers sont en droit d'attendre que les pouvoirs publics adoptent des mesures spécifiques pour leur assurer l' à l'internet.

38. L'*Indicateur 2.1.3* est basé sur le principe du service universel communautaire énoncé par la Recommandation N° R(99)14 du Comité des Ministres relative aux nouveaux services de communication et d'information. Ce principe fait valoir que les personnes vivant dans des zones rurales ou géographiquement isolées, les personnes à bas revenu et les personnes handicapées ou présentant des besoins particuliers sont en droit d'attendre des pouvoirs publics qu'ils adoptent des mesures spécifiques pour faciliter leur accès à l'internet. L'Etat devrait engager des efforts raisonnables pour faciliter l'accès à l'internet de catégories particulières d'individus, comme les personnes vivant dans des zones isolées ou les personnes handicapées. Cet indicateur s'appuie également sur le principe de non-discrimination inscrit à l'article 14 de la CEDH.

---

[15] Recommandation CM/Rec (2007) 16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'internet, adoptée par le Comité des Ministres le 7 novembre 2007 lors de la 1010e réunion des Délégués des Ministres.

[16] Recommandation CM/Rec(2011)8 du Comité des Ministres aux Etats membres sur la protection et la promotion de l'universalité, de l'intégrité et de l'ouverture de l'internet.

[17] Recommandation CM/Rec(2007)16, section II.

[18] Recommandation CM/Rec(2007)16, section II.

[19] CM/Rec(2007)16, annexe, section II ; Recommandation n° R(99)14 du Comité des Ministres aux Etats membres sur le service universel communautaire relatif aux nouveaux services de communication et d'information, Principe 1.

39. Cet indicateur a pour but de vérifier les efforts engagés par l'Etat pour assurer l'accès à l'internet des personnes vulnérables, comme les personnes handicapées, et des groupes minoritaires. Des données chiffrées à ce sujet pourront être obtenues à partir des rapports sur l'accessibilité de l'internet, notamment des initiatives ou des programmes d'aide à l'accès à l'internet des personnes handicapées et des minorités linguistiques.

40. L'*Indicateur 2.1.4* se fonde sur la jurisprudence de la Cour européenne des droits de l'homme, notamment en ce qui concerne les normes relatives à l'Etat de droit et au caractère proportionné des mesures prises par les pouvoirs publics qui restreignent le droit à la liberté d'expression. Lorsque de telles mesures sont prises, il est nécessaire qu'existe un cadre juridique garantissant à la fois un contrôle rigoureux de la portée des interdictions et un contrôle judiciaire efficace afin d'empêcher tout abus de pouvoir. Ce cadre doit aussi prévoir obligatoirement l'examen par les tribunaux de la proportionnalité des mesures. Un contrôle judiciaire efficace implique en outre de déterminer si l'adoption de mesures moins restrictives est possible[20]. Une interdiction totale d'accès à l'internet, par exemple sous la forme d'une mesure rendant les réseaux inaccessibles ou perturbant leur fonctionnement, est considérée comme incompatible avec ces critères. Cet indicateur doit aussi prendre en compte la possibilité que l'infrastructure soit complètement inaccessible à un groupe de la population ou dans une zone géographique donnée.

41. La vérification positive que les critères de cet indicateur sont satisfaits se basera sur tout texte de loi interdisant explicitement toute interdiction générale d'accès à l'internet. Les rapports de transparence sur la disponibilité du réseau émanant des régulateurs, des prestataires de services internet ou d'organes non gouvernementaux[21] seront des sources de vérification supplémentaires. Tout élément ou rapport technique indiquant que l'accès à l'internet est interdit ou régulièrement non disponible pour la population d'un pays ou de zones ou régions spécifiques entraînera une évaluation négative.

42. Les *Indicateurs 2.1.5 à 2.1.8.* portent spécifiquement sur les situations où des individus sont déconnectés d'internet en application d'une mesure décidée par les pouvoirs publics ou par un prestataire d'accès. Ces indicateurs ont pour but de vérifier que ces déconnexions sont compatibles avec l'article 10 de la CEDH. Une mesure de déconnexion d'un individu de l'internet a, en effet, un impact disproportionné sur le droit d'accès à l'information et sur la liberté d'expression, car elle rend inaccessibles de grandes quantités d'information. Bien que l'accès à l'internet ne soit pas encore formellement reconnu comme un droit fondamental (étant donné les différences qui existent entre les contextes nationaux, en particulier du point de vue de la législation et des politiques),il est considéré comme une condition nécessaire à l'exercice de la liberté d'expression et d'autres droits et libertés[22]. Par conséquent, couper l'accès d'un utilisateur à internet pourrait avoir des effets préjudiciables à l'exercice de ses droits et libertés, voire être assimilé à la restriction de son droit à la liberté d'expression, y compris le droit de recevoir et de communiquer des informations[23].

---

[20] *Yildirim c Turquie*, requête n° 3111/10, 18 mars 2013, par. 64 à 70.

[21] Voir, par exemple, le rapport de Freedom House intitulé « Freedom on the Net, a global assessment of Internet and digital media » (2013).

[22] 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, a souligné que « l'internet est devenu un outil indispensable pour la réalisation de toute une série de droits fondamentaux, pour combattre l'inégalité et pour accélérer le développement et le progrès humain. Assurer un accès universel à l'internet devrait donc devenir une priorité pour tous les Etats. Tout Etat devrait développer une politique concrète et efficace, en consultation avec des personnes appartenant à tous les segments de la société, y compris le secteur privé et les ministères gouvernementaux concernés, afin de faire en sorte qu'internet soit largement disponible, accessible et abordable pour tous les groupes de la population ». « En tant que catalyseur de l'exerce du droit à la liberté d'opinion et d'expression par les individus, l'internet rend possible la réalisation de bien d'autres droits de l'homme ».
Voir http://www2.ohchr.org/english/bodies/hrcouncil/docs/ 17session/a.hrc.17.27_en.pdf

[23] Dans une décision de juin 2009, le Conseil constitutionnel français a statué que la déconnexion peut constituer une restriction du droit à la liberté d'expression, y compris le droit de recevoir et de communiquer

43. Cela toutefois ne doit pas être compris comme empêchant l'application légitime de mesures de déconnexion telles que celles qui découlent d'obligations contractuelles. Les consommateurs qui ne paient pas leur service peuvent voir leur accès à internet interrompu. Une telle mesure devrait néanmoins être de dernier ressort. Les enfants peuvent par ailleurs se voir privés de l'accès à internet au titre de l'exercice de l'autorité parentale sur leur utilisation d'internet, selon leur âge et leur degré de maturité Enfin, l'Etat peut imposer des mesures de déconnexion dans les établissements pénitentiaires, en veillant à la conformité de ces mesures avec l'article 10 de la CEDH.

44. Tout citoyen, dans l'exercice de son droit à un jugement équitable, devrait pouvoir demander un réexamen des mesures de déconnexion par une autorité administrative ou judiciaire compétente. Dans le cas où la décision de couper l'accès à internet n'est pas prise par un tribunal[24], les utilisateurs d'internet devraient disposer de moyens de recours efficaces à l'encontre de cette décision, conformément à l'article 6 de la CEDH.

45. La vérification de cet indicateur pourra s'appuyer sur les rapports d'organisations non gouvernementales comme Article 19, le Center for Democracy and Technology[25], l'Electronic Frontier Foundation ou Freedom House.

2.2. Liberté d'opinion et droit de recevoir et de communiquer des informations

46. Les *Indicateurs 2.2.1. et 2.2.2* portent sur la législation et les politiques des Etats concernant les contenus disponibles ou diffusés à partir de plateformes internet et sur la conformité à l'article 10 de la CEDH. Dans le contexte d'internet, le droit de recevoir et de communiquer des informations, inscrit à l'article 10 de la CEDH, s'applique au téléchargement en amont (communication) de contenus, ainsi qu'au téléchargement en aval ou à d'autres formes d'accès aux contenus[26], et à l'utilisation de services, y compris de façon anonyme[27]. Le Comité des Ministres du Conseil de l'Europe a affirmé que tout utilisateur d'internet doit disposer de l'accès le plus large possible aux contenus, applications et services de son choix sur internet, que ceux-ci soient gratuits ou non, au moyen des dispositifs qui lui conviennent. Les utilisateurs d'internet doivent être libres d'exprimer leurs convictions politiques, ainsi que leurs convictions religieuses et non religieuses.

47. Ce dernier point correspond à l'exercice du droit à la liberté de pensée, de conscience et de religion, tel que consacré par l'article 9 de la CEDH. La liberté d'expression vaut non seulement pour les « informations » ou « idées » accueillies favorablement ou considérées comme inoffensives ou indifférentes mais aussi pour celles qui heurtent, choquent ou inquiètent[28]. La Cour a affirmé que l'exercice effectif du droit à la liberté d'expression peut également requérir des mesures positives de protection jusque dans les relations entre individus. La responsabilité de l'Etat peut être engagée s'il n'édicte pas la législation interne appropriée[29].

---

des informations, et partant qu'une décision de déconnexion de l'internet ne peut être prise que par un tribunal et non par un organe administratif ou tout autre acteur public ou privé (Décision n° 2009-580 du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet).

[24] Des exemples de déconnexion en l'absence d'une décision d'un tribunal sont cités dans le Rapport du Rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, Assemblée Générale des Nations Unies, 16 mai 2011, sections 29 et 30.

[25] Par exemple le rapport du Centre for Democracy and Technology intitulé « Regardless of frontiers : The international right to freedom of expression in the digital age » (2011).

[26] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet.

[27] Déclaration du Comité des Ministres sur la liberté de la communication sur l'internet, 28 mai 2003, Principe 7.

[28] *Handyside c. Royaume-Uni*, arrêt du 7 décembre 1976, série A n° 24, par. 49.

[29] Vgt Verein gegen Tierfabriken c. Suisse, requête n° 24699/94, par. 45.

48. Cet indicateur sera satisfait dès lors que la législation ou les mesures prévoyant des restrictions de l'accès à des contenus, des plateformes ou des services sur internet incluent des dispositions spécifiques visant à sauvegarder le droit à la liberté d'expression. Il vise en particulier les restrictions imposées, par exemple, au moyen de blocage ou de filtrage automatisé de contenus via l'infrastructure d'internet (par des prestataires de services internet ou d'autres types de fournisseurs de contenus ou de services). La vérification pourra s'appuyer sur les rapports d'organisations internationales des droits de l'homme comme ceux du Représentant de l'OSCE pour la liberté des médias, de l'ONU ou de l'UE.

49. L'*Indicateur 2.2.3.* a pour but de vérifier que la législation ou les politiques contiennent des sauvegardes suffisantes contre les mesures de restriction abusives, notamment en définissant de façon claire et précise leur champ d'application et en prévoyant des procédures efficaces de contrôle par un tribunal ou un autre organe juridictionnel indépendant[30]. Il porte également sur le caractère proportionné des décisions de blocage ou de filtrage ou d'autres mesures restrictives imposées par un tribunal ou un organe administratif indépendant. Cet indicateur devra être évalué en conjonction avec les indicateurs décrits dans la section 2.4.

50. Cet indicateur se base sur la jurisprudence de la Cour européenne des droits de l'homme qui énonce que le blocage ou le filtrage de l'accès à internet ou de contenus font partie des formes de restriction ou d'interférence pouvant mettre en cause la liberté d'expression[31]. Il devrait y avoir une surveillance stricte de la portée du blocage et un contrôle juridictionnel effectif afin d'empêcher tout abus de pouvoir. Ce dernier devrait évaluer les intérêts concurrents en jeu, ménager un équilibre entre eux et déterminer si une mesure de moins grande portée pourrait être envisagée pour bloquer l'accès à un contenu spécifique d'internet. Les principes généraux en matière de blocage et de filtrage établis dans la jurisprudence de la Cour ont été intégrés aux normes adoptées par le Comité des Ministres[32].

51. Les Etats devraient veiller à ce que tous les filtres soient évalués avant et pendant leur mise en œuvre, afin de vérifier que les effets du filtrage sont en adéquation avec l'objectif de la restriction et donc nécessaires dans une société démocratique, afin d'éviter tout blocage injustifié de contenus[33]. Les mesures prises pour bloquer des contenus particuliers ne doivent pas être utilisées arbitrairement comme moyen d'opérer un blocage général de l'information sur internet. Elles ne doivent pas avoir d'effets collatéraux et rendre inaccessibles de grandes quantités d'information en restreignant ainsi de façon substantielle les droits des utilisateurs d'internet[34]. Elles doivent en outre être prescrites par la loi.

52. Les restrictions de l'accès à internet comme les mesures de blocage et de filtrage doivent viser des contenus clairement identifiables et être basées sur une décision concernant la légalité de ces contenus rendue par une autorité nationale compétente, conformément aux normes de l'article 6 de la CEDH. Cette décision, en outre, doit pouvoir être réexaminée par un tribunal ou un organe de régulation indépendant et impartial[35]. Les normes et principes susmentionnés n'empêchent pas la mise en place de

[30] Cour européenne des droits de l'homme, requête n° 3111/10, *Yildirim c. Turquie*, arrêt définitif, 18 mars 2013, par. 64.
[31] Cour européenne des droits de l'homme, requête n° 3111/10, *Yildirim c. Turquie*, arrêt définitif, 18 mars 2013, par. 69.
[32] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, voir annexe, partie III, ii.
[33] *Ibid*., CM/Rec(2008)6, voir annexe, partie III, iv.
[34] Comité des Ministres, Déclaration sur la liberté de la communication sur l'internet ; *Yildirim c. Turquie*, paragraphes 52 et 66 à 68.
[35] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, voir annexe, partie III, ii.

filtres pour protéger les mineurs dans certains lieux spécifiques où ils ont accès à internet, comme les écoles et les bibliothèques[36].

53. L'*Indicateur 2.2.3.* a pour but d'évaluer le fondement juridique des méthodes technologiques utilisées pour imposer des restrictions à contenus sur internet. Le Comité des Ministres a souligné que « le droit des utilisateurs à accéder à l'information et à la diffuser en ligne, ainsi que le développement de nouveaux outils et services, pourraient être défavorablement affectés par une gestion non transparente du trafic, une discrimination à l'égard des contenus et des services ou des entraves à la connectivité des appareils »[37]. Le Comité a affirmé son engagement en faveur du principe de la neutralité du réseau, afin que tout usager puisse disposer de l'accès le plus large possible aux contenus, applications et services de son choix sur internet, que ceux-ci gratuits ou non, au moyen des dispositifs qui lui conviennent. Ce principe général s'applique quels que soient l'infrastructure ou le réseau utilisés pour la connexion internet.

54. Les exceptions à ce principe ne devraient être envisagées qu'avec une grande circonspection et être motivées par un intérêt public majeur[38]. A cet égard, les Etats membres attentifs aux dispositions de l'article 10 de la Convention européenne des droits de l'homme et à la jurisprudence pertinente de la Cour européenne des droits de l'homme pourront également juger utile de se référer aux Lignes directrices incluses dans la Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet.

55. La vérification s'appuiera sur toute loi, réglementation ou politique définissant les conditions de blocage et de filtrage d'internet et de gestion du trafic d'internet. Les rapports des autorités de régulation dans le domaine des télécommunications pourront aussi servir de sources de vérification.

56. L'*Indicateur 2.2.4.* examine la conformité avec l'article 6 de la CEDH sur le droit à un procès équitable en cas d'imposition de restrictions à des contenus sur internet. Les Etats, dans le cadre de leurs obligations positives de protéger les particuliers contre les violations des droits de l'homme par des entreprises privées, doivent prendre les mesures nécessaires pour assurer que, lorsque cela se produit, les victimes peuvent avoir accès à des mécanismes judiciaires et non judiciaires. Des voies de recours spécifiques doivent être ouvertes aux individus pour contester les restrictions imposées à leurs droits, y compris la durée de la procédure de détermination de ces droits[39]. Elles peuvent être du ressort d'une autorité publique dotée de compétences et offrant des garanties procédurales permettant de déterminer si tel ou tel moyen de réparation particulier est efficace[40]. Cette autorité ne doit pas nécessairement être une autorité judiciaire, mais elle doit présenter des garanties d'indépendance et d'impartialité.

58. Les Etats devraient aussi veiller à ce que les acteurs privés chargés d'appliquer les restrictions d'accès à internet mettent en place des mécanismes de réclamation ou d'appel. Ces mécanismes devraient être accessibles, prévisibles (prévoyant une procédure clairement établie, portée à la connaissance du public et assortie d'un calendrier indicatif pour chaque étape, un descriptif précis des types de procédures et d'issues possibles, et des moyens de suivre la mise en œuvre), équitables (assurant un accès aux sources d'information, aux conseils et aux compétences), transparents et

[36] Déclaration sur la liberté de la communication sur l'internet, Principe 3.
[37] Déclaration du Comité des Ministres sur la neutralité du réseau (adoptée par le Comité des Ministres le 29 septembre 2010 lors de la 1094e réunion des Délégués des Ministres).
[38] *Ibid*.
[39] *Kudla c. Pologne*, REQUETE N° 30210/96, par. 157.
[40] *Silver et Autres c. Royaume-Uni*, requêtes n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, par. 113 ; *Kaya c. Turquie*, requête n° 22729/93, par. 106.

capables d'offrir directement aux individus des réparations qui soient pleinement compatibles avec les normes internationales des droits de l'homme. Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme fournissent aussi des orientations utiles à ce sujet[41].

