

Bureau of the Steering Committee on Media and Information Society

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

22/10/2014

CDMSI-BU(2014)004

Rapport de la 6^e réunion (24 et 25 septembre 2014)

(Strasbourg, Bâtiment Agora, Salle G02)

1. & 2. Ouverture de la réunion - Adoption de l'ordre du jour

Mme Maja Rakovic (Serbie), présidente du CDMSI, ouvre la réunion. Le Bureau adopte l'ordre du jour de sa réunion en vue de la préparation de la réunion du CDMSI qui aura lieu du 18 au 21 novembre 2014. L'ordre du jour annoté figure en annexe 1 ; la liste des participants en annexe 2.

3. Informations communiquées par la présidente et le secrétariat

3.1 L'action du Conseil de l'Europe pour renforcer la protection de la liberté d'expression

Le Bureau est informé par le secrétariat et prend note des informations suivantes :

- une session de travail se tiendra le 16 octobre 2014 à Metz dans le contexte des « Assises internationales du journalisme », à laquelle participeront des représentants d'ONG qui sont des partenaires potentiels du Conseil de l'Europe concernant le projet de plateforme sur la sécurité des journalistes. Cette session de travail a pour objet de discuter des conditions concrètes dans lesquelles s'établirait un tel partenariat ;
- le Séminaire et dialogue interrégional sur la protection des journalistes aura lieu le 3 novembre 2014 (annexe 3) ; tous les membres du Bureau ainsi que les membres du Comité d'experts sur la protection du journalisme et la sécurité des journalistes (MSI-JO) qui sont également membres du CDMSI y seront invités ;
- le programme de M. Thorbjørn Jagland, Secrétaire Général du Conseil de l'Europe, pour son deuxième mandat a été présenté au Comité des Ministres lors de la 1206bis réunion des Délégués des Ministres (16 septembre 2014) ; le Bureau prend note du fait que l'accent est mis sur les questions liées à la liberté d'expression, notamment la liberté des médias, la sécurité des journalistes, les médias sociaux et la gouvernance de l'internet ; en particulier, le Bureau note que le Secrétaire Général espère présenter en début d'année prochaine une étude comparative des législations et des pratiques en matière de filtrage, de blocage et de suppression des contenus internet illégaux dans tous les Etats membres ; il

mentionne aussi la proposition faite au Comité des Ministres de mettre en place un mécanisme en faveur de la sécurité des journalistes sous l'égide de la Direction de la planification politique, dont le mandat sera redéfini ;

- la note conceptuelle révisée de l'Unesco sur un projet de recherche sur la sécurité des journalistes comme indicateur potentiel de l'Etat de droit, de la démocratie et du développement ; le Bureau déclare vouloir poursuivre sa coopération avec l'Unesco;
- une réunion interagences des Nations Unies sur la sécurité des journalistes et la question de l'impunité organisée par l'Unesco se tiendra au Conseil de l'Europe le 4 novembre 2014 à Strasbourg ;
- l'étude sur la diffamation sera sensiblement mise à jour et prête à être publiée début 2015 ; son annexe qui rassemble les législations nationales devrait être conçue sous la forme d'un outil en ligne permettant des mises à jour régulières ; les membres du CDMSI seront invités à y participer ;
- M. Nils Muižnieks, Commissaire aux droits de l'homme du Conseil de l'Europe, a annoncé lors de la 1207^e réunion des Délégués des Ministres le 17 septembre 2014 qu'il publierait un document thématique consacré à l'Etat de droit sur internet ; le secrétariat transmettra ce document au CDMSI dès sa publication.

3.2. Droits de l'homme des utilisateurs d'internet

Le Bureau du CDMSI est informé des activités prévues par le secrétariat concernant 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.

4. Suivi de la mise en œuvre des normes du Conseil de l'Europe adoptées dans les Etats membres sur les médias et la société de l'information

Le Bureau examine une proposition du secrétariat relative aux questions adressées aux membres du CDMSI sur la mise en œuvre des lignes directrices du Comité des Ministres pour éliminer l'impunité pour les violations graves des droits de l'homme (30 mars 2011), inscrivant ces lignes directrices dans le contexte spécifique de la sécurité des journalistes. Le Bureau revoit les questions et décide de les soumettre aux membres du CDMSI (annexe 4). Le Bureau rappelle que le CDMSI est d'accord sur une proposition du Secrétariat sur le format du suivi de la mise en œuvre des normes du Conseil de l'Europe dans les Etats membres et qu'il a décidé que le premier sujet de discussion à sa prochaine réunion en novembre 2014 sera la « Sécurité des journalistes ». Dans le but de faciliter cette discussion et sa préparation, le Bureau suggère d'inviter les membres du CDMSI qui sont aussi membres de la commission d'experts MSI-JO pour contribuer activement à la préparation de ce sujet et à la discussion en plénière.

5. Médias

Activités normatives

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

Le Bureau se déclare en faveur de la structure générale du projet de recommandation sur la protection du journalisme et la sécurité des journalistes proposée par le MSI-JO. Constatant que le MSI-JO tiendra sa deuxième réunion les 6 et 7 octobre 2014, le Bureau souligne que l'avant-projet de recommandation devra être envoyé au CDMSI dès que possible après la réunion du MSI-JO, afin qu'il puisse être examiné comme il convient lors de la plénière du CDMSI en novembre 2014.

Le Bureau encourage le MSI-JO à s'associer aux travaux futurs du CDMSI sur le sujet de « journalisme professionnel et éthique », reconnaissant que le mandat du MSI-JO ne couvre pas ce sujet. Le Bureau conseille au MSI-JO d'organiser, dans la mesure du possible, ses réunions avant celles du Bureau, et fait part de son souhait d'inviter le président du MSI-JO à la plénière du CDMSI en novembre 2014.

Le Bureau prend note de l'information communiquée par le Secrétariat sur l'état d'avancement des contributions par rapport au recueil de bonnes pratiques dans les Etats membres concernant les initiatives visant à renforcer la sécurité des journalistes, et invite le Secrétariat à relancer un appel aux contributions.

5.2 *Discours de haine*

Le Bureau accepte la proposition du secrétariat d'inviter le coordinateur du Conseil de l'Europe de la campagne contre le discours de haine ainsi qu'un jeune militant à la plénière de novembre du CDMSI afin d'obtenir des informations de première main.

5.3 *Egalité entre les femmes et les hommes et les médias*

Le Bureau prend note de l'information selon laquelle Mme Bissera Zankova participera à la 40^e réunion de l'EPRA, qui se tiendra du 8 au 10 octobre 2014, à Tbilisi, en Géorgie afin de présenter la recommandation et d'aborder sa mise en œuvre.

Le Bureau prend également note de l'information concernant le projet de boîte à outils sur la mise en œuvre de la recommandation. Il souhaite créer un groupe de travail sur l'égalité entre les hommes et les femmes et les médias. M. Emir Powlakic (Bosnie-Herzégovine), Mme Bissera Zankova (Bulgarie) et Mme Christina Lamprou (Grèce) se portent volontaires pour en faire partie. Le Bureau décide de soumettre cette suggestion au CDMSI lors de sa prochaine réunion plénière en novembre 2014.

5.4 *Transparence de la propriété des médias*

Le secrétariat informe le Bureau des discussions qui doivent avoir lieu le 1^{er} octobre 2014 au sein de la Commission de la culture, de la science, de l'éducation et des médias de l'Assemblée parlementaire, parallèlement à la présentation et à l'examen d'un rapport d'experts sur le renforcement de la transparence de la propriété des médias. Ce rapport sera mis à la disposition du CDMSI après la réunion de l'Assemblée parlementaire. Le Bureau décide d'inviter le CDMSI à sa prochaine réunion afin de créer un groupe de travail informel sur la question de la transparence de la propriété des médias.

5.5 *Médias de service public*

Le Bureau propose de poursuivre les discussions sur ce sujet lors des prochaines réunions du CDMSI.

