COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 12 September 2012 T-PD (2012)01_Rev_en

CONSULTATIVE COMMITTE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

Compilation of opinions

DG I – Human Rights and Rule of Law

INDEX

I. Opinion of the T-PD on Recommendation (1984)2011 of the Coucil of Europe's Parliamentary Assembly on « the protection of privacy and personal data on the internet and online media » *(doc. T-PD(2011)9)*

1. The T-PD welcomes the adoption by the Parliamentary Assembly (7 October 2011) of Recommendation (1984)2011 on "the protection of privacy and personal data on the Internet and online media" which contributes to raising awareness of Parliamentarians on the question of privacy and personal data protection on the internet and in the new media environment.

2. The T-PD firstly wishes to acknowledge the open and inclusive approach taken by the Rapporteur (Ms Rihter) when preparing her report. A T-PD representative participated in hearings organised by the competent Committee of the Parliamentary Assembly (the Committee on Culture, Science and Education) during the Internet Governance Forum (IGF) in Vilnius (September 2010) and again in March 2011 in order to present the work of the T-PD and modernisation of the Convention for the protection of individuals with regard to the automatic processing of personal data (hereafter Convention 108). In April 2011, the Secretariat was heard during a meeting of the Subcommittee on the Media.

3. Concerning the Parliamentary Assembly's recommendation, the T-PD fully subscribes to the call (paragraphs 2.1 and 2.2 of the Recommendation) for further states to become Parties to Convention 108, which is addressed to both Council of Europe member states (as four of the 47 member states remain to become parties to the Convention) and, in particular, to countries worldwide. In July 2011, Uruguay has become the first country outside Europe to be invited to accede to Convention 108. The accession by non-member states will strengthen the universal recognition of fundamental data protection principles called for since 2005 by the 27th International Conference of Data Protection and Privacy Commissioners (Montreux, 14-16 September 2005) and repeated in the Resolution adopted by the 32nd Edition (Jerusalem, 26-29 October 2010).

4. The T-PD furthermore considers as an absolute necessity that the call (paragraph 2.3. of the Recommendation) to provide adequate budgetary resources be followed of effects. Indeed, the constantly evolving normative work, the promotion of Convention 108 outside Europe (with the related capacity building activities) and the effective implementation of the Convention require adequate means. Data protection and privacy should continue to be priority areas for the Council of Europe.

5. As regards the European Union, the T-PD appreciates its support for the promotion of Convention 108, notably through the organisation of a series of conferences in 2011 organised by the Hungarian and Polish authorities. Data protection is a good example for complementarity between the activities of the Council of Europe and the European Union and it will be essential to ensure consistency also in the future. In line with the EU's Stockholm Programme, Convention 108 should be included in EÚ co-operation programmes and activities worldwide.

6. Concerning the modernisation work, the T-PD is grateful for the substantial input and interesting proposals made by the Parliamentary Assembly. It agrees with the Assembly that existing standards must not be lowered and that the Convention's follow-up mechanism needs to be strengthened notably to keep pace with the rapid development of ICT. The T-PD invites the Assembly to continue participating actively in the modernisation process, including by appointing a delegate to its meetings (in accordance with article 3 (4) of the T-PD's rules of procedure).

7. Finally, the T-PD notes the invitation made to the Secretary General to ensure the protection of personal data processed by the Organisation, and to reinforce the position of the Council of Europe's Commissioner for Data Protection. It recalls that at its 26th Plenary meeting (1-4 June 2010), the T-PD adopted proposals for a revised draft Regulation outlining a data protection system for personal data files in the Council of Europe, which should cover personal data processed by all bodies and institutions of the Organisation.

8. Further to the elections carried out during the 27th Plenary meeting (29 November – 2 December 2011), the T-PD is pleased to inform the Assembly of the nomination of Ms Eva Souhrada-Kirchmayer as the new Data Protection Commissioner of the Council of Europe and trust that this nomination will contribute to the strengthening of the protection of personal data within the Council of Europe.