59. L'*Indicateur 2.2.5.* porte sur la transparence de l'action ou des mesures des pouvoirs publics au regard de l'imposition d'une restriction quelconque. Il est important que les usagers d'internet puissent les contester . Les Etats devraient être attentifs à informer les usagers d'internet (à la fois ceux qui accèdent à l'information et ceux qui la diffusent) et faire en sorte qu'il soit possible de contester toute restriction imposée. Ils devraient fournir des informations sur le moment où le filtrage a été activé et expliquer pourquoi tel ou tel contenu a été filtré, afin que les usagers d'internet puissent comprendre comment et selon quels critères le filtrage opère (par exemple listes noires, listes blanches, blocage de mots clés, classement du contenu, désindexation ou filtrage de certains sites web ou contenus spécifiques par les moteurs de recherche). Des informations devraient aussi être mises à disposition sur les moyens de contourner manuellement un filtre actif, y compris les coordonnées du service à contacter[42].

60. Les utilisateurs devraient avoir accès à des informations claires et transparentes sur les moyens de recours à leur disposition. Ces informations pourraient être incluses dans les conditions d'utilisation du service ou d'autres lignes directrices et politiques des fournisseurs d'accès/de services internet. Les utilisateurs devraient pouvoir solliciter des informations et demander réparation. Ils devraient disposer de voies de recours et de réparation facilement accessibles, dont la suspension des filtres, lorsqu'un usager affirme qu'un contenu a été bloqué de façon injustifiée. Cela pourra être vérifié au moyen de l'information accessible au public sur le blocage de contenus, ainsi qu'en utilisant des rapports d'organisations non gouvernementales comme Freedom House[43].

2.3. Liberté des médias

61. L'*Indicateur 2.3.1.* porte sur la liberté des médias qui est le corollaire de la liberté d'expression. Ces libertés sont indispensables à une démocratie et à des processus démocratiques authentiques. La liberté et l'indépendance éditoriales sont des composantes essentielles de la liberté des médias[44], et les Etats ont le devoir de leur garantir la possibilité de publier des informations en toute indépendance, sans aucune ingérence. Cet indicateur permet de vérifier que cette garantie est maintenue dans le contexte d'internet où la notion de ce qui constitue un « média » évolue. En 2011, le Comité des Ministres a adopté une nouvelle conception des médias[45], qui englobe tous les acteurs impliqués dans la production et la diffusion d'informations.

62. La vérification de cet indicateur reposera sur l'existence d'une législation ou d'une politique qui garantit aux médias et aux nouveaux acteurs des médias la liberté de produire et de diffuser des contenus et des informations sans ingérence. Les rapports de la société civile ou d'organisations indépendantes concernant des cas documentés d'ingérence dans le processus de décision éditorial, comme les rapports de l'OSCE sur la liberté des médias[46], les rapports de Reporters sans frontières sur les « ennemis d'internet »[47], les rapports d'Index on Censorship sur la liberté des médias[48] et les

[41] Rapport du Représentant spécial du Secrétaire Général de l'ONU pour les droits de l'homme et les sociétés transnationales et autres sociétés, John Ruggie, 21 mars 2011.
[42] Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, voir annexe I.i.
[43] *Ibid*., « Freedom on the Net, a global assessment of Internet and digital media », Freedom House (2013).
[44] Recommandation CM/Rec(2011)7 du Comité des Ministres aux Etats membres sur une nouvelle conception des médias.
[45] Ibid.
[46] Voir, par exemple, Représentante de l'OSCE pour la liberté des médias, Dunja Mijatović, Regular Report to the Permanent Council for the period from 19 June through 26 November 2014, p. 8 et p. 36.
[47] Voir, par exemple, Reporters Without Borders (2012), Enemies of the Internet, 13 mars 2012.

rapports d'Article 19 et de Freedom House, pourront également servir de sources de vérification.

63. L'*Indicateur 2.3.1.* a pour but de vérifier que l'octroi des licences ou des autorisations nécessaires pour devenir un acteur des médias sur internet repose uniquement sur l'aptitude à créer une entreprise et n'est pas influencé par des considérations politiques.

64. Cet indicateur repose sur la Recommandation du Comité des Ministres aux Etats membres sur une nouvelle conception des médias qui conseille d'«évaluer la nécessité d'interventions pour tous les acteurs fournissant des services ou des produits dans l'écosystème médiatique, pour garantir à toute personne le droit de chercher, de recevoir et de transmettre des informations conformément à l'article 10 de la Convention européenne des droits de l'homme, et pour étendre à ces acteurs les garanties applicables contre les ingérences susceptibles de porter atteinte aux droits consacrés par l'article 10, notamment dans des situations risquant d'aboutir à une autolimitation et à une autocensure injustifiées ». Cette recommandation déclare également : « Etant entendu que la réglementation des médias, qui est une forme d'ingérence, devrait respecter les critères de nécessité stricte et d'intervention minimale, les cadres réglementaires spécifiques devraient répondre aux besoins de protéger les médias contre toute ingérence (reconnaissance des prérogatives, droits et privilèges au-delà du droit général, ou encadrement de leur exercice), de gérer des ressources limitées (pour assurer le pluralisme des médias et la diversité du contenu – voir article 10, paragraphe 1 *in fine,* de la Convention européenne des droits de l'homme) et de tenir compte des responsabilités des médias (dans les limites strictes fixées à l'article 10, paragraphe 2, de la Convention et la jurisprudence de la Cour européenne des droits de l'homme y relative) ».

65. Cet indicateur se fonde également sur la Résolution 1636 (2008) « Indicateurs pour les médias dans une démocratie » de l'Assemblée parlementaire du Conseil de l'Europe qui déclare que « les autorités de régulation du secteur de la radiodiffusion doivent fonctionner de manière impartiale et efficace, par exemple à l'occasion d'octroi de licences. Pour l'octroi d'une licence aux médias imprimés ou à internet, l'Etat devrait limiter ses exigences à un simple numéro d'identification fiscale ou à une inscription au registre du commerce ».

66. En outre, le Comité des Ministres a déclaré en 2011 que les plateformes de médias gérées par des exploitants privés doivent pouvoir fonctionner librement[49]. Les citoyens s'appuient sur les réseaux sociaux, les blogs, les sites internet et les applications en ligne pour avoir accès à des informations et les échanger, publier des contenus, interagir, communiquer et coopérer les uns avec les autres. Ces plateformes deviennent une partie intégrante du nouvel écosystème médiatique. Bien que gérées par des exploitants privés, elles occupent une place significative dans la sphère publique en facilitant les débats sur les questions d'intérêt général ; dans certains cas, elles peuvent, à l'instar des médias traditionnels, jouer un rôle de « chien de garde » social et elles ont démontré leur utilité en produisant des changements positifs dans le monde réel.

67. La vérification s'appuiera ici sur les rapports internationaux concernant la liberté des médias, comme ceux du Commissaire aux droits de l'homme du Conseil de l'Europe et de l'OSCE[50], ainsi que sur le rapport du Parlement européen sur la liberté des médias

[48] Index on Censorship : http://mediafreedom.ushahidi.com/reports.
[49] Déclaration du Comité des Ministres sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plateformes internet gérées par des exploitants privés et les prestataires de services en ligne, décembre 2011.
[50] Voir, par exemple, Représentante de l'OSCE pour la liberté des médias, Dunja Mijatović, Regular Report to the Permanent Council for the period from 19 June through 26 November 2014, p. 36.

dans les Balkans occidentaux[51] et les rapports d'Article 19, de Freedom House, d'Index on Censorship et de Reporters sans frontières.

68. L'*Indicateur 2.3.3.* a pour but de vérifier que l'Etat ne s'ingère pas dans le travail des journalistes et d'autres personnes remplissant un rôle de « chien de garde » public via des médias en ligne. Les obstacles mis en place par l'Etat pour empêcher l'accès aux informations d'intérêt public peuvent, en effet, non seulement décourager les journalistes et d'autres acteurs des nouveaux médias de remplir un tel rôle[52] mais aussi nuire à leur sûreté et à leur sécurité, ainsi qu'à leur aptitude à informer le public. Les attaques contre les journalistes et les autres acteurs des nouveaux médias constituent des violations particulièrement graves des droits de l'homme parce que non seulement elles visent des personnes précises mais en outre, elles privent les autres de leur droit de recevoir des informations, restreignant par là même le débat public qui est au cœur de la démocratie pluraliste.

69. La Cour européenne des droits de l'homme a jugé que le rôle joué par les journalistes dans une société démocratique leur confère certaines protections accrues au titre de l'article 10 de la CEDH. Les Etats ont le devoir de créer un environnement favorable à la participation de tous au débat public, en leur donnant la possibilité d'exprimer sans crainte leurs opinions et leurs idées[53]. A cette fin, ils doivent non seulement s'abstenir de toute ingérence dans la liberté d'expression des individus, mais sont aussi positivement tenus de protéger leur droit à la liberté d'expression contre le risque d'attaques, y compris de la part de personnes privées, en mettant en place un système de protection efficace.

70. Le Comité des Ministres a invité instamment les Etats membres à s'acquitter de leurs obligations positives de protéger les journalistes et les autres acteurs des médias contre toute forme d'attaque et de mettre fin à l'impunité, conformément à la CEDH et compte tenu de la jurisprudence de la Cour européenne des droits de l'homme. Dans ce contexte, il a également invité les Etats membres à réexaminer au moins tous les deux ans la conformité de leur législation et de leurs pratiques internes avec ces obligations. Ils ont aussi été encouragés à contribuer aux efforts concertés engagés au niveau international pour renforcer la protection des journalistes et des autres acteurs des médias, en assurant la pleine conformité de leurs cadres juridiques et pratiques de contrôle de l'application de la loi avec les normes internationales des droits de l'homme. La mise en œuvre du Plan d'action des Nations Unies sur la sécurité des journalistes et la question de l'impunité est une nécessité urgente et vitale[54].

71. La vérification de cet indicateur pourra s'appuyer soit sur des cas documentés de menaces et de harcèlement en ligne, soit sur des cas documentés d'enquête sur des journalistes et de poursuites en relation avec l'exercice de leur profession en ligne, comme par exemple ceux cités dans les rapports périodiques de la Représentante de l'OSCE pour la liberté des médias[55] ou dans les rapports de Reporters sans frontières publiés sous le titre « Enemies of the Internet »[56].

---

[51] Parlement européen, Direction générale des politiques externes, Freedom of the Media in the Western Balkans : http://www.europarl.europa.eu/RegData/etudes/STUD/2014/534982/EXPO_STU%282014%29534982_EN.pdf

[52] Voir à cet égard l'affaire *Társaság a Szabadságjogokért c. Hongrie*, requête n° 37374/05, arrêt du 14 avril 2009, paragraphe 38.

[53] *Dink c. Turquie*, requêtes n° 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09, arrêt du 14 septembre 2010, paragraphe 137.

[54] Déclaration du Comité des Ministres relative à la protection du journalisme et à la sécurité des journalistes et des autres acteurs des médias (adoptée le 30 avril 2014 lors de la 1198e réunion des Délégués des Ministres).

[55] Voir, par exemple, Représentante de l'OSCE pour la liberté des médias, Dunja Mijatović, Regular Report to the Permanent Council for the period from 19 June through 26 November 2014, p. 8.

[56] Voir, par exemple, Reporters Without Borders (2012), « Enemies of the Internet », 13 mars 2012.

72. L'*Indicateur 2.3.4.* a pour but de vérifier que la confidentialité des sources des journalistes est protégée et qu'ils ne sont pas soumis à surveillance. La surveillance des journalistes et d'autres acteurs des nouveaux médias et le suivi de leurs activités en ligne peuvent entraver l'exercice légitime du droit à la liberté d'expression sur internet et même menacer la sécurité des personnes concernées. Elle peut nuire à leurs sources ou les exposer. Dans le contexte d'internet, la surveillance peut entraîner le suivi ou la conservation de communications à caractère privé, y compris leur contenu, ou la collecte, le stockage et l'analyse des données ou métadonnées relatives au trafic de communications. Le Comité des Ministres du Conseil de l'Europe a émis des directives à ce sujet, notamment dans la Déclaration relative à la protection du journalisme et la sécurité des journalistes et des autres acteurs des médias et dans la Recommandation Rec(2000)7 sur le droit des journalistes à ne pas révéler leurs sources d'information.

73. La vérification de cet indicateur s'appuiera sur l'existence de tout texte de loi ou politique garantissant la confidentialité des sources journalistiques. L'existence de cas documentés de surveillance des communications et du travail de journalistes, comme ceux cités par Reporters sans frontières[57], devra aussi être prise en compte aux fins de la vérification.

74. L'*Indicateur 2.3.5.* porte sur la possibilité que la liberté de parole sur internet soit remise en cause par des moyens nouveaux. Par exemple, le Comité des Ministres a exprimé sa préoccupation au sujet d'attaques par déni de service distribué contre les sites web de médias indépendants, de défenseurs des droits de l'homme, de dissidents, de donneurs d'alerte et d'autres acteurs des nouveaux médias. Ces attaques représentent une atteinte au droit de communiquer et de recevoir des informations et à la liberté d'association. Elles peuvent être perçues de manière négative par les services d'hébergement et les conduire à refuser des contenus sensibles. La vérification de cet indicateur pourra s'appuyer sur tout rapport concernant des cas documentés d'attaques par déni de service, piratage, dégradation, hameçonnage ou compromission de comptes qui auraient été commises par l'Etat. Reporters sans frontières, par exemple, recense ces divers types d'attaques dans les pays où ils se produisent.

75. L'*Indicateur 2.3.6.* se fonde sur la jurisprudence de la Cour européenne des droits de l'homme et sur la Déclaration du Comité des Ministres relative à la protection du journalisme et à la sécurité des journalistes et des autres acteurs des médias, qui affirme : « L'éradication de l'impunité est une obligation cruciale qui incombe aux Etats, pour rendre justice aux victimes, pour dissuader les auteurs potentiels de violations des droits de l'homme et pour maintenir l'Etat de droit et la confiance de la population dans le système judiciaire »[7]. Toute attaque contre des journalistes et d'autres acteurs des médias devrait donner lieu à une enquête résolue et rapide et leurs auteurs devraient être poursuivis. Pour une enquête efficace sur de telles attaques, tout lien éventuel avec des activités journalistiques doit être dûment pris en compte de manière transparente.

76. L'*indicateur 2.3.7.* concerne la protection de la neutralité du réseau en tant que condition nécessaire à l'exercice du droit à l'accès à l'information et du droit à la liberté d'expression. Les fournisseurs de services internet (PSI) ont la capacité de gérer les flux de données et d'information qui transitent sur leurs réseaux. Le droit d'accès aux contenus sur internet est lié au droit d'y recevoir et d'y communiquer des informations, tel qu'inscrit à l'article 10 de la CEDH[58]. Le Comité des Ministres du Conseil de l'Europe a affirmé que tout usager d'internet doit disposer de l'accès le plus large possible aux contenus, applications et services de son choix sur internet, que ceux-ci soient gratuits ou non, au moyen des dispositifs qui lui conviennent. Il s'agit là d'un principe général, couramment appelé « neutralité du réseau », qui s'applique indépendamment de

[57] Reporters Without Borders (2012), Enemies of the Internet, 13 mars 2012, cite plusieurs cas de ce type.
[58] Voir plus haut note 2, par. 50.

l'infrastructure ou du réseau utilisé pour la connexion à internet[59]. La vérification de cet indicateur s'appuiera sur l'existence d'un texte de loi ou d'une politique affirmant de manière positive la neutralité du réseau. En revanche, l'existence de rapports d'ONG comme Freedom House ou Reporters sans frontières par exemple, décrivant en particulier des cas où la gestion du trafic est utilisée pour bloquer certains contenus entraînera une évaluation négative.

2.4. Légalité, légitimité et caractère proportionné des restrictions

78. L'*Indicateur 2.4.1.* demande aux Etats de vérifier que toute restriction est compatible avec les exigences de l'article 10, paragraphe 2, de la CEDH. Il doit être lu à la lumière des sections 2.1. et 2.2. Toute ingérence doit être prescrite par la loi. Cela implique que la loi doit être accessible, claire et suffisamment précise pour permettre aux individus de réguler leurs comportements. La loi doit prévoir des garanties suffisantes contre les mesures restrictives abusives, y compris un contrôle effectif par un tribunal ou un autre organe de règlement indépendant[60]. Toute ingérence doit aussi poursuivre un but légitime, dans l'intérêt de la sécurité nationale, de l'intégrité territoriale ou de la sécurité publiques, de la prévention des troubles à l'ordre public et de la criminalité, de la protection de la santé ou de la morale publiques, de 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. Cette liste est exhaustive, mais son interprétation et sa portée évoluent avec la jurisprudence de la Cour européenne des droits de l'homme.

