Visit of the European Union Civil Servant Tribunal

Privacy protection in litigation before administrative courts

October 29, 2012, Rome - palazzo Spada

Ladies and gentlemen,

I am particularly honoured to have been in charge of presenting to the members of the European Union Civil Service Tribunal the essential outlines regarding the protection of privacy during litigations before administrative courts in Italy.

In this short paper I will focus on three main aspects of the topic under consideration: first it will be briefly illustrated the national legislation concerning the protection of personal data; then it will be examined the ways in which data are handled by the whole administrative justice, viewed as a public body; and finally I will regard profiles concerning treatments done by the courts, properly regarded as a judge, taking care of the relationship between privacy and procedural code and of the arrangements for publication of judgments.

Italian laws regarding the protection of privacy

The Italian legislation on protection of personal data is contained in many texts, the most important of which is the Legislative Decree June 30, 2003, n. 196 “Code concerning the protection of personal data”, better known as “Data protection code”, which brings together in one place the law December 31, 1996, n. 675 (made following the EU Directive 46/1995) and other legislative decrees, regulations and codes of practice that have taken place after this.

The Data protection code (which also contains important innovations according to the decisions taken by the Italian Data Protection Authority and to the EU Directive 58/2000 on privacy in electronic communications) is a reorganization and simplification of the previous system and is divided into three parts : 1) the first part (articles 1-45) regards general rules, which have been rearranged in order to include all the requirements and the provisions of each treatment, both general or specific for those carried out by public and private parties; 2) the second part (articles 46-140) contains provisions relating to specific sectors. In particular, are regulated the treatments in general legal field (art. 46-49) and in legal Information technology (art. 51-52), and 3) eventually, the third part (articles 141-186) regulates the administrative and judicial safeguards, with its own system of penalties.

The legal system is then integrated with the various ethics codes that the Data Protection Authority can promote among categories involved in adoption of codes of ethics and good conduct.

Along with the Data protection code should also be reminded the existence of the Code of digital government (Legislative Decree 82/2005, current since 1 January 2006), which governs all the rules of digital administrative actions.

Elements of the discipline: a) the right to privacy

The key elements of the discipline of privacy are mainly three: a) the creation of the right to privacy, b) the establishment of an authority expressly responsible for controlling of system of data protection, and c) the regulation of treatment modalities.

Regarding the first aspect, the law considers specifically the protection of personal data of each person, whether natural or legal, ensuring the principle under which each processing of such data must be made in full and complete respect for human rights, fundamental freedoms, dignity and confidentiality. Italian jurisprudence already recognized a real right to privacy, even before and beyond the assumptions of the law, finding its legal basis in art. 2 of the Italian Constitution, and considered it as an inviolable right of the person. Now the law configures privacy as an absolute right, inviolable and deserving of protection.

For these reasons, the central discipline is given by art. 23 of Data protection code which provides that “the processing of personal data by private or public companies is permitted only with the express consent of the person concerned”. Anyway, in the law is possible to identify a number of cases of exclusion of need of that permit, including, as relevant here, that in art. 18 which provides: “public agencies do not need to require consent of the person concerned”.

Each person has in any case a number of tools to ensure proper performance in relation to the protection of data, being able in particular (article 7): a) to obtain confirmation of the existence or not of personal data concerning him or b) to be informed of the data, asking their eventual correction, c) to resist, in whole or in part, to the processing of personal data concerning himself.

Elements of the discipline: a) the Authority

With regard to the second aspect, and to give effect to this broad scope of protection, the law has established a body to guarantee respect for the rights of personality, regarding to the multiple activities of data processing. This body, specifically called

"Data Protection Authority" (better known as "Garante della privacy"), is configured as an independent administrative authority.

The Authority is responsible, among other things: a) to ensure that the processing of personal data obey the laws and regulations and to give any orders to the holders of treatments; b) to investigate complaints and reports and to decide appeals on the matter; c) to issue orders prohibiting processing of personal data.

Elements of the discipline: c) The data and their treatment

With regard to the third aspect and to the practical regulation of the treatment, the law takes care to identify the central concepts of "treatment" and "personal data" as generally defined in art. 4. In particular, the term "personal information" is defined as "any information relating to an individual, identified or identifiable, even indirectly, by reference to any other information including a personal identification number", while "treatment" means "any operation or set of operations, carried out with or without the aid of electronic instruments, concerning the collection, recording, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, circulation, erasure and destruction of data, even if not registered in a database".

The breadth of these concepts causes a very wide application of the law, taking care both of the matters and of the operations. The Code analyzes each case with respect to the different situations and with particular emphasis on the one hand, the "sensitive data", defined as "personal data revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations having that aim, as well as personal data disclosing health and sex life", and on the other hand to the "judicial data", i.e. "personal data disclosing the measures recorded at criminal registry or at administrative penalties resulting from crimes registry, and the charges pending or under investigation according to the Criminal Procedure Code".

Administrative justice considered as public administration

The rulebook now examined shows that the data treatment practices can concern the administrative justice in two different ways: on the one hand, as a public body managing data (e.g. the management of case files) and then as administration in the broadest sense; on the other as a judge, and then as a subject related to compliance with the rules of

procedural code (in particular, with regard to the treatment of the identification data of the parties and the events that affect them substantial).

The two profiles require different considerations.

