INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

COORDINATED BY DR. REINHARD KREISSL
IRKS INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
WEIN, AUSTRIA

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

LED BY PROFESSOR CLIVE NORRIS AND DR XAVIER L'HOIRY
DEPARTMENT OF SOCIOLOGICAL STUDIES
UNIVERSITY OF SHEFFIELD, UK

ITALY COUNTRY REPORTS

UNIVERSITA CATTOLICA DEL SACRO CUORE, ITALY

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN ITALY – ALESSIA CERESA & DR CHIARA FONIO

LOCATING THE DATA CONTROLLER IN ITALY – DR CHIARA FONIO, ALESSIA CERESA & PROFESSOR MARCO LOMBARDI

SUBMITTING ACCESS REQUESTS IN ITALY – DR CHIARA FONIO & ALESSIA CERESA

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN ITALY

Application (primary and secondary legislation) and interpretation (case law) of data protection principles

In Italy the several laws, codes and regulations on data protection, introduced since 1996, have been systematically re-organized in the s.c. "Data Protection Code" (DP Code): D.Lgs. 30 June 2003 n.196.[1] This law has been implemented by the Data Protection Agency (DPA), as it concerns any issue related to sensitive personal data protection and, *de relato*, the fundamental liberties and rights defined at a constitutional level, i.e. the privacy right,[2] the recognition of the identity right for each citizen,[3] etc. The objective necessity to develop specific regulation on this issue has been progressively realized in light of several EU Directives.[4]
In response to these social changes, the three key principles, which inspired the implementation of the DP Code, are as follows:[5]

- Simplification;
- Harmonization;
- Effectiveness.

In detail, the Data Protection Code is divided into three main parts:
Part I: general provisions;
Part II: specific sectors dispositions:
Part III: remedies and sanctions.

Part I specifies the framework of this legislation, clarifying concepts, principles and rules on data protection, data retention, privacy issues and related rights. In particular Art. 4 ("Definitions") refers to the basic set of definitions related to data protection issues. This is crucial in order to understand the *ratio* at the base of the whole DP Code structure. Among the several definitions, the most important basic concepts refer to the data, the subjects involved in the data processing and the relevant filing system. The very first definition refers to the concept of "processing",[6] i.e. "any operation or set of operations, including those without electronic device support, concerning the data gathering, organization, retention, consultation, elaboration, modification, selection, exploration, comparison, use, interconnection, block, communication, diffusion, deletion and destruction, even if the data are not stored in a proper database".

[1] D.L.gs. 30 June 2003 n. 196, in G.U. 29 July 2003 n. 174 – Supplemento Ordinario n. 123.
[2] Art. 15, Italian Constitution.
[3] Art. 22, Italian Constitution.
[4] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in OJ L 281/31-39, 23.11.95; European Parliament and the Council, Directive 2006/24/EC of 15.03.2006 on the retention of data generated or processed in connection with the provision of public available electronic communications services or of public communication networks and amending Directive 2002/58/EC, in OJ L 105/54-63, 13.04 2006.
[5] Garante per la protezione dei dati personali, *Data Protection Code – Legislative Decree n. 196/2003*, http://www.garanteprivacy.it/web/guest/home_en/Italian-legislation#1 (last accessed 15 June 2013).
[6] Art. 4, lett. a), D. Lgs 30 June 2003 n. 196.

Furthermore, the DP Code distinguishes three main categories of "personal data",[7] in line with the EU Directive 95/46/EC:[8]

> "a) "Common personal data": i.e. the data essential to identify a person, including photos and/or images of a person, personal data connected to phone calls and e-mails, time tracking applications at the workplace, etc.
> b) "Sensitive data": i.e. personal data through which it is possible to identify the race, religion, political opinions, including the personal *status* of an individual belonging to a political party, a religious community or particular associations/organizations, the health condition and sexual attitude and orientation of a person
> c) "Judicial data": i.e. personal data that reveal a particular judicial *status* of a person (e.g. a convicted person or one that is accused in a proceeding, etc)".

The DP Code further defines the different subjects entitled to manage the collected data[9] in different ways:

> "-The "data controller" is the natural or legal person, the public authority or any other agency or other body in charge of determining the aim and modality of the data processing, as well as which tools utilized in collecting the data and the security level to adopt.
> -The "data processor" is the person, the private company, the public administration or any other institution or association appointed by the data controller in order to manage the gathered personal data.
> -The "data subject" is the natural or legal person, the public authority or organization the personal data refer to".

The result of data gathering generates the consequent definition of "database",[10] intended in the DP Code as any complex set of organized data, divided in one or more units, located in one or more sites.

