International Working Group
on Data Protection
in Telecommunications

675.36.9 4 March 2008

Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. "Budapest Convention")

43rd meeting, 3 – 4 March 2008, Rome (Italy)

Whereas the Budapest Convention of 2001 on cybercrime is a major international co-operation tool with a view to harmonizing criminal offences, investigation procedures, and judicial and police assistance;

Considering that several provisions of the Convention and the relevant Protocol as undersigned in 2003 impact directly on the processing of personal data, and that it is important for data protection principles to be taken into consideration in ratifying and implementing those provisions;

Considering that the provisions of the Convention do not apply exclusively to cybercrime, but also to the collection of evidence in electronic format for whatever type of offence, whether committed by means of a computer system or not; considering that certain decisions made at domestic level in ratifying the Convention produce effects on international co-operation as well, especially with regard to mutual assistance procedures;

Considering that some criticalities in this sector have already been pointed out in the preparatory work to the Convention, inter alia by this Working Group[1], and by the Article 29 Working Party (Opinion no. 4/2001 rendered on 22 March 2001);

Considering that several countries have undersigned the Convention, and twenty-two of them have already ratified it;

RECOMMENDS

That special attention be paid to all the implications for the processing of personal data and the safeguards applying to citizens' rights in any instruments ratifying the Convention and the relevant Protocol, or in connection with the concrete implementation thereof by the competent investigational bodies, in particular with a view to the following:

1. ***(Proportionality)*** The principle of proportionality, as set out in several articles of the Convention, should be abided by in all criminal investigation activities performed by the competent law enforcement bodies (e.g. inspections, searches, seizure, custody, urgent inquiries, search for evidence) whenever the evidence is to be gathered on and/or by means of electronic tools;

[1] Cf. "Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe" (Berlin, 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/218/cy_en.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

2. ***(Safeguards for Third Parties' Rights)*** Whenever the said investigations activities are carried out, their impact on the rights vested in third parties that are alien to the facts investigated upon should always be assessed with the utmost care;
3. ***(Corporate Liability for Employees' Criminal Offences)*** As regards implementation of the provisions in the Convention related to corporate liability (article 12), which envisage the liability of legal persons employing individuals that are held liable for the criminal offences established in accordance with the Convention, consideration should be given to applying the respective punishments also if the criminal offences in question are established under domestic legislation on personal data protection;
4. ***("Freezing" of Traffic Data)*** The instruments implementing the provisions set out in the Convention with regard to the expedited preservation of stored computer data and the partial disclosure of traffic data (articles 16 and 17) should be applied on the basis of the careful assessment of purpose limitation and proportionality principles as well as in accordance with a selective approach, by also taking account of the safeguards partially laid down by the countries that envisage traffic data retention for law enforcement purposes;
5. ***(Countries' Jurisdiction in Investigating and Detecting Criminal Offences)*** In order to afford enhanced protection to cybercrime victims, ratification of the Convention and/or any subsequent regulatory amendments, especially at domestic level, should provide an opportunity for updating domestic law, in particular the provisions contained in criminal codes and/or criminal procedure codes, so as to expand the scope of national jurisdiction in prosecuting these offences, which might go unpunished if the conventional standards underlying criminal jurisdiction (type of conduct, facts, etc.) were applied.

The Working Group recognises the special importance of international co-operation in this area and reserves the right to undertake further initiatives in order to foster exchanges of information, monitoring of the appropriate application of the Convention and its Protocol, and the widest possible harmonization of regulatory approaches and implementing practices.