ITALY

MINISTRY OF FOREIGN AFFAIRS
Inter-ministerial Committee for Human Rights

Italy's contribution in relation to the request of the United Nations High Commissioner for Human Rights pursuant to UNGA Resolution 68/167 on the right to privacy in the digital age

June 2014

Italy's contribution in relation to the request of the United Nations High Commissioner for Human Rights pursuant to UNGA Resolution 68/167 on the right to privacy in the digital age

Further to your query, Italian Authorities are in a position to provide the following information.

1) What measures have been taken at national level to ensure respect for and protection of the right to privacy, including in the context of digital communication?

The main Italian Acts for personal data protection have been merged into the "Data Protection Code".

The right to protection of "personal data" is different from the right to respect private and family life; this distinction is notably made in the EU Charter of Fundamental Rights.

The main principles of the Code are coherent with European Acts in this matter. It provides that everyone has the right to protection of personal data concerning him or her. Personal information is collected, shared, used and stored by individuals, organizations and public authorities; a data subject shall have the right to obtain confirmation as to whether or not personal data concerning him exist and communication of such data, in intelligible form, also into digital communication.

A part of Data Protection Code deals with **electronic communication data**. It has implemented the provisions contained in the E-Communications privacy directive 2002/58/EC, that reflect the main principle in this matter. Other provisions are contained in the Act which transposed the provisions of the data retention directive (2006/24/EC).

Communications service providers are permitted to retain **traffic data** for only a six-month period, but they are required to retain traffic data for longer in connection with law enforcement purposes (twenty-four months for telephone traffic data and twelve months for electronic communications traffic data). Following ratification of **Council of Europe's Cybercrime Convention** (Act no. 48/2008), police authorities were enabled to order Internet service providers and operators **to retain** and protect Internet traffic data for no longer than **ninety days** (and exceptionally for sixty days more), in order to carry out pre-trial investigations. Such a retaining data would only be possible under certain conditions, without including Internet communication's contents. There is no Judge's authorization in this case, but a request must be made within 48 hours, and the order issued by police authorities must be validated by the competent public prosecutor. Other conditions are provided by Code of Criminal Procedure.

2) What measures have been taken to prevent violations of the right to privacy, including by ensuring that relevant national legislation complies with the obligations of Member States under international human rights law?

The Data Protection Code provides that **Public bodies** shall be permitted to collect and process personal data in order to discharge their institutional tasks, for legitimate purposes. Public bodies must collect and process data fairly and lawfully, complying with prerequisites and limitations set out in the Code. So Public Authorities are permitted to process personal data – except for sensitive and judicial data - in the absence of laws or regulations providing expressly for such processing; but the Code provides that communication to other public bodies shall be permitted only if it is envisaged by laws or regulations. The same rules apply to communication to private entities (or profit-seeking public bodies) and for dissemination by a public body. **Public and private** bodies must comply with specific rules for processing of judicial data and sensitive data (such as health data, or concerning political and religious opinions), especially genetic and biometric data; so, processing is allowed if it is provided for in laws or in regulations. Private bodies must obtain the authorization of the Italian Data Protection Authority.

Specific **technical arrangements** are implemented whenever data are processed by electronic means; moreover, judicial and sensitive data must be protected against unauthorized access through the use of suitable electronic means.

The Data Protection Code considers "**personal data breach**" a breach of security that leads to the accidental destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service. Everyone, under certain conditions, must be notified when a data breach involves their personal information. Specific rules provide when there are serious risks for personal data.

As far as the scholastic staff (school heads, teachers, administrative personnel, technical and auxiliary), they are public employee, subjected to the same rules of other public employees.
Regarding personal data of candidate teachers who are inserted in rankings ("ad esaurimento", "di circolo" and "di istituto"), Italian Ministry of Education adopted two notes: Circulars no. 45, 7th March 2012 and no. 510, 22 January 2013.
Regarding students, these are the main legislative actions activated by the Ministry of Education:
- Article 2, para 2, Decree of the President of the Italian Republic 249/1998 - Regulation containing the Statute on female and male students of the secondary school: "*Scholastic community promotes solidarity between its components and ensures student's right to privacy*";
- Note 10642/2004 of the General Directorate Scholastic System on the *lawfulness of the publication through the posting on the notice board of the school of the judgment on the students who chose to study Catholic Religion;*
- Ministerial Decree no. 305, 7th December 2006 – Regulation containing the identification of sensitive and judicial data utilized by Ministry of Education in compliance with articles 20 and 21 of the legislative decree n. 196/2003 "Data Protection Code".

3) What specific measures have been taken to ensure that procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data are coherent with obligations of Member States under international human rights law?

Public authorities can make **interceptions** in holding inquiries into specific crimes indicated in the Code of Criminal Procedure. An interception is allowed under the condition of a legal warrant granted by a judge.

Special investigations can be made without previous interception warrant, under certain conditions; however, the order issued by police authorities must always be validated by the competent public prosecutor.

Security measures are established if the processing is likely to present specific **risks** to data subjects' fundamental rights and freedoms and dignity on account of the nature of the data.

Every person shall have the right to a **judicial remedy** for any breach of the rights granted to him by the national law applicable to the processing in question.

4) What measures have been taken to establish and maintain independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data?

The Italian Constitution provides the personal liberty is inviolable. In accordance with it, public authorities must respect the right to freedom of opinion and expression and respect personal domicile, including digital data in personal computer.

An independent Authority (Italian Data Protection Authority) has the task of enforcing Protection Data Code and of making regulations, also. It cooperates with European Data Protection Supervisor. Italian Data Protection Authority hold **inquires** and makes decisions involving personal data issues. It is also **consulted** in making laws or regulations concerning data protection.
Regarding the school world, this Authority realized two useful compendia containing the main rules on privacy in this area, produced and distributed in 2010 and 2012, entitled respectively "Privacy among school desks" and "Privacy at school. From tablet to electronic school report. Rules to be remembered".

The online metadata of **internet** users cannot be stored if concerning contents of navigation, but there are problems with extra UE companies. On 25 January 2012, the Commission UE proposed a **reform** of data protection rules to strengthen online data protection rights, on both the General Data Protection Regulation and on the Data Protection Directive in the law enforcement context. The next meeting of Justice Ministers on the data protection reform will take place in June 2014.