II. Opinion by the T-PD on the draft declaration by the Committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies (doc CDMSI(2012)002rev3)

1. The T-PD received a request for an opinion from the Bureau of the Steering Committee on Media and Information Society (CDMSI) following the latter's first meeting, held on 29 and 30 May 2012. The request concerns a draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies.

2. The T-PD first wishes to welcome the fact that the CDMSI has taken the initiative of dealing with this matter that is nowadays of vital importance and can raise serious issues of respect for privacy and of protection of personal data.

3. The T-PD considers that the scope of the draft Declaration (as well as its title) should be clarified. Indeed, if the Declaration is meant to address the private use of such technologies (as can be understood from Article 13), references to misuse of power notably should be reviewed.

4. The T-PD would firstly point out that there is a difference in the numbering of the paragraphs between the French and English versions of the draft Committee of Ministers declaration. The comments below are based on the numbers used in the English version of the draft document.

5. The T-PD notes that paragraph 5 of the draft declaration makes mention of the storage of sensitive data (the English version should use the term "storage" rather than "storing" in this context). At a more general level, the T-PD would underline that the fundamental principles of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") are fully applicable to the processing of personal data using digital tracking and other surveillance technologies. These fundamental principles include the principle on the quality of data (Article 5 of Convention 108), the article relating to sensitive data (Article 6), Article 7 (data security) and, in particular, Article 8 on the safeguards to be afforded to data subjects. The T-PD considers that the document should include a general reference to each of these basic principles and to the strict conditions for departing from them (Article 9).

6. The following text could therefore be inserted in the draft declaration after paragraph 5:

"Data processing carried out in connection with digital tracking or by means of surveillance technologies must satisfy the requirements of legitimacy of the processing, the principles of proportionality and finality, of quality of the data processed (which, if sensitive, can be processed only where appropriate safeguards are provided for by law). A high level of data security must be guaranteed, having regard to the state-of-the-art technology utilised, the potentially sensitive nature of the data and the potential risks of infringement of human rights and fundamental freedoms, such as the respect for private life. Lastly, data subjects must be able to exercise the rights laid down in Article 8 of Convention 108. Departures from these fundamental principles shall be possible solely under the strict conditions that so allow (Article 9 of Convention 108)."

7. The T-PD proposes that the last sentence of paragraph 5 of the draft Declaration be reformulated as follows: “Also, data storage without the necessary safeguards and security constitutes a problem”. Furthermore the T-PD would welcome a clarification of the penultimate sentence of paragraph 5 which seems to duplicate paragraph 7 of the draft declaration and should thus either be deleted or rephrased.

8. The T-PD also refers to the need to take into account privacy requirements within the systems, products and services created (Privacy by Design/Privacy by Default). The minimisation of the possible risks and infringements to the right to privacy from the conception of the processing is then also to be underlined.

9. Concerning the development of technologies based on machine-to-machine communication and radio-frequency identification (RFID), mentioned in paragraph 8 of the draft declaration, the T-PD plans to address these issues under its work programme for 2012-2013, focusing on such technologies' potential impact on the right to respect for privacy and protection of personal data.

10. The T-PD also wishes to comment on the terminology used in the French version in paragraph 10 of the draft declaration ("collapse of privacy") on one hand and paragraph 13, sub-paragraph a, ("mechanisms for redress") of the draft declaration on the other hand. It might be appropriate to refer to the "collapse" of (the right to respect for) privacy in the first case and to "legal remedies" in the second.

11. As regards the recommendations made by the CDMSI, the T-PD fully concurs with the committee's proposed approach aimed at alerting member states to the risks that digital tracking and other surveillance technologies entail for fundamental rights and fully supporting member states' efforts to address these questions. Nonetheless, in the latter case, the T-PD considers that the reference in sub-paragraph b of paragraph 13 of the draft declaration to the benefits deriving from the use of such technologies should be preceded by considerations appearing in the first part of the draft declaration. In this connection, the T-PD proposes that the following commentary be inserted after paragraph 9 of the draft declaration: "The potential risks that tracking and surveillance technologies entail for fundamental rights must always be addressed when using these technologies so as to guarantee that the use made thereof benefits individuals, the economy and society at large, without imposing unjustified restrictions on the rights concerned."