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

Activités normatives

6.1 Neutralité du réseau

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 concernant la neutralité du réseau

Le Bureau rappelle le processus de révision du projet de recommandation qui s'est déroulé depuis la dernière réunion du CDMSI (du 23 au 26 mai 2014). Le projet a été transmis par courriel au CDMSI pour approbation ad referendum à deux reprises, soit le 2 juin 2014 (immédiatement après la réunion du CDMSI) et le 5 septembre 2014, avec les commentaires reçus. Le Bureau prend note des commentaires soumis par les délégations figurant à l'annexe 5.

Le Bureau adopte une version révisée du projet de recommandation qui tient compte des commentaires soumis de la façon la plus adaptée pour préserver l'équilibre et la dimension de droits de l'homme du texte (annexe 6). Compte tenu des longues discussions sur le texte et des consultations qui ont eu lieu jusqu'à présent avec les Etats membres, le Bureau souligne la nécessité de faire avancer la situation lors de la prochaine réunion du CDMSI (du 18 au 21 novembre 2014), notamment au vu du temps considérable déjà consacré à la finalisation de ce document majeur. Le Bureau encourage donc vivement le CDMSI à approuver le projet de recommandation lors de sa prochaine réunion et à le transmettre au Comité des Ministres pour adoption dans les plus brefs délais.

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

Le secrétariat informe le Bureau de la dernière réunion du MSI-INT (3 et 4 juillet 2014) et lui fait part des avancées des travaux de ce comité. Le Bureau se déclare globalement satisfait des résultats obtenus par le MSI-INT et prend note du fait qu'une réunion supplémentaire sera organisée les 23 et 24 octobre 2014. Le Bureau prend acte du projet de recommandation CM/Rec(2014) du Comité des Ministres aux Etats membres sur la libre circulation transfrontière des informations sur internet proposé par le MSI-INT. Ce projet de recommandation est considéré comme un très bon texte qui répond aux exigences du mandat du MSI-INT. Le Bureau examine le texte paragraphe par paragraphe, convient de certains changements et recommande ensuite au CDMSI d'approuver le projet de recommandation et de le transmettre au Comité des Ministres en vue de son adoption (annexe 7).

En ce qui concerne le projet de recommandation sur la liberté d'internet, le secrétariat informe le Bureau des premiers éléments élaborés par le rapporteur du MSI-INT en la matière et de la discussion du MSI-INT sur ce sujet (document MSI-INT(2014)07, daté du 16 juin 2014). Le Bureau est aussi informé d'une réunion informelle qui s'est tenue en marge du FGI (du 2 au 5 septembre 2014, à Istanbul) entre le président du MSI-INT et d'autres membres du Comité présents au FGI. Cette réunion informelle a permis d'examiner l'idée d'utiliser les premiers éléments pour élaborer des indicateurs relatifs à la liberté d'internet, discussion qui sera poursuivie lors de la réunion du MSI-INT qui se tiendra les 23 et 24 octobre 2014. Le Bureau prend note de cette information, se dit favorable à l'approche des indicateurs notamment en vue du nouveau programme du Secrétaire Général sur l'application de la législation et d'indices, et décide d'examiner

lors de sa prochaine réunion qui aura lieu en novembre 2014 le projet tel qu'il sera élaboré par le MSI-INT.

6.3 Stratégie du Conseil de l'Europe sur la gouvernance de l'Internet 2012-2015 et nouvelle stratégie sur la gouvernance de l'Internet 2016-2019

Le secrétariat fait part au Bureau de l'avancement de la mise en œuvre de la stratégie sur la gouvernance de l'Internet 2012-2015 et l'informe qu'un rapport sera soumis au CDMSI pour examen lors de sa prochaine réunion plénière prévue en novembre 2014.

Le Bureau prend note des éléments de discussion concernant la stratégie de gouvernance de l'Internet 2016-2019 et décide d'inviter le CDMSI à formuler des commentaires sur ces éléments qui devront être envoyés au secrétariat au plus tard le 27 octobre 2014 pour servir de base à la discussion en plénière.

Le Bureau reconnaît la nécessité de suivre la mise en œuvre de la stratégie actuelle.

Activités de coopération et de diffusion

6.4 Dialogue européen sur la gouvernance de l'Internet (EuroDIG – 12 et 13 juin 2014, Berlin) et Forum sur la gouvernance de l'internet (FGI, du 2 au 5 septembre 2014, Istanbul)

Le Bureau prend note des informations communiquées par le secrétariat sur sa participation à l'EuroDIG 2014 et au Forum sur la gouvernance de l'internet 2014, au cours desquels ont été présentés les travaux du Conseil de l'Europe sur la sécurité des journalistes, le Guide des droits de l'homme pour les utilisateurs d'internet et la neutralité du réseau.

6.5 ICANN

Le Bureau prend acte du rapport d'experts du Conseil de l'Europe, élaboré par Mme Monika Zalnieriute, chercheuse au département de droit de l'Institut universitaire européen en Italie et Thomas Schneider, vice-président du Comité directeur sur les médias et la société de l'information (CDMSI) : les procédures et la politique de l'ICANN en matière de droits de l'homme, des libertés fondamentales et de valeurs démocratiques.

6.6 Autres activités

Le Bureau prend note des informations communiquées par le secrétariat sur le NetMundial. Il prend également note des informations relatives à la réunion d'examen du Sommet mondial sur la société de l'information +10 menée par l'Onu. Le Bureau considère que la stratégie sur la gouvernance de l'internet doit tenir compte des éléments examinés lors de ces réunions.

M. Thomas Schneider communique des informations aux participants sur la Conférence de l'Unesco « Rassembler tous les éléments : conférence multipartite sur l'étude Internet de l'Unesco sur l'accès à l'information, la liberté d'expression, la vie privée et les dimensions éthiques de la société de l'information » qui se tiendra les 3 et 4 mars 2015 à Paris.

7. Activités de coopération

Le Bureau prend note des informations sur les projets accomplis et en cours dans le domaine des médias et de la liberté d'information et sur les activités en cours et planifiées dans le domaine de la gouvernance de l'Internet telles qu'elles figurent dans les documents pertinents.

8. Protection des données

Le Bureau prend note des informations communiquées par le secrétariat du T-PD sur la révision de la recommandation sur le traitement des données personnelles dans le contexte de l'emploi. Le projet de recommandation (document T-PD(2014)08) est le fruit de plusieurs années de travail du T-PD. Le projet a été approuvé par le T-PD lors de sa dernière réunion plénière (du 2 au 4 juin 2014) et transmis au CDMSI. Les délégations ont été invitées à formuler des commentaires écrits sur le projet de texte avant la réunion du Bureau (une délégation a déclaré y être globalement favorable). Le T-PD étant un comité conventionnel, les projets d'instruments juridiques qu'il élabore doivent être transmis au Comité des Ministres par le biais d'un comité directeur (le CDMSI depuis 2012). Il est rappelé que ce comité conventionnel se compose de représentants de 45 des 47 Etats membres du Conseil de l'Europe (Saint Marin et la Turquie ne sont pas Parties à la Convention 108), d'un représentant du premier pays non européen ayant adhéré à la Convention 108 (l'Uruguay), et de représentants de plusieurs Etats observateurs et observateurs non gouvernementaux. Le caractère spécialisé de l'expertise du Comité et ses travaux sont soulignés et il est reconnu que si le format et le libellé du projet de recommandation diffèrent de ceux des instruments du CDMSI, celui-ci peut décider d'approuver le texte et de le soumettre au Comité des Ministres sous le format du T-PD, en s'appuyant sur l'expertise du T-PD.

Le Bureau propose de recommander au CDMSI d'examiner le texte dans le cadre de son propre champ d'expertise lors de la prochaine réunion plénière en novembre, à laquelle participera le président du T-PD, en vue de le soumettre au Comité des Ministres pour adoption.