79. Toute ingérence doit aussi être nécessaire dans une société démocratique, ce qui veut dire qu'il doit être établi qu'elle répond à un besoin social pressant, qu'elle poursuit un objectif légitime et qu'elle constitue le moyen le moins restrictif pour l'atteindre[61]. Les Etats devraient à cet égard analyser l'équilibre atteint entre toute loi ayant pour effet de restreindre l'accès à internet ou à des contenus en ligne et le droit à la liberté d'expression consacré à l'article 10 de la CEDH. Dans l'affaire *Neij et Sunde Kolmisoppi c. Suède*, la Cour européenne des droits de l'homme a déclaré que les Etats doivent trouver un équilibre correct entre les droits concurrents en cause, comme l'a fait également la Cour de Justice de l'Union européenne (CJEU)[62].

80. Les *Indicateurs 2.4.2. et 2.4.3* portent sur la question spécifique du recours abusif à la loi se traduisant par une atteinte au droit à la liberté d'expression et demandent aux Etats de vérifier que leur législation n'aboutit pas à une violation de l'article 10.
81. Les lois, les actions en justice et les autres mesures étatiques qui restreignent le droit à la liberté d'expression doivent respecter les critères énoncés à l'article 10, paragraphe 2, de la CEDH. Elles ne sauraient être justifiées si elles ont pour but d'empêcher un débat public libre et ouvert, l'expression de critiques légitimes à l'encontre d'autorités publiques ou la dénonciation de fautes ou d'actes de corruption des autorités. L'application arbitraire des lois en vigueur a un effet dissuasif sur l'exercice du droit à communiquer des informations et des idées et elle conduit à l'autocensure[63].

82. Les lois sur la diffamation doivent être appliquées avec mesure, tant en ligne que hors ligne, et prévoir des garanties adéquates du point de vue de la liberté d'expression.

---

[59] Déclaration du Comité des Ministres sur la neutralité du réseau, adoptée par le Comité des Ministres le 29 septembre 2010. Voir aussi Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre règlementaire commun pour les réseaux et services de communications électroniques, article 8(4) g.
[60] *Yldirim c. Turquie,* requête n° 3111/10, par. 64.
[61] *Ibid*., par. 66 à 70.
[62] *Neij et Sunde Kolmisoppi c. Suède*, requête n° 40397/12, arrêt du 19 février 2013, p. 10-11 ; affaire C-70/10, *Scarlet Extended*, par. 44 à 49 ; affaire C-275/06, *Productores de Musica de España (Promusicae) c. Telefonica de España SAU* [2008].
[63] Déclaration du Comité des Ministres relative à la protection du journalisme et à la sécurité des journalistes et des autres acteurs des médias, 30 avril 2014, point 9.

La Cour européenne des droits de l'homme a maintenu de façon systématique un seuil de tolérance élevé à l'égard des critiques visant des hommes politiques, des membres d'un gouvernement ou des chefs d'Etat[64].En outre, elle a jugé que l'imposition de sanctions pénales dans les actions en diffamation a un effet dissuasif disproportionné sur l'exercice de la liberté d'expression des journalistes. Elle considère qu'une peine d'emprisonnement constitue une sanction particulièrement grave qui ne peut donc être appliquée qu'à titre exceptionnel lorsque les droits fondamentaux d'autrui ont été gravement lésés comme, par exemple, dans les affaires d'incitation à la violence ou à la haine[65]. En pratique, la Cour n'a encore jamais confirmé une sentence ferme d'emprisonnement pour diffamation. L'Assemblée parlementaire et le Commissaire aux droits de l'homme ont franchi un pas supplémentaire en appelant à dépénaliser la diffamation[66]. Les lois et pratiques prévoyant l'attribution de dommages-intérêts d'un montant disproportionné ou l'imputation des frais de procédure dans les affaires de diffamation peuvent aussi constituer une atteinte à la liberté d'expression[67].

83. La Commission de Venise et l'Assemblée parlementaire sont d'avis que, pour favoriser le pluralisme, la tolérance et l'ouverture d'esprit dans une société démocratique, il convient de protéger le droit d'avoir des convictions ou des opinions spécifiques plutôt que de protéger les systèmes de croyance contre la critique. Le droit à la liberté d'expression implique la liberté d'examiner, de discuter ouvertement et de critiquer, même âprement ou de façon déraisonnable, des systèmes de convictions, des opinions et des institutions tant que cela ne constitue pas une incitation à la haine contre un individu ou un groupe de personnes[68].

84. Les lois qui incriminent la propagation, la promotion ou la justification de la haine et de l'intolérance (y compris l'intolérance religieuse) et l'incitation à celles-ci doivent être d'application claire et les restrictions qu'elles imposent doivent être compatibles avec le but légitime poursuivi, conformément à la jurisprudence de la Cour.

85. Les lois sur la sûreté publique et la sécurité nationale, et notamment celles destinées à lutte contre le hooliganisme, l'extrémisme et le terrorisme, peuvent avoir pour effet de restreindre le droit de recevoir et de communiquer des informations, que ce soit en ligne ou hors ligne. Il est donc nécessaire que ces lois soient faciles à comprendre, non équivoques, conçues de manière étroite et précise, afin de permettre aux individus de connaître les sanctions auxquelles ils sont exposés. Elles doivent inclure des garanties adéquates contre tout abus, en particulier l'examen rapide, complet et efficace de la validité des restrictions par un tribunal ou une autre autorité indépendante. Si des sanctions pénales sont imposées, elles doivent être strictement nécessaires et compatibles avec le but légitime poursuivi, conformément à l'interprétation de la Cour[69].

3. Le droit à la liberté de réunion et d'association

86. L'*Indicateur 3.1.* vise à établir si l'Etat garantit l'application de l'article 11 de la CEDH dans le contexte d'internet et particulièrement des plateformes internet, des médias sociaux et des applications en ligne. L'exercice de ce droit n'est conditionné à aucune reconnaissance formelle de groupes sociaux ou associations par les autorités publiques.

[64] *Lingens c. Autriche* (1986) ; *Otegi Mondragon c. Espagne* (2012).
[65] *Cumpana et Mazare c. Roumanie* (2004) ; *Azevedo c. Portugal* (2008).
[66] Résolution 1577 (2007), « Vers une dépénalisation de la diffamation » ; *Human Rights in Changing Media Landscape*, 2011.
[67] *Tolstoy Miloslavsky c. Royaume-Uni* (1995) ; *M.G.N. Limited c. Royaume-Uni* (2004) ; *Independent News and Media PLC et Independent Newspapers Ireland Limited c. Irlande* (2005).
[68] Rapport sur les relations entre liberté d'expression et liberté de religion : Réglementation et répression du blasphème, de l'injure à caractère religieux et de l'incitation à la haine religieuse, CDL-AD(2008)026, 23 octobre 2008 ; Recommandation 1805 (2007) de l'APCE, « Blasphème, insultes à caractère religieux et incitation à la haine contre des personnes au motif de leur religion ».
[69] *Ozgur Gundem c. Turquie* (2000) ; *Urper et Autres c. Turquie* (2009) ; *Karatas c. Turquie* (1999) ; *Demiral et Ates c. Turquie* (2008).

Il inclut le droit de réunion pacifique et d'association avec d'autres personnes via internet, par exemple en formant, mobilisant et participant à des assemblées et des groupes sociétaux, y compris des syndicats, et en y adhérant, à l'aide d'outils basés sur internet. La vérification de cet indicateur s'appuiera sur l'existence de dispositions constitutionnelles, de lois et de politiques conformes aux normes internationales sur la liberté de réunion et d'association, étant entendu qu'elles garantissent l'exercice de ce droit dans le contexte d'internet et de la communication en ligne. A l'inverse, la consultation des rapports d'organisations non gouvernementales, comme les rapports par pays publiés par la Commission de Venise ou ceux de l'organisation non gouvernementale Article 19, pourra constituer une évaluation négative[70].

87. L'*Indicateur 3.2.* a pour but de déterminer si les associations créées dans un environnement hors ligne peuvent utiliser internet pour leurs activités. Les Lignes directrices conjointes sur la liberté d'association de la Commission de Venise et de l'OSCE/BIDDH déclarent à ce sujet : «Les nouvelles technologies ont amélioré la capacité des personnes et des groupes de personnes de créer tout type d'association, y compris les organisations non gouvernementales et les partis politiques. (…) Bon nombre des activités menées habituellement par les partis politiques, les organisations non gouvernementales et les autres associations peuvent être exercées en ligne. Ces activités peuvent englober l'enregistrement, la collecte de signatures, la collecte de fonds et la possibilité de faire des dons »[71].

88. Les individus doivent aussi avoir la possibilité de participer aux débats publics en ligne au niveau local, national et mondial et, en particulier, à la libre discussion des initiatives législatives et à l'observation citoyenne des processus décisionnels de l'Etat. Cet indicateur se fonde sur les recommandations du Comité des Ministres sur la valeur de service public d'internet qui encouragent l'utilisation des forums en ligne, des blogs, des sites de discussion politique, de la messagerie instantanée et d'autres formes de communication en ligne entre citoyens pour participer aux délibérations démocratiques, au cyber-activisme et à des cyber-campagnes, faire connaître leurs préoccupations, idées et initiatives, promouvoir dialogue et débat avec leurs représentants et le gouvernement, et observer les officiels et les hommes politiques sur les questions d'intérêt général[72]. Comme exemple de l'application de l'article 11 en ligne, on peut citer la signature d'une pétition ou la participation à une campagne d'action civique.

89. La vérification de cet indicateur pourra s'appuyer sur l'évaluation du développement et de la mise en œuvre de stratégies en faveur de la cyber-démocratie, de la cyber-participation et du cyber-gouvernement sur internet ou sur des plateformes basées sur internet comme les médias sociaux ou d'autres services en ligne, aux fins des processus et de la discussion démocratiques, comme le recommande le Comité des Ministres[73]. De telles stratégies en faveur de la cyber-démocratie peuvent s'appliquer à la fois aux relations entre les autorités publiques et la société civile et à la fourniture des services publics.

90. Les *Indicateurs 3.3. et 3.4* ont pour but de vérifier que toute restriction visant les plateformes internet, les médias sociaux ou les autres services en ligne qui facilitent l'exercice de la liberté de réunion et d'association est conforme à l'article 11 de la CEDH. Les Etats devraient noter à cet égard que les principes affirmés par la Cour européenne des droits de l'homme quant à la protection du discours politique au titre de l'article 10

[70] http://www.article19.org/resources.php.
[71] Lignes directrices conjointes sur la liberté d'association de la Commission européenne pour la démocratie par le droit (Commission de Venise) et du Bureau des institutions démocratiques et des droits de l'homme de l'OSCE (OSCE/BIDDH), 2014, par. 260.
[72] Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'internet, p. 4.
[73] Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'internet, annexe, première partie.

s'appliquent également à l'article 11. Dans l'affaire *Wingrove c. Royaume-Uni*, la Cour européenne des droits de l'homme a affirmé que l'article 10 ne laisse guère de marge aux Etats pour imposer des restrictions dans le domaine du discours politique ou des questions d'intérêt général[74]. La vérification de cet indicateur se basera sur l'absence de lois, de politiques ou d'autres mesures restreignant l'accès ou l'utilisation de plateformes internet, de médias sociaux ou d'autres services en ligne en vue de s'associer à d'autres personnes ou de créer une communauté d'intérêt. L'existence d'une restriction prescrite par la loi mais accompagnée de dispositions prévoyant un contrôle judiciaire ou administratif, y compris le droit d'être entendu, pourra aussi servir de vérification.

4. Le droit à la vie privée

4.1. Protection des données à caractère personnel

91. L'*Indicateur 4.1.1* affirme le droit au respect de la vie privée et familiale, du domicile et de la correspondance. Ce droit doit être garanti par les Etats conformément à l'article 8 de la CEDH. Il est interprété par la jurisprudence de la Cour européenne des droits de l'homme et complété et renforcé par la Convention 108 du Conseil de l'Europe. Le droit au respect de la correspondance englobe les communications postales et téléphoniques, comme établi dans l'affaire *Klass c. Allemagne*[75]. Dans l'arrêt *Copland c. Royaume-Uni*, la Cour européenne des droits de l'homme a interprété l'article 8 comme concernant également la correspondance électronique, y compris sur le lieu de travail, ainsi que l'information dérivée de l'utilisation personnelle d'internet[76]. Elle a jugé en outre que la vie privée couvre le droit d'une personne à sa propre image[77], par exemple sous forme de photographies ou de clips vidéo. Le droit au respect de la vie privée englobe aussi le droit à l'identité et au développement personnel et celui de nouer et de développer des relations avec ses semblables. Les activités de nature professionnelle ou commerciale sont également incluses[78].

92. L'*Indicateur 4.1.2.* porte sur la protection des données à caractère personnel, telles que définies dans la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[79]. Cet indicateur a pour but de vérifier que les Etats assurent la protection des données à caractère personnel dans le cadre plus large de leur obligation de protéger le droit au respect de la vie privée et familiale. La protection des données à caractère personnel tient donc une place fondamentale dans l'exercice du droit au respect de la vie privée et familiale consacré à l'article 8 et, par conséquent, la législation nationale doit inclure des dispositions appropriées afin d'empêcher toute utilisation des données à caractère personnel non conforme aux garanties prévues dans cet article et d'assurer une protection effective des données enregistrées à caractère personnel contre tout mésusage ou utilisation abusive.

93. L'*Indicateur 4.1.3.* vise à contrôler si les principes et normes de la Convention 108 sont respectés par les autorités publiques et les entreprises privées. Les données à caractère personnel doivent être obtenues et traitées loyalement et licitement et enregistrées à des fins déterminées et légitimes. Elles doivent être adéquates, pertinentes et non excessives par rapport aux buts poursuivis, exactes et si nécessaire mises à jour, conservées sous une forme permettant l'identification des personnes

[74] *Wingrove c. Royaume-Uni*, 25 novembre 1996, par. 58, Rapports 1996-V.
[75] *Klass et Autres c. Allemagne*, requête n° 5029/71, par. 41.
[76] *Copland c. Royaume-Uni*, requête n° 62617/00, 3 avril 2007, par. 41 et 42.
[77] *Von Hannover c. Allemagne* (n° 2), requêtes n° 40660/08 et 60641/08, par. 108 à 113 ; *Sciacca c. Italie*, requête n° 50774/99, par. 29.
[78] *Rotaru c. Roumanie* (n° 28341/95) ; *P.G. et J.H. c. Royaume-Uni* (n° 44787/98) ; *Peck c. Royaume-Uni* (n° 44647/98) ; *Perry c. Royaume-Uni* (n° 63737/00) ; *Amann c. Suisse* (n° 27798/95).
[79] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), article 2. On notera que les Propositions de modernisation adoptées le 18 décembre 2012 ont actualisé la Convention, entre autres au regard du contexte d'internet.

concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées[80].

94. L'accent est mis sur deux principes spécifiques du traitement des données personnelles : la légalité du traitement et le consentement de l'utilisateur. La Convention 108 stipule que les utilisateurs devraient pouvoir exercer un contrôle sur leurs données personnelles, et notamment qu'ils doient pouvoir rectifier ou effacer des données lorsqu'elles ont été traitées en violation de la loi, et qu'ils ontdroit à un recours s'il n'est pas donné suite à une demande de confirmation, de rectification ou d'effacement[81].

95. La Convention 108 s'applique à tout type de traitement de données qui a lieu dans le contexte d'internet – qu'il s'agisse du réseau ou des contenus – comme la collecte, le stockage, la modification, l'effacement, l'extraction ou la diffusion de données à caractère personnel[82]. En pratique, cela pourrait inclure le traitement automatisé de données personnelles lié à l'utilisation de navigateurs, du courrier électronique, de la messagerie instantanée, de la téléphonie sur protocole internet, de réseaux sociaux et de moteurs de recherche, ainsi que de services hébergés de stockage de données.

96. La Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux souligne l'importance du consentement éclairé. Les services de réseaux sociaux devraient, en particulier, obtenir le consentement éclairé des utilisateurs avant de diffuser ou de partager leurs données personnelles ou de les utiliser à d'autres fins que celles spécifiées lors de la collecte initiale. Les utilisateurs de réseaux sociaux devraient avoir la possibilité de consentir à un accès plus large à leurs données personnelles par des tiers (par exemple lorsque des applications tierces sont exploitées sur le réseau social). De la même façon, ils devraient pouvoir retirer ce consentement. La vérification de cet indicateur s'appuiera sur l'existence de tout texte de loi relatif au traitement des données à caractère personnel qui intègre les principes et normes inscrits dans la Convention 108. Les Propositions de modernisation de la Convention 108, adoptées le 18 décembre 2012 requièrent le consentement libre, spécifique, éclairé et explicite (non équivoque) de la personne concernée pour le traitement de ses données sur internet[83].

