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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

21/11/2014

7e réunion du Comité directeur sur les médias et la société de l'information (CDMSI) **CDMSI(2014)015**

18-21 novembre 2014

(Strasbourg, bâtiment Agora, salle G03)

Rapport de réunion abrégé

Le Comité directeur sur les médias et la société de l'information (CDMSI) a tenu sa 7e réunion du 18 au 21 novembre 2014 à Strasbourg, sous la présidence de Mme Maja Rakovic (Serbie). Le CDMSI a adopté l'ordre du jour tel qu'il figure à l'annexe I. La liste des participants fait l'objet de l'annexe II. Parité hommes-femmes : 71 participants, 27 femmes (38%), 44 hommes (62%).

Points soumis au Comité des Ministres pour décision

Le CDMSI a discuté, finalisé et approuvé:

1. le projet de Recommandation CM/Rec__ 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 (annexe III). Le CDMSI a décidé qu'en l'absence d'objections de la part des délégations d'ici le 15 décembre 2014, le projet de recommandation sera transmis au Comité des Ministres pour adoption éventuelle ;

2. le projet de Recommandation CM/Rec__ du Comité des Ministres aux Etats membres sur la libre circulation transfrontière des informations sur internet (annexe IV), sur la base d'une proposition du Comité d'experts sur la circulation transfrontière d'internet et la liberté d'internet (MSI-INT). Le CDMSI a décidé qu'en l'absence d'objections de la part des délégations d'ici le 15 décembre 2014, le projet de recommandation sera transmis au Comité des Ministres pour adoption éventuelle[1];

3. le projet de Recommandation CM/Rec__ du Comité des Ministres aux Etats membres sur le traitement des données à caractère personnel dans le cadre de l'emploi (annexe V), proposé par le Comité consultatif (TP-D) de la Convention STE No 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère

[1] Concernant les points 1 et 2 et le terme « orientation sexuelle » utilisé dans les principes généraux des deux recommandations, pendant la réunion la Fédération de Russie a déclaré que la clause générale sur la non-discrimination couvre déjà ce motif éventuel de discrimination et étant donné l'absence de toute définition explicite ou de disposition relative à tel groupe ou telles personnes bénéficiaires de droits distincts dans le droit international des droits de l'homme, ces termes ne devraient pas apparaître dans les recommandations.

personnel. Le CDMSI a décidé de le transmettre au Comité des Ministres pour adoption éventuelle.

Points soumis au Comité des Ministres pour information

4. Le CDMSI a élu M^me^ Maja Rakovic (Serbia) à la présidence pour un second mandat expirant le 31 décembre 2015 et M^me^ Elfa Ýr Gylfadóttir (Islande) à la vice-présidence pour un premier mandat expirant le 31 décembre 2015.

5. Le CDMSI a eu un échange de vue sur comment promouvoir les valeurs européennes au niveau global, notamment dans le contexte de la révision du SMSI +10 (Sommet mondial sur la société de l'information), du FGI et de l'ICANN sur la base de la Stratégie sur la gouvernance de l'Internet du Conseil de l'Europe. Dans ce contexte, dans le cadre de son mandat actuel, le CDMSI a décidé de préparer un ou plusieurs projet de déclaration sur ces sujets pour adoption éventuelle de la part du Comité des Ministres.

6. Afin d'assurer la mise en œuvre de son mandat, le CDMSI a décidé sur la base de la Résolution CM/Res(2011)24, de :

i. créer les groupes de travail suivants sur : pluralisme des médias et transparence de la propriété des médias, la dimension de l'égalité entre les femmes et les hommes dans la couverture médiatique des campagnes électorales, le journalisme professionnel et éthique et le discours de haine, les médias de service public, les questions liées à la surveillance,

ii. le Bureau fera une proposition concernant la portée du travail, les objectifs et le calendrier de ces groupes de travail sur la base de l'information donnée par le secrétariat d'ici le 15 janvier 2015.

***

De plus, le CDMSI a traité les questions suivantes :

7. Comité d'experts sur la protection du journalisme et sur la sécurité des journalistes et d'autres acteurs des médias (MSI-JO) :

i. il a pris note des informations données par le secrétariat sur l'état d'avancement des travaux dans ce comité ;

ii. il a discuté l'avant-projet de recommandation sur la protection du journalisme et sur la sécurité des journalistes et d'autres acteurs des médias, a procédé à un échange de vues et donné des conseils et a invité les délégations du CDMSI à soumettre leurs commentaires au secrétariat d'ici le 22 décembre 2014 ;

iii. il demandé au MSI-JO de préparer un projet révisé pour la prochaine réunion du CDMSI.

8. Comité d'experts sur la circulation transfrontière d'internet et la liberté d'internet (MSI-INT) :

i. il a pris note des informations données par le président du MSI-INT et le secrétariat sur l'état d'avancement des travaux dans ce comité ;

ii. il a discuté les éléments pour un projet de recommandation sur la liberté d'internet et le rapport sur la liberté de réunion, la liberté d'expression et l'accès au contenu sur internet, a procédé à un échange de vues et donné des conseils

et a invité les délégations à soumettre leurs commentaires au Secrétariat d'ici le 22 décembre 2014 ;

iii. il a désigné M. Vlasios Doumpiotis (Grèce) comme nouveau membre du MSI-INT à la suite du départ de M. Johan Hallenborg (Suède) qui a changé de fonctions ;

iv. a demandé au MSI-INT de préparer un projet révisé sur la liberté de l'Internet pour la prochaine réunion du CDMSI.

9. Concernant la mise en œuvre des normes adoptées, le CDMSI :

i. a discuté le contenu du questionnaire sur la mise en œuvre des lignes directrices du Comité des Ministres sur l'élimination de l'impunité pour des violations graves des droits de l'homme dans le contexte de la sécurité des journalistes et a décidé que le secrétariat devra préparer une liste concrète de questions d'ici le 15 janvier 2015 sur la base de ses discussions et de la liste des normes adoptées par le Comité des Ministres relatives à la sécurité des journalistes ;

ii. a décidé de nommer Mme Malgorzata Pek (Pologne) et Mme Christina Lamprou (Grèce) comme rapporteurs pour la préparation de la mise en œuvre du point sur la sécurité des journalistes pour la prochaine réunion du CDMSI. En particulier, les rapporteurs réviseront le questionnaire d'ici le 22 janvier 2015, il sera ensuite envoyé au Bureau puis au CDMSI.

10. Stratégie sur la gouvernance d'internet – le CDMSI :

i. a pris note des informations données par le secrétariat et discuté l'état de mise en œuvre de la Stratégie 2012-2015 ; a décidé que les délégués devraient envoyer leurs éventuels commentaires au secrétariat d'ici le 22 décembre 2014 ;

ii. a pris note des informations données par le secrétariat, a discuté les éléments pour une nouvelle Stratégie 2016-2019 et a décidé que les éventuels commentaires des délégués devraient être envoyés au secrétariat d'ici le 22 décembre 2014. Un premier projet de Stratégie 2016-2019 devra être discuté à la prochaine réunion du Bureau du CDMSI.

11. Concernant le Rapport d'experts demandé par le Conseil de l'Europe « Procédures et politiques de l'ICANN en matière des droits de l'homme, des libertés fondamentales et des valeurs démocratiques », le CDMSI :

i. a reçu une présentation par le Secrétariat et a pris note du fait que le Comité consultatif gouvernemental de l'ICANN a discuté le rapport du Conseil de l'Europe et a jeté les bases pour des discussions intercommunautaires ;

ii. a décidé qu'un groupe de travail doit être créé pour préparer une déclaration éventuelle du Conseil de l'Europe basée sur le rapport en vue de faire progresser les nouvelles discussions de l'ICANN sur la mise en œuvre des recommandations du rapport.

12. Dialogue Européen sur la gouvernance d'internet (EuroDIG) – le CDMSI :

i. a pris note des informations données par la Bulgarie sur l'Eurodig 2015 qui se tiendra du 4 au 5 juin 2015 à Sofia ;

ii. a invité les membres du Comité à faire des propositions pour les ateliers et y à participer. La délégation bulgare coordonnera les contributions reçues.

13. Protection des données – le CDMSI a pris note des informations données par M. Jean-Philippe Walter, Président du TP-D sur:

i. la révision de la recommandation sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

ii. la modernisation de la Convention 108 et la tenue de la troisième et dernière réunion du Comité ad hoc sur la protection des données (CAHDATA) prévue pour les 1-3 décembre 2014 ;

iii. d'autres sujets traités par le TP-D, notamment le traitement des données dans le cadre de la police, des données médicales et des « *big data* ».

14. Concernant l'information sur le travail d'autres organes du Conseil de l'Europe, le CDMSI a pris note de la Recommandation 364(2014) « Le rôle des médias régionaux dans la construction d'une démocratie participative » adoptée par le Congrès des pouvoirs locaux et régionaux, a discuté et décidé que le secrétariat rédigera une réponse sur la base des commentaires écrits envoyés par les délégations d'ici le 1er décembre 2014. Le projet de réponse sera considéré par le Bureau et le CDMSI par e-mail.

15. Concernant les demandes de statut d'observateurs, le CDMSI :

i. a décidé d'accorder le statut d'observateur à l'Internet Watch Foundation ;

ii. selon les critères qui ont été appliqués dans le passé, en particulier en ce qui concerne la représentativité au niveau européen, n'a pas accordé le statut d'observateur au Press Club de Prague ;

iii. a pris note des demandes de statut d'observateur de l'Internet Rights and Principles Coalition et de l'European Media Platform et a décidé d'inviter ces deux candidats à présenter leur candidatures à la prochaine réunion du CDMSI.

16. Le CDMSI a pris note des informations données par le secrétariat et les membres du CDMSI sur les activités, réunions et manifestations suivantes :

i. création d'une Plateforme pour la liberté d'expression destinée à promouvoir la protection du journalisme et la sécurité des journalistes,

ii. étude comparative des législations et des pratiques en matière de filtrage, de blocage et de suppression des contenus internet illégaux dans les 47 Etats membres qui sera réalisée à l'initiative du Secrétaire Général du Conseil de l'Europe ;

iii. projets achevés ou en cours dans le domaine des médias et de la gouvernance d'internet, en particulier la mise en œuvre de 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,

iv. NETMundial : Réunion mondiale multipartite sur l'avenir de la gouvernance d'internet (Sao Paolo, 23-24 avril 2014), le processus de révision sur le Sommet mondial sur la société de l'information (SMSI +10), la Commission mondiale sur la gouvernance d'internet,

v. mise en œuvre de la recommandation sur l'égalité entre hommes et femmes et les médias.