Un point est fait sur la modernisation de la Convention 108 (la troisième et dernière réunion du Comité ad hoc sur la protection des données est prévue du 1^{er} au 3 décembre 2014) et des informations sont communiquées sur les autres sujets traités par le T-PD (notamment le traitement de données dans un contexte politique, les données médicales et les données massives).

9. Informations relatives aux travaux d'autres organisations et organes du Conseil de l'Europe

9.1 Participation du CDMSI à des événements et des réunions

Le Bureau prend note des informations communiquées par ses membres et le secrétariat.

9.2 Assemblée parlementaire du Conseil de l'Europe (APCE)

Le Bureau rappelle que le CDMSI a formulé des commentaires sur les réponses du Comité des Ministres à l'Assemblée parlementaire concernant sa Recommandation 2036(2014) sur la « Révision de la Convention européenne sur la télévision transfrontière » et sa Recommandation 2041(2014) intitulée « Améliorer la protection et la sécurité des utilisateurs dans le cyberspace ». Le secrétariat informe le Bureau que le Comité des Ministres a adopté sa réponse concernant la Recommandation 2036(2014) le 19 septembre 2014 (CM/AS(2014)Rec2036 final, daté du 19 septembre 2014) qui tient

compte des commentaires du CDMSI. La réponse à la recommandation 2041(2014) sera examinée le 7 octobre par le groupe de rapporteurs du Comité des Ministres, le GR-J.

10. Questions budgétaires et administratives

Le Bureau prend note des informations communiquées par Jan Kleijssen, Directeur de la Direction de la société de l'information et de la lutte contre la criminalité, concernant deux décisions administratives : la désignation de M. Jan Malinowski en tant que Secrétaire exécutif du Groupe Pompidou et la désignation de M. Patrick Penninckx comme chef du service de la Société de l'information, qui devraient entrer en vigueur le 1^{er} décembre 2014 ; et l'intégration de l'Unité sur la gouvernance de l'internet à la Division des médias, qui prendra effet le 1^{er} octobre 2014. Le Bureau prend également note des informations relatives aux nouveaux membres du secrétariat, notamment le recrutement de Mme Giovanna Langella en tant qu'assistante administrative principale temporaire en l'absence d'Anne Boyer-Donnard.

11. Priorités et méthodes de travail du CDMSI

Le Bureau prend note d'un document d'information présenté par le secrétariat sur les priorités du CDMSI et décide de le soumettre lors de la prochaine réunion plénière du comité. Le Bureau suggère que les rapporteurs soient choisis ou de petits groupes de travail internes créés parmi les membres du CDMSI. Renvoyant au document d'information sur les priorités du CDMSI, le Bureau décide d'inviter le CDMSI à créer des groupes de travail informels sur les sujets suivants : le journalisme professionnel et éthique ; le pluralisme des médias et la transparence de la propriété des médias ; la dimension de l'égalité entre les femmes et les hommes dans la couverture des campagnes électorales par les médias. Le Bureau souligne que cette méthode de travail semble nécessaire à l'exécution du mandat du CDMSI.

De plus, le Bureau invite le CDMSI à envisager la création de groupes de travail informels éventuels sur les questions liées à la surveillance, les médias de service public et le discours de haine.

12. Questions diverses

12.1 *Coopération avec les observateurs*

Le Bureau tient un échange de vues sur le rôle du CDMSI concernant l'admission des observateurs au sein du comité. Il rappelle les dispositions pertinentes, spécifiquement la section III/C de la Résolution CM/Res(2011)24 concernant les comités intergouvernementaux et les organes subordonnés, leur mandat et leurs méthodes de travail. Le bureau rappelle également les critères généraux précédemment appliqués par le CDMSI quant aux demandes de statut d'observateur, qui sont une grande expérience du candidat dans le domaine de compétence du CDMSI ou d'autres organes subordonnés concernés, la capacité à apporter une contribution effective et de qualité à leurs activités et la représentativité du candidat au niveau européen.

12.2 *Demande de statut d'observateur de l'Internet Watch Foundation*

Concernant la candidature de l'Internet Watch Foundation au statut d'observateur, le Bureau prend note des informations supplémentaires communiquées par le candidat quant à son engagement international et à sa représentativité. Sur la base de ces

informations, le Bureau convient de se déclarer favorable à cette demande et de recommander au CDMSI d'approuver, lors de sa prochaine réunion (du 18 au 21 novembre 2014), l'octroi du statut d'observateur à l'Internet Watch Foundation.

12.3 Demande de statut d'observateur du Press Club de Prague

Concernant la demande du Press Club de Prague, le Bureau prend note que le candidat a été invité à fournir des informations supplémentaires concernant le critère de représentativité européenne. Le Bureau est informé de la réponse du candidat et du fait que Mme Bissera Zankova, membre du Bureau, a essayé de collecter des informations sur le candidat. Etant donné que le candidat n'a pas fourni suffisamment d'informations quant à sa représentativité européenne, le Bureau convient qu'il ne recommandera pas au CDMSI d'accorder le statut d'observateur auprès du CDMSI au Press Club de Prague.

13. Projet de programme de la 7^e réunion du CDMSI (du 18 au 21 novembre 2014)

Le Bureau décide d'adopter le projet de programme préliminaire de la 7^e réunion du CDMSI.

Ordre de jour

Appendix 1 **Annotated Agenda¹**

1. Opening of the meeting

2. Adoption of the agenda

Notes and expected action	Adopt the agenda in view of the preparation of the 7 th meeting of CDMSI (18-21 November 2014); discuss plenary meeting preparation.
---------------------------	---

3. Information by the Chair and the Secretariat

3.1 Council of Europe action to strengthen the protection of freedom of expression

SG/Inf(2014)2	Setting up of a Freedom of Expression Platform to promote the protection of journalism and safety of journalists - Proposals by the Secretary General to the Committee of Ministers
Report	Round Table on Safety of Journalists – From commitment to action, 19 May 2014 – Strasbourg
SG(2014)1-FINAL	Report by the Secretary General of the Council of Europe ‘State of Democracy, Human Rights and Rule of Law in Europe’
	Information on a comparative study on the laws and practices in respect of filtering, blocking and taking down of illegal content on the Internet in all 47 member States
	Commissioner for Human Rights issue paper on the Rule of Law on the Internet and in the wider digital world (subject to publication, foreseen for September)
	UNESCO Concept Note: Research project on the safety of journalists as potential indicator of rule of law, democracy and development.
Notes and expected action	Take note of information provided by the Secretariat on these Council of Europe initiatives and activities. Consider possible follow-up discussions in the CDMSI.

3.2. Human rights of Internet users

CM/Rec(2014)6	Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users
Notes and expected action	Take note of information provided by the Secretariat with regard to follow-up activities.

4. Follow-up on the implementation of Council of Europe adopted standards in member states regarding media and information society

CDMSI(2014)006	Implementation of adopted standards
CDMSI (2014)012	List of CM standards related to safety of journalists

¹ As it appears in document CDMSI-BU(2014)OJ2, date 23/09/2014.

Notes and expected action	Discuss preparation of the new format (workshops) of the new item "Follow up of the implementation of CoE adopted standards in MS" agreed during the last CDMSI meeting (theme: safety of journalists on the basis of the information provided by the Secretariat).
---------------------------	---

5. Media

Standard setting activities

5.1 Committee of experts on protection of journalism and safety of journalists (MSI-JO)

Terms of Reference	Terms of reference of the MSI-JO
MSI-JO(2014)01	Agenda of the 2 nd meeting of the MSI-JO (6-7 October 2014)
MSI-JO(2014)03	Report of the 1 st meeting of the MSI-JO
MSI-JO (2014)04	Proposal for collection of good practices, information document
	MSI-JO outline structure for draft recommendation on protection of journalism and safety of journalists
Notes and expected action	Take note of the information provided by the Secretariat and discuss elements for a draft recommendation on protection of journalism and safety of journalists and other media actors with a view to discussing the first draft of the recommendation at the next CDMSI plenary meeting in November (following the next MSI-JO meeting in October).