97. Les *Indicateurs 4.1.4. à 4.1.7.* ont pour but de vérifier que les individus sont en mesure d'exercer leurs droits dans le contexte du traitement des données à caractère personnel. Les utilisateurs d'internet doivent pouvoir exercer un contrôle sur leurs données personnelles, comme le prévoit la Convention 108, et notamment faire valoir leur droit de rectification ou d'effacement de données lorsqu'elles ont été traitées en violation de la loi, et leur droit à un recours s'il n'est pas donné suite à une demande de confirmation, de rectification ou d'effacement[84]. En ce qui concerne le profilage[85], l'utilisateur devrait pouvoir faire objection à l'utilisation de ses données personnelles à des fins de profilage et s'opposer à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur la seule base d'un profilage, à moins que la loi l'autorise et précise les mesures garantissant la sauvegarde de ses

[80] Voir Convention 108, article 5.
[81] Voir Convention 108, articles 8 et 10.
[82] Voir Convention 108, article 2.
[83] Les Propositions mettent l'accent sur le consentement de la personne dont les données à caractère personnel doivent être traitées comme condition préalable à ce traitement : « Chaque Partie prévoit que le traitement de données ne peut être effectué que sur la base du consentement spécifique, libre, éclairé et [explicite, non-équivoque] de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ».
[84] Voir Convention 108, article 8.
[85] Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes au regard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Le « profilage » désigne les techniques de traitement automatisé des données consistant à analyser les préférences, comportements et attitudes personnels d'un usager de l'internet afin de prendre des décisions à son sujet, par exemple en prédisant ses comportements futurs ou en en faisant la cible de publicités particulières.

intérêts légitimes, notamment en lui permettant de faire valoir son point de vue, ou que la décision ait été prise dans le cadre de l'exécution d'un contrat et que des mesures garantissant la sauvegarde de ses intérêts légitimes aient été mises en place[86]. La vérification de cet indicateur s'appuiera, par exemple, sur l'examen de la compatibilité des conditions contractuelles des prestataires de services et exploitants de plateformes avec la législation et les critères de l'article 8.

98. L'*Indicateur 4.1.6.* concerne en particulier la question de l'anonymat. Celle-ci se fonde sur la jurisprudence de la Cour européenne des droits de l'homme, la Convention de Budapest et d'autres instruments du Comité des Ministres. La Cour européenne des droits de l'homme a examiné la question de la confidentialité des communications sur internet dans une affaire où un Etat membre du Conseil de l'Europe avait manqué à son obligation d'obliger un fournisseur de service internet à révéler l'identité d'une personne qui avait publié une annonce indécente concernant un mineur sur un site de rencontres. La Cour européenne des droits de l'homme a estimé que, bien que la liberté d'expression et la confidentialité des communications soient des considérations primordiales et que les utilisateurs de télécommunications et de services sur internet doivent avoir la garantie que leur intimité et leur liberté d'expression sont respectées, cette garantie ne peut être absolue et doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. L'Etat a l'obligation positive d'établir un cadre permettant de concilier les intérêts concurrents[87].

99. La Convention de Budapest ne pénalise pas l'utilisation des technologies informatiques aux fins de communications anonymes. Selon son rapport explicatif, « la modification des données de trafic aux fins de faciliter les communications anonymes (comme dans le cas des activités des systèmes de réexpédition anonymes) ou la modification des données aux fins d'assurer la protection des communications (chiffrement, par exemple) sont considérées comme assurant la protection légitime de la vie privée et, de ce fait, sont considérées comme étant réalisées de façon légitime. Toutefois, les Parties [à la Convention de Budapest] peuvent incriminer certains actes abusifs se rapportant aux communications anonymes, comme dans le cas de la falsification des données d'un en-tête de paquet visant à dissimuler l'identité de l'auteur d'une infraction »[88].

100. Le Comité des Ministres du Conseil de l'Europe a affirmé le principe de l'anonymat dans sa Déclaration relative à la liberté de la communication sur l'internet[89]. En conséquence, pour assurer la protection contre la surveillance en ligne et renforcer la liberté d'expression, les Etats membres du Conseil de l'Europe devraient respecter la volonté des utilisateurs d'internet de ne pas révéler leur identité. Toutefois, le respect de l'anonymat n'empêche pas les Etats membres de prendre des mesures pour retrouver la trace de responsables d'actes délictueux, conformément à la législation nationale, à la CEDH et aux autres traités internationaux dans le domaine de la justice et de la police.

101. Cet indicateur apparaîtra négatif par l'existence de toute loi ou politique interdisant aux utilisateurs d'internet d'utiliser un logiciel de chiffrement pour protéger leurs communications ou de toute loi ou politique restreignant l'utilisation des logiciels de chiffrement ou d'autres logiciels de sécurité ou encore permettant aux organes gouvernementaux d'avoir accès aux clés et algorithmes de chiffrement. La vérification positive de cet indicateur requiert l'absence de telles lois ou politiques.

---

[86] Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes au regard du traitement automatisé des données à caractère personnel dans le cadre du profilage, section 5.
[87] *K.U. c. Finlande*, requête n° 2872/02, par. 49.
[88] Convention de Budapest sur la cybercriminalité, article 2, et Rapport explicatif, par 62.
[89] Voir Déclaration sur la liberté de la communication sur l'internet, Principe 7.

4.2. Droit d'être libre de toute surveillance

102. L'*Indicateur 4.2.1.* s'appuie sur la jurisprudence de la Cour européenne des droits de l'homme. Il a pour but de vérifier que toutes les mesures de surveillance sont conformes à l'article 8 de la CEDH et font l'objet d'un contrôle indépendant et impartial. Les mesures de surveillance peuvent être générales (surveillance de masse) ou ciblées. La Cour européenne des droits de l'homme a interprété l'article 8 de manière telle que la notion de correspondance englobe le courrier postal, les télécommunications[90] et le courrier électronique[91]; l'interprétation de cette notion évolue afin de s'adapter aux développements technologiques. Garantir la confidentialité des communications implique de les protéger de toutes les formes de surveillance, y compris l'interception. Dans le contexte d'internet, la surveillance englobe l'écoute, l'enregistrement, le suivi et le stockage de communications privées. Elle peut aussi viser à s'assurer le contenu des données en obtenant un accès sous couverture aux systèmes, ou bien au moyen d'écoutes électroniques ou d'autres dispositifs de surveillance. Dans le contexte d'internet, la surveillance peut impliquer également la collecte, le stockage et l'analyse des données ou métadonnées sur les flux de communications. Ces données ne révèlent pas le contenu des communications, mais renseignent sur l'émetteur, les détails de la transmission et son objet.

103. La Cour européenne des droits de l'homme, en interprétant l'article 8 de la CEDH dans le cadre d'affaires de surveillance, s'est prononcée sur l'importance de la supervision des mesures de surveillance par d'autres autorités que celles qui appliquent ces mesures. Bien que les affaires examinées par la Cour européenne des droits de l'homme ne concernent pas les technologies internet, les principes qu'elle a établis sont valides dans le contexte d'internet. Cela découle du principe général établi par la Cour selon lequel « quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus »[92]. La surveillance peut subir un contrôle à trois stades : lorsqu'elle est ordonnée, pendant qu'elle est menée ou après qu'elle a cessé[93]. La Cour européenne des droits de l'homme infère du principe général de la prééminence du droit que, dans le contexte de la surveillance, une ingérence de l'exécutif dans les droits d'un individu doit être soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière[94].

104. L'*Indicateur 4.2.2.* a pour but de vérifier que toute forme d'interception ou de surveillance de la correspondance ou d'activités privées sur internet est fondée en droit. Cependant, une loi qui institue un système de surveillance en vertu duquel tous les individus d'un pays peuvent être concernés par une surveillance de leurs courriels et télécommunications, touche directement tous les utilisateurs ou utilisateurs potentiels des services postaux et de télécommunication nationaux. L'existence même d'une législation permettant la surveillance des télécommunications peut donc être considérée comme une ingérence dans le droit à la vie privée. La Cour européenne des droits de l'homme a accepté que, dans certaines conditions, un individu puisse se prétendre victime d'une violation occasionnée par la simple existence de mesures secrètes ou d'une législation qui les permette, sans devoir alléguer qu'il a lui-même fait l'objet de telles mesures[95].

---

[90] *Association for European Integration and Human Rights et Ekmidzhiev c. Bulgarie*, requête n° 62540/00, par. 58 ; *Klass et Autres c. Allemagne*, n° 5029/71 ; *Malone c. Royaume-Uni*, n° 8691/79, et *Weber et Saravia c. Allemagne*, n° 54934/00.
[91] Voir *Copland c. Royaume-Uni*, n° 62617/00, paragraphe 41.
[92] *Klass et Autres c. Allemagne*, n° 5029/71, paragraphe 50.
[93] *Klass et Autres c. Allemagne*, n° 5029/71, paragraphe 55.
[94] *Klass et Autres c. Allemagne*, n° 5029/71, paragraphe 55.
[95] *Klass et Autres c. Allemagne*, n° 5029/71, par. 30 à 38 ; *Malone c. Royaume-Uni*, n° 8691/79, par. 64 ; *Weber et Saravia c. Allemagne*, n° 54934/00, par. 78 et 79 ; *Association for European Integration and Human Rights et Ekmidzhiev c. Bulgarie*, n° 62540/00, par. 58 et 69-70.

105. Ces principes établis par la Cour européenne des droits de l'homme définissent les exigences que doit satisfaire toute législation prévoyant des mesures de surveillance secrète des correspondances et des communications par les autorités publiques. La loi doit prévoir en détail un minimum de garanties pour l'exercice du pouvoir d'appréciation des pouvoirs publics. Elles doivent inclure des dispositions sur : (i) la nature des infractions susceptibles de donner lieu à un mandat d'interception ; (ii) la définition des catégories de personnes susceptibles d'être mises sur écoute ; (iii) une limite à la durée de l'exécution de la mesure ; (iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; (v) les précautions à prendre pour la communication des données à d'autres parties ; et (vi) les circonstances dans lesquelles on peut ou on doit effacer ou détruire des enregistrements[96].

106. La vérification de cet indicateur devra donc s'appuyer non seulement sur l'existence d'une loi, mais aussi sur la teneur de cette loi qui doit inclure des garanties contre les abus[97]. La loi doit affirmer le principe de prévisibilité, c'est-à-dire qu'elle doit être accessible à toute personne concernée qui doit être en mesure de prévoir les conséquences de son application. La loi doit aussi être formulée de façon suffisamment claire et précise, afin de donner aux citoyens une indication adéquate des conditions et des circonstances dans lesquelles les autorités peuvent s'ingérer en secret, et d'une manière potentiellement préjudiciable, dans leur droit au respect de la vie privée et de la correspondance[98]. La vérification pourra s'appuyer sur les rapports des organisations internationales, d'organes comme le Commissaire aux droits de l'homme du Conseil de l'Europe, la Commission de Venise et le Rapporteur spécial des Nations Unies sur la liberté d'expression, et d'ONG comme Reporters sans frontières, Freedom House, Article 19 et Index on Censorship.

107. L'*Indicateur 4.2.2.* vise à déterminer si les lois et les politiques au titre desquelles sont mises en œuvre des mesures de surveillance poursuivent un objectif légitime d'intérêt public, conformément aux buts envisagés à l'article 8, paragraphe 2. Cet objectif doit être de portée restreinte et défini avec précision. L'indicateur se fonde aussi sur le paragraphe 2 de l'article 8 qui exige que toute législation, politique ou ordre de surveillance constitue une mesure nécessaire dans une société démocratique[99]. Cela signifie qu'il faut prouver qu'elle correspond à un besoin social impérieux et qu'elle représente le moyen le moins restrictif d'atteindre son objectif. Pour établir la nécessité d'une telle loi, il convient de peser l'objectif poursuivi au regard des droits et libertés concurrents. L'indicateur a pour but de déterminer si une telle évaluation a eu lieu.

108. Cet indicateur se fonde sur la jurisprudence de la Cour européenne des droits de l'homme, qui souligne que de telles mesures ne peuvent être considérées comme « nécessaires dans une société démocratique » que « si le système de surveillance adopté s'entoure de garanties suffisantes contre les excès »[100]. La Cour européenne des droits de l'homme a jugé que, bien que les mesures qui s'ingèrent dans la vie privée des individus puissent avoir été conçues pour protéger la démocratie, elles comportent une possibilité intrinsèque d'abus de pouvoir pouvant avoir des conséquences préjudiciables pour la société démocratique toute entière. Cet indicateur pourra être vérifié *a contrario* par l'existence de rapports sur des activités de surveillance par l'Etat qui ne semblent pas poursuivre un but légitime. De tels rapports pourront émaner des organisations

[96] Voir *Kruslin c. France*, n° 11801/85, par. 33 ; *Huvig c. France*, n° 11105/84, par. 32 ; *Amann c. Suisse*, n° 27798/95, par. 56 ; *Weber et Saravia c. Allemagne*, n° 54934/00, par. 93 ; *Association for European Integration and Human Rights et Ekmidzhiev c. Bulgarie*, n° 62540/00, par. 76.
[97] *Kopp c. Suisse*, paragraphes 62 à 66.
[98] *Malone c. Royaume-Uni*, n° 8691/79, par. 67 ; *Valenzuela Contreras c. Espagne*, arrêt du 30 juillet 1998, Rapports 1998-V, p. 1925, par. 46 (iii) ; et *Khan c. Royaume-Uni*, n° 35394/97, par. 26, *Association for European Integration and Human Rights et Ekmidzhiev c. Bulgarie*, n° 62540/00, par. 71.
[99] Voir *Malone c. Royaume-Uni*, paragraphes 81 et 82.
[100] Arrêt du 2 août 1984, *Malone c. Royaume-Uni*, Cour européenne des droits de l'homme (Plénière), n° 8691/79, série A, paragraphe 81.

internationales ou d'ONG comme, par exemple, Article 19, Freedom House, Index on Censorship et Reporters sans frontières.

109. L'*Indicateur 4.2.3.* se fonde sur la jurisprudence de la Cour européenne des droits de l'homme qui exige que, lorsqu'un Etat met en place un système de surveillance, il s'entoure de garanties efficaces contre les excès. La Cour européenne des droits de l'homme reconnaît aux Etats une certaine latitude pour apprécier l'existence et l'étendue de cette nécessité, mais cette latitude est soumise au contrôle européen. La Cour doit rechercher si les procédures de contrôle du déclenchement et de la mise en œuvre de mesures restrictives sont de nature à circonscrire l'ingérence à ce qui est nécessaire dans une société démocratique[101].

110. Cet indicateur vise spécifiquement l'autorisation préalable des mesures de surveillance. La Cour européenne des droits de l'homme a jugé souhaitable un contrôle judiciaire des mesures de surveillance[102]. Bien qu'elle ne fasse pas du contrôle judiciaire préalable une condition applicable dans tous les cas, sa jurisprudence exige clairement que l'organe qui autorise les mesures de surveillance soit indépendant du service qui applique ces mesures et de l'exécutif[103].

111. La vérification de cet indicateur s'appuiera sur l'existence de mécanismes de supervision et de contrôle par des autorités compétentes, par exemple une commission parlementaire ou d'autres organes publics chargés de telles fonctions. Ces organes publics doivent être indépendants de l'exécutif et de toute autorité chargée de conduire la surveillance.

112. Les *Indicateurs 4.2.5. à 4.2.7.* ont pour but de vérifier qu'il existe un contrôle adéquat des mesures de surveillance pendant ou après leur mise en œuvre. Ils découlent des critères adoptés par la Cour européenne des droits de l'homme pour déterminer si des dispositifs de contrôle fournissent ou non des garanties suffisantes pour empêcher les excès. La Cour a toujours maintenu que le contrôle des mesures de surveillance doit être effectué par un organe indépendant[104]; il doit exister un fondement juridique qui en précise les modalités[105]. La Cour a recensé les compétences des organes de contrôle qui sont pertinentes pour déterminer l'existence de garanties suffisantes contre les excès. Les critères qu'elle examine incluent la question de savoir si ces organes ont accès à l'ensemble de l'information pertinente, y compris l'information classifiée, et s'ils disposent du pouvoir d'annuler un ordre de surveillance et d'exiger que les éléments recueillis au moyen des mesures de surveillance soient détruits[106].

