



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 12 septembre 2012

T-PD (2012)01_Rev_fr

**COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES
A L'EGARD DU TRAITEMENT AUTOMATISÉ
DES DONNÉES A CARACTÈRE PERSONNEL [STE n°108]**

Compilation des avis

DG I – Droits de l'Homme et Etat de droit

TABLE DES MATIERES

- I. Avis du T-PD sur la Recommandation 1984(2011) de l'Assemblée Parlementaire du Conseil de l'Europe sur « la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne »**

- II. Avis sur le projet de déclaration du Comité des Ministres sur les risques du suivi numérique et des autres technologies de surveillance pour les droits fondamentaux**

I. Avis du T-PD sur la Recommandation 1984(2011) de l'Assemblée Parlementaire du Conseil de l'Europe sur « la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne » (doc. T-PD(2011)9)

1. Le T-PD se félicite de l'adoption par l'Assemblée parlementaire (le 7 octobre 2011) de la Recommandation 1984(2011) sur « la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne » qui contribue à sensibiliser les Parlementaires à la question de la vie privée et de la protection des données personnelles sur internet et dans le nouvel environnement médiatique.

2. Le T-PD souhaite en premier lieu saluer l'approche ouverte et inclusive adoptée par le Rapporteur (Mme Rihter) dans la préparation de son rapport. Un représentant du T-PD a participé aux auditions organisées par la Commission compétente de l'Assemblée Parlementaire (la Commission de la culture, de la science et de l'éducation) à l'occasion du Forum de la Gouvernance de l'Internet (IGF) à Vilnius (septembre 2010) ainsi qu'au mois de mars de cette année, afin de faire état des travaux du T-PD et de la modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après Convention 108). En avril 2011, le Secrétariat a été entendu lors d'une réunion de la Sous-commission sur les médias.

3. S'agissant des recommandations formulées par l'Assemblée Parlementaire, le T-PD souscrit pleinement à l'appel (paragraphe 2.1 et 2.2 de la Recommandation) à de nouvelles signatures et ratifications de la Convention 108, à la fois par les Etats membres du Conseil de l'Europe (quatre des 47 Etats n'étant pas encore Parties à la Convention) ainsi, qu'en particulier, à tous les pays du monde. En juillet 2011, l'Uruguay est devenu le premier pays hors Europe à être invité à adhérer à la Convention 108. L'adhésion d'états non-membres renforcera la reconnaissance universelle des principes fondamentaux de protection des données à caractère personnel appelée dès 2005 par la 27^{ème} Conférence Internationale des Commissaires à la Protection des données et à la vie privée (Montreux, 14-16 septembre 2005) et répétée lors de leur 32^{ème} Edition (Jérusalem, 26-29 octobre 2010).

4. Le T-PD estime par ailleurs indispensable que la demande faite (paragraphe 2.3) de prévoir un budget adéquat soit suivie d'effets. En effet, l'évolution constante du travail normatif, la promotion de la Convention 108 hors des frontières de l'Europe (et les activités liées de renforcement des capacités) ainsi que la mise en œuvre effective de la Convention nécessitent des moyens adaptés. La protection des données personnelles et le respect du droit à la vie privée doivent demeurer des domaines prioritaires pour le Conseil de l'Europe.

5. S'agissant de l'Union européenne, le T-PD salut le soutien qu'elle apporte à la promotion de la Convention 108, notamment au travers de l'organisation d'une série de conférences en 2011 sous l'impulsion des autorités hongroises et polonaises. La protection des données est un parfait exemple de complémentarité entre les activités du Conseil de l'Europe et celles de l'Union européenne, et il sera essentiel de maintenir cette cohérence à l'avenir. Conformément au Programme de Stockholm de l'Union européenne, la Convention 108 devrait être intégrée dans les programmes de coopération de l'Union européenne et les activités menées de par le monde.

6. Pour ce qui a trait au travail de modernisation, le T-PD est reconnaissant de la contribution substantielle et des propositions intéressantes faites par l'Assemblée Parlementaire. Tout comme l'Assemblée Parlementaire, le Comité est d'avis que les normes existantes ne peuvent être amoindries et que le mécanisme de suivi de la Convention devrait être renforcé en vue de permettre notamment de suivre le développement rapide des technologies de l'information et de la communication. Le T-PD invite l'Assemblée Parlementaire à continuer à participer activement au

processus de modernisation, notamment par la désignation d'un représentant aux réunions du Comité (conformément à l'article 3.4 du règlement intérieur du T-PD).

