



**5403/01/EN/Final
WP 53**

Opinion 10/2001

on the need for a balanced approach in the fight against terrorism

Adopted on 14 December 2001

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

The European Commission, Internal Market DG, Functioning and impact of the Internal Market. Coordination. Data Protection.

Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C100-6/136

Telephone: direct line (+32-2)299.27.19, switch-board 299.11.11. Fax: 296.80.10

Internet address: <http://europa.eu.int/comm/privacy>

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹

having regard to Articles 29 and 30 paragraphs 1 and 3 of that Directive,
having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof

has adopted the following OPINION:

The tragic terrorist attacks against the United States have highlighted the necessity for democratic societies to engage in a fight against terrorism. This objective is both a necessary and valuable element of democratic societies. In this fight certain conditions have to be respected which also form part of the basis of our democratic societies.

In this particular context different measures are discussed at the moment at EU level² as on the Member State level. Some of them are very innovative, others are not really so, but merely constitute an update of existing projects receiving renewed enthusiasm. In many cases, those measures cover more areas than just the fight against terrorism. One can observe a proliferation of the use of means of identifying, and more generally, gathering data relating to individuals through the use, for instance, of biometrics. Furthermore, one notes an increase of the criminalisation of certain behaviour linked to the Information Society – «cyber-crime » - as an intrusion into information systems, but also the copying of works protected by copyright³. The definitions of these offences are often broad and thus lead to questions on the respect of the fundamental principles of legal security and legality of offences and sanctions⁴. At the same time, the existing procedural measures legitimising the intrusion by public authorities into individuals' privacy are reinforced and new questionable measures are discussed or yet adopted. This concerns not only telephone tapping, but also other measures as the prior and generalised retention of telecommunication data by electronic communications services providers and operators, the adoption of measures enabling « real time » surveillance of citizens, the surrender of the dual criminality principle as a condition for the exchange of certain personal data concerning criminals, the sharing of personal data for different purposes as the fight against crime, immigration and Foreign Counterintelligence and the premature transfer of personal data to third countries. In particular such transfers can be

¹ Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

² See in particular the conclusions of the EU Justice and Home Affairs summit of 20 September 2001, the "roadmap" of the European Union following the attacks in the United States (13880/1) of 15 November 2001.

³ In the United States, the Recording Industry Association of America (RIAA) tried to have an amendment adopted in the discussion around the "Patriot Act". This amendment would have given this sector the legal permission for intrusion into information systems in order to identify persons responsible for copyright infringements.

⁴ See Convention of the Council of Europe on cyber-crime, signed in Budapest on 23 November 2001.

especially dangerous if the recipient States do not offer sufficient data protection safeguards.

All these measures have a direct or indirect impact on the protection of personal data. The Working Party has presented several opinions on related issues⁵ with full knowledge of the serious problem of terrorism, a phenomenon which, unfortunately, has been known for quite some time in Europe.

In this context the Working Party recalls the commitment of our democratic societies to ensure respect for the fundamental rights and freedoms of the individual. The individual's right to protection of personal data forms part of these fundamental rights and freedoms⁶. The Community Directives on the protection of personal data (directives 95/46/EC and 97/66/EC) form part of this commitment⁷. These Directives aim to ensure respect for fundamental rights and freedoms, in particular, the right to privacy with regard to the processing of personal data and to contribute to the respect of the rights protected by the European Convention on Human Rights, in particular article 8 thereof. In all these instruments, exceptions to combat crime are provided for but have to respect specific conditions.

The Working Party underlines, in particular, the necessity to take into account the long term impact of urgent policies rapidly implemented or envisaged at this moment. This long-term reflection is all the more necessary in view of the fact that terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon. The Working Party also underlines the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy as required by Art. 8 of the European Convention on Human Rights and the relevant case-law. This implies inter alia, the obligation to demonstrate that any measure taken corresponds to a « imperative social need ». Measures which are simply « useful » or « wished » may not restrict the fundamental rights and freedoms. The Working Party therefore underlines the need to establish a comprehensive debate on the initiatives to fight terrorism analysing all their consequences on the fundamental rights and freedoms of persons and in particular refusing the amalgam between fight against real terrorism and the fight against criminality in general, as well as limiting the procedural measures which are invasive to privacy to those really necessary.

⁵ See in particular the Working document "Processing of Personal Data on the Internet" of 23 February 1999, Recommendations 1/99 on "Invisible and Automatic Processing of Personal Data on the Internet performed by software and hardware" and 2/99 on the "Respect of privacy in the context of interception of telecommunications" and 3/99 on the "Preservation of traffic data by Internet Service Providers for law enforcement purposes", the Working document "Privacy on the Internet - An integrated EU Approach to On-line Data Protection" of 21 November 2000, Opinions 2/2000 concerning "The general review of the telecommunications legal framework" and 7/2000 "On the European Commission proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 – COM(2000)385", Opinion 4/2001 on "the Council of Europe's Draft Convention on Cyber-crime" and Opinion 9/2001 on the Commission communication "Creating a safer Information Society by improving the security of information infrastructures and combating computer-related crime". All documents are available at http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

⁶ See in particular Art. 8 Charter of Fundamental Rights of the European Union as well as case-law of the European Court of Human Rights in the recent affairs Aman of 16 February 2000 and Rotaru of 4 May 2000.

⁷ See whereas's 1, 2, 10 and 11 of directive 95/46/EC and whereas 2 of directive 97/66/EC.

Furthermore, the Working Party recalls that the legislative measures limiting the right to privacy of individuals have to be accessible and foreseeable as regards their implications for the persons concerned. This is a requirement involving legislation sufficiently clear in its definitions of the circumstances, the scope and the modalities of the exercise of interference measures. The provisions have to be clear and go into detail to indicate under which circumstances the public authority is authorised to take measures limiting fundamental rights. They should in particular specify where such measures may be used and should exclude all general or exploratory surveillance and offer protection against arbitrary attacks from public authorities⁸.

Finally the Working Party notes with concern that there is an increasing tendency to represent the protection of personal data as a barrier to the efficient fight against terrorism. The Working Party wishes to recall that on the one hand the texts on data protection (which include directives 95/46/EC and 97/66/EEC as well as Art. 8 of the Charter of fundamental rights of the European Union) aim to protect the fundamental rights of the citizen and on the other hand that those texts contain the necessary exceptions to fight against criminality within the limits authorised by the European Convention of human rights.

Measures against terrorism should not and need not reduce standards of protection of fundamental rights which characterise democratic societies. A key element of the fight against terrorism involves ensuring that we preserve the fundamental values which are the basis of our democratic societies and the very values that those advocating the use of violence seek to destroy.

Done at Brussels, 14 December 2001

For the Working Party

The Chairman

Stefano RODOTA

⁸ See in particular the jurisprudence of the European Court of Human Rights, in the cases Chappell (30 March 1989, n° 152, point 56), Malone (2 August 1984, point 67 and 68), Sunday Times (26 April 1979, point 49), Valenzuela Contreras (30 July 1998, point 46) and Lambert (24 August 1998).