113. Les *Indicateurs 4.2.8 à 4.2.10.* font écho aux recommandations du Commissaire aux droits de l'homme du Conseil de l'Europe sur le contrôle démocratique des services de sécurité nationale. Le Commissaire souligne que le mandat de ces organes doit inclure le contrôle de la conformité avec les droits de l'homme des activités de coopération des services de sécurité avec des organes étrangers, y compris la coopération sous forme d'échange de renseignement, d'opérations conjointes et de fourniture de matériel et de formations. Le contrôle externe de la coopération avec des organes étrangers devrait porter notamment sur les éléments suivants : « a. directives ministérielles et règlement interne portant sur la coopération internationale dans le

[101] *Klass et Autres c. Allemagne*, n° 5029/71, paragraphes 54 à 56 ; *Kennedy c. Royaume-Uni*, paragraphe 154.
[102] *Klass et Autres c. Allemagne*, n° 5029/71, paragraphe 56 : « La Cour estime en principe souhaitable que le contrôle soit confié à un juge en un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière ».
[103] Dumitru Popescu c. Roumanie, par. 70 à 73 ; Klass et Autres c. Allemagne, n° 5029/71, par. 56 ; Kennedy c. Royaume-Uni, par. 167.
[104] Association for European Integration and Human Rights et Ekmidzhiev c. Bulgarie, par. 85 à 87.
[105] Iordachi et Autres c. Moldova, par. 49.
[106] Kennedy c. Royaume-Uni, par. 166 et 167.

secteur du renseignement ; b. processus d'évaluation des risques pour les droits de l'homme et de gestion des risques concernant les rapports avec des services de sécurité étrangers et les cas spécifiques de coopération opérationnelle ; c. données à caractère personnel sortantes et conditions attachées à celles-ci ; d. demandes de services de sécurité adressées à des partenaires étrangers : i) demandes d'informations sur certaines personnes ; et ii) demandes de placer certaines personnes sous surveillance ; e. accords de coopération entre services de renseignement ; f. opérations et programmes conjoints de surveillance réalisés avec des partenaires étrangers »[107].

114. La vérification de cet indicateur s'appuiera sur l'existence de mécanismes de supervision et de contrôle par des autorités compétentes, comme une commission parlementaire ou d'autres organes publics chargés de ces fonctions de contrôle.

5. Les mesures de réparation

115. L'*Indicateur 5.1.* a pour but de vérifier que les utilisateurs d'internet sont en mesure d'exercer leur droit à un procès équitable qui est consacré à l'article 6 de la CEDH. Cela renvoie à la détermination des droits civils et des obligations ou des chefs d'inculpation pénale eu égard aux activités des utilisateurs d'internet. Sont en jeu ici, en particulier, les principes clés énoncés par la Cour européenne des droits de l'homme, et notamment le droit à une audience équitable, publique et dans un délai raisonnable par un tribunal indépendant et impartial, le droit d'ester en justice, le droit à un règlement du différend, à un jugement raisonné et à l'exécution du jugement, le droit à une procédure contradictoire et à l'égalité des armes. La Cour européenne des droits de l'homme, bien que ce ne soit pas dans des affaires en relation avec internet, a établi des principes généraux eu égard à l'administration de la justice (indépendance, impartialité, compétence du tribunal) et à la protection du droit des parties (jugement équitable, égalité des armes et audience publique), ainsi qu'en ce qui concerne l'efficience de l'administration de la justice (délai raisonnable).
116. Il faut qu'existe une autorité nationale chargée de se prononcer sur les allégations de ces violations des droits garantis[108]. Il n'est pas nécessaire que cette autorité soit une autorité judiciaire si elle présente des garanties d'indépendance et d'impartialité. Néanmoins, ses compétences et les garanties procédurales en place devraient permettre de déterminer si un mode de réparation particulier est suffisant[109]. La procédure suivie par l'autorité nationale compétente devrait permettre d'enquêter de manière efficace sur une violation. Elle devrait permettre à l'autorité compétente de se prononcer sur le bien-fondé d'une plainte pour violation des droits de la CEDH, de sanctionner toute violation et de garantir à la victime que la décision prise sera exécutée. Cette procédure légale devrait être complétée par une voie juridique spécifique permettantà un individu de se plaindre de délais déraisonnables pour la détermination de ses droits[110].

117. Les *Indicateurs 5.2. et 5.3.* ont pour but de vérifier que le droit à un recours effectif, inscrit à l'article 13 de la CEDH, est respecté. Toute personne dont les droits ou libertés ont été violés ou restreints sur internet a droit à un recours effectif. Ces indicateurs se fondent sur la jurisprudence de la Cour européenne des droits de l'homme. Dans le cadre de leurs obligations positives de protéger les particuliers contre les violations des droits de l'homme par des entreprises privées, les Etats doivent prendre les mesures nécessaires pour assurer que, lorsque de telles violations ont lieu, les victimes ont accès à des mécanismes judiciaires et non judiciaires. Ces indicateurs concernent l'article 13 de la CEDH qui garantit l'existence en droit interne d'un recours

[107] CommDH/IssuePaper(2015)2, 5 juin 2015, La surveillance démocratique et effective des services de sécurité nationale.
[108] *Silver et Autres c. Royaume-Uni*, n° 5947/72 ; 6205/73 ; 7052/75 ; 7061/75 ; 7107/75 ; 7113/75 ; 7136/75, par. 113 ; *Kaya c. Turquie*, n° 22729/93, par. 106.
[109] *Silver et Autres c. Royaume-Uni*, n° 5947/72 ; 6205/73 ; 7052/75 ; 7061/75 ; 7107/75 ; 7113/75 ; 7136/75, par. 113 ; *Kaya c. Turquie*, n° 22729/93, par. 106.
[110] *Kudla c. Pologne*, N° 30210/96, par. 157.

permettant de se prévaloir des droits et libertés de la CEDH, tels qu'ils peuvent s'y trouver consacrés. L'article 13 exige un recours interne habilitant à examiner le contenu du grief fondé sur la CEDH et à offrir le redressement approprié[111]. Les Etats ont une obligation positive d'enquêter de manière diligente, approfondie et efficace sur toute allégation de violation de la CEDH. Les procédures suivies doivent permettre à l'organe compétent de décider du bien-fondé de la plainte pour violation de la Convention et de sanctionner toute violation constatée, mais aussi de garantir l'exécution des décisions prises[112].

118. Le recours doit être effectif en pratique comme en droit et ne pas dépendre de la certitude d'une issue favorable pour le requérant[113]. L'ensemble des recours offerts par le droit interne peut remplir les exigences de l'article 13, même si aucun d'entre eux n'y répond en entier à lui seul[114]. Les voies de recours effectives doivent être disponibles, connues, accessibles, abordables et permettre d'obtenir une réparation appropriée. Un recours effectif doit pouvoir être obtenu des pouvoirs publics ou d'autres institutions nationales des droits de l'homme. Dans le contexte d'internet, un recours effectif peut être obtenu des prestataires de service à haut débit, mais ils ne jouissent pas d'une indépendance suffisante pour que cela soit compatible avec l'article 13 de la CEDH.

119. L'*Indicateur 5.4.* a pour but de vérifier la mise en œuvre des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme qui spécifient que les entreprises devraient mettre en place des mécanismes de réclamation qui soient accessibles, prévisibles (prévoyant une procédure clairement établie, communiquée au public et assortie d'un calendrier indicatif pour chaque étape, et un descriptif précis des types de procédures et d'issues disponibles et des moyens de suivre la mise en œuvre), équitables (assurant un accès aux sources d'information, aux conseils et aux compétences), transparents et en capacité d'offrir directement aux individus des mesures de réparation qui soient pleinement compatibles avec les droits de l'homme internationalement reconnus[115].

120. La vérification s'appuiera sur les conditions d'utilisation des services et plateformes internet, afin de déterminer si les usagers d'internet reçoivent des informations claires et transparentes sur les moyens de recours qui s'offrent à eux. Ils doivent disposer d'outils pratiques et accessibles leur permettant de contacter les fournisseurs d'accès etde services internet pour leur soumettre leurs problèmes. Ils doivent pouvoir solliciter des informations et demander réparation. Parmi les exemples de recours figurent les lignes d'assistance ou les permanences téléphoniques gérées par les fournisseurs de services internet ou les associations de protection des consommateurs vers lesquelles les utilisateurs d'internet peuvent se tourner en cas de violation de leurs droits ou des droits d'autres personnes. Des conseils devraient également être mis à disposition par les pouvoirs publics ou d'autres institutions nationales de droits de l'homme (médiateurs), les autorités de protection des données, les autorités de régulation des communications électroniques, les services d'aide aux particuliers, les associations de protection des droits de l'homme ou des droits numériques, ou les organisations de défense des consommateurs.

121. Les autres sources de vérification incluront les rapports de transparence publiés par les prestataires de services internet ou les plateformes internet. Google publie des

[111] *Kaya c. Turquie*, n° 22729/93, par. 106.
[112] *Smith et Grady c. Royaume-Uni*, n° 33985/96, 33986/96.
[113] *Kudla c. Pologne*, n° 30210/96, par. 157.
[114] *Silver et Autres c. Royaume-Uni*, n° 5947/72 ; 6205/73 ; 7052/75 ; 7061/75 ; 7107/75 ; 7113/75 ; 7136/75, par. 113 ; *Kudla c. Pologne*, n° 30210/96, par. 157.
[115] Voir Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies (A/HRC/17/31), adoptés par le Conseil des droits de l'homme par la Résolution « Les droits de l'homme et les sociétés transnationales et autres entreprises » (A/HRC/RES/17/4), chapitre III, principes 28-31.

rapports de transparence[116] énumérant en détail les demandes de retrait de son moteur de recherche, de son site de blogs et de YouTube. Les demandes de retrait proviennent des pouvoirs publics et des organes d'application de la loi et aussi des détenteurs de droits. Lorsqu'une demande concerne des droits d'auteur, Google indique les noms des personnes à l'origine de la demande et l'URL concerné. Dans le cas des demandes émanant des pouvoirs publics, Google fournit des informations génériques, sans révéler de nom. Twitter publie des rapports de transparence concernant les demandes de suppression de contenus émanant des pouvoirs publics et des organes d'application de la loi, et aussi des rapports sur les demandes de suppression de contenus au titre de la législation des Etats-Unis sur le droit d'auteur. Dans ces rapports, Twitter ne présente que des données agrégées, sans donner de précisions sur chaque demande[117]. Vodafone publie un rapport de divulgation pays par pays sur l'aide qu'elle apporte aux organes de répression, en annexant des précisions supplémentaires sur certains pays[118]. Elle indique comment elle traite les demandes de suppression de contenus, conformément aux Principes directeurs de l'ONU relatif aux entreprises et aux droit de l'homme[119], mais sans divulguer les demandes elles-mêmes. Les rapports des organisations internationales des droits de l'homme qui analysent les décisions de blocage de contenus sur internet pourront également servir de sources de vérification.

122. Les rapports de transparence émanant d'intermédiaires pourront, dans une certaine mesure, servir d'outils de vérification, mais les données publiées ne portent souvent en fait que sur le nombre total de demandes reçues et de demandes satisfaites. Google publie des rapports de transparence[120] indiquant le nombre de demandes d'information des pouvoirs publics sur ses utilisateurs[121]. Twitter publie des rapports de transparence sur les demandes de données concernant ses utilisateurs reçues des pouvoirs publics et des organes d'application de la loi[122]. Facebook publie des rapports de transparence sur les demandes de données à caractère personnel concernant ses utilisateurs qui émanent des organes de répression[123]. Vodafone publie un rapport de transparence sur les Etats qui exigent la divulgation de données sur le trafic des communications[124], en indiquant la base juridique sur laquelle reposent ces demandes.

[116] http://www.google.com/transparencyreport/
[117] https://transparency.twitter.com/
[118] Vodafone.com, Country-by-country disclosure of law enforcement assistance demands, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html
[119] Voir Conseil des droits de l'homme, Résolution « Les droits de l'homme et les sociétés transnationales et autres entreprises » (A/HRC/RES/17/4).
[120] http://www.google.com/transparencyreport/
[121] http://www.google.com/transparencyreport/userdatarequests/?hl=en
[122] https://transparency.twitter.com/
[123] https://www.facebook.com/about/government_requests
[124] http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf

ANNEXE VI

Déclaration interprétative du Représentant de la Fédération de Russie (RF) concernant le projet de recommandation du Comité des Ministres aux Etats membres sur la liberté d'internet

Le projet de recommandation du Comité des Ministres aux Etats membres sur la liberté d'internet interfère substantiellement avec des questions de compétence interne des Etats et nécessite des améliorations du point de vue du consentement des Etats avec l'idée même du projet et la méthodologie de sa mise en œuvre au niveau national. Le document ne répond pas à la question de savoir comment les indicateurs proposés seront appliqués au cours de l'évaluation, qui seront les acteurs d'un tel processus, quelle sera la procédure et qui mesurera les résultats de l'évaluation, de même que s'il existe un cadre quelconque pour la procédure mentionnée plus haut.

De ce fait, la Fédération de Russie ne peut pas soutenir le projet de document tant que toutes les parties prenantes ne sont pas précisées et les procédures clarifiées.

Se référant aux considérations énoncées plus haut, la Fédération de Russie s'abstient de soutenir ce document, considère qu'il n'engage pas la Russie et soumet cette déclaration pour qu'elle soit intégrée au rapport de la 9è réunion du CDMSI.

ANNEXE VII

Stratégie sur la gouvernance d'internet 2016-2019

Démocratie, droits de l'homme et prééminence du droit dans le monde numérique
Projet final[125]

Introduction

1. Internet joue un rôle de plus en plus important dans les activités quotidiennes des citoyens européens. Il est donc essentiel que cet environnement soit sûr, ouvert et stimulant pour tous, sans discrimination aucune[126]. Il importe que tous les citoyens soient en mesure d'exercer leurs droits humains et leurs libertés fondamentales sur internet, y compris le droit au respect de la vie privée et à la protection des données personnelles, sauf restrictions strictement limitées à certains cas. Ils doivent être protégés contre la criminalité et l'insécurité en ligne ainsi que contre une surveillance illégale de leurs activités . Ils doivent être libres de communiquer sans être soumis à la censure ou à d'autres ingérences et se sentir en confiance lorsqu'ils partagent leurs données personnelles et lorsqu'ils créent et agissent en ligne. En tant qu'outil et espace public pour la démocratie, la gouvernance d'internet devrait faciliter le dialogue et l'interaction entre tous les segments de la population afin de promouvoir le respect, l'égalité, la tolérance et le vivre ensemble qui permettre ainsi à chacun de s'engager et de participer à une société démocratique. Avant tout, internet devrait demeurer universel et novateur et continuer à servir les intérêts des utilisateurs. Il s'agit d'une ressource mondiale dont l'intégrité devrait être protégée et gérée dans l'intérêt général. Le Conseil de l'Europe devrait promouvoir la participation de toutes les parties prenantes, dans leurs rôles respectifs, à la gouvernance de l'Internet.

Une continuité de valeurs fondamentales

2. La stratégie sur la gouvernance de l'internet 2012-2015 a regroupé les normes pertinentes du Conseil l'Europe et les activités de suivi, de coopération et de renforcement des capacités. La stratégie a établi des liens entre les traités juridiquement contraignants de l'Organisation, tels que les conventions de Budapest[127], d'Istanbul[128] et de Lanzarote[129], les stratégies transversales sur l'égalité entre les femmes et les hommes et les droits de l'enfant, la plateforme dynamique pour la participation des jeunes, et a donné lieu à la rédaction du Guide des droits de l'homme pour les utilisateurs d'internet. Elle a permis aux États membres de débattre des enjeux culturels d'internet. Elle a aussi facilité une meilleure coordination interne au sein du Conseil de l'Europe.

3. Le Conseil de l'Europe est reconnu pour ses travaux sur la protection de l'universalité, de l'intégrité et de l'ouverture d'internet. Il a réaffirmé la nécessité de protéger et de responsabiliser les citoyens sans entraver leur liberté d'utiliser internet dans leurs activités quotidiennes. Il a reconnu la mission de service

[125] La Fédération de Russie s'est abstenue de soutenir le projet.

[126] Ils ne doivent subir aucune discrimination sous quelque motif que ce soit, qu'elle se fonde sur le sexe, la race, la couleur, la langue, la religion ou les convictions, les opinions politiques ou autres, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance, l'appartenance ethnique, l'âge ou l'orientation sexuelle (par. 4 de l'annexe à la Recommandation du CM sur le Guide des droits de l'homme pour les utilisateurs d'internet).
[127] Convention du Conseil de l'Europe sur la cybercriminalité (STCE n° 185).
[128] 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).
[129] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).

public d'internet et notamment les attentes légitimes de ses utilisateurs. L'organisation a également été en relation avec de nombreux acteurs publics et privés aux niveaux européen et mondial et a pu transmettre des messages importants en insistant en particulier sur la nécessité de ne pas nuire au fonctionnement d'internet et de ne pas diffuser de discours de haine en ligne.

Buts et objectifs

4. La stratégie est un instrument multidisciplinaire qui traite de questions concernant les contenus, les services et les appareils connectés à l'internet, ainsi que les aspects pertinents de son infrastructure et de son fonctionnement qui peuvent avoir une incidence sur les droits de l'homme et les libertés fondamentales. Elle recense les nombreux défis liés à internet et fournit aux gouvernements et autres parties prenantes - dont la société civile, le secteur privé et les milieux techniques et universitaires - les moyens de les relever.