7. Enfin, le T-PD prend note de l'invitation faite au Secrétaire Général de garantir la protection des données à caractère personnel traitées par l'Organisation et de renforcer la position du Commissaire à la protection des données du Conseil de l'Europe. Le Comité rappelle qu'à sa 26^{ème} réunion Plénière (1-4 juin 2010), il a adopté un projet révisé de Règlement instaurant un système de protection des données pour les fichiers de données à caractère personnel au Conseil de l'Europe, ayant vocation à s'appliquer à toute donnée à caractère personnel traitée par les instances et institutions de l'Organisation.

8. Suite aux élections menées lors de la 27^{ème} réunion Plénière (29 novembre – 2 décembre 2011), le T-PD se félicite de la nomination de Mme Eva Souhrada-Kirchmayer en qualité de Commissaire à la protection des données du Conseil de l'Europe et veut croire que cette nomination contribuera au renforcement de la protection des données à caractère personnel au sein du Conseil de l'Europe.

II. Avis sur le projet de déclaration du Comité des Ministres sur les risques du suivi numérique et des autres technologies de surveillance pour les droits fondamentaux

1. Le T-PD a été saisi d'une demande d'avis du Bureau du Comité directeur sur les médias et la société de l'information (CDMSI) suite à la première réunion de ce dernier qui a eu lieu les 29 et 30 mai 2012. La demande concerne un projet de déclaration du Comité des Ministres, relatif aux risques du suivi numérique et des autres technologies de surveillance pour les droits fondamentaux.

2. Le T-PD souhaite tout d'abord saluer l'initiative du CDMSI de traiter d'une problématique qui de nos jours est d'une importance cruciale et peut poser des défis sérieux au respect de la vie privée et à la protection des données à caractère personnel.

3. Le T-PD considère opportun de clarifier le champ d'application du projet de Déclaration (et donc également son titre), qui, s'il est destiné à traiter de l'usage fait à titre privé de telles technologies (comme semble l'indiquer le paragraphe 13), mériterait notamment que les références aux abus possibles des autorités publiques soient revues.

4. Le T-PD note à titre liminaire une différence dans la numérotation des paragraphes de la version française et anglaise du texte du projet de déclaration du Comité des Ministres. Le T-PD se base dans les remarques qui suivent sur la numérotation de la version anglaise du projet.

5. Le T-PD note au paragraphe 5 du Projet de déclaration qu'il est fait mention de la conservation des données sensibles (il conviendrait à cet égard d'utiliser dans la version anglaise le terme de 'storage' plutôt que 'storing'). De façon plus générale, le T-PD souhaite souligner que les principes de base de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («Convention 108») sont pleinement applicables aux traitements de données à caractère personnel réalisés au moyen d'un suivi numérique et d'autres technologies de surveillance. Ces principes de base comprennent notamment le principe de qualité des données (article 5 de la Convention 108) tout comme l'article relatif aux données sensibles (article 6), l'article 7 (sécurité des données) ou bien encore notamment l'article 8 relatif aux garanties dont doivent disposer les personnes concernées. Le T-PD est d'avis qu'il serait nécessaire de prévoir une référence générale à chacun de ces principes de base, ainsi qu'aux conditions strictes dans lesquelles il est possible d'y déroger (article 9).

6. Le projet de déclaration pourrait ainsi comprendre à la suite du paragraphe 5 le texte qui suit :

« Le traitement de données réalisé dans le cadre d'un suivi numérique ou au moyen de technologies de surveillance doit répondre aux impératifs de légitimité du traitement, aux principes de proportionnalité et de finalité, de qualité des données traitées (qui lorsqu'elles sont de nature sensibles, ne peuvent par ailleurs être traitées qu'à la condition que des garanties appropriées soient prévues par la loi). Un niveau élevé de sécurité des données doit être assuré, tenant compte de la technologie de pointe utilisée, de la nature potentiellement sensible de la donnée et des risques potentiels d'atteinte aux droits de l'homme et libertés fondamentales, et plus particulièrement au respect de la vie privée. Enfin, les personnes concernées doivent pouvoir exercer les droits prévus à l'article 8 de la Convention 108. Il ne saurait être dérogé à ces principes de base autrement qu'en vertu des conditions strictes le permettant (article 9 de la Convention 108). »

7. Le T-PD propose que la dernière phrase du paragraphe 5 du projet de Déclaration soit reformulée de la façon suivante : « la conservation des données sensibles sans aucune garantie et sécurité constitue également un problème ». Par ailleurs, le T-PD souhaiterait que soit clarifiée la phrase qui précède cette dernière phrase du paragraphe 5, qui semble être en lien avec le contenu du paragraphe 7 du projet de Déclaration et devrait donc soit être supprimée, soit remaniée.

