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

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

CDMSI(2012)002Rev6
30/10/2012

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

1. La propension à interférer avec le droit au respect de la vie privée a considérablement augmenté en raison du développement rapide de la technologie et de la lenteur des cadres juridiques à s'adapter.

2. Le traitement des données effectué dans la société de l'information sans les garanties et la sécurité nécessaires peut soulever de graves problèmes en matière de droits de l'homme. Une législation qui permet de surveiller largement les citoyens peut être jugée contraire au droit au respect de la vie privée. De telles possibilités et pratiques peuvent dissuader les citoyens de participer à la vie sociale, culturelle et politique et à plus long terme, avoir des effets dommageables sur la démocratie. Elles peuvent aussi saper le droit à la confidentialité associé à certaines professions, comme la protection des sources des journalistes, et même menacer la sécurité des personnes concernées. D'une façon plus générale, elles peuvent compromettre l'exercice de la liberté d'expression et le droit de recevoir et de communiquer des informations protégées par l'article 10 de la Convention européenne des droits de l'homme.

3. A cet égard, il est rappelé que, conformément à l'article 8 de la Convention européenne des droits de l'homme, les Etats membres du Conseil de l'Europe se sont engagés à garantir à toute personne relevant de leur juridiction le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Les restrictions de ce droit ne peuvent se justifier que si elles sont nécessaires dans une société démocratique, sont conformes à la loi et visent à l'un des objectifs précis indiqués au paragraphe 2 de l'article 8 de la Convention.

4. Corollaire de la Convention et de la jurisprudence applicable de la Cour européenne des droits de l'homme, les Etats membres ont des obligations négatives, en ce sens qu'ils doivent s'abstenir de toute atteinte aux droits fondamentaux, et des obligations positives, c'est-à-dire qu'ils doivent protéger activement ces droits ; cela comprend la protection des personnes contre les actes d'acteurs non étatiques.

5. On peut aujourd'hui utiliser des appareils fixes ou mobiles - dont l'offre ne cesse de se développer, qui améliorent les possibilités de communiquer, de participer et de gérer les aspects de la vie quotidienne. Or un nombre de plus en plus grand de ces appareils possède des logiciels capables de collecter et de stocker des données, y compris des données à caractère personnel (par exemple, des frappes de touches qui révèlent les mots de passe) et des informations privées comme du contenu produit par les utilisateurs, les sites web visités et des localisations géographiques permettant potentiellement un suivi et une surveillance des individus. Ces données peuvent révéler des informations personnelles délicates ou sensibles (comme des informations financières, sanitaires, politiques, préférences religieuses, habitudes sexuelles) qui peuvent être rassemblées pour établir des profils détaillés et intimes des utilisateurs.

6. Les technologies de suivi et de surveillance peuvent être utilisées dans des buts légitimes, par exemple pour mettre au point de nouveaux services, améliorer l'expérience des utilisateurs ou faciliter la gestion de réseaux ou encore pour assurer le respect de la loi. Mais elles peuvent aussi être utilisées à des fins illicites conduisant à des accès illégaux, à l'interception de données ou à une ingérence, à la surveillance de systèmes et à l'utilisation abusive d'appareils ou à d'autres formes de mauvaises pratiques ; la géolocalisation peut, par exemple, servir à harceler des femmes et à les rendre plus vulnérables aux mauvais traitements et à la violence liés à leur sexe.

7. Dans tous les cas, les modalités de traitement des données à caractère personnel devraient être conformes aux normes applicables du Conseil de l'Europe, ce qui implique de veiller à ce que les mesures de suivi et de surveillance prises dans le cadre d'actions répressives respectent les sauvegardes relatives aux droits de l'homme prévues à l'article 15 de la Convention du Budapest sur la cybercriminalité (STCE n° 185). Il convient aussi de respecter rigoureusement les limites, les exigences et les garanties énoncées dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108) ainsi que dans d'autres instruments comme la Recommandation CM/Rec(2010)13 sur la protection des données à caractère personnel dans le cadre du profilage.

8. Dans ce contexte, le Comité des Ministres :

- attire l'attention des États membres sur les risques que présentent les technologies de suivi numérique et les autres technologies de surveillance pour les droits de l'homme, la démocratie et l'État de droit et rappelle la nécessité de garantir leur utilisation légitime au profit des personnes, de l'économie et de la société dans son ensemble, ainsi que celle de respecter la loi ;
- encourage les États membres à garder à l'esprit ces risques lors des discussions bilatérales avec des pays tiers et, le cas échéant, à envisager la mise en place de contrôles à l'exportation appropriés afin d'éviter que la mauvaise utilisation des technologies n'affaiblissent ces normes ;

- se félicite des mesures prises dans certains États membres par les organes chargés de la protection des données pour sensibiliser aux implications des technologies de suivi et de surveillance et pour enquêter sur ces pratiques afin

de garantir le respect des dispositions de la Convention n°108 et de la législation nationale ;

- attire l'attention sur les implications pénales d'activités de surveillance et de suivi illicites dans le cyberespace et sur l'importance de la Convention de Budapest dans la lutte contre la cybercriminalité ;

- se félicite des mesures prises par les acteurs publics et privés pour sensibiliser les utilisateurs et, a fortiori, le secteur privé et les concepteurs de technologies, aux effets potentiels de l'utilisation de ces technologies sur les droits de l'homme et aux mesures qui peuvent être prises au moment de la conception pour réduire au minimum les risques d'atteintes à ces droits et libertés (par exemple la « prise en compte du respect de la vie privée dès la conception » et la « prise en compte du respect de la vie privée par défaut ») ;

- rappelle la Stratégie du Conseil de l'Europe sur la gouvernance de l'internet 2012-2015 qui comprend un certain nombre de lignes d'action pertinentes en regard des problèmes relevés dans cette Déclaration et attend avec intérêt les résultats concrets des travaux des organes compétents du Conseil de l'Europe.