5. Son objectif global est de faire en sorte que les politiques publiques relatives à internet soient centrées sur les personnes, ce qui signifie qu'elles doivent respecter les valeurs fondamentales de la démocratie, des droits de l'homme et de l'État de droit. Elle a pour objectifs stratégiques de construire une démocratie en ligne, de protéger les utilisateurs d'internet et de veiller au respect et à la protection des droits de l'homme en ligne. À cette fin, la stratégie propose une série d'activités spécifiques.

Objectifs stratégiques

Construire la démocratie en ligne

6. Internet revêt une valeur essentielle pour la démocratie. La possibilité qu'il offre aux personnes de communiquer et d'échanger leurs idées, leurs connaissances et leurs opinions, ainsi que de partager et de stocker de grandes quantités d'informations est à une échelle sans précédent. Il permet aussi d'améliorer la compréhension mutuelle et la tolérance entre personnes de cultures, d'origines et de convictions diverses. Il favorise l'inclusion et la participation de tous sans discrimination et aide à mettre en relation ceux qui peuvent se sentir vulnérables ou marginalisés, facilitant ainsi leur accès aux services publics. En faisant entendre leur voix sur internet, les personnes vivant dans des régions reculées ou sous-développées, y compris les personnes handicapées, contribuent au pluralisme et à la diversité des échanges ainsi qu'à l'amélioration du dialogue entre les Etats et les citoyens.

7. Il ne suffit pourtant pas de mettre en œuvre des initiatives en matière de démocratie et de vote électronique, de gouvernement et de justice électroniques, l'application dans les faits de la mission de service public devrait être davantage développée. Il faut aussi permettre la participation en ligne dans la vie publique, y compris au niveau local, en respectant la vie privée des citoyens (et leur liberté face à la surveillance de masse) tout en veillant à ce que le traitement des informations à caractère personnel ne donne pas lieu à une gestion ou une utilisation à mauvais escient. La mise en place d'une démocratie en ligne dépend d'un certain nombre de conditions préalables et notamment de l'accès à une culture numérique durable et à un contenu numérique authentique ainsi qu'à des documents et données à caractère public. Il importe aussi de mettre en place de nouvelles approches de l'administration publique et de la prestation de services pour améliorer la gouvernance électronique au niveau local, ainsi que d'introduire des méthodes innovantes d'engagement et de participation au processus démocratique. Il est important d'intégrer l'éducation à la citoyenneté numérique dans les systèmes d'enseignement formels dans les programmes officiels. Cela

suppose aussi d'encourager les citoyens à s'intéresser à la culture numérique, à tirer parti de son potentiel d'inclusion et d'innovation et à établir une relation saine et équilibrée avec internet, fondée sur la liberté de se connecter mais aussi de se déconnecter (ce que l'on appelle « désintoxication numérique »).

8. Dans ce contexte, le Conseil de l'Europe :

   a. continuera à développer son réseau d'innovateurs de la démocratie (numérique) à l'occasion du Forum mondial de la démocratie. Parmi les sujets de discussion qui pourraient être examinés figurent l'avenir d'internet et de sa gouvernance, les gains en termes d'efficacité et de responsabilisation permis par les outils numériques, la participation citoyenne et la transparence dans la démocratie, une éventuelle « Magna Carta » d'internet et une « citoyenneté internet ».

   b. explorera les moyens de prévenir et combattre les discours de haine en ligne, notamment les discours conduisant à la violence, et proposera pour ce faire des mesures concrètes. Celles-ci incluent l'organisation de campagnes de sensibilisation destinées à éviter et combattre les manifestations de haine envers tout membre ou tout groupe au sein de la société, ainsi que la poursuite de la campagne contre le discours de haine.

   c. lancera une consultation et une enquête sur l'éducation européenne formelle et non-formelle, les connaissances importantes, les compétences et les attitudes dans le monde numérique en vue d'élaborer un livre blanc sur l'éducation aux médias et à l'information. Par ailleurs, des Lignes directrices sur l'éducation à la citoyenneté numérique dans les établissements scolaires européens seront développées et un réseau européen d'écoles de la citoyenneté numérique, ainsi que des insignes numériques de reconnaissance des compétences démocratiques, fondés sur le cadre des compétences pour une culture démocratique, seront créés.

   d. Eu égard au consensus international sur l'importance de la transition d'une société de l'information à une société de la connaissance, favorisera activement le principe de multilinguisme pour promouvoir la diversité culturelle et linguistique,

   e. encouragera le travail des jeunes en favorisant leur participation en ligne, leur éducation aux médias et à l'environnement numérique, y compris les jeunes marginalisés et défavorisés.

   f. continuera à renforcer le dialogue européen et l'échange de bonnes pratiques concernant la création et la gestion de la culture numérique, ainsi que l'accès à cette culture, en vue d'encourager la participation des citoyens, l'ouverture, l'inclusion et la tolérance dans les sociétés démocratiques. Cela consistera notamment à organiser une plateforme d'échanges multipartites, à élaborer des lignes directrices à l'intention des Etats membres, des institutions culturelles et des professionnels et à concevoir un site web interactif sur l'internet des citoyens.

Assurer la sûreté et la sécurité en ligne pour tous

9. La sûreté et la sécurité en ligne des usagers d'internet relèvent d'une responsabilité partagée. Cela passe entre autres par la lutte contre la l'extrémisme violent et la radicalisation, la cybercriminalité, ainsi que l'exploitation, le harcèlement et l'intimidation d'usagers d'internet. Cela comprend aussi la protection des enfants contre l'exploitation et les abus sexuels en ligne, la

lutte contre le trafic d'organes, la traite des êtres humains, et la vente de médicaments contrefaits et de drogues. Des efforts constants pour faire face à ces menaces sont indispensables pourvu que les mesures prises soient soumises aux conditions et aux garanties pour une protection adéquate des droits de l'homme et des libertés fondamentales.

10. Dans ce contexte, le Conseil de l'Europe :

    a. continuera à agir pour faire de la Convention de Budapest sur la cybercriminalité et de la « Convention n° 108 » sur la protection des données[130] des normes mondiales du Conseil de l'Europe et encouragera le plus grand nombre possible de pays à y adhérer. La mise en œuvre de ces Conventions nécessite un travail de renforcement des capacités ainsi que de favoriser la coopération internationale. Cela comprend aussi la mise en place de politiques et de principes communs pour la gouvernance d'internet, y compris en matière de sécurité des réseaux et de l'information.

    b. animera le débat et proposera des mesures concrètes concernant les questions de surveillance de masse et d'interception massive de données, par exemple la mise en place de failles et de « backdooors » dans la sécurité de l'information et des systèmes de communication, ainsi que les défis relatifs à la protection des données personnelles et plus généralement des droits de l'homme, tout en garantissant la sécurité et sûreté.

    c. élaborera une stratégie pour lutter contre l'extrémisme violent et la radicalisation sur internet appliquée à tous les niveaux de gouvernement, en synergie avec le Plan d'action 2015-2017 du Conseil de l'Europe et de la Convention pour la prévention du terrorisme, y compris de son Protocole additionnel sur les combattants terroristes étrangers.

    d. assurera le suivi des mesures prises pour protéger toute personne, en particulier les femmes et les enfants, contre les abus commis en ligne tels que le cyber-harcèlement, le sexisme et les menaces de violence sexuelle.

Respecter et protéger les droits fondamentaux de chacun dans le monde numérique

11. Les individus utilisent internet dans leurs activités quotidiennes et on peut se féliciter qu'ils soient de plus en plus nombreux à accéder aux services en ligne. Pour beaucoup, notamment les enfants et les jeunes, c'est leur principal moyen d'information et d'expression. Internet est donc un espace précieux pour l'exercice des droits fondamentaux tels que la liberté d'expression et d'information. De plus, une meilleure prise de conscience des attentes légitimes et des restrictions attachées aux services internet et des voies de recours et de réparation en cas de violation des droits de l'homme est nécessaire. Les acteurs des médias, anciens et nouveaux, jouent un rôle important de facilitateurs d'accès à une information pluraliste et diversifiée qu'il convient de souligner, sans perdre de vue qu'il est toujours possible de filtrer le trafic internet et d'intervenir dans les contenus.

12. Les droits fondamentaux des usagers d'internet sont de plus en plus exposés car il est de plus en plus facile de se connecter ou d'être connecté à l'internet et aux technologies de l'information et de la communication (TIC) en utilisant quotidiennement des appareils ou objets (domestiques), par exemple, une voiture ; ceci est communément appelée "internet des objets". Le suivi et la

[130] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108).

surveillance numériques, la collecte de données à caractère personnel à des fins de profilage, dont des données sensibles relatives à la santé, constituent une menace pour la vie privée et l'exercice général des droits humains, y compris la liberté d'expression et l'accès à l'information. Les outils de protection de l'anonymat et de chiffrement peuvent aider les usagers d'internet à se prémunir contre ces menaces ; les Etats membres doivent respecter leur volonté de ne pas divulguer leur identité, ce qui ne doit pas pour autant les empêcher de prendre des mesures et de coopérer afin de repérer les auteurs d'actes criminels.

13. Dans ce contexte, le Conseil de l'Europe :

    a. favorisera la création d'un réseau d'institutions nationales ayant pour but de guider les utilisateurs d'internet qui souhaitent introduire un recours et demander réparation lorsque leurs droits de l'homme ont été restreints ou violés, sur la base du Guide des droits de l'homme pour les utilisateurs d'internet élaboré par le Conseil de l'Europe. Il s'agira d'aider à l'instauration d'une coopération grâce à des actions de sensibilisation du public et de mettre au point des outils pour renforcer les capacités.

    b. rédigera un rapport triennal sur l'état de la protection des données et du respect de la vie privée sur internet en Europe, eu égard à la « Convention n° 108 » (modernisée) sur la protection des données.

    c. élaborera des politiques sur le rôle des intermédiaires et leur importance pour la liberté d'expression et la liberté des médias, à la lumière de la jurisprudence de la Cour européenne des droits de l'homme et en tenant compte des meilleures pratiques en matière de blocage, de filtrage et de suppression de contenus sur internet .

    d. établira des rapports périodiques sur la situation des médias et de la liberté sur internet conformément aux normes du Conseil de l'Europe, en s'appuyant notamment sur la Plateforme du Conseil de l'Europe visant à renforcer la protection du journalisme et la sécurité des journalistes et sur les rapports du Secrétaire Général sur la liberté d'expression en Europe.

    e. Créera une plateforme réunissant les gouvernements, les grandes entreprises actives sur internet et les associations représentatives sur leur respect des droits de l'homme en ligne, y compris les mesures qu'ils prennent pour protéger et respecter ces droits et pour remédier aux violations qu'ils subissent (telles que les dispositions contractuelles types relatives aux conditions de service des plateformes internet, et les principes de responsabilité et de transparence envers les multiples parties prenantes eu égard à la collecte, le stockage et l'analyse de données personnelles).

    f. évaluera et réexaminera, en coopération avec les gouvernements, la Commission européenne et d'autres parties prenantes à la gouvernance d'internet, la gouvernance de la « santé mobile » (m-santé) et de la « santé électronique » (télésanté), afin de préserver et améliorer l'accès des patients à tous les produits médicaux et de soins de santé (de qualité), ainsi qu'aux services d'information et services connexes. Il s'agira notamment d'étudier les moyens d'empêcher la vente illégale de drogues et de médicaments contrefaits, ainsi que le trafic illicite de drogues en ligne.

<u>Partenariats et synergies</u>

14. Le Conseil de l'Europe reconnaît les travaux des principaux acteurs dans le domaine de la gouvernance d'internet, notamment les organisations

internationales compétentes, le secteur privé et la société civile, et s'engage fermement à coopérer avec eux. Il appuie également les travaux des autres acteurs de la gouvernance d'internet qui contribuent à orienter les politiques publiques dans ce domaine.

15. La protection et la promotion effectives de la démocratie, des droits de l'homme et de l'Etat de droit dans le monde numérique sont des tâches et un objectif communs à de nombreuses parties prenantes. Cela suppose des partenariats et des synergies entre les Etats, les organisations internationales, la société civile, le secteur privé et les milieux techniques et universitaires. C'est pourquoi le Conseil de l'Europe examinera, renforcera et développera des synergies et des partenariats avec les principales parties prenantes, notamment:

    e. l'Union européenne ;
    f. l'Organisation pour la sécurité et la coopération en Europe (OSCE) ;
    g. l'Organisation de coopération et de développement économiques (OCDE) ;
    h. l'Organisation des Nations Unies et ses institutions, notamment celles participant au suivi et la mise en œuvre du Sommet mondial sur la société de l'information (SMSI) : l'Organisation des Nations Unies pour l'éducation, la science et la culture (Unesco), le Haut-Commissariat aux droits de l'homme, l'Office des Nations Unies contre la drogue et le crime (ONUDC) et l'Union internationale des télécommunications (UIT) ;
    i. les organisations, réseaux et initiatives œuvrant contre la cybercriminalité et pour la cybersécurité telles qu'Europol, Interpol, le Groupe de travail virtuel international, le Commonwealth, etc. ;
    j. l'Union européenne de radio-télévision (UER) ;
    k. la Banque mondiale ;
    l. des réseaux et organes de gouvernance d'internet, en particulier le Dialogue européen sur la gouvernance de l'internet (EuroDIG), le Forum sur la gouvernance de l'internet (FGI), l'Internet Corporation for Assigned Names and Numbers (ICANN)., les initiatives nationales en matière de gouvernance d'internet, la « Freedom Online Coalition », le « London Process », l'initiative « NETmundial » et l'Internet Society (ISOC) ;
    m. le secteur privé et les associations représentatives, notamment l'Association européenne des fournisseurs de services internet (EuroISPA) ;
    n. le Forum européen de la jeunesse et les réseaux de jeunesse associés ;
    o. les réseaux culturels et les associations professionnelles représentatives telles que CultureActionEurope;
    p. le monde de la recherche.

<u>Méthodes de travail et incidences budgétaires</u>

16. Le Conseil de l'Europe mettra en œuvre la stratégie en conformité avec la Convention européenne des droits de l'homme et la jurisprudence de la Cour européenne des droits de l'homme et de ses traités et mécanismes juridiquement contraignants, le cas échéant en collaboration avec l'Assemblée parlementaire, le Congrès des pouvoirs locaux et régionaux, la Conférence des OING, et le Commissaire aux droits de l'homme. Il s'appuiera sur ses comités directeurs et ses comités conventionnels, ses stratégies transversales en matière d'égalité entre les femmes et les hommes et des droits de l'enfant, ses organes de suivi, ses commissions, ses réseaux, dont les comités nationaux chargés de la campagne contre le discours de haine et ses programmes de coopération et de

renforcement des capacités, ainsi que sur l'action de son Secrétariat. Il comprendra notamment une évaluation continue des instruments juridiques et autres travaux relatifs à la gouvernance d'internet.

17. La stratégie s'étendra sur deux cycles budgétaires bisannuels du Conseil de l'Europe (2016-2017 et 2018-2019). Les principales actions et activités mises en œuvre correspondent aux priorités du Secrétaire Général pour 2016-2017 (voir document CM (2015) 81) telles que reflétées par le programme et le budget. Des ressources extrabudgétaires et des financements au titre de programmes conjoints pourront également être utilisés.

Planification, mise en œuvre et évaluation de la stratégie

18. La stratégie sera exécutée par les comités conventionnels et les comités directeurs compétents du Conseil de l'Europe ainsi que par l'intermédiaire de ses réseaux et plateformes qui rassemblent, notamment, des jeunes, des ONG, des pouvoirs publics et des professionnels du droit. Le Comité directeur sur les médias et la société de l'information (CDMSI) sera chargé de superviser la mise en œuvre de la stratégie en étroite coopération avec le Coordinateur thématique sur la politique d'information du Comité des Ministres (TC-INF)

19. Le Secrétaire Général assurera la planification stratégique, la mise en œuvre et l'évaluation de la stratégie.

20. De même, le Secrétaire Général veillera à ce que les travaux relatifs à la gouvernance d'internet soient préparés en concertation avec les parties prenantes pertinentes. Il veillera à l'équilibre entre les femmes et les hommes dans le cadre de ces processus, qui seront aussi inclusifs que possible et s'inspireront des bonnes pratiques..

21. Des méthodes de travail transversales seront mises au point, s'il y a lieu, pour faciliter la réalisation des objectifs stratégiques. Les bonnes pratiques et le cas échéant, les actions en cours résultant de la stratégie de gouvernance de l'internet 2012-2015 seront poursuivies.

22. Le Secrétaire Général fera le point sur l'état d'avancement de la mise en œuvre de la stratégie dans un rapport d'évaluation à mi-parcours et un rapport final qui seront soumis au Comité des ministres pour examen en temps opportun.

Projet de Stratégie du Conseil de l'Europe sur la gouvernance de l'internet 2016-2019

Glossaire terminologique

- **« Désintoxication numérique »** : période pendant laquelle une personne s'abstient d'utiliser des appareils électroniques comme des smartphones ou des ordinateurs, considérée comme une occasion de réduire le stress ou de se concentrer sur les relations sociales dans le monde physique[131].