8. Par ailleurs, le T-PD fait notamment référence au principe de prise en compte de la vie privée au sein même des systèmes, produits et services créés (*Privacy by Design/Privacy by Default*). Le fait de prendre en compte la minimisation des risques et atteintes possibles au respect de la vie privée dès la conception d'un traitement est donc également à souligner.

9. Quant au développement des technologies basées sur la communication de machine à machine et l'identification par fréquence radio (RFID) mentionnés au paragraphe 8 du Projet de déclaration, le T-PD a envisagé d'aborder ces aspects dans le cadre de son Programme de travail 2012-2013, soulignant l'impact potentiel de telles technologies sur le droit au respect de la vie privée et à la protection des données personnelles.

10. Le T-PD souhaite en outre revenir sur la terminologie utilisée dans la version française au paragraphe 10 du Projet de déclaration d'une part (« destruction de la vie privée ») et au paragraphe 13 alinéa a (« mécanismes de redressement ») d'autre part. Il pourrait être opportun de viser une « détérioration » ou un « effondrement » (du droit au respect de) la vie privée d'une part et des « voies de recours » d'autre part.

11. S'agissant des recommandations formulées par le CDMSI, le T-PD souscrit pleinement à l'approche proposée par le Comité visant à alerter les États membres sur les risques que présentent le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux et à soutenir pleinement les efforts réalisés par ces mêmes États pour examiner ces questions. Néanmoins, sur ce dernier point, le T-PD estime que la référence faite à l'alinéa b du paragraphe 13 du projet de déclaration aux bénéfices de l'usage de telles technologies devrait faire l'objet d'un développement antérieur dans la première partie du texte de ce même projet. A cet égard, le T-PD propose d'y introduire le développement suivant, après le paragraphe 9 du texte du Projet de déclaration : « Les risques potentiels sur les droits fondamentaux des technologies de suivi et de surveillance doivent toujours être examinés lors de l'utilisation de ces technologies, afin de garantir que cet usage bénéficie aux individus, à l'économie et à la société dans son ensemble, sans imposer de restrictions injustifiées aux droits concernés. »

12. Pour ce qui a trait à la prise de conscience des acteurs de l'industrie et des créateurs de technologie, mais aussi des utilisateurs, le T-PD, s'il souscrit également à la position reflétée dans le projet de déclaration, souhaite rappeler par ailleurs le rôle très important joué par les autorités de contrôle nationales chargées de veiller au respect de la protection des données (ci-après les autorités de contrôle) en matière de sensibilisation du public face aux implications de ces développements sur la protection de la vie privée et des données à caractère personnel. Le T-PD considère à cet égard qu'il est important pour ces autorités, dont l'objectif est de comprendre et d'anticiper les développements technologiques dans toutes leurs dimensions, d'être également investies, outre les actions de formation et de sensibilisation qu'elles peuvent conduire, d'une mission générale d'information des personnes de leurs droits et obligations au terme des lois nationales applicables en la matière. Le T-PD, qui travaille actuellement à la modernisation de la Convention 108, souligne également le rôle éducatif de ces mêmes autorités.

13. Par conséquent, le T-PD est d'avis que les autorités de contrôle concernées devraient également être associées aux travaux mentionnés à l'alinéa d du paragraphe 13 du Projet de déclaration et ce, afin notamment de contribuer à la sensibilisation du public face aux implications des développements technologiques et à la nécessité d'adopter une approche vigilante face à ceux-ci.

14. Enfin, le T-PD se félicite de la référence faite au paragraphe 7 du projet de Déclaration à la Recommandation (2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, qui est pleinement pertinente et applicable à la matière visée.

ANNEXE I.



**Comité directeur sur les médias et la société de l'information
(CDMSI)**

**CDMSI(2012)002rev3
24/05/2012**

**Projet de déclaration du Comité des Ministres sur les risques du suivi numérique
et des autres technologies de surveillance pour les droits fondamentaux**

1. Les Etats membres du Conseil de l'Europe reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (STE n° 5, ci-après dénommée « la Convention »). Au vu de la jurisprudence de la Cour européenne des droits de l'homme, les obligations qui leur incombent peuvent être négatives, c'est-à-dire s'abstenir de toute ingérence, ou positives, impliquant, entre autres, de protéger les individus contre les actes de personnes privées qui pourraient porter atteinte à leur jouissance de ces droits¹.