In his capacity as public entity and administration, administrative justice is subjected to a series of requirements, deadlines and responsibilities regarding privacy and information management, with serious consequences in the area of organization. In particular, administrative justice, like every other administration, has had to provide for changes due to the use of IT tools, providing new job profiles and responsibilities in different organizational functions, developed on the basis of technical and legal expertise.

Apart from the profiles of less importance, it is important to point out that every public office, and so each Tribunal, is equipped with a document on security (DPS, art. 34), which represents a sort of picture of all personal data treatments carried out by the body and of all security measures implemented to protect these treatments. The preparation of this plan is related to technical specifications contained in the Code (Annex B paragraph 19). And the failure to adopt it is a criminal offense.

It is also provided to adopt internal rules on the proper handling of personal data, sensitive and judicial, according to art. 20 of the Code (regarding administrative justice, this rule was adopted by decree of the CPGA - Council of Presidency of administrative justice - of May 12, 2006 "Regulations regarding the treatment of sensitive and judicial data in the offices of the administrative justice"). This document is the instrument by which the public authorities shall make clear to the citizens of the type of sensitive and judicial personal data used, of the aims pursued and of the means of their treatment. The document is adopted following a complex inquiry which requires a preliminary study concerning the detailed structure of the body, the definition of roles, responsibilities and safety measures to be implemented.

Administrative justice as jurisdiction: a) the data in the lawsuit

With regard to the protection of privacy during the lawsuit, the central theme concerns how to coordinate the rules provided for in the procedural code with that resulting from the law related to the protection of personal data, how many times they do not match. In practice, it may happen to have different requirements for privacy protection and for proper execution of the trial, and then it is to decide which of the two disciplines should be preferred.

In the face of different possible solutions, the Italian law chose for the indisputable prevalence of reasons of justice. As recently seen in an interesting decision (Cass. Civ. United Sections, February 8, 2011, n. 3034, because the court regarding the protection of personal data is the ordinary court, as court of the rights), it was said that the procedural code can not tolerate exceptions or additions regarding the point of privacy protection, since the legislator, at the moment of enactment and also in successive integration, has always taken care of relevant profiles to that extent.

Practically, the only limit is the failure to comply with procedural rules. In this case only, the failure could lead to an unlawful injury to the rules governing the protection of privacy. On the contrary, the proper exercise of the powers granted by the procedural rules makes in any case not relevant any facts harmful to the personal data of the stakeholders (in detail, the events examined by the Court concerned the notification of an act, in accordance with the provisions of the Civil Procedural Code, the contents of which had appeared injurious to the personal data protection, since it led a third party to know the existence of a civil trial).

Consequences of this configuration is the fact that the Data protection code can not affect the mode of preparation and publication of judgments (as we shall see in the next section), nor in terms of the procedural provisions concerning the vision and the issue of extracts and copies of deeds and documents (article 51, paragraph 1).

Administrative justice as jurisdiction: b) the publication of pleadings

The clear prevalence of procedural rules is limited in cases where the judicial decision is intended to be known outside the circle of those concerned with the matter by publication in legal journals, electronic media or through electronic communications networks.

Art. 51 and 52 of the Code sharply deal with the subject of legal information technology (theme dealt also with a resolution of December 2, 2010 of the Data Protection Authority, concerning "Guidelines on processing of personal data in reproduction of judicial decisions for the purpose of legal information"), without affecting the activity of the original preparation of judgments and other judicial decisions and their content (art. 52, paragraph 1), or its publication by releasing in the judicial registry, in accordance with rules governing those activities.

On the one hand, the Code encourages the widest possible circulation of the judgments and of the other judicial measures, providing that the knowledge of these

measures can be realized by the same judicial authority "through the information system and the institutional Internet sites" (article 51, paragraph 2), observing a few precautions required by the Code (art. 52, paragraphs 1 to 6), aimed at protecting the rights and dignity of the persons concerned, as well as through the "circulation in any form of the contents of judgments and other judicial proceedings" (art. 52, paragraph 7).

On the other hand, there is a procedure for concealment of only personal data contained in judicial proceedings, so as not to affect the ability to know the legal reasons for the decision. This procedure has two different forms: one follows the request of the concerned part; the other is officially acted.

The first form is governed by art. 52, that provides that any interested party may ask, by application lodged at the registry of the court, to omit any personal information and other data suitable to identify him in case of public reproduction of the measure. The data considered are the standard identification data and any other data capable of identifying directly the person concerned (art. 4, paragraph 1, lett. C).

The decision on the request, which was adopted by the competent court, takes the form of a decree, written at the bottom of the same instance.

The second form is that the decree ordering the concealing of data can be ordered by the judge, for the same purposes of legal information, even ex officio, ie without application of a party. This rule obliges the court to carefully evaluate the opportunity of concealing, especially in regard to measures containing sensitive data.

Once the court has given the record about data concealing, it becomes effective the prohibition (art. 52, paragraph 4). This ban regards, as object, all the data suitable to identify the concerned person and, as subject, is addressed to all those who, not party in the lawsuit, could be interested in circulation of that measure for the purposes of legal information.

Finally, it exists a statutory prohibition of circulation (art. 52, paragraph 5) designed to protect children's data and the parties in court proceedings relating to family relationships and status of persons. This rule guarantees a wider protection because it extends also to "other data relating to third parties from which may be also indirectly inferred the identity of these subjects".