5.2 Hate speech

Campaign	No Hate Speech campaign
DDCP-YD/CHS (2014)2rev	Hate speech draft strategic objectives
	Presentation to CDMSI by young activist and Ms Bridget O'Loughlin, Campaign Co-ordinator of the No Hate Speech Movement.
Notes and expected action	Take note of the information provided by the Secretariat and discuss possible follow-up.

5.3 Gender equality and the media

CM/Rec(2013)01	Recommendation of the Committee of Ministers to member States on gender equality and media
CDMSI (2014)013	Implementation of the Committee of Ministers recommendation CM (2013)1 gender equality and media: Terms of reference toolkit implementation
CM(2013)136final	Gender Equality Strategy 2014-2017
Report	UNESCO Global Forum on Media & Gender – Report by Margaret Gallagher
	Gender Equality and the Media at national level - Compilation of good

	practices in member States
Notes and expected action	Take note of the information provided by the Secretariat and discuss possible follow up.

5.4 Transparency of media ownership

Resolution 2	Belgrade Resolution on Preserving the essential role of media in the digital age
CM Rec No.R(94)13	CM Recommendation No. R(94)13 on measures to promote media transparency
CM Dec (2007)	CM Declaration (2007) on protecting the role of the media in democracy in the context of media concentration
PACE motion of 30/01/2013	PACE motion of 30/01/2013 on “Increasing transparency of media ownership”
10 recommendations	Ten recommendations on transparency of media ownership, paper by Access Info
Conference programme	Conference on transparency of media ownership – Brussels, 24 September 2013
Presentation	Presentation by Fiona Harrisson (Access Info)
Agenda	Regional Conference Transparency in Media Ownership and Preventing Media Concentration, 25-26 September 2014, Skopje
	Digital Agenda for Europe (New meeting) - Exchange of best practices on transparency of media ownership, Brussels, 3 October 2014
Notes and expected action	Discuss possible follow up action.

5.5. Public service media

Resolution 2	Declaration of the Committee of Ministers on Public Service Media Governance Recommendation CM/Rec(2012)1 of the Committee of Ministers to member States on public service media governance Belgrade Resolution on Preserving the essential role of media in the digital age
Notes and expected action	Consider possible follow-up action or discussions in the CDMSI with regard to public service media matters.

6. Information Society and Internet Governance

Standard setting activities

6.1. Network Neutrality

CDMSI(2014)005Rev7	Draft Recommendation CM/Rec(2014)___of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality
------------------------------------	---

CDMSI(2014)Misc2 rev	Compilation of comments by CDMSI members.
Notes and expected action	Consideration of a revised version of the draft recommendation in light of comments by CDMSI members.

6.2 Committee of Experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT)

MSI-INT(2014)10	Report of the 2 nd meeting of the MSI-INT (3-4 July 2014)
MSI-INT(2014)06rev2	Draft recommendation CM/Rec(2014)___ of the Committee of Ministers to member states on free transboundary flow of information on the Internet
MSI-INT(2014)07	Preliminary elements for a draft recommendation on Internet Freedom
Resolution 1	Belgrade Resolution on Internet Freedom
Notes and expected action	Take note of the information provided by the Secretariat on the progress of MSI-INT work. Discuss Draft recommendation CM/Rec(2014)___ of the Committee of Ministers to member states on free transboundary flow of information on the Internet with a view to its submission to the CDMSI plenary meeting in November for finalisation. Discuss preliminary elements for a draft recommendation on Internet freedom.

6.3 Council of Europe Internet Governance Strategy 2012-2015 and new Internet Governance Strategy 2016-2019

Internet Governance Strategy	Synthesis and follow-up chart to the Council of Europe Internet Governance Strategy 2012-2015 – verbal up-date by the Secretariat
CDMSI(2014)Misc4	Discussion elements for Internet Governance Strategy (2016-2019)
CDMSI(2014)Misc3	Comments received on Council of Europe expert report on ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values
Notes and expected action	Take note of the information provided by the Secretariat on the state of implementation of the CoE Internet Governance Strategy 2012-2015. Take note of and discuss proposals by member states for the new Council of Europe strategy 2016-2019.

Cooperation and outreach activities

6.4 European Dialogue on Internet Governance (EuroDIG – 12-13 June 2014, Berlin) and Internet Governance Forum (IGF, Istanbul, 2-5 September 2014)

EuroDIG programme	EuroDIG 2014
Messages	EuroDIG Messages from Berlin
IGF programme paper	IGF 2014

Notes and expected action	Take note of information provided by Committee members who participated in EuroDIG and IGF and of information from the Secretariat. Consider possible follow-up.
---------------------------	--

6.5 ICANN

DGI(2014)12	Council of Europe Expert Report: ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values
	Overview of comments by CDMSI members
Notes and expected action	Take note of information provided by the Secretariat. Take note and discuss comments by CDMSI members. Consider possible follow-up.

6.6 Other activities

NETmundial Multistakeholder Statement	NETmundial: Global multi-stakeholder meeting on the future of Internet governance (São Paulo, 23-24 April 2014)
WSIS + 10 Open Consultation Process	World Summit on Information Society (WSIS) +10 Review Process
GCIC	Global Commission on Internet Governance
	Contacts and cooperation with other international organisations
Notes and expected action	Take note of information provided by the Secretariat and consider possible follow-up discussion in the CDMSI. Discuss Council of Europe contribution to the WSIS +10 Review Process.

7. Cooperation activities

MEDIA.COOP(2014)04	On-going and planned activities in the fields of media
	On-going and planned activities in the field of Internet governance
Notes and expected action	Take note of on-going and planned activities. Consider possible CDMSI proposals.

8. Data protection

Standard setting activities

T-PD (2014) WP rev	Work programme of the T-PD for 2014-2015
T-PD(2014)RAP31Abr_rev	Abridged Report of the 31st Plenary meeting of the T-PD (2-4 June 2014)
T-PD(2014)08	T-PD Draft Recommendation on the processing of personal data in the context of employment (Presentation by T-PD Chair to CDMSI plenary)
ToR CAHDATA	Terms of reference of the ad hoc Committee on data protection (CAHDATA)

CAHDATA(2014)3	Working document – Convention 108 with Additional Protocol and Modernisation proposals
CAHDATA (2014)RAP02Abr	Abridged Report of the 2nd meeting (28-30 April 2014)
Notes and expected action	Take note of the state of play and information provided by the Secretariat. Examine the draft recommendation with a view to approval by CDMSI at its next meeting.

9. Information about work of other organisations and other CoE bodies

9.1 Participation of CDMSI in events and meetings

Agenda	New Media Literacy Leonardo da Vinci project – Seminar (Bratislava, 29-30 May 2014)
Agenda	Conference on “Orbital Slots and Spectrum Use in an Era of Interference” organised by the French Institute for International Relations (IFRI), Brussels, 9 October 2014
Notes and expected action	Take note of the information provided by Bureau members.

9.2 Parliamentary Assembly of the Council of Europe (PACE)

CDMSI(2014)009rev	CDMSI comments on PACE Recommendation 2041(2014) Improving user protection and security in the cyberspace List of documents under preparation in the PACE Committee on culture Science, Education and Media
CM/AS(2014)Rec2036	Reply adopted by the Committee of Ministers to “Revision of the European Convention on Transfrontier Television” Parliamentary Assembly Recommendation 2034 (2014)
Notes and expected action	Take note of comments finalised by the CDMSI via E-mail and information provided by the Secretariat with regard to PACE activities and initiatives of relevance to the work of the CDMSI.