17. Le CDMSI a pris note des informations données par M. Jan Kleijssen, Directeur de la Société de l'Information et de la Lutte contre la Criminalité, Direction générale des Droits

de l'Homme et de l'Etat de Droit, sur les développements au Conseil de l'Europe relatifs au travail du CDMSI ainsi que sur les dispositions administratives concernant le secrétariat.

18. Le CDMSI a exprimé sa profonde gratitude pour toutes les contributions faites par M. Jan Malinowski qui ont permis de faire progresser son travail et d'accroître la sensibilité aux questions des droits de l'homme dans la société de l'information ainsi que la pertinence de l'expérience du Conseil de l'Europe dans ce secteur aux niveaux régional et mondial. Le Comité lui a souhaité bonne continuation dans sa future position. Le Comité a souhaité la bienvenue à M. Patrick Penninckx, successeur de Jan Malinowski.

ANNEXE I

Ordre du jour

1. Ouverture de la réunion

2. Adoption de l'ordre du jour

3. Informations de la présidente et du secrétariat

3.1 Action du Conseil de l'Europe destinée à renforcer la protection de la liberté d'expression
3.2. Droits de l'homme pour les utilisateurs d'internet

4. Suivi de la mise en œuvre, dans les Etats membres, des normes adoptées par le Conseil de l'Europe qui concernent la société de l'information

5. Médias

Activités normatives

5.1 Comité d'experts sur la protection du journalisme et sur la sécurité des journalistes (MSI-JO)
5.2 Discours de haine
5.3 Médias et égalité entre les femmes et les hommes
5.4 Transparence de la propriété des médias

6. Société de l'information et gouvernance d'internet

Activités normatives

6.1. Neutralité du réseau
6.2 Comité d'experts sur la circulation transfrontière d'internet et la liberté d'internet (MSI-INT)
6.3 Stratégie du Conseil de l'Europe sur la gouvernance d'internet 2012-2015 et nouvelle stratégie sur la gouvernance d'internet 2016-2019

Activités de coopération et de diffusion

6.4 Dialogue européen sur la gouvernance de l'internet (EuroDIG – 12-13 juin 2014, Berlin) et Forum sur la gouvernance de l'internet (FGI, Istanbul, 2-5 septembre 2014)
6.5 ICANN
6.6 Autres activités

7. Activités de coopération

8. Protection des données

Activités normatives

9. Informations sur les travaux d'autres organisations et d'autres organes du CdE

9.1 Participation du CDMSI à des événements et à des réunions
9.2 Assemblée parlementaire du Conseil de l'Europe (APCE)

10. Questions budgétaires et administratives

11. Priorités du CDMSI et méthodes de travail

12. Autres questions

12.1 Demande de statut d'observateur de l'Internet Watch Foundation
12.2 Demande de statut d'observateur du Press Club de Prague

13. Election du/de la président(e) et du/de la vice-président(e)

14. Questions diverses

15. Adoption du rapport abrégé

Documents de référence généraux

Rapports de réunion récents

APPENDIX II

LIST OF PARTICIPANTS / *LISTE DES PARTICIPANTS*

Total number of participants/ *nombre total de participants* : 71
Gender distribution – 44 men (62%) / 27 women (38%)
Parité hommes / femmes - 44 hommes (62%) / 27 femmes (38%)

ALBANIA/ALBANIE
Mr/M. Glevin Dervishi
Albanian Ministry of Foreign Affairs / *Ministère des affaires étrangères d'Albanie*

AUSTRIA/AUTRICHE
Mr/M. Matthias Traimer
Federal Chancellery, Head of Department, Media Affairs and Information Society, Federal Chancellery, Constitutional Service
Chancellerie fédérale, Chef de service, Média et Société de l'Information, service constitutionnel de la Chancellerie fédérale

AZERBAIJAN
Ms/Mme. Jeyran Amiraslanova
Chief Advisor for Public and Political Issues, Office of the President of the Republic of Azerbaijan
Conseiller en chef pour les questions publiques et politiques, Bureau du Président de la République d'Azerbaidjan

BELGIUM/BELGIQUE
Apologised / *Excusé*

BOSNIA AND HERZEGOVINA/BOSNIE-HERZEGOVINE
Mr/M. Emir Povlakic
Head of Division for Licensing, Digitalization and Coordination in Broadcasting, Communications Regulatory Authority
Chef de division, Licences, numérisation et coordination, Autorité de régulation des communications et de la radiodiffusion

BULGARIA/BULGARIE
Ms/Mme. Bissera Zankova, Media Expert – Consultant / *Consultante, expert en médias*
Ministry of Transport, IT and Communications / *Ministère des transports, des technologies de l'information et des communications*

CROATIA/CROATIE
Mr Milan F. Zivkovic
Head Advisor for Communication Policy, Ministry of Culture
Conseiller en chef pour les polotiques de communication, Ministère de la culture

Ms/Mme. Vesna Roller
The Council for Electronic Media / *Conseil pour les médias électroniques*

CYPRUS/CHYPRE
Ms/Mme. Eleonora Gavrielides
Ministry of Interior / *Ministère de l'intérieur*

CZECH REPUBLIC/REPUBLIQUE TCHEQUE
Mr Artuš Rejent
Media and Audio-Visual Department, Ministry of Culture / *Service médias et audio-visuel*, *Ministère de la culture*

DENMARK/DANEMARK
Ms/Mme. Katja Just Maarbjerg (19th–21/11/2014)
Ministry of Culture / *Ministère de la culture*

ESTONIA/ESTONIE
Mr/M. Indrek Ibrus
Senior specialist of audiovisual affairs, Estonian Ministry of Culture
Spécialiste des affaires audio-visuelles, *Ministère de la culture d'Estonie*

FINLAND/FINLANDE
Commercial Secretary, Information Society and ICT, Ministry for Foreign Affairs
Secrétaire commercial, Société et technologies de l'information, Ministère des affaires étrangères

FRANCE
Ms/Mme. Joanna Chansel
Ministry of Culture and Communications / *Ministère de la culture et de la communication*

Mr/M. Julien Plubel
Ministry for Foreign Affairs, Directorate for cultural, university and research co-operation, External audio-visual department /.*Ministère des Affaires étrangères, Direction de la coopération culturelle, universitaire et de la recherche, Pôle de l'audiovisuel extérieur*

GEORGIA/GEORGIE
Ms/Mme. Irine Bartaia
Deputy Director, Department of International Law, Ministry of Foreign Affairs
Directeur adjoint, service des législations internationales, Ministère des Affaires étrangères

GERMANY/ALLEMAGNE
Mr/M. Oliver Schenk (18–19/11/2014)
Division K 31, International Media Co-operation, Federal Government Commissioner for Culture and the Media / *Division K 31, Coopération internationale pour les médias, Commissaire du gouvrnement fédéral pour la culture et les médias*

Mr/M. Jan Wiegandt (20-21/11/2014)
Vertretung des Landes Rheinland-Pfalz to the EU/ *Représentation de l'Etat de Rhénanie Palatinat auprès de l'UE*

Ms/Mme. Annick Kuhl
EU Representation of the Free State of Bavaria to the EU / *Représentation de l'Etat libre de Bavière auprès de l'UE*

GREECE/GRECE
Ms/Mme. Christina Lamprou
Head of the Department of Audiovisual Affairs, Directorate of Mass Media - General Secretariat of Information and Communication
Chef du service des affaires audio-visuelles, Direction des médias de masse – Secrétariat général de l'information et de la communication

HUNGARY/HONGRIE
Mr/M. György Ocskó
International Legal Adviser, National Media and Infocommunications Authority
Conseiller juridique international, Autorité nationale des médias et de l'info-communication

Mr/M. János Auer
Member of the Media Council of the National Media and Infocommunications Authority
Membre du Conseil pour les médias de l'Autorité nationale des médias et de l'info-communication

ICELAND/ISLANDE
Ms/Mme Elfa Ýr Gylfadóttir
Media Commission, Ministry of Education, Science and Culture
Commission des médias, Ministère de l'éducation, des sciences et de la culture

IRELAND/IRLANDE
Mr/M. Éanna O'Conghaile
Principal Officer, Broadcasting Policy Division, Department of Communications, Energy & Natural Resources
Officier principal, Division des politiques de radio-diffusion, Service de la communication, de l'énergie et des ressources naturelles

Mr Richard Browne,
Department of Communications, Energy & Natural Resources / *Service de la communication, de l'énergie et des ressources naturelles*

ITALY/ITALIE
Mr/M. Piergluigi Mazzella

Director General, Agency for the right to university education, Professor of Information and Communication, University of Rome
Directeur général, Agence pour les droits à l'éducation universitaire, Professeur en information et communication, Université de Rome

LATVIA/LETTONIE
Mr/M. Andris Mellakauls
Information Space Integration, Ministry of Culture / *Intégration de l'espace de l'information, Ministère de la culture*

LITHUANIA/LITUANIE
Ms/Mme. Vida Česnaitė
Department advisor, Ministry of culture, Information Society Development Division
Conseiller , Ministère de la culture, Division du développement de la société de l'information

LIECHTENSTEIN
Mr/M. Claudio Nardi,
Officer for Foreign Affairs / *Officier pour les affaires étrangères*

MALTA/ MALTE
Ms/Mme. Nancy Caruana,
Ministry for the Economy, investment and Small Business, Office of the Permanent Secretary
Ministère de l'économie, de l'investissement et des petites entreprises, Bureau du secrétaire permanent

MONACO
Mr/M. Serge Robillard,
Head of Division, Digital Communications Directorate / *Chef de Division, Direction des Communications Électroniques*

MONTENEGRO
Mr/M. Ranko Vujovic,
Executive Director, UNEM / *Directeur exécutif, UNEM*

REPUBLIC OF MOLDOVA / REPUBLIQUE MOLDAVE
Ms/Mme. Ana Taban,
Head of Information and Media Outreach Office, Ministry of Foreign Affairs and European Integration
Chef du bureau de l'information et du développement des médias, Ministère des affaires étrangères et de l'intégration européenne