A recent judgement on the violation of personal data reveals how delicate this issue is when a technological instrument is involved, i.e. the internet. In detail, this was a case of a clear infringement of Art. 167 L. n. 196/03 (DP Code), as it referred to a person who violated the personal data and privacy of an individual, because he publicized the private mobile phone number of a person he was chatting with online, without his consent. The person who recognized his mobile number on the internet reported the situation and the proceeding came to the Supreme Court (*Corte di Cassazione, Sez. III Pen., Sent. 01.06.2011, n. 21839 - personal data infringement*).[11] The court confirmed the condemnation decided by the judge of the Tribunal of Milan and subsequently at the Milan Court of Appeal.[12] The defense adduced, as justification of the behavior, that the DP Code specifies the responsibility of data protection managed by the data controller and the data processor (intended as both a natural

[7] Art. 4, lett. b), c), d), e), D. Lgs 30 June 2003 n. 196.
[8] Art. 2, lett. a), European Parliament and the Council, Directive 95/46/EC of 24.10.1995, in OJ L 281/31-39, 23.11.95.
[9] Art. 4, lett. f), g), D. Lgs 30 June 2003 n. 196.
[10] Art. 4, lett. p), D. Lgs 30 June 2003 n. 196.
[11] Corte di Cassazione, Sez. III Pen., Sent. 01.06.2011, n. 21839, www.penale.it/page.asp?idpag=960; www.cortedicassazione.it/Documenti/21839_06_11.pdf (last accessed 15 June 2013).
[12] Tribunale di Milano, Sent. 04.02.2009 and Corte d'Appello di Milano, Sent. 11.05.2010.

and legal person),[13] but never refers to private citizen responsibility, as it was in this case. Therefore, the sanction described in Art. 167 L. n. 196/2003 was intended to be addressed only to the defined subjects but excluded instances of personal data misuse by a private citizen. The judge responded to this argument by outlining that Art. 4 let. f) of the DP Code, when referring to the sensitive data responsibility of the "natural person", has to be interpreted as any kind of person (extended interpretation principle). It is addressed not only to the data controller and processor, but even to any person that is using personal data, whatever the aim of this use is and however the sensitive data have been obtained. Secondly, the defense justified the convicted person's behavior in light of the fact that the publication, on the internet, of a mobile phone number cannot lead to a serious prejudice of the person the mobile number belongs to. *A contrario*, the judge dissented from this explanation, as the Tribunal initially and the Appeal Court and finally the Supreme Court clearly recognized the unanimous violation of a person's personal data. In fact, the Supreme Court judge's motivation explained that the diffusion on the internet of sensitive data is, *ipso jure*, an objective prejudice, as the virtual channel of information diffusion, i.e. the internet, is difficult to control, as is the consequent (mis)use of online personal data. As the judge pointed out, it is not important how long the sensitive data is diffused through the chat-line, as it is impossible to control who and how that private mobile number might be (mis)used by any person who can access the internet.

Application (primary and secondary legislation) and interpretation (case law) of the right of access to data

Art. 7 of the DP Code, entitled "data subject rights", defines the "right of access to personal data and further rights". According to this article, the data subject has different rights relating to his/her (natural person) or its (legal person, e.g. private company, institution, organization, etc.) personal data. The data subject has the right to obtain the confirmation of his/her personal data gathering, even if the data have not been stored in any database yet. The communication of such a confirmation must be made in an intelligible form (Art. 7, clause 1, DP Code).

The data subject has the right to obtain the following basic information:

> "a) the origin of his/her data;
> b) the aim and modality of data retention;
> c) the criterion according to which the data are stored in an electronic system;
> d) the identification of the data controller and processor;
> e) the subjects and related categories of subjects the personal data could be transmitted to, as representatives of the State or persons responsible for the data retention and management" (Art. 7, clause 2, DP Code).
>
> "Furthermore, the data subject has the right to obtain:
>
> a) the update, the modification and, when necessary, the integration of his/her personal data;

[13] Art. 4, let. f), L. n. 196/2003.

b) the deletion, the conversion into an anonym form or the block of data retained infringing the law, included those data for which is not necessary to gather in light of the aims according to which they have been collected or afterwards retained;
c) the guarantee that any of the operations described in a) and b) above would be communicated to the data subject by the person to whom the data have been transmitted and diffused. The exception is the case when this communication is objectively impossible because it is disproportional compared to the protected right" (Art. 7, clause 3, DP Code).

"The data subject has the right to make a (complete or partial) opposition:

a) for legitimate motives concerning the data retention, also related to the aim of the data gathering[14];
b) against the data retention aimed at publicity or for direct sales or marketing research or commercial communications" (Art. 7, clause 4, DP Code).

In practice, the right of access to data is a crucial issue, as it could refer to several contexts of a different nature. For instance, in Italy the protection of data access within the health care system is a big issue, as recent legislation introduced the patients' electronic case-history,[15]available online (intra/inter-net), to facilitate the improvement of network information sharing activities by doctors and medical staff working in the same hospital or in different health contexts, to guarantee a better health care service to the patient. Specifically, the issue concerns the electronic protection in order to avoid easy online access to "sensitive data" (as defined by the Art. 4, let. d), L. n. 196/2003 -DP Code-) or the possibility that any hacking/cracking activity on the internet could violate the software and lead to the misuse of personal data of an individual, specifically regarding the health condition of the person.

An *excursus* of the jurisprudence on this issue can be represented by the following cases, which cover different aspects and involve different subjects in the exercise of data access rights:

1. *TAR (Tribunale Amministrativo Regionale)*[16] *Firenze, Sez. I, 12.05.2011, Sent. n. 809* - data access right for judicial reasons.