10. Budget and administrative matters

11. Priorities of CDMSI work and working methods

Belgrade Political declaration and resolutions	Council of Europe Conference of Ministers responsible for Media and Information Society – Freedom of Expression and Democracy in the Digital Age – Opportunities, Rights, Responsibilities. Adopted Political Declaration and Resolutions
CM(2013)162	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Report of the Secretary General
CM decisions	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Decisions of the Committee of Ministers
CDMSI(2014)011	Priorities of CDMSI, information document

Notes and expected action	Discuss priorities for the work plan of the CDMSI on the basis of an information document prepared by the Secretariat. Discuss possible themes for hearings at the next CDMSI meeting.
---------------------------	--

12. Other questions

12.1 Co-operation with observers

CM/Res(2011)24	Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods.
Notes and expected action	Discuss co-operation with observers and application procedures for observer status in light of Resolution CM/Res(2011)24.

12.2 Application for observer status by Internet Watch Foundation

Application letter	Application letter
Memo IWF	Memorandum of Association of Internet Watch Foundation
Service Level Agreement Association ACPO/IWF	Service level agreement
Annual report 2013	IWF annual report
Human Rights Audit (2014)	2014 Audit
Notes and expected action	Discuss and recommend decision by the CDMSI on the application for observer status by Internet Watch Foundation.

12.3 Application for observer status by Press Club Prague

Application letter	Application letter
Notes and expected action	Discuss and recommend decision by the CDMSI on the application for observer status by Press Club Prague.

13. Draft agenda of the 7th CDMSI meeting (18-21 November 2014)

CDMSI(2014)OJ2	<i>Draft preliminary agenda of the 7th CDMSI meeting</i>
--------------------------------	--

GENERAL REFERENCE DOCUMENTS

Terms of reference	CDMSI terms of reference 2012-2013
Terms of Reference	CDMSI terms of reference 2014-2015
CM/Res(2011)24	Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods
CM/Res(2011)7	Resolution CM/Res(2011)7 on Council of Europe conferences of specialised ministers
CDMSI(2014)001 Rev	List and timetable of meetings relevant to the CDMSI in 2014
Political declaration and resolutions	Council of Europe Conference of Ministers responsible for Media and Information Society – Freedom of Expression and Democracy in the Digital Age – Opportunities, Rights, Responsibilities. Adopted Political Declaration and Resolutions
CM(2013)162	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Report of the Secretary General
CM Decisions	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Decisions of the Committee of Ministers

RECENT MEETING REPORTS

CDMSI-BU(2014)002	Report of the 5th meeting of the Bureau of the CDMSI (19-20 March 2014)
CDMSI-(2014)008	Report of the 6th meeting of the CDMSI (20-23 May 2014)

Annexe 2

Liste de participants

Ms Maja Rakovic (Chair/ Présidente), Counsellor, Ministry of Foreign Affairs, Serbia/Serbie

Mr Thomas Schneider, (Vice-Chair / Vice-président) International Affairs, Federal Office of Communication, Federal Department for the Environment, Transport, Energy and Communication, Switzerland/Suisse

Mr Mark Carvell, Media Team, Department for Culture, Media and Sport, United Kingdom /Royaume-Uni

Ms Christina Lamprou, Head of the Department of Audiovisual Affairs, Directorate of Mass Media - General Secretariat of Information and Communication, Hellenic Republic

Apologised / Excusé

Mr Éanna O'Conghaile, Principal Officer, Broadcasting Policy Division, Department of Communications, Energy & Natural Resources; Ireland/Irlande

Mr Emir Povlakic, Head of Division for Licensing, Digitalization and Coordination in Broadcasting, Communications Regulatory, Bosnia and Herzegovina/Bosnie-Herzegovine

Ms Bissera Zankova, Media Expert / Consultant, Ministry of Transport, IT and Communications, Bulgaria/Bulgarie

SECRETARIAT

M. Jan Kleijssen, Directeur, Direction de la Société de l'Information et de la lutte contre la criminalité (DG I)

M. Jan Malinowski, Chef du service de la Société de l'information, Direction générale des droits de l'homme et de l'Etat de droit (DGI)

Mme. Silvia Grundmann, Secrétaire du CDMSI, Chef de la division médias, Direction générale des droits de l'homme et de l'Etat de droit (DGI)

Mme. Onur Andreotti, Administratrice, division médias, DG I

Mme. Elvana Thaçi, Administratrice, division médias, DG I

M. Lee Hibbard, Administrateur, Unité de la gouvernance d'Internet, DG I

Mme. Loreta Vioiu, Administratrice, Unité de la gouvernance d'Internet, DG I

M. Luca Belli, Administrateur, Unité de la gouvernance d'Internet, DG I

Mme. Sophie Kwasny, Administratrice, Unité de la protection des données, DG I

Mme. Giovanna Langella, Assistante administrative principale, division médias, DG I

(Répartition des sexes des 6 membres du Bureau: 3 femmes (50%), 3 hommes (50%))

Annexe 3

Séminaire et Dialogue Inter-régional sur la protection des journalistes

*Pour une protection effective du travail des journalistes
et l'éradication de l'impunité des crimes commis contre les journalistes*

<http://www.inter-justice.org/>

Organisé par

Conseil de l'Europe
UNESCO

Centre for Freedom of the Media (CFOM), Université de Sheffield
European Lawyer's Union / Union des Avocats Européens (ELU/UAE)

En coopération avec

Région Alsace

Ville de Strasbourg

Commission Interaméricaine des Droits de l'Homme

Commission Africaine des Droits de l'Homme et des Peuples

Media Legal Defence Initiative

Open Society Foundations

Cour européenne des droits de l'homme, Strasbourg (SALLE DE PRESSE)

Lundi, 3 novembre 2014

8.30 -18.00

Les organisateurs remercient Open Society Foundations pour leur contribution à cet évènement



Union des avocats européens

ORDRE DU JOUR (22.10.2014)

8.30-9.00	ENREGISTREMENT
9.00	ALLOCUTIONS D'OUVERTURE <ul style="list-style-type: none">• Guido Raimondi, Vice-Président de la Cour européenne des droits de l'homme• Gabriella Battaini-Dragoni, Secrétaire Générale adjointe du Conseil de l'Europe• Anne Brasseur, Présidente de l'Assemblée Parlementaire du Conseil de l'Europe• Nils Muižnieks, Commissaire aux droits de l'homme du Conseil de l'Europe• Guy Berger, Directeur, Division liberté d'expression et développement des médias, UNESCO
9.30 – 11.00	SESSION I. Protection nationale et internationale des journalistes : examen des preuves <p><i>Modérateur: William Horsley, Directeur International, Centre for Freedom and Media, Université de Sheffield</i></p> <ul style="list-style-type: none">• La protection légale des journalistes au niveau international <i>Jane Connors, Directeur, Division de la recherche et du droit au développement, HCDH</i>• Les protections légales et les mécanismes de protection au niveau régional au sein de l'Organisation des États Américains <i>Ona Flores, Juriste Senior auprès du Rapporteur spécial pour la liberté d'expression de la Commission interaméricaine des droits de l'homme, Organisation des États Américains (OAS)</i>• La protection légale des journalistes au niveau régional : l'exemple de la Commission africaine des droits de l'homme et des peuples <i>Faith Pansy Tlakula, Rapporteur Spécial pour la liberté d'expression et accès à l'information de la Commission africaine des droits de l'homme et des peuples (ibc)</i>• La protection des journalistes en droit international pénal <i>James Stewart, Procureur Général adjoint, Cour pénale internationale</i>• Discussions et interventions diverses
11.00 – 11.20	Pause
11.20 – 12.30	SESSION II. La protection des droits des journalistes dans l'exercice de leur fonction d'intérêt public: lacunes et avancées. Points de vue exprimés par des juristes spécialisés en droits de l'homme, les médias et la société civile <p><i>Modérateur: Grégory Thuan dit Dieudonné, avocat, Union des Avocats Européens</i></p> <ul style="list-style-type: none">• Gestion et prévention des risques : dans quelles situations envoyer - ou non - des journalistes sur le terrain ? <i>Loïck Berrou, France 24 TV, responsable des équipes de reportage de France 24</i>• L'impunité des crimes contre les journalistes : le point de vue d'un avocat <i>Karina Moskalenko, Directrice Fondatrice du centre de la protection internationale (CPI)</i>• Les programmes nationaux de protection: le modèle de la Colombie <i>Maria Teresa Ronderos, Présidente du programme sur le journalisme indépendant de Open Society Foundations</i>• Le droit des traités en tant qu'«instrument vivant»: un renforcement du niveau de protection <i>Barbora Bukovska, Directrice Principale en matière du droit et des politiques, Article 19</i>• Discussions and interventions diverses
12:30 – 14.30	Déjeuner au Conseil de l'Europe ou au Palais des Droits de l'Homme (sur invitation – les informations concernant le déjeuner seront envoyées individuellement au participants)