THE NETHERLANDS/PAYS-BAS
Ms/Mme. Pien van den Eijnden (18-20/11/2014)
Legal Adviser, Constitutional Affairs, Ministry of the Interior and Kingdom Relations
Conseiller juridique, Affaires constitutionnelles, Ministère de l'intérieur

NORWAY/NORVEGE
Mr/M. Olav Guntvedt
Assistant Director General, Departement of Media Policy and Copyright, Ministry of Culture
Directeur général adjoint, Service des politiques des médias et du droits d'auteur, Ministère de la culture

POLAND/POLOGNE
Ms/Mme. Małgorzata Pek
Deputy Director of Strategy Department, Office of the National Broadcasting Council
Directrice adjointe du service de la stratégie, Conseil national de la radiodiffusion

Mr/M.Maciej Gron
Director of the Department of Information Society, Ministry of Administration and Digitization
Directeur du Service de la société de l'information, Ministère de l'administration et de la numérisation

PORTUGAL
Mr/M. Pedro Ruivo
GMCS, Cabinet pour les Medias ("Gabinete para os Meios de Comunicação Social")
GMCS, Bureau des médias

ROMANIA / ROUMANIE
Ms/Mme. Delia Mucica,
Ministry of Culture and National Heritage / *Ministère de la culture et du patrimoine*

RUSSIAN FEDERATION / FEDERATION RUSSIE
Mr/M. Alexander Surikov
Deputy Director, Department of Information and Press, Ministry of Communication
Directeur adjoint, Service de l'information et de la presse, Ministère de la communication

SERBIA/SERBIE
Ms/Mme. Maja Rakovic,
1st Adviser, Serbian Embassy in France / *1er conseiller, Ambassade de Serbie en France*

Ms/Mme. Maja Zaric,
Adviser, Sector for International Relations, EU integration and projects, Ministry of Culture and Information
Conseiller, Seteur des relations internationales, de l'intégration dans l'UE et des projets, Ministère de la culture et de l'information

SLOVENIA/SLOVENIE
Mr/M. Skender Adem
Undersecretary, Ministry of Culture / *Sous-secrétaire, Ministère de la culture*

SLOVAKIA/SLOVAQUIE
Ms/M. Ivana Maláková,
Head of Unit Media Law and Audiovisual Unit Media, Audiovisual and Copyright Department, Ministry of Culture
Chef d'unité, Unité législation des médias et de l'audiovisuel, Service de l'audiovisuel et du droit d'auteur, Ministère de la culture

SWEDEN
Mr/M. Christoffer Lärkner
Department of Culture / *Service de la culture*

SWITZERLAND
Mr/M.Thomas Schneider
International Affairs, Federal Office of Communication, Federal Department for the environment, transport, energy and communication
Affaires internationales, Office fédéral de la communication, Service fédéral pour l'environnement, les transports, l'énergie et les communications

Mr/M. Frédéric Riehl
Head of International Affairs, Federal Office of Communication, Federal Department for the environment, transport, energy and communication
Chef des affaires internationales, Office fédéral de la communication, Service fédéral pour l'environnement, les transports, l'énergie et les communications

„Former Yugoslav Republic of Macedonia"/ „Ex république yougoslave de Macédoine"
Ms/Mme. Vesna Poposka
Head of International PR Department, Government of the Republic of Macedonia
Chef du service des relations publiques internationales, Gouvernement de la République de Macedoine,

TURKEY/TURQUIE
Mr/M. Mehmet Bora Sönmez
Media Expert, Radio and Television Supreme Council / *Expert des médias, Conseil supèrieur de la radio et de la télévision*

Mr/M. Nurullah Öztürk,
Member of the Supreme Council, Radio and Television Supreme Council / *Membre du Conseil supérieur de la radio et de la télévision*

UKRAINE
Ms/Mme. Olga Herasymiuk,
First Deputy Chair of the National Council of Ukraine for Television and Radio Broadcasting
Première vice-présidente du Conseil national d'Ukraine pour la télévision et la radio et télédiffusion

Ms/Mme. Larysa Vasylenko
Head of International Relations Division of the National Television and Radio Broadcasting Council

Chef de la division des relations internationales du Conseil national d'Ukraine pour la télévision et la radio et télédiffusion

UNITED KINGDOM/ROYAUME-UNI
Mr/M. Mark Carvell
Media Team, Department for Culture, Media and Sport / *Equipe Médies, Service de la culture, des médias et des sports*

* * *

OBSERVERS/PARTICIPANTS

BELARUS
Ms/Mme. Maria Vanshina
Deputy Head of Communication Department, Head of Press Service, Ministry of Foreign Affairs
Chef adjoint du service de la communication, chef du service de presse, Ministère des affaires étrangères

BLACK SEA BROADCASTING REGULATORY AUTHORITIES FORUM (BRAF)
Dr Hamit Ersoy
Secretary General / *Secrétaire général*

EUROPEAN AUDIOVISUAL OBSERVATORY/OBSERVATOIRE EUROPEEN DE L'AUDIOVISUEL
Ms/Mme. Nikoltchev Susanne,
Executive Director / Directrice exécutive

EUROPEAN ASSOCIATION FOR VIEWERS INTERESTS (EAVI)
Ms/Mme. Krstina Stoycheva

EUROPEAN UNION/UNION EUROPEENNE
Mr/M.Maciej Tomaszewski (20–21/11/2014)
Policy officer – international, DG Connect, Unit D1, European Commission
Responsable des politiques – international, DG Connect, Unité D1, Commission Européenne

EUROPEAN BROADCASTING UNION (EBU) / UNION EUROPEENNE DE RADIO-TELEVISION (UER)
Ms/Mme Anne-Catherine Berg,
Legal Adviser, Legal Department / *Conseiller juridique, Service juridique*

Mr/M. Giacomo Mazzone,
Head of Institutional Relations, Public Affairs & Communications / *Chef des relations institutionelles, des affaires publiques et de la communication*

EuroISPA
Mr/M.Michael Rotert
Honorary Spokesman / *Porte-parole honoraire*

ASSOCIATION OF EUROPEAN JOURNALISTS (AEJ) / MEDIA FREEDOM REPRESENTATIVE
Mr/M William Horsley (18–20/11/2014)
Media Freedom Representative / *Représentant pour la liberté des médias*

EUROPEAN NEWSPAPER PUBLISHERS ASSOCIATION (ENPA) / ASSOCIATION EUROPEENNE DES EDITEURS DE JOURNAUX
Mr/M. Holger Rosedal,
Head of Legal Department / *Chef du service juridique*

CONFERENCE OF INTERNATIONAL NON-GOVERNMENTAL ORGANISATIONS OF THE COUNCIL OF EUROPE / CONFÉRENCE DES ORGANISATIONS INTERNATIONALES NON GOUVERNEMENTALES DU CONSEIL DE L'EUROPE
Mr/M. Didier Schretter
Member of the Standing Commitee, Vice-chair Education and Culture Committee
Membre du comité permanent, vice-président du Comité de l'éducation et de la culture

COPEAM
Ms/Mme. Alessandra Paradisi

HOLY SEE / SAINT SIEGE
Dr Michael Lukas
Episcopal Press Office / *Bureau de presse épiscopal*

ICANN
Mr/M.Nigel Hickson (20–21/11/2014)
VP, IGO Engagement / *Vice-président, Engagement IGO*

ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE (OSCE)
Dr. Juan (Joan) Barata Mir,
Principal Advisor, Representative on Freedom of Media
Conseiller principal, Représentant pour la liberté des médias

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA / COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL (T-PD)
Mr/M. Jean-Philippe Walter, Chairman / *Président*

MEXICO / MEXIQUE
Mr/M. Diego Sandoval Pimentel
Deputy Permanent Representative of Mexico to the Council of Europe / Adjoint à l'Observateur Permanent du Mexique auprès du Conseil de l'Europe

PARLIAMENTARY ASSEMBLY OF THE COUNCI OF EUROPE / ASSEMBLEE PARLEMENTAIRE DU CONSEIL DE L'EUROPE
Mr/M. Rüdiger Dossow
Secretary of the Committee on Culture, Science and Education / *Secrétaire du Comité de la culture, de la science, de l'éducation et des médias*

* * *

INTERPRETERS / INTERPRETES
Ms/Mme Sarah Adlington
Ms/Mme Gillian Wakenhut
Ms/Mme Bettina Ludewig
Mr/M. Jean-Louis Wunsch

* * *

SECRETARIAT

Mr/M. Jan Kleijssen, Director of Information Society and Action against Crime, Directorate General Human Rights and Rule of Law / *Directeur de la Société de l'information et de la lutte contre la criminalité, Direction générale Droits de l'Homme et Etat de Droit*
Mr/M. Jan Malinowski, Head of Information Society Department, Directorate General Human Rights and Rule of Law / Chef du service *Société de l'information, Direction générale Droits de l'Homme et Etat de Droit*
Mr/M. Patrick Penninckx, Executive Secretary, Cooperation Group to Combat Drug Abuse and Illicit Trafficking in Drugs, Directorate General of Human Rights and Rule of Law / *Secrétaire exécutif, Groupe de coopération pour la lutte contre l'abus et le traffic de drogue, Direction générale Droits de l'Homme et Etat de Droit*
Ms/Mme. Silvia Grundmann, Head of Media Division, Directorate General of Human Rights and Rule of Law, Secretary to the Steering Committee on Media and Information Society / *Chef de la division médias*, *Direction générale Droits de l'Homme et Etat de Droit, Secrétaire du Comité directeur pour les médias et la société e l'information*
Ms/Mme. Onur Andreotti, Administrator, Media Division, Directorate General Human Rights and Rule of Law / *Administratice, division médias, Direction générale Droits de l'Homme et Etat de Droit*
Mr/M. Luca Belli, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law / *Administrateur, Unité société de l'information, Direction générale Droits de l'Homme et Etat de Droit*
Ms/Mme Ana Gascón-Marcén, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law / *Administratrice, Unité société de l'information, Direction générale Droits de l'Homme et Etat de Droit*