2. Le droit au respect de la vie privée énoncé à l'article 8 de la Convention est crucial pour protéger les personnes contre les abus de pouvoir ou d'autorité et leur permettre de participer aux processus de gouvernance. Les restrictions de ce droit ne peuvent se justifier que si elles sont nécessaires dans une société démocratique, conformes à la loi et si elles poursuivent l'un des objectifs précis indiqués à l'article 8, paragraphe 2. Dans certains cas, la Cour européenne des droits de l'homme a jugé que la simple existence d'une loi autorisant la surveillance de citoyens pouvait affecter leur droit fondamental au respect de la vie privée².

3. Le défaut de protection de la vie privée, et par conséquent des données à caractère personnel, peut avoir des répercussions néfastes sur l'exercice d'autres droits fondamentaux. Cela est particulièrement vrai pour les libertés d'expression, de réunion et d'association et, par conséquent, pour le droit de participer aux processus et aux débats concernant la gouvernance démocratique. A cet égard, afin de pouvoir prendre des décisions vraiment en toute liberté, les personnes doivent se sentir à l'abri de toute intrusion, surveillance ou autre forme d'ingérence dans leur vie privée.

¹ X et Y c. Pays-Bas ; Young, James et Webster c. Royaume-Uni ; Plattform Ärzte für das Leben c. Autriche ; Powell et Rayner c. Royaume-Uni ; Costello-Roberts c. Royaume-Uni ; Lopez Ostra c. Espagne ; August c. Royaume-Uni ; A. c. Royaume-Uni ; Z et autres c. Royaume-Uni ; Calvelli et Ciglio c. Italie ; Osman c. Royaume-Uni ; Marcks c. Belgique ; Airey c. Irlande ; Gaskin c. Royaume-Uni ; Gül c. Suisse ; Ahmut c. Pays-Bas ; D. c. Royaume-Uni ; Guerra c. Italie ; Botta c. Italie ; L.C.B c. Royaume-Uni ; Z. et autres c. US; et Marper c. Royaume-Uni. Note de bas de page destinée à informer le CDMSI ; à supprimer après examen et approbation éventuelle.

² Klass et autres c. Allemagne ; Malone c. Royaume-Uni ; Weber et Saravia c. Allemagne ; Halford c. Royaume-Uni ; Association for European Integration and Human Rights et Ekimdzhiev c. Bulgarie, etc. Note de bas de page destinée à informer le CDMSI ; à supprimer après examen et approbation éventuelle.

4. De nos jours, les gens dépendent de l'utilisation d'appareils fixes ou mobiles dont l'offre ne cesse de se développer, améliorant les possibilités de communiquer, d'interagir, de participer à différents types d'activités, notamment celles qui ont trait à des questions d'intérêt général, et de gérer des aspects pratiques de la vie quotidienne.

5. Ces appareils permettent aux fournisseurs de collecter, conserver et traiter de nombreuses données à caractère personnel des utilisateurs, y compris la nature voire le contenu de leurs communications, les informations auxquelles ils ont eu accès ou les sites internet qu'ils ont consultés et, dans le cas des appareils mobiles, leur localisation et leurs déplacements. La collecte et le traitement de telles données peuvent révéler des informations délicates (comme des données financières) ou sensibles (concernant par exemple la santé, les convictions politiques ou religieuses, les pratiques sexuelles) sur les personnes concernées. Ces appareils peuvent ainsi fournir des profils détaillés et intimes de leurs utilisateurs. La conservation des données sensibles dans de mauvaises conditions constitue également un problème.

6. Certains logiciels installés sur les appareils mobiles seraient conçus ou programmés pour collecter toute une série de données à caractère personnel – y compris des données sensibles – liées à l'utilisation de ces appareils. Ces informations seraient accessibles ou transmissibles à des tiers à l'insu des intéressés et ne leur permettraient pas de changer ou d'ajuster l'application de ce logiciel dans leurs appareils mobiles. Conscientes des implications sur le droit des utilisateurs au respect de la vie privée et à la protection des données à caractère personnel, les autorités d'un certain nombre d'Etats membres chargées de la protection des données ont décidé d'enquêter sur ces cas.