14.30 – 15.50	<p>SESSION III. La coopération judiciaire et nationale en vue d'améliorer les normes en matière de protection, de prévention et de poursuites dans les affaires ayant trait aux journalistes et à la liberté d'expression</p> <p><i>Modérateur: Peter Noorlander, Directeur exécutif de 'Media Legal Defence Initiative'</i></p> <ul style="list-style-type: none"> • Les juridictions nationales et les questions d'adhésion aux normes internationales : un bilan global <i>Michael O'Flaherty, Professeur en droit international des droits de l'homme à l'Université nationale d'Irlande (NUI Galway), ancien vice-président du Comité des droits de l'homme de l'ONU</i> • Etudes de cas et leçons tirées de l'expérience africaine <i>Maureen Kondowe, Vice-Présidente de l'Union panafricaine des avocats (PALU)</i> • Le rôle des procureurs spéciaux et les mécanismes de protection d'urgence en Amérique Latine <i>Eduardo Bertoni, Ecole de droit de l'Université de Palermo (Argentine) et ancien Rapporteur Spécial pour la liberté d'expression de la Commission interaméricaine des droits de l'homme</i> • Discussions et interventions diverses
15.50 – 16.10	Pause
16.10 - 17.15	<p>SESSION IV. Un agenda pour un dialogue inter-régional en vue d'un renforcement de la protection et de l'éradication de l'impunité</p> <p><i>Modérateur: Dirk Voorhoof, Professeur à l'Université de Gand (Belgique)</i></p> <ul style="list-style-type: none"> • Contentieux stratégique et mesures provisoires en vue de la protection des journalistes en Amérique: prévention, protection et poursuites <i>Catalina Botero, ancienne Rapporteur Spéciale pour la liberté d'expression de l'Organisation des Etats Américains (OAS)</i> • Les perspectives internationales des Cours régionales des droits de l'homme: l'exemple de la Cour européenne des droits de l'homme <i>Lawrence Early, Jurisconsulte, Greffe de la Cour européenne des droits de l'homme</i> • L'exemple d'un cadre normatif pour la protection régionale des journalistes en Asie <i>Harry L. Roque, Professeur de droit, Université de Philippines, Manille</i> • Discussions et interventions diverses
17.15 – 17.45	<p>Un dialogue interrégional: besoins, objectifs et attentes</p> <p><i>Modérateur: David Kaye, Rapporteur Spécial de l'ONU sur la liberté d'expression</i></p> <ul style="list-style-type: none"> • Manuel Ventura Robles, Juge à la Cour interaméricaine des droits de l'homme •, Cour africaine des droits de l'homme et des peuples (<i>à confirmer</i>) • Lawrence Early, Jurisconsulte, Greffe de la Cour européenne des droits de l'homme
17.45-17.55	<p>Conclusions du rapporteur</p> <p>Dr Tarlach McGonagle, Chercheur en chef de l'Institut du droit à l'information (IViR), Faculté de droit de l'Université d'Amsterdam</p>
17.55-18.00	<p>Remarques de clôture</p> <p>Jan Kleijssen, Directeur, Direction 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, Conseil de l'Europe</p>
18.00	Fin du séminaire
19.00 – 21.00	<p>Apéritif et cocktail dinatoire dans les locaux de l'Association Parlementaire Européenne (Villa Schutzenberger, 76 Allée de la Roberstau)</p>

Liens utiles

[Cour européenne des droits de l'homme](#)
[Plan de Strasbourg](#)
[UNESCO](#)
[Centre for Freedom of the Media](#)
[Union des Avocats Européens](#)

Personnes de contact

CENTRE FOR FREEDOM OF THE MEDIA (CFOM)

William Horsley, william@inter-justice.org

UNION DES AVOCATS EUROPEENS (Commission des Droits de l'Homme)

Gregory Thuan dit Dieudonné, Gregory.thuan.avocat@gmail.com; gthuan@hincker-associes.com
Valeria Reva, Assistante, vreva@hincker-associes.com

CONSEIL DE L'EUROPE

Onur Andreotti, onur.andreotti@coe.int
Elisabeth Maetz, Assistante, elisabeth.maetz@coe.int

UNESCO

Ming Kuok Lim, mk.lim@unesco.org
Sylvie Coudray, s.coudray@unesco.org;

* * *

Appendix 4 : Questions for CDMSI members (CDMSI(2014)Misc6)

anglais uniquement

Questions for CDMSI members on the implementation of the guidelines of the CM on eradicating impunity for serious human rights violations, in the context of safety of journalists (30 March 2011)

- I. Have the guidelines of the CM on eradicating impunity for serious human rights violations been translated into the national language, have they been widely disseminated in particular among all authorities responsible for the fight against impunity?
- II. Which are the existing mechanisms to ensure investigation and prosecution of attacks against journalists and other media actors?
- III. The members are invited to provide information on the execution of ECtHR judgements related to safety of journalists and the issue of impunity, if there are such judgements v. their country. In case of difficulties in the execution of such ECtHR judgements, the members may wish to specify what are the main obstacles (i.e. legislation, practice, other) for the execution and what measures have been taken to overcome these.
- IV. Are there any non-judicial mechanisms, such as parliamentary or other public inquiries, ombudspersons, independent commissions, as useful complementary procedures to the domestic judicial remedies guaranteed under the ECtHR, specifically dealing with threats and crimes targeting journalists and other media actors?

Appendix 5 Addendum to compilation of comments on the draft recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (Addendum to CDMSI(2014)Misc2rev 2 - 29 September 2014)

anglais uniquement

This document compiles all comments sent to the Secretariat by CDMSI delegations on the Draft Recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (contained in document CDMSI(2014)005Rev7) during the period of time from 5 September to 19 September 2014.

FRANCE

19/10/2014

We thank you for the opportunity to comment on this new version of the text. Thank you for the work that has been done. We find the text convenient with the exception of two small points of formulation explained in the attachment.

In any case we regret that this recommendation on network neutrality does not cover the neutrality of the value chain (as service platforms and applications)

Paragraph 1.2., 1st line, suggestion to delete the word equally and related comment "the concept of equality is very strict and impossible to put in place in practice (data packets take different paths, only the point of departure and the point of arrival are in common).The principle of non-discrimination is sufficient to attain the objective that is pursued".

Paragraph 5.1, last line, suggestion to add before the phrase "Internet speeds" the words "an estimation of".

GERMANY

21/09/2014

"I am sorry to inform you that due to the ongoing process of national decision finding the German Government neither has a final position on the substance of the draft nor on its proceeding. We would like to withdraw our comments that were made at an earlier stage of the draft."

THE RUSSIAN FEDERATION

19/10/2014

"Dear CDMSI members,

I have studied the remastered Draft recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (CDMSI (2014) 005Rev7 dated by August 19 of 2014 and appreciating the work done by the Secretariat and Bureau Members have to state with some regret that the fundamental ideas of the Russian position described at the last CDMSI meeting and the last June 20 Statement were not taken into account , the suggestions to balance the document were ignored. In this situation I have only to inform all of you that I cannot give my approval for the Draft."