Mr/M. Lee Hibbard, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law / *Administrateur, Unité société de l'information, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme Elvana Thaçi, Administrator, Media Division, Directorate General Human Rights and Rule of Law / *Administratice, division médias, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme. Loreta Vioiu, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law / *Administratrice, Unité société de l'information, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme Maria Michaelidou, Programme Advisor, Data Protection Unit, Directorate General Human Rights and Rule of Law / *Conseillère de programme, Unité protection des données*, *Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme Anne Boyer-Donnard, Principal Administrative Assistant, Media Division, Directorate General Human Rights and Rule of Law / *Assistante administative principale, Division médias, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme. Giovanna Langella, Principal Administrative Assistant, Media Division, Directorate General Human Rights and Rule of Law / *Assistante administative principale, Division médias, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme.Sarah Gregg, Assistant, Information Society Unit, Directorate General Human Rights and Rule of Law / *Assistante, Unité société de l'information, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme.Krystyna Khokhlova, Assistant, Media Division, Directorate General Human Rights and Rule of Law / *Assistante, Division médias, Direction générale Droits de l'Homme et Etat de Droit*

Ms/Mme. Julia Whitham, Assistant, Media Division, Directorate General Human Rights and Rule of Law / *Assistante, Division médias, Direction générale Droits de l'Homme et Etat de Droit*

Mr/M.Naser Bislimi, Trainee, Media Division, Directorate General Human Rights and Rule of Law / *Stagiaire, Division médias, Direction générale Droits de l'Homme et Etat de Droit*

ANNEXE III

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

1. Dans la société de l'information, l'exercice et la jouissance du droit à la liberté d'expression des personnes, y compris le droit de recevoir et de communiquer des informations et des idées, ainsi que leur participation à la vie démocratique, dépendent de plus en plus sur l'accessibilité et la qualité d'une connexion à l'internet.

2. Les fournisseurs d'accès à l'internet ont la capacité de contrôler les flux de données et d'informations (le trafic internet) qui transitent sur leurs réseaux. Ils peuvent appliquer des mesures de gestion du trafic internet à des fins légitimes spécifiques, par exemple pour préserver l'intégrité et la sécurité du réseau. Ils peuvent également prendre des dispositions pour empêcher l'accès à des contenus illicites et préjudiciables ou leur diffusion, par exemple en mettant en place des systèmes d'autorégulation en coopération avec les pouvoirs publics. Cependant, d'autres interférences avec le trafic internet peuvent affecter la qualité des services internet délivrés aux usagers et peuvent aboutir au blocage, à la discrimination ou à la priorisation de types de contenus, d'applications ou de services spécifiques. Par ailleurs, certaines des techniques utilisées dans ce contexte permettent d'inspecter ou de surveiller les communications, ce qui peut saper la confiance des utilisateurs dans l'internet.

3. Ces questions suscitent des préoccupations quant au respect de la protection et de la promotion du droit à la vie privée et du droit à la liberté d'expression qui sont garantis respectivement par les articles 8 et 10 de la Convention européenne des droits de l'homme (STE n° 5, si après la CEDH) ainsi qu'eu égard à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108). En outre, elles ont des implications sur l'accès à des informations diverses et pluralistes et au contenu des médias de service public sur l'internet, fondamentaux pour la démocratie et la diversité culturelle. Le droit à la liberté d'expression, notamment le droit de recevoir ou de communiquer des informations, n'est pas un droit absolu. Cependant, toute restriction à l'exercice de ce droit doit répondre aux exigences de l'article 10, paragraphe 2 de la CEDH.

4. Le principe de la neutralité du réseau sous-tend un traitement non discriminatoire du trafic internet et l'accès des usagers aux informations et services de leur choix. Il renforce le plein exercice et la pleine jouissance de la liberté d'expression puisque l'article 10 de la CEDH s'applique non seulement au contenu des informations mais aussi aux moyens de leur diffusion. De même, le principe de la neutralité du réseau soutient l'innovation technologique et la croissance économique.

5. Le Comité des Ministres rappelle l'article 1 du Statut du Conseil de l'Europe ainsi que les instruments normatifs pertinents du Conseil de l'Europe[2]. En vue de protéger et promouvoir le droit à la vie privée et le droit à la liberté d'expression en pleine conformité avec les articles 8 et 10 de la CEDH et de promouvoir la valeur de service public d'internet, le Comité des Ministres recommande aux Etats membres :

- de prendre toutes les mesures nécessaires, en coopération avec l'ensemble des parties prenantes, pour sauvegarder le principe de la neutralité du réseau dans leurs

[2] Déclaration du Comité des Ministres sur la protection du rôle des médias dans les démocraties dans le contexte de la concentration des médias (31 janvier 2007) ; Recommandation Rec(2007)3 sur la mission des médias de service public dans la société de l'information ; Recommandation CM/Rec(2007)16 sur des mesures visant à promouvoir la valeur de service public de l'Internet ; Recommandation CM/Rec(2008)6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet ; Déclaration du Comité des Ministres sur la neutralité du réseau (29 septembre 2010) ; Déclaration du Comité des Ministres sur les principes de la gouvernance d'internet (21 septembre 2011) ; Recommandation CM/Rec (2014)6 aux Etats membres sur un Guide des droits de l'homme pour les utilisateurs d'internet.

cadres de politique générale en tenant pleinement compte des lignes directrices fixées dans la présente recommandation,

- de promouvoir ces lignes directrices dans d'autres enceintes régionales et internationales qui traitent de la question de la neutralité du réseau.

Lignes directrices sur la neutralité du réseau

1. Principes généraux

1.1. Dans l'exercice de leur droit à la liberté d'expression, conformément à l'article 10 de la CEDH, les utilisateurs d'internet ont le droit d'accéder à des informations, des applications et des services, de les diffuser, et d'utiliser les dispositifs de leur choix. La jouissance de ce droit doit être assurée sans distinction aucune, fondée notamment sur le sexe, l'orientation sexuelle, la race, la couleur, la langue, la religion, les opinions politiques ou toute autre opinion, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation.

1.2. Le trafic internet devrait être traité à égalité, sans discrimination, restriction ni ingérence, quels que soient l'émetteur, le destinataire, le contenu, l'application, le service ou le dispositif. Aux fins de la présente recommandation, c'est ce que l'on appelle le principe de la neutralité du réseau.

1.3. La liberté de choix des utilisateurs d'internet ne devrait pas être limitée par l'application d'un traitement favorable ou faisant obstacle à la transmission de trafic internet lié à des contenus, services, applications ou dispositifs particuliers, ou de trafic lié à des services fournis sur la base d'accords exclusifs ou de tarifs particuliers.

1.4. Le principe de la neutralité du réseau devrait s'appliquer à tous les services offrant une connexion à l'internet (services d'accès à l'internet), indépendamment des infrastructures ou réseaux utilisés pour la connexion et de la technologie sous-jacente permettant d'acheminer les signaux.

2. Gestion du trafic

2.1. Les fournisseurs d'accès à l'internet ne devraient pas restreindre la liberté de choix des utilisateurs d'internet en bloquant, ralentissant, modifiant, dégradant ou défavorisant certains contenus, applications ou services spécifiques.

2.2. Les mesures de gestion du trafic internet, le cas échéant, devraient être non discriminatoires, transparentes, nécessaires et proportionnées aux buts suivants :

- pour donner effet à une décision de justice ou à celle d'une autorité de régulation

- pour préserver l'intégrité et la sécurité du réseau, des services offerts via le réseau et de l'équipement terminal employé par les utilisateurs d'internet ;

- pour empêcher la transmission de communications non sollicitées à des fins de marketing aux utilisateurs finaux qui ont accepté au préalable de telles mesures restrictives ;

- pour réduire les conséquences d'une surcharge exceptionnelle ou temporaire du réseau, à condition de traiter à égalité les différents types de trafic équivalents,

- pour respecter un contrat passé avec l'utilisateur afin de lui garantir un certain niveau de qualité de service, sous réserve que cela ne nuise pas à la qualité de

l'accès à l'internet et ne constitue pas une pratique discriminatoire ou anticoncurrentielle.

2.3. Les mesures de gestion du trafic internet ne devraient être maintenues que pour une durée strictement nécessaire, et les politiques de gestion du trafic devraient faire l'objet d'un examen régulier par les autorités compétentes au sein de chaque Etat membre.

3. Pluralisme et diversité de l'information

3.1. Les fournisseurs d'accès à l'internet ne devraient pas défavoriser le trafic provenant d'autres fournisseurs de contenus, d'applications et de services qui sont en concurrence avec leurs propres produits. Il faut pour cela que les décisions relatives à la gestion du trafic soient strictement dissociées des processus décisionnels de l'opérateur concernant les contenus, dans l'esprit de la Déclaration de 2007 du Comité des Ministres sur la protection du rôle des médias dans les démocraties dans le contexte de la concentration des médias.

3.2. Un traitement préférentiel du trafic fondé sur des accords conclus entre des fournisseurs d'accès à l'internet et des fournisseurs de contenus, d'applications et de services ne devrait pas diminuer ni affecter l'accessibilité économique, la performance ou la qualité de l'accès des utilisateurs à l'internet. De tels accords accords ne devraient pas avoir d'effets négatifs sur la capacité des utilisateurs à accéder à l'information, à des contenus publics divers et pluralistes, aux applications et aux services de leur choix et à les utiliser.

3.3. Dans le cadre de réseaux gérés, les Etats peuvent envisager d'imposer des obligations raisonnables, transparentes et proportionnées d'acheminement des contenus répondant à des objectifs d'intérêt général.

4. Vie privée

4.1. Des mesures de gestion du trafic ne devraient donner lieu à un traitement des données personnelles que dans la mesure où celui-ci est nécessaire et proportionné à la réalisation des objectifs énoncés à la deuxième setion de la présente recommandation, et devraient être conformes à la législation en vigueur en matière de droit à la vie privée et de protection de données à caractère personnel.

4.2. Certaines techniques utilisées à des fins de gestion du trafic internet sont capables d'analyser le contenu des communications. La manière dont ces techniques sont appliquées peut constituer une atteinte au droit à la vie privée. Un tel usage doit donc être pleinement conforme à l'article 8 de la CEDH, faire l'objet d'un contrôle de conformité par rapport à la législation en vigueur sur le droit à la vie privée et à la protection des données à caractère personnel et être contrôlé par une autorité compétente au sein de chaque Etat membre afin de vérifier le respect de la législation.