12. Concerning awareness-raising among industry actors and technical developers, and also among users, while the T-PD likewise concurs with the position reflected in the draft declaration, it would also point out the very important role played by the national supervisory authorities responsible for enforcing data protection (hereafter the supervisory authorities) when it comes to raising public awareness of these developments' implications in terms of protection of privacy and of personal data. In this respect, the T-PD deems it important that, apart from possibly carrying on training and awareness-raising activities, these supervisory authorities, whose objective is to understand and anticipate all the dimensions of technological developments, should also be given the general task of informing individuals of their rights and obligations under the national legislation applicable in these matters. The T-PD, which is currently working on the modernisation of Convention 108, also draws attention to these authorities' educational role.

13. The T-PD accordingly considers that the supervisory authorities concerned should also be involved in the work mentioned in sub-paragraph d of paragraph 13 of the draft declaration, in particular so as to help raise public awareness of the implications of the technological developments and the need for vigilance with regard to them.

14. Lastly, the T-PD welcomes the fact that paragraph 7 of the draft declaration makes reference to Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, which is entirely relevant and applicable to the question under consideration.

APPENDIX I.

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Steering Committee on Media and Information Society (CDMSI)

CDMSI(2012)002Rev3
24/05/2012

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

1. Council of Europe member states have undertaken to secure to everyone within their jurisdiction the rights and freedoms defined in the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 5, hereinafter referred to as the Convention). Having regard to the case law of the European Court of Human Rights, the resulting obligations for member states can be negative, that is to refrain from interference, or positive, involving, inter alia, the protection of individuals from action by private parties which could jeopardize their enjoyment of those rights[1].

2. The right to private life, as provided for in Article 8 of the Convention, is essential for protecting people against misuse of power or authority and for enabling their participation in democratic governance processes. Restrictions of this right can only be justified when it is necessary in a democratic society, in accordance with the law and for one of the limited purposes set out in Article 8, paragraph 2. In some cases, the European Court of Human Rights has ruled that the mere existence of legislation allowing the surveillance of citizens may impinge on their fundamental right to private life[2].

3. A deficit in the protection of private life, and its corollary personal data, can have adverse effects on the enjoyment of other fundamental rights. This is particularly the case as regards freedom of expression, freedom of assembly and association and, in consequence, people's right to participation and deliberation in governance processes. In this latter respect, for people to be able

[1] X and Y v. the Netherlands; Young, James and Webster v. the UK; Plattform Ärste für das Leben v. Austria; Powell and Rayner v.the UK; Costello –Roberts v. the UK; Lopez Ostra v. Spain; August v. the UK; A. v. the UK; Z and Others v. the UK; Calvelli and Ciglio v. Italy; Osman v. the UK; Marcks v. Belgium; Airey v. Ireland; Gaskin v. the UK; Gül v. Switzerland; Ahmut v. the Netherlands; D. v. the UK; Guerra v. Italy; Botta v. Italy; L.C.B v. the UK; Z and others v. the U; S. and Marper v. the UK. Footnote for CDMSI information, to be deleted after consideration and possible approval.

[2] Klass and Others v. Germany; Malone v. the UK; Weber and Saravia v. Germany; Halford v. the UK; the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, etc. Footnote for CDMSI information, to be deleted after consideration and possible approval.

to make genuinely free decisions, they need to feel free from intrusion, surveillance and other forms of interference with their privacy.

4. People nowadays rely on a constantly growing range of both fixed-location and mobile devices which enhance their possibilities to communicate, interact, participate in different kinds of activities, including those which involve matters of public interest, and manage practical aspects of their everyday life.

