Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Resolution 1843 (2011)[1]

The protection of privacy and personal data on the Internet and online media

Parliamentary Assembly

1. While welcoming the epochal progress in information and communication technologies (hereafter "ICTs") and the resulting positive effects on individuals, societies and human civilisation as a whole, the Parliamentary Assembly notes with concern that the digitalisation of information has caused unprecedented possibilities for the identification of individuals through their data. Personal data are processed by an ever-growing number of private bodies and public authorities throughout the world. Personal information is put into cyberspace by users themselves as well as by third parties. Individuals leave identity traces through their use of ICTs. Profiling of Internet users has become a widespread phenomenon. Companies sometimes monitor employees and business contacts by means of ICTs.

2. In addition, ICT systems are often hacked into in order to obtain data from legal entities, in particular commercial companies, financial institutions, research institutes and public authorities. Such access may cause economic losses to the private sector and may negatively impact the economic well-being of states, public safety or national security.

3. The Assembly is alarmed by these developments which challenge the right to privacy and data protection. In a democratic state governed by the rule of law, cyberspace must not be regarded as a space where the law, in particular that concerning human rights, does not apply.

4. The Assembly recalls the fundamental human right to respect for private and family life, home and correspondence as guaranteed by Article 8 of the European Convention on Human Rights (ETS No. 5). This right includes the right to the protection of personal data as well as the obligation of states to establish appropriate safeguards under domestic law in this regard.

5. The Assembly underlines the need to effectively combat the collection, distribution and consultation of child pornography which are carried out through information and communication technologies, notably through the Internet, as regulated by the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

6. Recalling its long-standing support of the right to protection of privacy, since its Recommendation 509 (1968) on human rights and modern scientific and technological developments, the Assembly welcomes and supports Resolution No. 3 on data protection and privacy in the 3rd millennium, which was adopted by the 30th Council of Europe Conference of Ministers of Justice (Istanbul, 24-26 November 2010).

7. As the Assembly stated in its Resolution 428 (1970) on the declaration on mass communication media and human rights, "where regional, national or international computer databanks are instituted, the individual must not become completely exposed and transparent by the accumulation of information referring to his private life. Data banks should be restricted to the necessary minimum of information required".

---

1. Assembly debate on 7 October 2011 (36th Sitting) (see Doc. 12695, report of the Committee on Culture, Science and Education, rapporteur: Ms Rihter; and Doc. 12726, opinion of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Salles). Text adopted by the Assembly on 7 October 2011 (36th Sitting). See also Recommendation 1984 (2011).

8. Referring to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, hereafter "Convention No. 108"), the Assembly emphasises that the right to the protection of personal data includes, in particular, the right to have such data processed fairly and securely, for specified purposes on a legitimate basis only, and that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data which have been processed without the right to do so. Compliance with these obligations must be supervised by an independent authority in accordance with the Additional Protocol to Convention No. 108, regarding supervisory authorities and transborder data flows (ETS No. 181).

9. The Assembly reaffirms that member states should only agree to transfer personal data to another state or organisation where such state or organisation is a Party to Convention No. 108 and its Additional Protocol or otherwise ensures an equally adequate level of protection for the intended data transfer. Transfers of personal data which violate the right to protection of private life under Article 8 of the European Convention on Human Rights may be the subject of proceedings before the national courts and, as a last resort, before the European Court of Human Rights.

10. The Assembly welcomes the fact that Convention No. 108 has been signed and ratified by nearly all Council of Europe member states – with the regrettable exceptions of Armenia, the Russian Federation, San Marino and Turkey – and notes that Articles 7 and 8 of the Charter of Fundamental Rights of the European Union contain largely the same principles. With the growing globalisation of ICT-based services, it is of utmost urgency for Europe as a whole to adhere to the same standards and seek to involve other countries around the world.

11. While Article 17 of the International Covenant on Civil and Political Rights (hereafter "ICCPR") recognises the right to privacy, the legal interpretation and practical implementation of this article falls significantly short of European standards. The Assembly therefore believes that any global initiative should be based on Convention No. 108 and its additional protocol, both of which are in principle open for signature by non-member states of the Council of Europe.