5. Transparence

5.1. Les fournisseurs d'accès à l'internet devraient fournir aux usagers des informations claires, complètes et publiques sur toute procédure de gestion du trafic qu'ils appliquent et qui pourrait avoir une incidence sur l'accès aux contenus, applications ou services et sur leur diffusion. Les utilisateurs d'internet devraient pouvoir obtenir de la part des fournisseurs d'accès à l'internet des informations sur la gestion du trafic et sur les vitesses du réseau.

5.2. Les autorités compétentes de chaque Etat membre devraient assurer le suivi des pratiques de gestion du trafic internet et faire rapport sur ces pratiques. Les rapports devraient être élaborés de façon ouverte et transparente et mis gratuitement à la disposition du public.

6. Responsabilisation

6.1. Les fournisseurs d'accès à l'internet devraient mettre en place des procédures adaptées, claires, ouvertes et efficaces pour traiter, dans des délais raisonnables, les réclamations des utilisateurs d'internet invoquant des manquements aux principes énoncés dans les dispositions qui précèdent. Les utilisateurs devraient avoir la possibilité de saisir les autorités compétentes au sein de chaque Etat membre.

6.2. Le cadre de politique générale mis en place par les Etats devrait obliger les fournisseurs d'accès à l'internet à rendre compte de leur respect du principe de la neutralité du réseau. Cette responsabilisation suppose aussi l'existence de mécanismes permettant de traiter les plaintes relatives à la neutralité du réseau.

ANNEXE IV

Projet de recommandation CM/Rec(2014)___ du Comité des Ministres aux Etats membres sur la libre circulation transfrontière des informations sur l'internet

1. Le droit à la liberté d'expression, notamment le droit de recevoir ou de communiquer des informations et des idées sans ingérence et sans considération de frontières, est une pierre angulaire de la société démocratique et une condition fondamentale de sa pérennité et de son développement ainsi que du développement de chaque être humain. Les dispositions sur les droits et libertés figurant dans la Convention européenne des droits de l'homme (ci-après la CEDH) et l'article 19 du Pacte international relatif aux droits civils et politiques s'appliquent de la même façon en ligne et hors ligne. L'article 10 de la CEDH concerne non seulement le contenu des informations, mais aussi les moyens de leur diffusion ou d'hébergement, dans la mesure où toute restriction apportée à ceux-ci a nécessairement un impact sur le droit de recevoir et de communiquer des informations.

2. De manière analogue, le droit à la liberté de réunion et d'association, tel qu'il est garanti par l'article 11 de la CEDH, revêt lui aussi une importance fondamentale pour la démocratie. En outre, la protection du droit au respect de la vie privée, garanti par l'article 8 de la CEDH, et la protection des données personnelles conformément à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après Convention 108) sous-tendent l'exercice du droit à la liberté d'expression et contribuent à la libre circulation des informations sur internet.

3. La circulation transfrontière libre des informations est une condition nécessaire au plein exercice de ces droits et libertés, au maintien du pluralisme et de la diversité de l'information, au développement de la culture et de l'innovation, et à la croissance économique. Les politiques ou mesures nationales, les activités commerciales ou les pratiques technologiques qui interfèrent, intentionnellement ou non, avec le trafic internet ou qui imposent des restrictions aux contenus ou aux services sur internet dans un Etat, peuvent avoir des répercussions, au-delà des frontières de cet Etat, sur le droit à la liberté d'expression et le droit à la liberté d'association. En conséquence, l'exercice de la souveraineté nationale peut être affecté.

4. Un seul et même contenu ou service sur internet peut être considéré par plusieurs Etats comme relevant de leur compétence nationale, auquel cas les utilisateurs peuvent être confrontés à des règles incohérentes ou contradictoires. La variété et la diversité des législations nationales concernant les contenus et les services illicites et une application de lois nationales concurrentes ou contradictoires, créent un environnement juridique complexe ; dans ce contexte, il peut être difficile pour les utilisateurs d'obtenir la protection qui leur est garantie par l'article 10 de la CEDH. Le niveau de complexité est appelé à augmenter sous l'effet de nouveautés technologiques telles que les réseaux de fourniture de contenus et les services qui hébergent et traitent des données dans des sites distants (informatique en nuage) plutôt qu'à proximité du propriétaire, du responsable ou du destinataire de l'information.

5. Il est nécessaire de promouvoir une approche commune au niveau international, de consolider les normes et d'appliquer les bonnes pratiques relatives à la libre circulation transfrontière des informations sur internet tout en maintenant la pleine conformité avec les accords internationaux relatifs à la protection des enfants sur internet, la lutte contre la cybercriminalité, la protection des données personnelles et d'autres accords pertinents. A cet égard, les Etats devraient agir sur la base de la Recommandation CM/Rec(2011)8 du Comité des Ministres qui énonce leur engagement en faveur de la protection et de la promotion de l'universalité, de l'intégrité et de l'ouverture d'internet. L'engagement reconnaît que les Etats ont la responsabilité de s'assurer que les activités exercées dans leur juridiction ne font pas obstacle à l'accès aux contenus en dehors de leurs frontières ni n'entravent le flux transfrontalier du trafic internet. Les Etats devraient également tenir dûment compte des normes du Conseil de l'Europe mentionnées dans l'annexe à la présente recommandation ainsi que de l'importance de l'autorégulation. Celle-ci contribue à l'élaboration de bonnes

pratiques et de modèles de conduite qui encouragent la libre circulation des informations, des opinions et des idées sur internet.

6. En conséquence, le Comité des Ministres recommande que les Etats membres, lorsqu'ils élaborent et mettent en œuvre des politiques relatives à l'internet au niveau national et au sein de la communauté internationale :

- promeuvent et protègent la libre circulation transfrontière des informations en tenant dûment compte des principes énoncés dans la présente recommandation, en veillant notamment à ce que ces principes soient reflétés dans les cadres réglementaires, dans les politiques et dans la pratique ;

- encouragent les acteurs du secteur privé, la société civile et les milieux techniques à soutenir et promouvoir la mise en œuvre des principes énoncés dans la présente recommandation.

Principes relatifs à la libre circulation transfrontière des informations sur internet

1. Principes généraux

1.1. Les Etats sont tenus de garantir à toute personne relevant de leur juridiction le droit à la liberté d'expression et le droit à la liberté de réunion et d'association, en pleine conformité avec les articles 10 et 11 de la CEDH, lesquels s'appliquent également à l'internet. Ces droits et libertés doivent être garantis sans discrimination aucune, fondée notamment sur le genre, l'orientation sexuelle, la race, la couleur, la langue, la religion, les opinions politiques ou autres, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation.

1.2. Les Etats devraient protéger et promouvoir la libre circulation mondiale des informations sur internet. Ils devraient veiller à ce que les ingérences dans le trafic internet survenant sur leur territoire visent les objectifs légitimes énoncés à l'article 10 de la CEDH et dans d'autres accords internationaux pertinents, et n'ont pas d'incidences inutiles ou disproportionnées sur la circulation transfrontière des informations.

2. Principes relatifs au devoir de diligence

Les Etats devraient faire preuve de diligence lorsqu'ils élaborent, évaluent et mettent en œuvre leurs politiques nationales afin de détecter et d'éviter les incidences sur le trafic internet qui peuvent nuire à la libre circulation transfrontière des informations sur internet.

- *Evaluation* - toute mesure réglementaire ou autre pouvant avoir de telles incidences devrait être évaluée à l'aune de la responsabilité de l'Etat de respecter, de protéger et de promouvoir les droits de l'homme et les libertés fondamentales énoncés dans la CEDH.

- *Transparence, prévisibilité et responsabilisation* - lorsqu'ils élaborent des politiques et des cadres réglementaires pouvant avoir des incidences sur la libre circulation des informations sur internet, les Etats devraient appliquer des principes de transparence - notamment aux résultats des évaluations mentionnées ci-dessus- de prévisibilité concernant leur mise en œuvre, et de responsabilisation. En particulier, les projets de cadres réglementaires envisagés devraient être publiés dans des délais et selon des modalités à même de permettre une consultation publique.

- *Proportionnalité et révision des mesures* - les Etats sont tenus de veiller à ce que tout blocage de contenus ou de services jugés illégaux soit conforme aux articles 8, 10 et 11 de la CEDH. En particulier, les mesures adoptées par les pouvoirs publics pour

combattre des activités ou des contenus illégaux sur internet ne devraient pas entraîner de conséquences inutiles ou disproportionnées en dehors des frontières de l'Etat. Les Etats devraient privilégier les mesures les moins intrusives ou les moins perturbantes, mises en œuvre de façon transparente et responsabilisante. Les mesures adoptées ou promues par les Etats devraient être régulièrement examinées afin que leur efficacité pratique soit établie et que soit vérifié si elles sont encore nécessaires et proportionnées.

3. Importance de l'autorégulation

Les Etats devraient encourager, faciliter et soutenir l'élaboration de codes d'autorégulation selon les besoins, de façon à ce que tous les acteurs respectent le droit à la liberté d'expression, le droit à la liberté de réunion et d'association et le droit à la vie privée, notamment en ce qui concerne la libre circulation du trafic internet.

4. Promotion des bonnes pratiques techniques

4.1. Les Etats devraient promouvoir la coopération des acteurs concernés dans l'élaboration et la mise en œuvre de bonnes pratiques techniques qui respectent le droit à la liberté d'expression et le droit à la liberté d'association, y compris par l'évaluation du caractère nécessaire d'actions et de la proportionnalité de mesures pouvant avoir des incidences transfrontières sur le trafic internet.

4.2. Les Etats devraient s'assurer que les politiques nationales respectent l'architecture mondiale d'internet. Cela comprend l'adhésion aux bonnes pratiques concernant le système d'adressage (Domain Name System).

5. Dialogue et politiques au niveau international

5.1. Lorsque des politiques nationales ou des activités commerciales interfèrent avec le trafic internet au-delà des frontières d'un Etat, les parties concernées ne disposent pas nécessairement des moyens de déposer des réclamations dans cet Etat. Les Etats devraient veiller à ce qu'il existe des structures et des procédures pour recevoir les réclamations des parties concernées et les résoudre. A cet égard, les Etats devraient nouer un dialogue international afin d'élaborer progressivement des approches communes ainsi que des normes et des standards internationaux et afin de s'accorder sur des bonnes pratiques concernant les lois applicables et les juridictions compétentes dans les situations où la liberté d'expression et d'accès à l'information fait l'objet de lois concurrentes (ou contradictoires).