THE UNITED KINGDOM

19/10/2014

"Following further consultations with policy leads on net neutrality in the UK administration, the UK hereby requests an extension of the period for receiving comments on this important CM text until the start of the next Committee meeting in November. By that time we in UK will have had Ministerial clearance which necessarily also takes into account the progress and outcome of the current negotiations in Brussels. I hope therefore that CDMSI colleagues can agree to this extension of the period for comments."

Annexe 6

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, y compris le droit de recevoir et de communiquer des informations et des idées, ainsi que la participation à la vie démocratique, reposent de plus en plus sur l'accessibilité et la qualité d'une connexion à internet.

2. Les fournisseurs d'accès à internet ont la capacité de contrôler les flux de données et d'informations (le trafic internet) qui transitent sur les réseaux ils gèrent. Ils peuvent appliquer des mesures de gestion du trafic internet à différentes fins légitimes, par exemple pour préserver l'intégrité et la sécurité du réseau. 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 contenu, d'applications ou de services spécifiques. En outre, certaines des techniques utilisées dans ce contexte permettent d'inspecter ou de surveiller les communications, ce qui peut saper la confiance des utilisateurs d'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 Convention), 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 internet, fondamentaux pour la démocratie et la diversité culturelle.

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 Convention 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. Rappelant les instruments normatifs pertinents du Conseil de l'Europe² et afin de promouvoir et d'optimiser la valeur de service public d'internet, le Comité des Ministres recommande aux Etats membres :

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

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.

1. Principes généraux

1.1. Dans l'exercice de leur droit à la liberté d'expression, conformément à l'article 10 de la Convention, 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, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, 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. C'est 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.

1.4. Le principe de la neutralité du réseau devrait s'appliquer à tous les services offrant une connexion à internet (services d'accès à 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 internet ne devraient pas restreindre la liberté de choix des utilisateurs d'internet en bloquant, en ralentissant, en modifiant, en dégradant ou en défavorisant certains contenus, applications ou services.

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

- donner effet à une décision de justice ;
- 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 ;
- empêcher la transmission de communications non sollicitées de marketing direct aux utilisateurs finaux qui ont accepté au préalable ces mesures restrictives ;
- réduire le plus possible les conséquences d'une surcharge exceptionnelle ou temporaire du réseau, à condition de traiter à égalité les classes de trafic équivalentes.

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 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. Le traitement préférentiel du trafic fondé sur des accords conclus entre des fournisseurs d'accès à 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 internet. Ces 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.

3.4. Pour permettre aux utilisateurs de recevoir par internet les services audiovisuels, de presse et de radiodiffusion de leur choix, 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. Les 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 au second paragraphe, et devraient être conformes à la législation en vigueur en matière de droit à la vie privée et de protection des données à caractère personnel.

4.2. L'application de techniques capables d'analyser le contenu des communications aux fins de la gestion du trafic internet constitue une atteinte au droit à la vie privée. Un tel usage doit donc être pleinement conforme à l'article 8 de la Convention, 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 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 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 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 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.

Appendix 7 Draft Recommendation CM/Rec(2014)___of the Committee of Ministers to member States on free transboundary flow of information on the Internet*

anglais uniquement

The right to freedom of expression, including the right to receive and impart information and ideas without interference and regardless of frontiers constitutes a cornerstone of democratic society and is one of the basic conditions for its sustainability and progress and for the development of every human being. The rights and freedoms set out in the European Convention on Human Rights (hereinafter the ECHR) and in the Universal Declaration on Human Rights apply equally online and offline. Article 10 of the ECHR applies not only to the content of information but also to the means of its dissemination or hosting, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.

The right to freedom of assembly and association, as guaranteed by Article 11 of the ECHR, is similarly fundamental to democracy. In addition, safeguarding the right to private life as enshrined in Article 8 of the ECHR and ensuring the protection of personal data in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, hereinafter Convention 108) underpins the exercise of the right to freedom of expression and contributes to the free flow of information on the Internet.

The unimpeded transboundary flow of information is critical for the full realisation of these rights and freedoms, safeguarding pluralism and diversity of information, the development of culture and innovation and economic growth. National policies or measures, commercial activities or technological practices which interfere, whether deliberately or inadvertently, with Internet traffic or which place restrictions on Internet content or services within one state may have a bearing beyond that state's frontiers on the exercise of the right to freedom of expression and the right to freedom of association. Consequently, the exercise of national sovereignty may be affected by such interferences.

Multiple states may claim jurisdiction over the same information and services on the Internet, which may leave individuals subject to inconsistent or conflicting rules. The variety/diversity of national laws on illegal content and services, as well as the application of competing and conflicting national laws, creates a complex legal environment which can make it difficult for individuals to claim the protection to which they are entitled under Article 10 of the ECHR. Developments in technology, for example content delivery networks and the growth of services that store and process data in remote locations rather than in locations proximate to the information owner or custodian/recipient (cloud services) will also increase complexities.

There is a need to promote a common international understanding, to consolidate norms and adhere to best practices on free transboundary flow of information on the Internet while ensuring full compliance with international agreements on the protection of children online, combatting cybercrime, protection of personal data and other relevant agreements. State action in this context should rely on Recommendation CM/Rec(2011)8 of the Committee of Ministers which sets out a commitment of member states to protect and promote the universality, integrity and openness of the Internet. This includes state responsibility to ensure that actions within one state do not illegitimately interfere with access to information in other states or negatively impact the transboundary Internet traffic. States should also have due regard to other Council of Europe standards which are referenced in the appendix of this recommendation as well as to the value of self-regulation. This contributes to the elaboration of best practices and new models of behaviour that promote the unhampered flow of information, opinion and ideas on the Internet.

Therefore, the Committee of Ministers recommends that member states, when developing and implementing Internet-related policies at national level and within the international community:

- promote and protect free transboundary flow of information having due regard to the principles of this recommendation, in particular by ensuring that these principles are reflected in regulatory frameworks or policies and in practice;

* As contained in document MSI-INT (2014)06 Rev3, date 24 September 2014

- encourage private sector actors, civil society and technical communities to support and promote the implementation of the principles included in this recommendation.

Principles for free transboundary flow of information on the Internet

1. General principles

- 1.1. States have an obligation to guarantee to everyone within their jurisdiction the right to freedom of expression and the right to freedom of assembly and association, in full compliance with Articles 10 and 11 of the ECHR which apply equally to the Internet. These rights and freedoms must be guaranteed without discrimination on any ground such as gender, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.
- 1.2. States should protect and promote the global free flow of information on the Internet. They should ensure that actions and omissions within their territory pursue the legitimate aims set out in the ECHR and other relevant international agreements and do not have an unnecessary or disproportionate impact on the transboundary flow of information.

2. Due diligence principles

States should exercise due diligence when developing, assessing and implementing their national policies with a view to identifying and avoiding interferences with Internet traffic which have an adverse transboundary impact on the free flow of information on the Internet.

- [Evaluation] Regulatory or other measures that are capable of having such an impact must be evaluated with regard to state responsibility to respect, protect and promote the human rights and fundamental freedoms enshrined in the ECHR.
- [Transparency, foreseeability, accountability] When developing policy and regulatory frameworks that may impact free flows of information on the Internet states should ensure transparency, including the results of evaluations mentioned above, foreseeability as to their implementation and accountability. In particular, proposed regulatory frameworks should be published with sufficient time and opportunity for public comment.
- [Proportionality and review of measures] States must ensure that the blocking of content or services deemed illegal is in compliance with Articles 8, 10 and 11 of the ECHR. In particular, measures adopted by state authorities in order to combat illegal content or activities on the Internet should not result in unnecessary and disproportionate impact beyond the state's borders. States should strive towards measures which are least intrusive and least disruptive and which are carried out through a transparent and accountable process. Measures adopted or promoted by states should be regularly reviewed to determine their practical effectiveness and ongoing necessity and proportionality.

3. Value of self-regulation

States should encourage, facilitate, support and participate as appropriate in the development of self-regulatory codes of conduct so that all stakeholders respect the right to freedom of expression, the right to freedom of assembly and association and the right to private life, with particular regard to the free flow of Internet traffic.