- **Dialogue européen sur la gouvernance de l'internet (EuroDIG)** : EuroDIG est une plate-forme ouverte multi-partenariale d'échange de points de vue sur internet et la façon dont il est géré. Créée en 2008 par diverses organisations, représentants gouvernementaux et experts, elle encourage le dialogue et la collaboration avec la communauté des internautes sur les politiques publiques concernant internet. Lors d'une conférence annuelle qui a lieu dans une capitale différente chaque année, les « messages » d'EuroDIG sont préparés et présentés au Forum sur la gouvernance de l'internet, organisé sous l'égide de l'ONU. EuroDIG est soutenu par un groupe de partenaires institutionnels, à savoir le Conseil de l'Europe, la Commission européenne, l'Internet Society (ISOC), la European Regional At-Large Organization (EURALO), l'Union européenne de radiodiffusion (UER), le centre de coordination des Réseaux IP Européens (RIPE NCC) et l'Office fédéral Suisse de la communication (OFCOM, Suisse).

- **Freedom Online Coalition** : la Freedom Online Coalition est un groupe de gouvernements qui se sont engagés à œuvrer ensemble pour défendre la liberté d'internet et protéger les droits fondamentaux de l'homme – liberté d'expression, d'association, de réunion et respect de la vie privée en ligne – partout dans le monde. Elle a été créée en 2011, lors de la conférence inaugurale « Freedom Online Conference » à La Haye, aux Pays-Bas, à l'initiative du ministère néerlandais des Affaires étrangères. Aujourd'hui, elle compte 28 membres, de l'Afrique à l'Asie en passant par l'Europe, les Amériques et le Moyen-Orient. Tous les Etats membres ont signé le document fondateur de la coalition (Freedom Online: Joint Action for Free Expression on the internet) et se sont engagés en faveur du principe selon lequel les droits garantis aux citoyens en ligne sont les mêmes que les droits hors ligne. Les membres de la coalition coordonnent leurs efforts diplomatiques, partagent des informations sur les violations des droits de l'homme en ligne et œuvrent ensemble pour faire connaître leurs préoccupations relatives aux mesures qui restreignent les droits de l'homme en ligne. La coalition collabore aussi en publiant des déclarations communes, en partageant les approches politiques de questions complexes, en échangeant des points de vue sur la stratégie et en organisant la participation à des forums pertinents dans ce domaine.

- **L'internet des citoyens** : renvoie au projet de recommandation du Comité des Ministres du même nom, qui dispose que: « Outre l'investissement dans l'aspect technique et infrastructurel de « l'internet des objets », il convient d'être tout aussi attentif à la dimension culturelle de celui-ci et à « l'internet des citoyens ». Le terme « citoyen » s'entend ici non pas au sens juridique mais au sens général, c'est-à-dire de simple personne. »

- **Société pour l'attribution des noms de domaine et des numéros sur internet (ICANN)**: L'ICANN est un organisme à but non lucratif responsable de

[131] http://www.oxforddictionaries.com/definition/english/digital-detox

la sécurité, la stabilité et la coordination mondiale du système d'identificateurs uniques de l'internet.[132]

- **Gouvernance de l'internet :** élaboration et 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[133].

- **Forum sur la gouvernance de l'internet (FGI)** : dans le cadre du Sommet mondial des Nations unies sur la société de l'information (SMSI), en particulier conformément au paragraphe 72 de l'Agenda de Tunis pour la société de l'information, le Forum sur la gouvernance de l'internet a pour mandat :

  a. de traiter les questions de politique publique relatives aux principaux éléments de la gouvernance de l'internet afin de contribuer à la viabilité, à la solidité, à la sécurité, à la stabilité et au développement de l'internet ;
  b. de faciliter le dialogue entre les organes s'occupant de différentes politiques publiques internationales multisectorielles concernant l'internet et de débattre des questions qui ne relèvent pas de la compétence d'un organe déjà existant ;
  c. de faire l'interface avec les organisations intergouvernementales et d'autres institutions appropriées sur les questions relevant de leur mandat ;
  d. de faciliter l'échange d'informations et de bonnes pratiques et, à cet égard, d'utiliser pleinement les compétences des communautés universitaires, scientifiques et techniques ;
  e. de conseiller toutes les parties prenantes en vue de proposer les moyens qui permettront que l'internet soit disponible et financièrement abordable plus rapidement dans les pays en développement ;
  f. de renforcer et d'accroître l'engagement des parties prenantes, en particulier celui des pays en développement, dans les mécanismes de gouvernance de l'internet existants ou futurs ;
  g. de recenser les nouvelles questions et de les porter à l'attention des organes compétents et du public en général et, s'il y a lieu, de faire des recommandations ;
  h. de contribuer au renforcement des capacités en matière de gouvernance de l'internet dans les pays en développement, en s'appuyant pleinement sur les sources de savoir et de compétences locales ;
  i. de promouvoir la prise en compte des principes du SMSI dans les mécanismes de gouvernance de l'internet et de l'évaluer régulièrement ;
  j. de traiter notamment les questions relatives aux ressources fondamentales de l'internet ;
  k. d'aider à trouver les solutions aux problèmes découlant de l'utilisation et de la mauvaise utilisation de l'internet qui préoccupent particulièrement l'usager ordinaire ;
  l. de publier ses travaux.

- **Internet Society (ISOC)** : l'ISOC est une organisation non gouvernementale internationale pour la coopération et la coordination mondiales relatives à l'internet et à ses technologies et applications de mise en réseau. Les membres de cette société, qu'il s'agisse d'individus ou d'organisations, sont liés l'objectif commun, de maintenir la viabilité et l'évolutivité de l'internet. Ce sont des entreprises, des agences gouvernementales et les fondations qui ont créé internet

[132] https://www.icann.org/fr

[133] Rapport du Groupe de travail sur la gouvernance de l'internet, Château de Bossey, juin 2005 : http://www.wgig.org/docs/WGIGREPORT.pdfhttp://www.wgig.org/docs/WGIGREPORT.pdf

et ses technologies, ainsi que de nouvelles sociétés d'innovation entrepreneuriale contribuant à maintenir cette dynamique.[134]

- **« Processus de Londres »** : Conférence mondiale sur le cyberespace (également connue sous le nom de « processus de Londres ») - il est d'une conférence annuelle depuis 2011, où les gouvernements, le secteur privé et la société civile se réunissent pour promouvoir une coopération concrète dans le cyberespace, renforcer les cybercapacités et discuter de normes pour un comportement responsable dans le cyberespace. La première conférence s'est tenue en novembre 2011 à Londres. Un ensemble de principes « pour un comportement responsable dans le cyberespace » a été élaboré à l'issue de discussions rassemblant 700 participants. La deuxième conférence a eu lieu les 4 et 5 octobre 2012 à Budapest, la troisième les 17 et 18 octobre 2013 à Séoul. La quatrième s'est tenue sous la forme d'un forum mondial organisé les 16 et 17 avril 2015 à La Haye.[135]

- **« Cyber-citoyenneté »** : le « net-citoyen » est une personne qui participe activement aux communautés en ligne ou un internaute actif en général. Ce terme implique aussi habituellement un intérêt et un engagement actif en faveur de l'amélioration d'internet afin qu'il devienne une ressource intellectuelle et sociale, ou des structures politiques environnantes, plus particulièrement en ce qui concerne le libre accès à internet, la neutralité du réseau et la liberté d'expression. Les net-citoyens sont aussi connus sous le nom de « cyber-citoyens », terme qui a des connotations similaires[136].

- **« NETmundial » et l'initiative NETmundial :** la réunion NETmundial, qui s'est tenue à São Paulo, au Brésil, en avril 2014, a constitué une référence pour les gouvernements, le secteur privé, la société civile, les milieux techniques et les universités à travers le monde afin de relever les défis liés à la gouvernance de l'internet. Son document de conclusions (lien extérieur), la déclaration multipartite NETmundial, a reconnu qu'internet est une ressource mondiale qui doit être gérée dans l'intérêt public. Elle a également réaffirmé l'importance des droits de l'homme sur internet et fourni un ensemble de principes de gouvernance de l'internet, ainsi qu'une feuille de route pour l'évolution future et l'amélioration du cadre existant de gouvernance de l'internet qui garantit la participation pleine et entière de toutes les parties prenantes. L'initiative NETmundial reconnaît les principes de NETmundial pour le processus de gouvernance de l'internet : une gouvernance démocratique, multipartite, ouverte, participative, basée sur le consensus, transparente, responsable, inclusive et équitable, distribuée, concertée et permettant une participation significative. Elle cherche à promouvoir l'esprit de coopération de São Paulo en proposant des occasions de collaboration et de coopération à toutes les parties prenantes.[137]

- **La valeur de service public de l'internet :** tiré de la Recommandation CM/Rec(2007)16
du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public d'internet compris comme « le recours manifeste des personnes à l'internet comme outil essentiel de leurs activités quotidiennes (communication, information, savoir, transactions commerciales) ainsi que

[134] http://www.businessdictionary.com/definition/internet-society-ISOC.html
[135] https://en.wikipedia.org/wiki/Global_Conference_on_CyberSpace .
[136] https://fr.wiktionary.org/wiki/net-citoyen; https://fr.wiktionary.org/wiki/cybercitoyen

[137] https://www.netmundial.org/fr/principes

l'attente légitime de services internet accessibles, abordables, sécurisés, fiables et continus qui en résulte. »[138]

[138] https://wcd.coe.int/ViewDoc.jsp?id=1207291

Projet de stratégie sur la gouvernance d'internet 2016-2019 – Annexe des activités

Pilier et thème	Activités	Calendrier	Entité administrative
Construire la démocratie en ligne			
Vote électronique	Mise à jour de la Recommandation Rec(2004)11 du Conseil de l'Europe sur les normes juridiques, opérationnelles et techniques relatives au vote électronique, et travaux de suivi de l'instrument, notamment des réunions biennales consacrées à son examen, un suivi du respect de sa mise en œuvre dans les Etats membres, l'élaboration de lignes directrices complémentaires, l'identification de bonnes pratiques, la fourniture d'une assistance technique aux Etats membres pour l'adoption d'un système de vote électronique, l'organisation d'actions de sensibilisation et d'éducation des électeurs, la surveillance avec les observateurs nationaux des élections par voie électronique.		DG2 – Direction de la gouvernance démocratique, Service des institutions et de la gouvernance démocratiques, Division Elections
Démocratie et participation	Présentation et analyse de plateformes de participation électronique dans le cadre de chaque édition annuelle du Forum mondial de la démocratie. Soutien à l'introduction de plateformes de participation électronique aux plans local et national, renforcement des capacités et échange de bonnes pratiques. Développement et mise à l'essai d'un outil d'évaluation de la démocratie participative au niveau local, y compris la participation par le biais d'internet.		DG2- Direction de la gouvernance démocratique, Service des initiatives démocratiques, Division Forum mondial de la démocratie
Mouvement contre le discours de	La campagne du Conseil de l'Europe contre le discours de haine poursuivra ses actions en 2016-2017, en insistant davantage sur l'éducation aux droits de l'homme et à la citoyenneté numérique,		DG2- Direction de la citoyenneté démocratique et de la

haine	sur l'amélioration et la diffusion de mécanismes de signalement et de suivi des discours de haine. Au titre du Plan d'action de lutte contre l'extrémisme violent et la radicalisation conduisant au terrorisme, la campagne joue un important rôle de prévention de ce phénomène sur internet. Des contre-arguments seront développés afin de permettre aux internautes de répondre aux discours de haine en ligne ou de les neutraliser. La Commission européenne contre le racisme et l'intolérance (ECRI) doit adopter, début 2016, une Recommandation de politique générale sur la lutte contre le discours de haine. Promouvoir la mise en œuvre du Protocole additionnel à la Convention de Budapest relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STCE 189) en tant qu'outil de lutte contre le discours de haine en ligne		participation, Service Jeunesse, Division Education non formelle et formation DG2- Direction de la dignité humaine et de l'égalité, Service de l'anti-discrimination et de la cohésion sociale, Commission européenne contre le racisme et l'intolérance (ECRI) DG1-Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Division Cybercriminalité
Citoyenneté numérique	Examiner la documentation officielle et informelle (disponible sur les blogs, wikis et sites internet), pour analyser le concept de citoyenneté numérique, les politiques et pratiques actuelles et contemporaines d'éducation numérique et les difficultés rencontrées dans les écoles.		DG2- Direction de la citoyenneté démocratique et de la participation, Service de l'éducation, Division Politiques éducatives

	Organiser des consultations/débats multipartites sur les questions politiques concernant la place et une meilleure utilisation des ressources en ligne et des technologies de l'information d'aujourd'hui (sites de réseaux sociaux et Web 2.0 ou sites éducatifs Web 2.0, ainsi que les équipements personnels) dans les structures scolaires (programmes et associations scolaires) et cartographie des responsabilités administratives et juridiques des chefs d'établissements, enseignants, élèves et parents. Élaborer des lignes directrices pour soutenir davantage les instances nationales dans la formulation de politiques d'éducation à la citoyenneté numérique afin de traiter les problèmes d'apprentissage ainsi que les besoins des étudiants, et fournir des conseils dans l'élaboration de politiques permettant de mieux protéger les étudiants qui travaillent dans des environnements ouverts et collaboratifs en ligne. Promouvoir et partager de bonnes pratiques des Etats membres sur des programmes interactifs efficaces pour l'acquisition par les élèves de compétences citoyennes numériques via le programme d'étude et, pour les enseignants, via la formation initiale et continue. A partir de l'expérience des Etats membres, définir un ensemble de descripteurs de compétence en matière d' éducation à la citoyenneté numérique et établissement de critères pour l'intégration de ce type de descripteurs dans les programmes actuels d'éducation à la citoyenneté. Elaboration, en partenariat avec d'autres entités du Conseil de l'Europe, d'orientations politiques concernant les questions éducatives et juridiques transversales auxquelles les instances scolaires peuvent aujourd'hui faire face : cyber intimidation (y compris cyber misogynie, cyber harcèlement d'enseignants), respect de la vie privée, texto pornographie, addiction numérique, relations élèves/enseignants via les médias sociaux (Facebook, etc.), établissements scolaires et sécurité sur internet, liberté		

	d'expression en ligne et droits fondamentaux des élèves dans les environnements numériques.		
Éducation aux médias et à l'information	Une consultation, une enquête et un livre blanc consacrés à l'éducation, aux compétences, aux attitudes et à la pensée critique européennes sont en cours de préparation.		DG2- Direction de la citoyenneté démocratique et de la participation, Service de l'éducation, Division Pratiques éducatives et renforcement des capacités
Culture et numérisation	Les Plateformes d'échanges annuelles du Conseil de l'Europe sur l'incidence du numérique sur la culture seront organisées durant la période 2016-2019 (la prochaine aura lieu en octobre 2016 à Tallinn dans le cadre de la présidence estonienne du Comité des Ministres du Conseil de l'Europe), en vue notamment de recueillir des pratiques culturelles numériques novatrices et les possibilités dans ce domaine pour orienter la formulation de politiques publiques, y compris dans la perspective de relever les défis en matière d'inclusion. De nouvelles lignes directrices politiques seront préparées au terme du processus de consultation de l'ensemble des parties prenantes. Des recueils de bonnes pratiques seront constitués et diffusés en ligne.		DG2-Direction de la gouvernance démocratique, Service des institutions et de la gouvernance démocratiques, Division Culture et démocratie

Privilégier la sécurité en ligne pour tous			
Protection des droits des enfants	Suivre et soutenir la mise en œuvre de la Convention sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote)		DG2-Direction de la dignité humaine et de l'égalité, Service de l'égalité et de la dignité humaine, Division Droits des enfants
Action de lutte contre la cybercriminalité	Achèvement en 2016 du 3e cycle d'évaluation « sanctions et mesures », et démarrage d'autres cycles d'évaluation. Elaboration de solutions concernant l'accès de la justice pénale aux données stockées sur des serveurs d'hébergement dans le nuage et les problèmes connexes de juridiction. L'une des solutions pourrait être l'établissement d'un Protocole à la Convention de Budapest sur la cybercriminalité. Soutien à plus d'une centaine d'activités de renforcement des capacités par an dans toutes les régions du monde et suivi des résultats des évaluations menées par le T-CY. Encourager les enquêtes financières et la confiscation des produits du crime sur internet. Mise en place d'une plateforme de coopération entre les secteurs public et privé.		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Division Cybercriminalité