5.2. Dans le contexte de l'élaboration de politiques ou de réglementations internationales concernant internet, les Etats devraient protéger et promouvoir la connectivité à l'internet ainsi que la disponibilité et l'accessibilité d'une information diverse et pluraliste, facteurs qui contribuent à la libre circulation transfrontière des informations sur internet.

5.3. En ce qui concerne les services qui hébergent ou traitent des informations dans des sites distants, les Etats devraient garantir le droit à la protection des données personnelles conformément à la Convention 108 et le droit à la vie privée conformément à l'article 8 de la CEDH. Ces conditions sont importantes pour le plein exercice des droits énoncés à l'article 10 de la CEDH. S'agissant des services en question, les Etats devraient en outre nouer un dialogue international afin d'élaborer des normes, des pratiques et des approches partagées pour traiter les questions de juridiction et de droit applicable.

Annexe

Normes pertinentes du Conseil de l'Europe

- Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201)

- Convention sur la cybercriminalité (STE n° 185) et Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189)

- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181)

- 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

- Recommandation CM/Rec(2009)5 visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication.

- Déclaration sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet (20 février 2008)

- Recommandation CM/Rec(2008)6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet

- Recommandation CM/Rec(2007)16 sur des mesures visant à promouvoir la valeur de service public de l'Internet

- Déclaration sur la neutralité du réseau (29 septembre 2010)

ANNEXE V

PROJET DE RECOMMENDATION CM/REC(2014)… DU COMITE DES MINISTRES AUX ETATS MEMBRES SUR LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL DANS LE CADRE DE L'EMPLOI.

(Adoptée le … 2014 par le Comité des Ministres lors de la … réunion des Ministres délégués)

Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Conscient de l'utilisation croissante des nouvelles technologies et des instruments de communication électronique dans les relations entre employeur et employés, ainsi que des avantages qui en découlent ;

Estimant, toutefois, que l'utilisation de méthodes de traitement de données par les employeurs devrait être gouvernée par des principes destinés à réduire les risques que de telles méthodes pourraient éventuellement présenter pour les droits et les libertés fondamentales des employés, notamment leur droit à la vie privée ;

Ayant à l'esprit les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (ci-après la Convention 108), ainsi que celles de son Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001, et compte tenu de l'intérêt de convertir l'application de ces principes au secteur de l'emploi ;

Reconnaissant également que les intérêts devant être pris en compte lors de l'élaboration de principes dans le secteur de l'emploi sont individuels ou collectifs, privés ou publics ;

Considérant que les données à caractère personnel dans les documents officiels détenus par une autorité publique ou un organisme public peuvent être divulguées par l'autorité ou l'organisme conformément à la législation nationale à laquelle l'autorité ou l'organisme public est soumis, afin de concilier le droit d'accès à ces documents officiels avec le droit à la protection des données à caractère personnel conformément aux principes de la présente recommandation ;

Conscient des traditions différentes existant dans les Etats membres en ce qui concerne la réglementation des divers aspects des relations employeur-employé, et constatant que la réglementation par voie législative ne constitue qu'une des méthodes utilisées ;

Conscient des changements intervenus à l'échelle internationale dans le monde du travail et activités qui y sont liées, du fait notamment du recours accru aux technologies de l'information et de la communication (TICs) et de la mondialisation de l'emploi et des services ;

Considérant que ces changements appellent à une révision de la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi en vue de continuer à assurer un niveau de protection adéquat des personnes dans le secteur de l'emploi ;

Rappelant l'article 8 de la Convention européenne des droits de l'homme, qui protège le droit à la vie privée, comprenant, tel qu'interprété par la Cour européenne des droits de l'homme, les activités de nature professionnelle et/ou commerciale ;

Rappelant l'application des principes établis par d'autres recommandations pertinentes du Conseil de l'Europe, en particulier la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, la Recommandation R(97)5 relative à la protection des données médicales et la Recommandation R(92)3 sur les tests et le dépistage génétiques à des fins médicales ;

Rappelant les «Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance » adoptés par le Comité européen de coopération juridique (CDCJ) du Conseil de l'Europe en mai 2003 et mentionnés dans la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe qui sont particulièrement pertinents ;

Rappelant la Charte sociale européenne (STCE n° 163), dans sa version révisée du 3 mai 1996, ainsi que le Code de conduite du Bureau international du travail de 1997 sur la protection des données à caractère personnel des travailleurs ;

Recommande aux gouvernements des Etats membres :

- d'assurer que les principes contenus dans l' annexe de la présente recommandation , qui remplace la Recommandation R N° (89)2 susmentionnée, soient reflétés dans la mise en œuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi, ainsi que dans d'autres branches de toute loi portant sur l'utilisation des données à caractère personnel à des fins d'emploi;

- d'assurer, à cette fin, que la présente recommandation et son annexe soient portées à l'attention des autorités établies conformément à la législation nationale en matière de protection de données et chargées de contrôler l'application de cette législation ;

- et de promouvoir par ailleurs l'acceptation et l'application des principes contenus dans l'annexe de la présente recommandation, au moyen d'instruments complémentaires tels que des codes de conduite, en s'assurant que ces principes soient bien assimilés/ admis et mis en application par tous les intervenants du secteur de l'emploi, incluant les organes représentatifs des employeurs et des employés et pris en compte dans la conception, le déploiement et l'utilisation des TICs dans ce secteur.

Annexe à la Recommandation

Partie I – Principes généraux

1. Champ d'application

1.1. Les principes de la présente recommandation s'appliquent au traitement de données à caractère personnel à des fins d'emploi dans les secteurs public et privé.

1.2. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent aussi aux activités des agences pour l'emploi, dans les secteurs public et privé, qui traitent des données à caractère personnel afin de permettre l'établissement d'un ou de plusieurs contrats de travail simultanés, y compris de contrats à temps partiel, entre les personnes concernées qui figurent sur leurs listes et d'éventuels employeurs, ou afin de faciliter les démarches pour les employeurs dérivant desdits contrats.

2. Définitions

Aux fins de la présente recommandation :

– «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée »).

– « traitement» s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, et notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement, la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques aux données ; lorsqu'aucun procédé automatisé n'est utilisé, le traitement de données s'entend des opérations effectuées au sein d'un ensemble structuré établi selon tout critère qui permet de rechercher des données à caractère personnel ;

– « systèmes d'information » signifie tout dispositif isolé ou groupe de dispositifs interconnectés ou liés entre eux, qui assurent [ou dont un ou plusieurs éléments assure(nt)] conformément à un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques enregistrées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance ;

– « à des fins d'emploi» concerne les rapports entre employeurs et employés relatifs au recrutement, à l'exécution du contrat de travail et à son encadrement, y compris à l'exécution des obligations découlant de la loi ou de conventions collectives, ainsi qu'à la planification et la gestion efficace d'une organisation et la fin des rapports de travail. Les conséquences de la relation contractuelle peuvent s'étendre au-delà du terme du contrat de travail ;

– « employeur » signifie toute personne physique ou morale, l'autorité publique ou l'agence, engagée dans un lien d'emploi avec l'employé ou qui envisage d'engager un tel lien avec un candidat à un emploi et qui détient la responsabilité légale de l'entreprise ou de l'établissement ;

– « employé » signifie toute personne concernée engagée dans une relation de travail avec un employeur ou employeur potentiel.

3. Respect des droits de l'homme, de la dignité humaine et des libertés fondamentales

Le respect de la dignité humaine, de la vie privée et de la protection des données à caractère personnel devrait être garanti lors du traitement de données à des fins d'emploi, notamment pour permettre aux employés le développement libre de leur personnalité et afin de préserver la possibilité de relations sociales et individuelles sur leur lieu de travail.

4. Application des principes de traitement

4.1. Les employeurs devraient veiller à ce que le traitement des données à caractère personnel ne porte que sur les données strictement nécessaires pour atteindre l'objectif déterminé dans les cas individuels concernés.

4.2. Les employeurs devraient développer des mesures appropriées, visant à respecter en pratique les principes et obligations en matière de traitement de données à des fins d'emploi. A la demande des autorités de contrôle, les employeurs devraient être en mesure de démontrer qu'ils sont en conformité avec des tels principes et obligations. Ces mesures devraient être adaptées au volume et à la nature des données traitées et aux activités entreprises ; elles tiendront également compte des conséquences possibles pour les droits et les libertés fondamentales des employés.

5. Collecte et enregistrement des données

5.1. Les employeurs devraient collecter les données à caractère personnel directement auprès de la personne concernée. Lorsqu'il est nécessaire et licite, de traiter des données collectées auprès de tiers, par exemple pour obtenir des références professionnelles, la personne concernée devrait en être préalablement dûment informée.

5.2. Les données à caractère personnel collectées par les employeurs à des fins d'emploi devraient être pertinentes et non excessives, compte tenu du type d'emploi ainsi que des besoins évolutifs d'information de l'employeur.

5.3. Les employeurs devraient s'abstenir d'exiger ou de demander à un employé ou à un candidat à l'emploi d'avoir accès à des informations que celui-ci partage avec d'autres en ligne, notamment sur des réseaux sociaux.

5.4. Les données relatives à la santé ne peuvent être collectées qu'aux fins prévues au principe 8.2 de la présente recommandation.

5.5. L'enregistrement de données à caractère personnel à des fins d'emploi n'est possible que si les données ont été collectées conformément aux règles définies aux principes 4, 9 et 14 à 20 de la présente recommandation et uniquement pour le temps nécessaire à la poursuite des finalités du traitement. Ces données devraient être pertinentes, adéquates et non-excessives. Lorsque des données d'évaluation relatives à la productivité ou à la capacité d'un employé sont enregistrées, de telles données ne devraient servir qu'à évaluer les compétences professionnelles.

6. Utilisation interne des données

6.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être traitées par les employeurs qu'à de telles fins.

6.2. Les employeurs devraient adopter des politiques de protection des données, des règles et/ou d'autres instruments relatifs à l'usage interne des données à caractère personnel conformément aux principes de la présente recommandation.