12. Although precautionary technologies and software, voluntary self-regulation by ICT companies and private users, as well as improved user awareness, may reduce the risk of interference with privacy and the harmful processing of personal data through ICTs, the Assembly believes that only specific legislation and effective enforcement can sufficiently protect the right to protection of privacy and personal data as required by Article 17 of the ICCPR and Article 8 of the European Convention on Human Rights.

13. The Assembly deplores that the absence of globally accepted international legal standards on data protection regarding ICT-based networks and services leads to legal insecurity and to the need for national courts to fill this void through the interpretation of domestic laws on a case-by-case basis, in the light of Article 17 of the ICCPR and Article 8 of the European Convention on Human Rights. This not only exposes individuals to an unequal protection of their rights, but also entails different and changing requirements for ICT companies and users globally, causing virtually unpredictable liabilities.

14. The Assembly welcomes the international co-operation established among independent data protection authorities and supports their efforts to ensure the common international protection of privacy and personal data in the wake of technological progress, as expressed in their resolutions adopted in Madrid in 2009 and Jerusalem in 2010. The Assembly shares their view that Convention No. 108 should be promoted globally, as it is the most advanced set of standards in this sector under public international law.

15. Recalling the Convention on Cybercrime (ETS No. 185), the Assembly welcomes the fact that more than 100 states have passed legislation which complies with the spirit of this convention. Under Articles 2, 3 and 4 of this convention, its parties are obliged to consider as an offence punishable under domestic criminal law any intentional access to, interception of and interference with computer data without the right to do so. Such computer data may include personal data of natural persons or secret data of legal persons on computer networks.

16. Recalling Article 10 of the Convention on Human Rights and Biomedicine (ETS No. 164) and Article 16 of its Additional Protocol concerning Genetic Testing for Health Purposes (CETS No. 203), the Assembly emphasises the right of everyone to the protection of personal health data, including the right to be informed of, and consent to or refuse, any collection and processing of such data through ICTs. Medical and health data of persons require the highest level of data protection, as they constitute one of the core elements of a person's private life and human dignity.

17. The Assembly also recalls the obligation to respect the right to privacy and data protection under the Council of Europe Convention on Access to Official Documents (CETS No. 205), as well as the limits to the protection of personal data under the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198), and the Convention on Mutual Administrative Assistance in Tax Matters (ETS No. 127) and its amending protocol (CETS No. 208).

18. The Assembly endorses the following general principles concerning the protection of privacy and personal data in an ICT environment:

18.1. the protection of private life is a necessary element of human life and the humane functioning of a democratic society; where the privacy of a person is violated, his or her dignity, liberty and security are at stake;

18.2. the right to protection of privacy and personal data is a fundamental human right, which imposes on states the obligation to provide an adequate legal framework for such protection against interference by public authorities as well as by private individuals and entities;

18.3. everyone must be able to control the use of their personal data by others, including any accessing, collection, storage, disclosure, manipulation, exploitation or other processing of personal data, with the exception of the technically necessary or lawful retention of ICT traffic data and localisation data; the control of the use of personal data shall include the right to know and rectify one's personal data and to have erased from ICT systems and networks all data which were provided without legal obligation;

18.4. personal data may not be used by others, unless the person concerned has given his or her prior consent, which requires an expression of consent in full knowledge of such use, namely the manifestation of a free, specific and informed will, and excludes any automatic or tacit usage; consent can be subsequently withdrawn at any time; where consent has been withdrawn, personal data may not be used further;

18.5. where personal data are to be used with the intention to exploit such data commercially, the person concerned shall also be informed of this commercial use in advance; where personal data may be used by others, because of individual consent or the public availability of otherwise anonymous data, the intentional accumulation, interconnection, personalisation and use of such accumulated data shall nevertheless require the consent of the person concerned;