4. Promoting technical best practices

- 4.1. States should promote multi-stakeholder co-operation in the development and implementation of technical best practices that respect the right to freedom of expression and the right to freedom of association, including evaluations of the necessity of actions and proportionality of measures that may have a transboundary impact on Internet traffic.
- 4.2. States should ensure that national policies respect the global Internet architecture. This includes adherence to best practices regarding the domain name system.

5. International dialogue and policy

- 5.1. When national policies and commercial activities interfere with Internet traffic beyond the state's boundaries, the parties concerned may not have standing to raise their grievances within that state. States should ensure that structures and procedures exist for hearing and resolving the grievances of these parties. In this regard, states should engage in international dialogue to progressively develop shared understandings, international standards and norms and to adhere to best practices with regard to applicable law and competent jurisdiction in cases where competing (conflicting) laws apply to freedom of expression and access to information.
- 5.2. In the context of development of international policy or regulation for the Internet, states should protect and promote Internet connectivity as well as availability and accessibility of diverse and pluralistic information as these impact the free transboundary flow of information on the Internet.
- 5.3. In relation to services that store or process information in remote locations, states should safeguard the right to personal data protection in accordance with Convention 108 and the right to privacy in compliance with Article 8 of the ECHR. This is important for the full exercise of the rights in Article 10 of the ECHR. Regarding such services, states also should engage in international dialogue to develop shared norms, practices and understandings to address questions about jurisdiction and applicable law.

Appendix

Relevant Council of Europe standards

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.201)
- Convention on Cybercrime (ETS No. 185) and Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)
- Recommendation CM/Rec(2009)5 on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment.
- Declaration on protecting the dignity, security and privacy of children on the Internet (20 February 2008)
- Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters
- Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet
- Declaration on network neutrality (29 September 2010)

Annexe 8

**COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES
PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A
CARACTERE PERSONNEL [STE n°108]**

(T-PD)

**Projet de Recommandation³ sur le traitement des données à caractère
personnel dans le cadre de l'emploi**

³ Projet de Recommandation tel qu'il a été approuvé par le T-PD lors de sa 31^{ème} réunion Plénière (2-4 juin 2014) et communiqué au CDMSI en vue de sa transmission au Comité des Ministres pour adoption.

INDEX

PREAMBULE

ANNEXE :

Partie I – Principes généraux

1. Champ d'application
2. Définitions
3. Respect des droits de l'homme, de la dignité et des libertés fondamentales
4. Application des principes de traitement
5. Collecte et enregistrement des données
6. Utilisation interne des données
7. Communication des données et utilisation des TICs pour la représentation des employés
8. Communication externe des données
9. Traitement de données sensibles
10. Transparence du traitement
11. Droit d'accès, de rectification et d'opposition
12. Sécurité des données
13. Conservation des données

Partie II – Formes particulières de traitement

14. Utilisation de l'Internet et de communications électroniques sur le lieu de travail
15. Systèmes et technologies de l'information pour le contrôle des employés, notamment la vidéosurveillance
16. Appareils permettant de localiser les employés
17. Mécanismes internes de signalement
18. Données biométriques
19. Tests psychologiques, analyses et procédures analogues
20. Autres traitements de nature à présenter des risques spécifiques au regard des droits des employés
21. Garanties complémentaires

**PROJET DE RECOMMANDATION 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 qu'il doit être tenu compte, lors de l'élaboration de principes dans le secteur de l'emploi, d'autres intérêts (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 à 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 la présente recommandation et son annexe, 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 un candidat à un emploi et détenant la responsabilité légale de l'entreprise ou de l'établissement ;
- « employé » ou « candidat à l'emploi » 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 de demander à un employé ou à un candidat à l'emploi d'avoir accès à des informations que l'employé ou le candidat à l'emploi 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 doit 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.

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 d'autres fins 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 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. En ce qui concerne le secteur public, les dispositions relatives à la divulgation de données à caractère personnel afin d'assurer la transparence du gouvernement et de toute autre autorité publique ou organisme et / ou de surveiller l'utilisation correcte 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 personnes.

8.4. Les employeurs devraient prendre les mesures appropriées afin de veiller à ce que seules les données pertinentes, exactes et à jour soient traitées, et à plus forte raison s'agissant des données ouvertement disponibles sur internet.

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 doivent 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. Le traitement de données génétiques, pour déterminer par exemple l'aptitude professionnelle d'employés ou candidats est interdit, même avec le consentement de l'intéressé. Le traitement de données génétiques peut être permis à titre exceptionnel lorsque cela est prévu par le droit interne et moyennant des garanties appropriées, en particulier pour éviter toute atteinte grave à la santé de la personne concernée ou de tiers.

9.4. Les données de santé et - lorsque leur traitement est licite - les données génétiques, ne devraient être collectées qu'auprès de l'employé concerné 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, comme l'administration du personnel, 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 n'aient accès à ces données.

9.7. Les données de santé relatives à des tiers ne feront en aucune circonstance l'objet d'un traitement, à moins que la personne concernée n'ait donné au préalable son entier consentement, 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 destinataires⁴ 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 traitement¹ 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 selon les modalités prévues par le droit interne.

⁴ Conformément à la définition visée à l'article 2 de la Convention 108

11.4. Un employé ne doit 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 doit 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. Par ailleurs, dans le cas d'une enquête interne effectuée par un employeur, l'exercice de ces droits 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. Les employeurs devraient garantir de manière adéquate la sécurité des données lors de l'utilisation des TICs pour le traitement de données à caractère personnel à des fins d'emploi.

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. 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 tenter 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 relatives 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 manière graduée et utilisant dans un premier temps par sondages non individuels des données anonymes ou agrégées.

14.3. L'accès aux communications électroniques professionnelles des employés en ayant été informés au préalable ne peut, le cas échéant, survenir 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 doit 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 peuvent faire l'objet d'une surveillance.

14.5. Lorsqu'un employé quitte son emploi, l'employeur doit prendre des mesures techniques et organisationnelles afin que la messagerie électronique de l'employé soit désactivée automatiquement à son départ. Si le contenu de la messagerie doit être récupéré pour la bonne marche de l'entreprise, l'employeur doit 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 comme finalité directe et principale le contrôle de l'activité et du comportement des employés ne doivent pas être permises. L'introduction et l'utilisation des systèmes et technologies de l'information nécessaires aux fins de la protection de la production, de la santé, de la sécurité, et de la gestion efficace d'une organisation, menant, de façon indirecte, à la possibilité de contrôler l'activité des employés, doivent être soumises aux garanties appropriées visées au principe 21, et notamment la consultation des représentants des employés.

15.2. De tels systèmes et technologies de l'information doivent en tout état de cause être spécialement conçus et placés de façon à ne pas porter préjudice aux droits fondamentaux des employés. 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 réalisés doit être limitée dans le temps.

16. Appareils permettant de localiser les employés

16.1. Les appareils permettant de localiser un employé ne peuvent 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 doit 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 doivent 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 doivent 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 doivent assurer la protection des données à caractère personnel de toutes les parties concernées. En particulier, les employeurs doivent 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 doivent être utilisées uniquement aux fins des procédures internes appropriées relatives aux dits signalements, à la loi ou à la procédure judiciaire.

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 doit 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-traitants⁵, doivent procéder à une analyse de l'impact potentiel du 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 :

- Informer préalablement les employés de l'introduction des systèmes et technologies d'information permettant le contrôle de leur activité. L'information fournie doit être mise à jour, et le droit d'information doit s'effectuer conformément au principe 10 de la présente recommandation. Les informations doivent 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 ;
- Prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux employés ;

⁵ Conformément à la définition visée à l'article 2 de la Convention 108

- Avant l'introduction d'un système de surveillance ou lorsqu'un système existant doit 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 doit être assuré ;
- Consulter, conformément à la législation nationale les autorités nationales de contrôle sur les traitements de données à caractère personnel.