6.3. A titre exceptionnel, lorsque des données doivent être traitées à des fins d'emploi mais pour des finalités autres que celles pour lesquelles elles ont été initialement collectées, les employeurs devraient prendre des mesures appropriées pour éviter que ces données ne soient mal interprétées pour cette autre finalité et en informer l'employé. En cas de décision importante concernant l'employé, fondée sur des données ainsi utilisées, celui-ci devrait être avisé en conséquence.

6.4. Sans préjudice des dispositions du principe 8, lors de changements au sein de l'entreprise, de fusions et d'acquisitions, il convient de veiller au respect des principes de proportionnalité et de finalité dans l'utilisation ultérieure des données. Toute modification substantielle du traitement devrait être communiquée à la personne concernée.

7. Communication des données et utilisation des TICs pour la représentation des employés

7.1. Conformément aux législations et pratiques nationales, ainsi qu'aux conventions collectives, des données à caractère personnel peuvent être communiquées aux représentants des employés uniquement si de telles données sont nécessaires pour permettre à ces derniers de représenter de façon appropriée les intérêts des employés concernés ou si elles sont nécessaires afin de garantir l'exécution et la supervision des obligations prévues par les conventions collectives.

7.2. Conformément aux législations et pratiques nationales l'utilisation de systèmes et technologies d'information pour la communication des données aux représentants des employés devrait faire l'objet d'accords spécifiques, visant à définir au préalable des règles transparentes stipulant leur utilisation et garantissant la protection des communications confidentielles, conformément au principe 10.

8. Communication externe des données

8.1. Les données à caractère personnel collectées à des fins d'emploi devraient être communiquées à des organismes publics uniquement pour l'accomplissement de leur mission officielle et dans les limites des obligations légales des employeurs ou conformément à d'autres dispositions du droit interne.

8.2. La communication de données à caractère personnel à des organismes publics à des fins autres que l'accomplissement de leur mission officielle ou à des parties autres que les organismes publics, y compris les entreprises du même groupe, ne devrait s'effectuer que :

a. lorsque la communication est nécessaire à des fins d'emploi qui ne seraient pas incompatibles avec les finalités pour lesquelles les données ont été collectées à l'origine et si les employés concernés ou leurs représentants, selon le cas, en sont informés au préalable ; ou

b. avec le consentement exprès, libre et informé de l'employé concerné ; ou

c. si la communication est prévue par le droit interne et notamment lorsqu'elle est nécessaire à l'exécution d'obligations découlant de la loi ou des conventions collectives.

8.3. Les dispositions relatives à la divulgation de données à caractère personnel afin d'assurer la transparence dans le secteur public (le gouvernement et toute autre autorité publique ou organisme), y compris le contrôle de l'utilisation régulière des fonds et ressources publiques, devraient également prévoir des garanties appropriées eu égard au droit au respect de la vie privée et à la protection des données à caractère personnel des employés.

8.4. Les employeurs devraient prendre les mesures appropriées afin de veiller à ce que seules les données pertinentes, exactes et à jour soient communiquées [à l'extérieur], et à plus forte raison s'agissant des données publiées en ligne et accessibles à un plus large public.

9. Traitement des données sensibles

9.1. Le traitement des données sensibles, visé à l'article 6 de la Convention 108, est permis uniquement dans des cas particuliers, lorsque cela est indispensable pour un recrutement spécifique ou à l'exécution d'obligations légales dérivant du contrat de travail, dans les limites prescrites par le droit interne et moyennant des garanties appropriées, venant compléter celles de la Convention 108 et de la présente recommandation. Les garanties appropriées devraient être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales des employés concernés, notamment le risque de discrimination. Le traitement des données biométriques est sujet aux dispositions du principe 18 de la présente recommandation.

9.2. Conformément au droit interne, un employé ou un candidat à l'emploi peut être interrogé sur son état de santé et/ou faire l'objet d'un examen médical uniquement aux fins de :

a. déterminer son aptitude à un emploi actuel ou futur ;

b. couvrir les besoins de la médecine préventive ;

c. garantir sa réadaptation appropriée au poste de travail ou répondre à toute autre exigence de l'environnement professionnel ;

d. sauvegarder les intérêts vitaux de la personne concernée ou d'autres employés ou personnes ;

e. octroyer des prestations sociales ; ou

f. répondre à une procédure judiciaire.

9.3. Les données génétiques ne peuvent pas faire objet d'un traitement afin de pouvoir déterminer, par exemple, l'aptitude professionnelle d'employés ou de candidats à l'emploi, même avec le consentement de l'intéressé. Le traitement de données génétiques peut être permis uniquement à titre exceptionnel, par exemple, afin d'éviter une atteinte grave à la santé de la personne concernée ou des tiers et uniquement lorsque cela est prévu par le droit interne et moyennant des garanties appropriées.

9.4. Les données de santé et - lorsque leur traitement est licite - les données génétiques, ne devraient être collectées qu'auprès de l'employé, lorsque cela est prévu par la loi et moyennant des garanties appropriées.

9.5. Les données de santé couvertes par le secret médical ne devraient être accessibles et traitées que par du personnel lié par le secret médical ou par d'autres règles régissant le secret professionnel et les obligations de confidentialité. Ces données devraient :

a. se rapporter directement à l'aptitude de l'employé à exercer ses fonctions, ou

b. être nécessaires pour prendre des mesures en faveur de la santé de l'employé, ou

c. être nécessaires pour prévenir un risque pour d'autres personnes.

Lorsque ces données sont communiquées à l'employeur, cette communication devrait être faite par une personne dûment habilitée, telle qu'une personne travaillant dans l'administration du personnel, ou ayant des responsabilités dans le secteur de la santé et de la sécurité au travail et l'information ne devrait être communiquée que si elle est indispensable pour la prise de décision par l'administration du personnel et conformément au droit interne.

9.6. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques devraient, le cas échéant, être enregistrées séparément des autres catégories de données détenues par les employeurs. Des mesures de sécurité techniques et organisationnelles devraient être prises afin d'éviter que des personnes étrangères au service médical de l'employeur n'aient accès à ces données.

9.7. Les données de santé relatives à des tiers ne devront en aucune circonstance faire l'objet d'un traitement, à moins que la personne concernée n'ait donné au préalable son entier consentement, libre informé et non-équivoque, ou que ce traitement ne soit autorisé par l'autorité de contrôle compétente ou que la collecte des données ne soit indispensable à l'exécution des obligations légales.

10. Transparence du traitement

10.1. Des informations sur les données à caractère personnel détenues par des employeurs devraient être mises à la disposition de l'employé concerné, soit directement, soit par l'intermédiaire de ses représentants, ou être portées à sa connaissance par d'autres moyens appropriés.

10.2. Les employeurs devraient fournir à leurs employés les informations suivantes :

- les catégories de données qui seront traitées et une description des finalités du traitement,
- les destinataires ou catégories de destinataires de ces données,
- les moyens d'exercer les droits énoncés au principe 11 de la présente recommandation, sans pour autant porter préjudice à des moyens plus favorables prévus dans le droit interne ou le système législatif,
- toute autre information nécessaire pour garantir un traitement loyal et licite des données.

10.3. Une description particulièrement claire et complète des catégories de données à caractère personnel qui peuvent être collectées au moyen de TICs, telle que la

vidéosurveillance, et de leur utilisation potentielle, devrait être fournie. Ce principe vaut pour toutes les formes particulières de traitement de données à caractère personnel prévues à la partie II de la présente recommandation.

10.4. Les informations devraient être fournies sous une forme accessible et tenues à jour. Ces informations devraient, en tout état de cause, être fournies avant que l'employé n'exerce effectivement l'activité ou l'action prévue, et être mises à disposition au moyen des systèmes d'information habituellement utilisés par l'employé.

11. Droit d'accès, de rectification et d'opposition

11.1 Un employé devrait pouvoir obtenir, à sa demande, à fréquence raisonnable et dans un délai normal, la confirmation d'un traitement de données le concernant. La communication devrait être faite sous une forme intelligible, inclure toutes informations disponibles sur l'origine des données, ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements, en particulier les informations prévues au principe 10.

11.2 Un employé devrait avoir le droit d'obtenir la rectification, le blocage ou l'effacement de ses données à caractère personnel en cas d'inexactitude et/ou lorsqu'elles sont traitées en violation du droit interne ou des principes énoncés dans la présente recommandation. Il devrait également être autorisé à s'opposer à tout moment au traitement des données à caractère personnel le concernant, à moins que ce traitement ne soit nécessaire à des fins d'emploi ou ne soit prévu par la loi.

11.3. Le droit d'accès devrait également être garanti s'agissant des données d'évaluation, y compris celles relatives aux appréciations de la performance, de la productivité ou du potentiel de l'employé, au plus tard lorsque le processus d'appréciation est terminé, sans préjudice du droit de défense des employeurs ou des tiers impliqués. Bien que ces données ne puissent être directement corrigées par l'employé, les évaluations purement subjectives devraient pouvoir être contestées conformément au droit interne.

11.4. Un employé ne devrait pas être soumis à une décision l'affectant de manière significative, qui serait uniquement basée sur un traitement automatisé de données, sans que son point de vue soit pris en compte.

11.5. Un employé devrait également pouvoir obtenir, à sa demande, des informations concernant le raisonnement qui sous-tend le traitement de données dont les résultats lui sont appliqués.

11.6. Des dérogations aux droits auxquels il est fait référence aux paragraphes 10, 11.1. 11.2, 11.4., et 11.5 peuvent être admises lorsqu'elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique, à la protection de la sécurité nationale à la sûreté publique, à des intérêts économiques et financiers importants de l'Etat ou à la prévention et à la répression des infractions pénales, ainsi qu'à la protection de la personne concernée et des droits et libertés d'autrui.

11.7. En outre, dans le cas d'une enquête interne effectuée par un employeur, l'exercice des droits auxquels il est fait référence aux paragraphes 10 et 11.1 à 11.5 peut être différé jusqu'à la conclusion de cette enquête si cet exercice devrait porter préjudice à l'enquête.

11.8. Sauf dispositions nationales contraires, l'employé devrait pouvoir désigner une personne de son choix pour l'assister lors de l'exercice de son droit d'accès, de rectification ou d'opposition ou afin d'exercer ces droits en son nom.

11.9. Des voies de recours devraient être prévues par le droit interne lorsqu'un employé se voit refuser l'accès aux données le concernant ou la possibilité de rectifier ou d'effacer certaines de ses données.