18.6. personal ICT systems as well as ICT-based communications may not be accessed or manipulated if such action violates privacy or the secrecy of correspondence; access or manipulation through "cookies" or other unauthorised automated devices violate privacy, in particular where such automated access or manipulation serves other interests, especially of a commercial nature;

18.7. higher protection should be afforded to private images, personal data of minors or persons with mental or psychological disabilities, personal ethnic data, personal medical, health or sexual data, personal biometric and genetic data, personal political, philosophical or religious data, personal financial data and other information forming part of the core area of private life; higher protection should also be afforded to personal data related to court proceedings or the professional secrecy of lawyers, medical professionals and journalists; such higher protection may be achieved through self-regulatory, technical or legal means ensuring due accountability in case of infringements of data protection or privacy; periods should be specified beyond which such data shall no longer be kept or used;

18.8. public and private entities which collect, store, process or otherwise use personal data should be obliged to reduce the amount of such data to the absolute minimum; personal data should be deleted when they are outdated or unused or where the purpose for their collection has been met or no longer exists; the random collection and storage of personal data should be avoided;

18.9. everyone should have an effective remedy against any unlawful interference with his or her right to protection of privacy and personal data before domestic courts; voluntary arbitration and self-regulatory bodies as well as independent data protection authorities should complement the judicial system in ensuring the effective protection of this right; public authorities and commercial companies should be encouraged to establish mechanisms for receiving and processing complaints against them by individuals alleging infringements of their right to data protection or privacy, as well as mechanisms for ensuring internal compliance with the right to the protection of privacy and personal data; unlawful infringements of privacy and data protection should be punishable by law.

19. The Assembly welcomes the fact that the Parties to Convention No. 108 have started to prepare a possible revision of this convention in the wake of technological progress and increasingly fierce commercial competition in ICT-based services.

20. The Assembly therefore calls on:

20.1. the Parliaments of Armenia, the Russian Federation, San Marino and Turkey to initiate their ratification of Convention No. 108 without delay, thus enabling their countries to play an active role in the further development of this convention;

20.2. its observer delegations from Canada, Israel and Mexico to initiate debate in their respective parliaments about signing and ratifying Convention No. 108 and participating in its further development. The observer delegations are invited to report on progress in this regard to the Assembly in due course;

20.3. the other states co-operating with the Council of Europe, in particular the Council of Europe's other observer states Japan, the United States and the Holy See, to promote their authorities' accession to Convention No. 108;

20.4. the European Commission for Democracy through Law (Venice Commission) to report to the Assembly on the extent to which the domestic legislation of its member and observer states is in accordance with the universal human right to protection of privacy and personal data in the light of Convention No. 108 and its additional protocol, and on whether those states which are not yet parties to this convention would consider signing and ratifying it.

21. The Assembly asks the Secretary General of the Council of Europe to:

21.1. seek high-level support from the United Nations in promoting accession to Convention No. 108 by states worldwide, in particular through the United Nations Internet Governance Forum (IGF), the International Telecommunication Union and the United Nations Educational, Scientific and Cultural Organization (UNESCO);

21.2. make sure that the broad use of ICTs within the Council of Europe and its extraterritorial legal status do not compromise the protection of privacy and personal data. In this context, the position and work of the Council of Europe's Commissioner for Data Protection should be strengthened and the internal regulatory framework revised accordingly.

22. The Assembly calls on the European Union to continue to support broad accession to Convention No. 108 and its Additional Protocol and to become itself a party once the necessary amendments enabling this accession have entered into force.

23. Welcoming international efforts by different stakeholders to ensure the right to protection of personal data in the ICT environment, such as the Madrid 2009 and Jerusalem 2010 resolutions by independent data protection authorities and the various data protection initiatives by the International Chamber of Commerce, the Assembly invites all stakeholders to join forces with the Council of Europe in order to ensure that individual initiatives do not contradict one another or risk being used in order to blur a common approach to the universal right to respect for privacy and the protection of personal data, or to lower existing legal standards.