	Promouvoir la mise en œuvre du Protocole additionnel à la Convention de Budapest relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STCE 189).		
Surveillance de masse	Promotion de la Convention 108 au niveau international (Conférence internationale annuelle des autorités chargées de la protection des données, Association francophone des autorités de protection des données) et fourniture d'une assistance aux pays intéressés (par ex. initiatives nationales relatives à la surveillance de masse).		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Unité Protection des données
Extrémisme et radicalisation sur internet	Elaboration d'une stratégie européenne de lutte contre l'extrémisme et la radicalisation sur internet, menée dans le cadre du Comité d'experts sur le terrorisme (CODEXTER).		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la lutte contre la criminalité
Abus commis en ligne, tels que le cyber harcèlement, le sexisme et les menaces de violence sexuelle	Suivi de la mise en œuvre de la « Convention d'Istanbul ». Le Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO) mènera une première évaluation de la mise en œuvre de la Convention d'Istanbul. Plus spécifiquement, le GREVIO préparera, d'ici mars 2016, un questionnaire de référence et examinera ensuite les rapports soumis en réponse par les Parties. Le GREVIO est également susceptible de mener des visites de pays avant d'élaborer ses rapports d'évaluation. La phase initiale de suivi est censée se poursuivre pendant toute la		DG2- Direction de la dignité humaine et de l'égalité, Service de l'égalité et de la dignité humaine, Division Violence à l'égard des femmes

	durée de la stratégie relative à la gouvernance d'internet 2016-2019, voire au-delà.		
Respecter et protéger les droits fondamentaux de chacun dans le monde numérique			
Autonomisation des enfants	Dans le cadre de la Stratégie sur les droits de l'enfant (2016-2021) : Création et diffusion d'outils pour donner aux enfants, parents et éducateurs les moyens d'exploiter pleinement le potentiel des TIC et des médias numériques. Attention particulière à l'autonomisation des enfants en situation vulnérable, comme les enfants handicapés. Elaboration de lignes directrices pour une approche de la parentalité fondée sur les droits à l'ère numérique. Elaboration de lignes directrices destinées aux Etats membres pour une approche intégrée des droits de l'enfant dans l'environnement numérique.		DG2- Direction de la dignité humaine et de l'égalité, Service de l'égalité et de la dignité humaine, Division Droits des enfants
Voies de recours effectifs en ligne	Soutenir la mise en œuvre du Guide des droits de l'homme pour les utilisateurs d'internet du Conseil de l'Europe en encourageant la création d'un réseau d'institutions nationales, conformément aux travaux du Comité européen de coopération juridique (CDCJ) sur l'efficacité des mécanismes de règlement en ligne des litiges, eu égard aux articles 6 et 13 de la Convention européenne des droits de l'homme.		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information DG1-Direction des droits de l'homme, Service de la coopération judiciaire et juridique, Division Coopération juridique

Protection et confidentialité des données sur internet en Europe	Etablissement de rapports triennaux par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) (sous réserve de la disponibilité des résultats de l'évaluation et conclusions du mécanisme de suivi de la Convention 108 « modernisée » - pas avant 2018).		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Unité Protection des données
Intermédiaires de l'internet, et législations et pratiques nationales en matière de blocage, de filtrage et de suppression de contenus sur internet	Préparation d'un nouvel instrument sur les intermédiaires de l'internet (fournisseurs de services internet et plateformes internet). Finaliser et assurer le suivi de l'étude juridique comparative sur le blocage, le filtrage et la suppression de contenus sur internet dans les 47 Etats membres du Conseil de l'Europe et en assurer le suivi.		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Division Médias et gouvernance de l'internet (2016 – 2017)
Liberté des médias et d'internet en Europe	Plateforme du Conseil de l'Europe sur la sécurité des journalistes et la protection du journalisme. Rapports du Secrétaire Général sur la situation de la démocratie, des droits de l'homme et de l'Etat de droit en Europe, avec une attention particulière accordée à la liberté d'expression sur internet. Adoption prévue début 2016 de la Recommandation du Comité des Ministres sur la liberté d'internet, ainsi que sa mise en œuvre assortie d'activités de renforcement de capacités en matière de gouvernance d'internet et de développement de bonnes pratiques. Etude de faisabilité sur un éventuel instrument normatif sur la couverture médiatique des élections, avec une attention		Direction de la planification politique DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Division Médias et gouvernance de l'internet (2016 – 2017)

	particulière accordée à l'égalité entre les femmes et les hommes et l'utilisation d'internet dans un cadre électoral. Etude sur les questions liées aux droits de l'homme des techniques de traitement automatisé des données (en particulier les algorithmes) et leurs éventuelles conséquences réglementaires. Réflexion et dialogue sur la liberté d'expression à l'ère de la convergence numérique, et en particulier sur l'avenir du journalisme, les organisations de médias et les circuits de production de l'information, le sentiment de peur, l'autocensure et l'éthique journalistique, le développement de la télévision connectée et les défis en matière de pluralisme ou diversité des contenus et de respect des droits de l'homme, ainsi que le juste équilibre entre le droit à la liberté d'expression et le droit au respect de la vie privée dans le contexte de la suppression de résultats produits par des moteurs de recherche.		
Droits de l'homme et entreprises sur internet	Mise en place d'une plateforme entre les gouvernements, les grandes sociétés actives sur internet et les associations représentatives, concernant le respect des droits de l'homme en ligne. Adoption prévue début 2016 du projet de recommandation du Comité des Ministres sur les droits de l'homme et les entreprises, combinée à l'organisation, par le Conseil de l'Europe, d'un événement parallèle au Forum des Nations Unies sur les entreprises et les droits de l'homme (Genève, novembre/décembre 2016 - A confirmer)		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information DG1-Direction des droits de l'homme, Service des politiques et de la coopération en matière de droits de l'homme, Division Coopération intergouvernementale en matière de droits de l'homme

Santé mobile (m-santé) et santé électronique (e-santé), notamment accès à des produits médicaux et des soins de santé (de qualité), et prévention de la vente illicite de drogues et de médicaments contrefaits	Révision de la recommandation de 1997 relative à la protection des données médicales de manière à en élargir le champ d'application et à répondre aux enjeux dans ce domaine. Mise en place par le Groupe Pompidou d'activités de formation et de renforcement des capacités pour les autorités judiciaires et d'application de la loi, et fourniture d'une expertise et d'un éclairage sur le marché de la drogue en ligne (détection et investigation, y compris open source intel) et moyens de paiement (crypto monnaies). Réunion du groupe d'experts du Groupe Pompidou sur la cybercriminalité liée à la drogue (Strasbourg, novembre 2016 – à confirmer) et autres activités visant à encourager la coopération internationale et le partage de bonnes pratiques (y compris une analyse éventuelle des cadres juridiques et lois types). Exploration des possibilités offertes par internet en matière de prévention, de traitement et de réduction des risques, et collecte et partage de bonnes pratiques. Suivi de la conférence internationale « Technologies émergentes et droits de l'homme ».		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information, Unité Protection des données DG1- Direction de la société de l'information et de la lutte contre la criminalité, Groupe Pompidou DG1- Direction des droits de l'homme, Service des politiques et de la coopération en matière de droits de l'homme, Bioéthique

			Direction européenne de la qualité du médicament et soins de santé, Service de la standardisation biologique, des OMCL et des soins de santé, Section Suivi pharmaceutique, Protection sanitaire du consommateur et Lutte contre la contrefaçon
Partenariats et synergies			
Coopération avec les principales parties prenantes	Soutien et participation du Conseil de l'Europe à l'EuroDIG 2016 (Bruxelles, 9-10 juin 2016) Participation du Conseil de l'Europe au Forum sur la gouvernance de l'internet (FGI) 2016 (Mexico, dates à confirmer) Participation du Conseil de l'Europe aux réunions de l'ICANN (ICANN55 - Marrakech, 6-11 mars ; ICANN56 - ville de Panama, 27-30 juin ; ICANN57 - San Juan, 29 octobre - 4 novembre)		DG1- Direction de la société de l'information et de la lutte contre la criminalité, Service de la société de l'information

Annexe VIII

Déclaration interprétative du Représentant de la Fédération de Russie (RF) concernant le projet de Stratégie pour la gouvernance d'inetrnet 2016-2019

Déclaration interprétative du Représentant de la Fédération de Russie (RF) concernant le projet de Stratégie pour la gouvernance d'internet 2016-2019
La Fédération de Russie considère que l'internet, outre les bénéfices économiques qu'il apporte, joue un rôle unique comme base de dialogue entre les citoyens et l'Etat. La RF pense que l'internet doit préserver son architecture ouverte et non-fragmentée en tant que ressource mondiale avec un mécanisme de gouvernance juste et réellement international qui promeuve la confiance ainsi que des capacités universelles et égalitaires pour le développement économique.
La Fédération de Russie défend une internationalisation de la gouvernance de l'internet qui assure un droit égal à tous les Etats de participer au processus ainsi que leur droit souverain à une gouvernance des segments nationaux de l'internet sur la base du droit international.
On observe que le projet de Stratégie pour la gouvernance d'internet 2016-2019 a été élaboré sur la base d'instruments du Conseil de l'Europe non consensuels, incluant la Convention (de Budapest) sur la cybercriminalité, la Convention (d'Istanbul) sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique et la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Dans ce contexte, la Fédération de Russie ne peut mettre en œuvre les parties de la "Stratégie" qui ont été élaborées sur la base des dispositions des conventions susmentionnées.
De même, la Fédération de Russie ne peut soutenir la Plate-forme pour renforcer la protection du journalisme et la sécurité des journalistes dans sa version actuelle puisqu'elle considère que ce n'est pas un mécanisme de monitoring consensuel qui fait doublon avec le travail du bureau du représentant de l'OSCE sur la liberté des médias.
Dans la mesure où ces remarques, comme d'autres et les propositions faites sur le projet par la délégation russe ont été rejetées et ne sont pas reflétées dans le texte, le représentant de la Fédération de Russie n'approuve pas le document cité plus haut dans sa version actuelle.

Annexe IX

Composition of the
Committee of experts on media pluralism and transparency of media ownership - MSI-MED

Composition du
Comité d'experts sur le pluralisme des médias et la transparence de leur propriété – MSI-MED

MEMBER STATES REPRESENTATIVES

1. Ms Helena Mandić - Director of Broadcasting - Communications Regulatory Agency - Bosnia and Herzegovina
2. Mr Nol Reijnders - Senior Adviser - Department for Media, Literature, Libraries - Ministry of Culture, Education and Science - The Netherlands
3. Ms Maria Donde - International Policy Manager in Ofcom – United Kingdom
4. Ms Maja Zaric - Media Advisor - Media Department - Ministry of Culture and Information - Republic of Serbia
5. Mr Evangelos Valmas - Head of Department for Audiovisual Media and Archives - Secretariat General of Information and Communication - Greece
6. Ms Natalie Fercher - Expert on Media and Communication Law - Department of Media Law and Coordination Information Society - Federal Chancellery - Austria
7. Mr Gudbrand Guthus - Director Licensing and Supervision Department - Norwegian Media Authority – Norway

REPRESENTANTS DES ETATS MEMBRES

1. *Mme Helena Mandić - Directrice de la radiodiffusion - Autorité de régulations des communications - Bosnie-Herzégovine*
2. *M Nol Reijnders - Conseiller principal - Service des médias, de la littérature et des bibliothèques - Ministère de la culture, de l'éducation et des sciences - Pays-Bas*
3. *Mme Maria Donde - Gestionnaire des politiques internationales de l'Ofcom - Royaume-Uni*
4. *Mme Maja Zaric - Conseillère des médias - Service des médias - Ministère de la culture et de l'information - République de Serbie*
5. *M Evangelos Valmas - Chef du service des médias et archives audio-visuels - Secrétariat général de l'information et de la communication - Grèce*
6. *Mme Natalie Fercher - Experte en droit des médias et de la communication - Service du droit des médias et coordination de société de l'information - Chancellerie fédérale – Autriche*
7. *M Gudbrand Guthus - Directeur du service des licences et de la surveillance - Autorité des médias de Norvège – Norvège*

INDEPENDENT EXPERTS

1. Damian Tambini - Associate Professor - Director of the Media Policy Project - Programme Director: MSc Media & Communications (Governance) -London School of Economics
2. Mr Tarlach McGonagle - Senior Researcher and Lecturer, Institute for Information Law (IViR) - University of Amsterdam
3. Ms Elda Brogi - Scientific Coordinator - Centre for Media Pluralism and Media Freedom - Robert Schuman Centre for Advanced Studies - European University

EXPERTS INDÉPENDANTS

1. *M Damian Tambini – Professeur agrégé - Directeur du projet de politiques des médias - Directeur du programme MSc Media & Communications – London School of Economics*
2. *M Tarlach McGonagle - Chercheur principal et conférencier à l'Institut pour le droit de l'information (IViR) - Université d'Amsterdam*
3. *Mme Elda Brogi - Coordinatrice scientifique - Centre pour le pluralisme et la liberté des médias - Centre d'études avancées Robert Schuman - Institut de l'université*

Institute

4. Ms Helena Sousa - Associate Professor - Department of Communications Sciences - University of Minho
5. Mr Josef Trappel - Professor for media policy and media economics - Head of the Department of Communication Research at the University of Salzburg
6. Mr Pierre François Docquir - Senior Legal Officer - ARTICLE 19

européenne

4. *Mme Helena Sousa - Professeur agrégé - Service des sciences de la communication - Université de Minho*
5. *M Josef Trappel - Professeur en politiques des médias et économie des médias - Chef du service de recherche en communications de l'Université de Salzbourg*
6. *M Pierre François Docquir - Juriste principal - ARTICLE 19*

Annexe X
Composition of the
Committee of experts on Internet intermediaries - MSI-NET

Composition du Comité d'experts sur les intermédiaires internet - MSI-NET

MEMBER STATES REPRESENTATIVES

1. Ms Karmen Turk – Trinity Tallinn – Estonia

2. Mr Bertrand de la Chapelle – Co-founder and Director of the Internet & Jurisdiction Project, member of ICANN Board – France

3. Ms Sabine Maass – Head of Division 'Legal framework for digital services, media industry', Federal Ministry for Economic Affairs and Energy – Germany

4. Mr Pēteris Podvinskis – Ministry of Foreig Affairs, International Organisations, Public Polic related to Internet – Latvia

5. Mr Arseny Nedyak – Deputy Director, Department of media state policy, Ministry of telecommunication – Russian Federation

6. Ms Tanja Kerševana Smokvina – Principal Advisor to Director General, Agency for Communication Networks and Services – Slovenia

7. Mr Thomas Schneider – Deputy Director of International Affairs, International Information Society Coordinator, Federal Department of the Environment, Transport, Energy and Communication DETEC, Federal Office of Communications (OFCOM) – Switzerland

INDEPENDENT EXPERTS

1. Ms Julia Hornle – Professor of Internet Law, Queen Mary University of London

2. Mr Matthias Kettemann – Postdoc Fellow, Cluster of Excellence "Normative Orders" University of Frankfurt/Main, Germany – Austria

3. Mr Wolfgang Schulz – Professor, Faculty of Law at the University of Hamburg and the Hans-Bredow-Institut

4. Ms Sophie Stalla-Bourdillon – Associate Professor in Information Technology / Intellectual Property Law, Director of ILAWS, Southampton Law School at the University of Southampton

REPRESENTANTS DES ETATS MEMBRES

1. *Mme Karmen Turk – Trinity Tallinn – Estonie*

2. M Bertrand de la Chapelle – Co-fondateur et Directeur du Projet Internet & Jurisdiction, membre du board des directeurs de l'ICANN – France

3. Mme Sabine Maass – Chef de la division « Cadre juridique pour les services numériques, l'industrie des médias »', Ministère Fédéral de l'Economie et de l'Energie - Allemagne

4. M Pēteris Podvinskis – Ministère des affaires étrangères, des Organisations Internationales, des Politiques publiques dans le domaine de l'Internet – Lettonie

5. M Arseny Nedyak – Directeur adjoint, Service des politiques nationales des médias, Ministère de la télécommunication – Fédération de Russie

6. Mme Tanja Kerševana Smokvina - Conseillère principale au directeur général - L'Agence pour les réseaux et services de communication - Slovénie

7. M Thomas Schneider – Directeur adjoint des affaires internationales, Coordinateur de la société d'information internationale, Service fédéral de l'environnement, transport, énergie et communication DETEC, Office fédéral des communications (OFCOM) – Suisse

EXPERTS INDÉPENDANTS

1. Mme Julia Hornle – Professeur des lois dans le domaine d'Internet, Queen Mary University of London

2. M Matthias Kettemann – Postdoc Fellow, Cluster of Excellence "Normative Orders" Université de Francfort-sur-le-Main, Allemagne – Autriche

3. M Wolfgang Schulz – Professeur, Faculté de droit de l'Université de Hambourg et l'Institut de Hans-Bredow

4. Mme Sophie Stalla-Bourdillon – Professeur agrégée en technologie d'information / droit de la propriété intellectuelle, Directrice de ILAWS, Faculté de droit de Southampton de l'université de Southampton

5. Mr Dirk Voorhoof – Professor at Ghent University, member of the CMPF Scientific Committee, Centre for Media Pluralism and Press Freedom

5. M Dirk Voorhoof – Professeur à l'université de Ghent, membre du comité scientifique CMPF, Centre pour le pluralisme des médias et la liberté de la presse

6. Mr Ben Wagner – Director of the Centre for Internet & Human Rights at European University Viadrina.

6. M Ben Wagner – Directeur du Centre pour Internet & droits de l'Homme de l'université européenne Viadrina.