5. The use of these devices enables providers to collect, store and process vast amount of users' personal data, including the nature and, in some cases, the content of their communications, the information they accessed or the websites they visited and, in case of mobile devices, their whereabouts and movements. Such data gathering and processing can reveal delicate (e.g. financial data) or sensitive information (e.g. as regards health, political, religious preferences, sexual habits) on the persons concerned. Those devices can therefore provide detailed and intimate portrayals of the individuals using them. Also, data storing in inappropriate conditions constitutes a problem.

6. Reportedly, certain software installed on mobile devices is designed or programmed to collect a wide range of personal data – including sensitive data – related to the use of those devices. Such information can apparently be accessed by or transmitted to third parties without the knowledge of the users and without permitting them to change or adjust the application of the software in their mobile devices. Conscious of the implications for users' right to privacy and protection of personal data, a number of member states' data protection authorities have decided to investigate these cases.

7. Profiles based on the use of new technologies by individuals can be created and used for different purposes, potentially leading to decisions significantly affecting the people concerned even without their knowledge, as highlighted in Recommendation CM/Rec(2010)13 on the protection of personal data in the context of profiling, with clear repercussions on individuals' autonomy and on society as a whole.

8. The development of technologies based on machine-to-machine communication and radio-frequency identification (RFID) raise additional concerns about their impact on fundamental rights and freedoms.

9. The questions stemming from the use of digital tracking technologies can have significant rule of law implications, which require effective safeguards for individuals' rights and freedoms against arbitrary interferences. Similarly, tracking and geolocation can have serious consequences on peoples' right to free movement. Unlawful surveillance activities in cyberspace, whether they concern illegal access, data interception or interference, system surveillance, misuse of devices may have criminal law implications; the Convention on Cybercrime (ECTS 185) is highly relevant in this respect.

10. The practices described above have considerable consequences for the protection of personal data and undermine privacy, which is an essential guarantee of freedom and democracy. A collapse of privacy will have direct consequences for democracy and, ultimately, for society as a whole. The Convention for the protection of individuals with regard to automatic processing of personal data (CETS no 108) is fully applicable in respect of the issues described above.

11. In addition, such practices may pose very specific threats to the rights associated to specific professions, such as journalists as well as other participants in the new communications environment such as bloggers and users as creators of content. The use of certain devices and technologies by journalists and the associated surveillance and tracking could, for example, seriously undermine their right to protection of sources of information which, as highlighted by

Recommendation CM R(2000)7 on the right of journalists not to disclose their sources of information, is a basic condition for journalistic investigative work and for the freedom of the media. Moreover, surveillance and tracking technologies could attract additional threats against the personal safety of journalists.

12. As underlined in the Council of Europe Strategy on Internet Governance for 2012-2015, private sector actors should be encouraged to ensure that their corporate policies and practices respect human rights and fundamental freedoms in all of the countries in which they operate. Concerns in this respect may lead to the introduction of suitable export controls to prevent the misuse of technology in third countries to undermine the freedom, dignity and privacy of Internet users

13. Against this background, the Committee of Ministers:

a. alerts member states to the risks that covert surveillance through the use of user tracking devices entails for the right to private life as a fundamental right and as a pre-condition for the exercise of democratic citizenship and underlines member states' responsibility to ensure that citizens are adequately protected in this context, in particular by ensuring transparency and compliance with legal procedures and providing mechanisms for redress in case of violations of rights;

b. fully supports member states' efforts to address the question of tracking and surveillance technologies and their impact on people's exercise and full enjoyment of fundamental rights and freedoms as well as their impact on society as a whole whilst recognising that digital technologies such as tracking, profiling or geolocation can also be used for legitimate interests for the benefit of users, the economy and society at large;

c. welcomes measures being taken to raise awareness among industry actors and technology developers, and also among users, about the possible impact of these technologies on fundamental rights and freedoms in a democratic society and in this regard encourages the application of principles such as privacy by design;

d. considers that further Council of Europe work on these issues is necessary, in consultation with relevant industry and other actors, including as regards the implications of these technologies for Internet governance, information society media freedom and the protection of journalistic sources, and data protection.