www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 2 juillet 2012 T-CY (2012) 16 F

Comité de la Convention Cybercriminalité (T-CY)

Avis du T-CY

sur

Projet de déclaration du Comité des Ministres sur les risques du suivi numérique et des autres technologies de surveillance pour les droits fondamentaux
[Version CDMSI(2012)002Rev3 (24/05/2012)]

Opinion of the T-CY

on

Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies

[Version CDMSI(2012)002Rev3 (24/05/2012)]

1. The T-CY welcomes the opportunity to express its opinion on the Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies [Version CDMSI(2012)002Rev3 (24/05/2012)] prepared by the Steering Committee on Media and Information Society (CDMSI).

2. The T-CY notes the importance of protecting people and their rights, including their privacy rights.

3. The T-CY underlines that a clear distinction is to be made between intrusion, surveillance and other forms of interference by private sector entities, criminals, and public authorities.

4. The T-CY is of the opinion that the three types of situations must not be confused. Each situation would require different recommendations.

5. In order to clarify the scope of the Declaration, the T-CY, therefore, suggests two options:

a. The declaration could be limited to "the risks to fundamental rights stemming from the private use of digital tracking and other surveillance technologies", and to omit discussion of use by governments and criminals of such methods. The title and the text would then need to be adjusted accordingly (for example, paragraphs 2 and 9 to be deleted, paragraph 13 to specify that the declaration is related to risks of the private use of tracking and surveillance technologies). This option would add clarity and specificity to the Declaration and would support the Declarations of paragraph 13.

b. Alternatively, situations of surveillance and other interference by (i) private sector entities, (ii) criminals and (iii) public authorities (with a further distinction between legitimate use and risks of misuse of powers) should be clearly distinguished, for example, in paragraphs 2 and 9. In paragraph 13, recommendations would then need to be made addressing each specific situation. These could include that all Council of Europe member states, but also other states, fully implement the Budapest Convention on Cybercrime, including Article 15 on conditions and safeguards as well as law enforcement powers permitting the lawful interception of data (Article 21). If this option is followed, the concept of "surveillance" would need to be defined more clearly in order to avoid misunderstandings.

Annexe

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

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

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 droits[1].

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 privée[2].

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.

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

---

[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.

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 cyberespace, 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 blogeurs 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 :

a. 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 ;

b. 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 ;

c. 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 ;

d. 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.