12. Sécurité des données

12.1. Les employeurs, ou les entités auprès desquelles le traitement de données peut être sous-traité, devraient mettre en œuvre des mesures techniques et organisationnelles appropriées, qui seront mises à jour si cela s'avère nécessaire, en réponse aux examens périodiques d'évaluation des risques et des politiques de sécurité. De telles mesures devraient garantir la sécurité et la confidentialité des données à caractère personnel traitées à des fins d'emploi, contre la modification, la perte ou la destruction accidentelles ou non autorisées de données à caractère personnel, ainsi que contre l'accès, la diffusion ou la divulgation non autorisées des données.

12.2. Conformément au droit interne, les employeurs devraient garantir de manière adéquate la sécurité des données lors de l'utilisation des TICs pour toute opération de traitement de données à caractère personnel à des fins d'emploi, y compris leur enregistrement.

12.3. Le service du personnel ainsi que toute autre personne intervenant dans le traitement des données devraient être tenus informés de ces mesures et de la nécessité de les respecter, ainsi que de garder la confidentialité concernant ces mesures.

13. Conservation des données

13.1. Les employeurs ne devraient pas traiter des données à caractère personnel pendant une période plus longue que ne le justifient les finalités d'emploi définies au principe 2 ou que ne le nécessite l'intérêt d'un employé en poste ou d'un ancien employé.

13.2. Les données à caractère personnel fournies à la suite d'un acte de candidature devraient en principe être effacées dès qu'il devient clair que la candidature ne sera pas retenue par l'employeur ou retirée par le candidat. Lorsque de telles données sont conservées en vue d'une demande d'emploi ultérieure, l'intéressé devrait en être informé en conséquence et les données devraient être effacées à sa demande.

13.3. Lorsque pour intenter ou soutenir une action en justice ou pour toute autre finalité légitime, il est indispensable de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pour la période nécessaire à cette finalité.

13.4. Les données à caractère personnel traitées aux fins d'une enquête interne réalisée par des employeurs et qui n'a entraîné l'adoption d'aucune sanction à l'égard d'un employé devraient être effacées dans un délai raisonnable, sans préjudice de l'exercice du droit d'accès de l'employé jusqu'à ce qu'elles soient effacées.

Partie II – Formes particulières de traitement

14. Utilisation de l'Internet et des communications électroniques sur le lieu de travail

14.1. Les employeurs devraient éviter de porter des atteintes injustifiées et déraisonnables au droit au respect de la vie privée des employés. Ce principe s'étend à tous les dispositifs techniques et aux TICs utilisés par un employé. Les personnes concernées devraient être convenablement et périodiquement informées à l'aide d'une déclaration claire en matière de respect de la vie privée conformément au principe 10 de la présente recommandation. L'information fournie devrait être mise à jour et inclure la finalité du traitement, la durée de conservation des données collectées ainsi que la sauvegarde des données de connexion et l'archivage des messages électroniques professionnels.

14.2. En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel relatif aux pages Internet ou Intranet consultées par l'employé, il conviendrait d'une

part d'adopter des mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations, et d'autre part de prévoir éventuellement des contrôles des données à caractère personnel, effectués, de préférence, de manière graduée et par sondages non-individuels, en utilisant des données anonymes ou, en quelque sorte, agrégées.

14.3. L'accès par les employeurs aux communications électroniques professionnelles de leurs employés, qui ont été informés au préalable de cette éventualité, ne peut survenir, le cas échéant, que si cela est nécessaire pour des raisons de sécurité, ou pour d'autres raisons légitimes. En cas d'absence d'un employé, les employeurs devraient prendre les mesures nécessaires et prévoir les procédures appropriées visant à permettre l'accès aux communications électroniques professionnelles, uniquement lorsqu'un tel accès est nécessaire d'un point de vue professionnel. L'accès devrait t intervenir de la façon la moins intrusive possible et uniquement après avoir informé les employés concernés.

14.4. En aucun cas le contenu, l'envoi et la réception de communications électroniques privées dans le cadre du travail ne devront faire l'objet d'une surveillance.

14.5. Lorsqu'un employé quitte son emploi, l'employeur devrait prendre des mesures techniques et organisationnelles afin que la messagerie électronique de l'employé soit désactivée automatiquement. Si le contenu de la messagerie devrait être récupéré pour la bonne marche de l'organisation, l'employeur devrait prendre des mesures appropriées afin de récupérer son contenu avant le départ de l'employé et si possible en sa présence.

15. Systèmes et technologies de l'information pour le contrôle des employés, notamment la vidéosurveillance

15.1. L'introduction et l'utilisation des systèmes et technologies d'information ayant pour finalité directe et principale le contrôle de l'activité et du comportement des employés ne devraient pas être permises. Lorsque leur introduction et leurs utilisation sont nécessaires pour d'autres finalités légitimes, telles que la protection de la production, de la santé, de la sécurité, ou la gestion efficace d'une organisation, menant, de façon indirecte, à la possibilité de contrôler l'activité des employés, elles devraient être soumises aux garanties complémentaires visées au principe 21, notamment la consultation des représentants des employés.

15.2. Les systèmes et technologies de l'information qui contrôle l'activité et le comportement des employés de façon indirecte, devraient être spécialement conçus et placés de façon à ne pas porter préjudice à leurs droits fondamentaux. L'utilisation de la vidéosurveillance pour le contrôle d'endroits tenant à la vie intime des employés n'est en aucun cas autorisée.

15.3. En cas de litige ou d'action en justice, les employés devraient, le cas échéant, pouvoir obtenir la copie des enregistrements réalisés, conformément aux dispositions du droit interne. La conservation des enregistrements devrait être limitée dans le temps.

16. Appareils permettant de localiser les employés

16.1. Les appareils permettant de localiser un employé ne devraient être introduits que s'ils s'avèrent nécessaires pour atteindre les finalités légitimes poursuivies par les employeurs et que leur utilisation ne conduit pas à un contrôle permanent des employés. Plus particulièrement, le contrôle ne devrait pas être la finalité principale, mais uniquement une conséquence indirecte de l'action visant la protection de la production, de la santé, de la sécurité, et de la gestion efficace d'une organisation. Considérant les risques d'atteinte aux droits et aux libertés des personnes que présente l'utilisation de ces appareils, les employeurs devraient prendre toutes les garanties nécessaires à la protection des données à caractère personnel et au respect de la vie privée des employés, y compris les garanties prévues au principe 21. Conformément aux règles définies aux principes 4 et 5, les employeurs devraient accorder une attention particulière aux finalités pour lesquelles de tels appareils sont utilisés et aux principes de minimisation et de proportionnalité.

16.2. Les employeurs devraient prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux personnes concernées.

17. Mécanismes internes de signalement

Lorsque les employeurs sont tenus par la loi ou les règles internes de mettre en œuvre des mécanismes internes de signalement, tels que les numéros d'urgence, ils devraient assurer la protection des données à caractère personnel de toutes les parties concernées. En particulier, les employeurs devrait garantir la confidentialité à l'égard de l'employé qui signale les comportements illicites ou contraires à l'éthique (tel qu'un donneur d'alerte). Les données à caractère personnel des parties en cause devraient être utilisées uniquement aux fins des procédures internes appropriées relatives aux dits signalements, tel que prévu par la loi ou pourrait être prévu par des procédures judiciaires ultérieures.

A titre exceptionnel, les employeurs peuvent permettre le signalement anonyme. Un signalement anonyme ne saurait être l'unique origine d'enquêtes internes, à moins que ce signalement soit dûment circonstancié et concerne de graves infractions au droit interne.

18. Données biométriques

18.1. La collecte et le traitement de données biométriques ne devraient être réalisés que lorsqu'ils sont nécessaires à la protection des intérêts légitimes des employeurs, des employés ou des tiers, uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement moins intrusives pour la vie privée et lorsque le traitement s'accompagne de garanties appropriées, y compris les garanties prévues au principe 21.

18.2. Le traitement des données biométriques devrait être fondé sur des méthodes scientifiquement reconnues et soumis à des exigences strictes de sécurité et de proportionnalité.

19. Tests psychologiques, analyses et procédures analogues

19.1. Le recours à des tests, à des analyses et à des procédures analogues effectués par des professionnels spécialisés, soumis au secret médical, et destinés à évaluer le caractère ou la personnalité d'un employé ou d'un candidat à l'emploi ne devraient être permis que s'il est légitime et nécessaire au regard de la catégorie d'activité exercée dans l'emploi et que le droit interne prévoit des garanties appropriées.

19.2. L'employé ou le candidat à l'emploi devrait être informé au préalable des modalités d'utilisation des résultats de ces tests, analyses ou procédures analogues et, par la suite, de leur contenu. Les principes 11.1 et 11.2 s'appliquent en conséquence.

20. Autres traitements de nature à présenter des risques spécifiques au regard des droits des employés

20.1. Les employeurs, et le cas échéant, les sous-traitants, devraient procéder à une analyse de l'impact potentiel de tout traitement de données envisagé sur les droits et libertés fondamentales des employés et concevoir les traitements de données de manière à prévenir ou pour le moins à minimiser les risques d'atteinte à ces droits et libertés fondamentales.

20.2. A moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale, l'accord des représentants des employés devrait être recherché préalablement à l'introduction ou à la modification des TICs lorsque la procédure révèle des risques d'atteinte au regard des droits des employés.

21. Garanties complémentaires

Pour toutes formes particulières de traitement, établies dans la Partie II de la présente recommandation, les employeurs sont notamment tenus de prendre en particulier les garanties suivantes :

a. Informer préalablement les employés de l'introduction des systèmes et technologies d'information permettant le contrôle de leur activité. L'information fournie devrait être mise à jour, et le droit d'information devrait s'effectuer conformément au principe 10 de la présente recommandation. Les informations devraient inclure la finalité du dispositif, la durée de conservation, l'existence ou non des droits d'accès et de rectification et la façon dont ces droits peuvent être exercés ;

b. Prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux employés ;

c. Avant l'introduction d'un système de surveillance ou lorsqu'un système existant devrait être modifié, les représentants des employés devraient être consultés, conformément aux législations et pratiques nationales. Lorsque la procédure de consultation révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine d'un employé, l'accord des représentants devrait être assuré ;

d. Consulter, conformément à la législation nationale les autorités nationales de contrôle sur les traitements de données à caractère personnel.