7. Des profils basés sur la manière dont les personnes utilisent les nouvelles technologies peuvent être créés et utilisés à différentes fins qui peuvent conduire à des décisions ayant un impact significatif sur les personnes concernées, même à leur insu, comme le souligne 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 ; cela a des répercussions évidentes sur l'autonomie des individus et la société tout entière.

8. Le développement des technologies basées sur la communication de machine à machine ainsi que l'identification par fréquence radio (RFID) soulèvent des préoccupations supplémentaires concernant leur impact sur les droits et les libertés fondamentaux.

9. Les questions liées à l'utilisation des technologies de suivi numérique constituent des enjeux importants pour l'Etat de droit, qui nécessitent de défendre efficacement les droits et libertés individuels contre les ingérences arbitraires. De même, le suivi et la géolocalisation peuvent avoir de graves conséquences sur le droit des personnes à la libre circulation. Les activités de surveillance illégale dans le cyberspace, qu'elles concernent un accès illégal, une interception de données ou une ingérence, la surveillance d'un système ou l'utilisation abusive d'appareils, peuvent avoir des implications pénales ; à cet égard, la Convention sur la cybercriminalité (STCE n° 185) est extrêmement pertinente.

11. Les pratiques décrites ci-dessus ont de lourdes conséquences sur la protection des données à caractère personnel et portent atteinte à la vie privée, garantie essentielle de la liberté et de la démocratie. La destruction de la vie privée aurait des conséquences redoutables sur la démocratie et, au final, sur la société tout entière. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108) est pleinement applicable aux problèmes décrits plus haut.

12. Ces pratiques peuvent aussi créer des menaces très spécifiques pour des droits propres à des professions particulières telles que les journalistes ainsi que pour les droits des autres participants dans les nouveaux environnements de communication telles que les blogueurs et les usagers

comme créateurs de contenus. L'utilisation par des journalistes de certains appareils et de certaines technologies et la surveillance et la géolocalisation qui vont avec pourraient, par exemple, sérieusement mettre en cause leur droit à la protection des sources d'information lequel, comme le souligne la recommandation CM R(2007) sur le droit des journalistes de ne pas révéler leurs sources d'information, est une condition de base du travail de journalisme d'investigation et de la liberté des médias. De plus, les technologies de surveillance et de géolocalisation pourraient attirer de nouvelles menaces sur la sécurité personnelle des journalistes.

13. Comme le souligne la Stratégie du Conseil de l'Europe sur la gouvernance de l'internet pour 2012-2015, les acteurs du secteur privé devraient être encouragés à veiller à ce que leurs politiques et leurs pratiques d'entreprises respectent les droits de l'homme et les libertés fondamentales dans tous les pays où ils sont actifs. Des craintes à cet égard pourraient conduire à l'introduction de mesures de contrôle à l'exportation afin de prévenir tout mauvais usage dans un pays tiers d'une technologie qui nuirait à la liberté, la dignité et la vie privée des utilisateurs d'internet.

14. Dans ce contexte, le Comité des Ministres :

- attire l'attention des Etats membres sur les risques que présente la surveillance secrète par le biais d'outils de suivi des utilisateurs pour le droit au respect de la vie privée, à la fois en tant que droit fondamental et en tant que condition préalable à l'exercice de la citoyenneté démocratique, et souligne que les Etats membres ont la responsabilité de garantir la protection adéquate des citoyens dans ce domaine, notamment en assurant la transparence, en respectant les procédures juridiques et en offrant des mécanismes de redressement en cas de violations des droits ;
- soutient pleinement les efforts réalisés par les Etats membres pour examiner la question des technologies de suivi et de surveillance, leur impact sur l'exercice et la pleine jouissance des droits et libertés fondamentaux individuels ainsi que leur incidence sur la société tout entière telles que le suivi, le profilage ou la géolocalisation peuvent également être utilisées à des fins légitimes qui bénéficient aux utilisateurs, à l'économie et à la société dans son ensemble ;
- se félicite des mesures prises pour permettre la prise de conscience des acteurs de l'industrie et des créateurs de technologies, mais aussi des utilisateurs, de l'impact que peuvent avoir ces technologies sur les droits et les libertés fondamentaux dans une société démocratique, et de ce fait, doit encourager l'application de principes comme le respect de la vie privée dès la conception ;
- estime que le Conseil de l'Europe doit poursuivre ses travaux sur ces questions, en consultation avec les acteurs pertinents de l'industrie et les autres acteurs, notamment sur l'implication de ces technologies sur la gouvernance de l'internet, la société de l'information, la liberté des media et la protection des sources journalistiques et la protection des données.