This case refers to an employee of the University of Pisa (Tuscany) who complained about her salary, comparing it to the contract for her position in the administrative department of the University. To prove the discrepancy between her job position and the salary, she required access to internal documents (i.e. contracts, salary details, etc.) of the University regarding three of her colleagues who held the same position as her in the administrative office. The Administrative Director denied access reasoning that these documents contained information which included data that the DP Code defines as "sensitive" and "super-sensitive" (Art. 4, clause 1 let. d), e)) referring to third parties (external to the judicial case). In fact, besides the salary earned by these employees and their job position described in the

[14] The data protection legislation does not provide a clear definition or any guidance on what the term 'legitimate motive' means. Instead, this is subject to interpretation on a case by case basis.
[15] Art. 13, D.L. 18.10.2012, n. 179, in G.U. 19.10.2012 n. 194/L – Supplemento Ordinario n. 245 – Serie Generale
[16] TAR: *Tribuanle Amministrativo Regionale* (Administrative Regional Tribunal). It is the first instance of the administrative justice in the Italian judicial system.

contract, the documents also contained an historical description of the career and private life of these people, i.e. sick-leave, leave of absence, etc. In reality, the employee formally requested permission to access the personal documents from one of the three colleagues, although the colleague denied her the access to his private data.

The sentence of the administrative judge was in favor of the plaintiff, granting access to the documents referring to the other colleagues. The judge made this decision on the basis of different valuations of the situation.

a) The employee of University had a direct, concrete and motivated interest to access the documents of her colleagues. The right of access in this case was motivated by the fact that the main and exclusive interest of the plaintiff referred to the comparison of her role in the University with those of her colleagues and for this reason there was no infringement of personal data, as the aim was the development of a defense strategy by the plaintiff.

b) The judge recognized that the documents the plaintiff required access to contained sensitive data belonging to other individuals (colleagues), but other previous judgments in similar cases decided in favor of document access. Therefore, many magistrates would not recognize an infringement of personal data in this case (*Consiglio di Stato*, sez. V, 17 September 2010, Sent. n. 6953; *Consiglio di Stato*, Sez. V, 7 September 2004, Sent. n. 5873; *Consiglio di Stato*, Sez. VI, 22 October 2002, Sent. n. 5814). Besides, this decision is in line with Art. 27, clause 7 of the L. n. 241/1990, according to which the "right of data protection" is overcome by the "right of defense" when the document access reveals sensitive data belonging to a different subject not directly involved in the judicial proceeding.

c) The previous principle that the "right of data protection"[17] has the priority, in reality has only one exception: i.e. when the data are extremely "sensitive data", namely "the data through which it is possible to identify the race, religion, political opinions, including the personal *status* of an individual belonging to a political party, a religious community or particular associations/organizations, the health condition and sexual attitude and orientation of a person" (Art. 4, clause 1, let. d) of D.L.gs n. 196/2003). Usually this right needs to be protected, although access is allowed under certain conditions defined *ex* Art. 60 of the DP code (D.L.gs n. 196/2003): i.e. when the right to protect is qualitatively comparable to the "right of data protection", as in this case where the "right of defense" is a constitutional and fundamental right of any individual.

d) In light of the previous point, it is evident that the documents the plaintiff required access to contained "sensitive data" about third parties, but it was sufficient in this situation to "censure" these kinds of data (e.g. the health condition of the employee, the career progress, etc.), which are not of specific interest for the defense strategy of the plaintiff and *a priori* the plaintiff always declared she was not interested in those aspects of the documents for which she required access.[18]

[17] The right of data protection in this context should be taken to mean the right of access to information.

[18] *TAR Firenze, Sez. I, 12.05.2011, Sent. n. 80,* in www.giustizia-amministrativa.it/DocumentiGA/Firenze/Sezione%202/2011/201101050/Provvedimenti/201300220_01.XML (last accessed 15 June 2013).

2. *Cass. Civile,*[19] *Sez.I, 09.01.2013, Sent. n. 349* - right of access to bank documents when referring to the profiling of the customer in the case of a loan request.

In this case, a customer discovered he had a negative rating through the Credit Bureau EXPERIAN Information Services S.p.A. when he asked for a loan from a financial institution and his request was rejected. In consequence and on the basis of Art. 7 of the DP Code (data access right) and the related procedure determined by Art. 8 and 9 of the DP Code, he faxed a request to access his data. He sought to know why his "credit profiling" had a negative rating. The consumer never received an answer to his fax and the financial institution denied the receipt of that fax. However, the financial institution declared, in the course of the judicial proceeding, of having already sent the information required by the customer and in any case this institution enclosed this document containing the required personal data information as part of the written evidence.

The judge declared that the appeal to the Supreme Court (*Corte di Cassazione*) by the financial institution *a priori* was not applicable. In fact, the magistrate underlined in his judgment's reasoning, the two main concepts defined by the DPA. Firstly, the terms of answering within 15 days of a data access request by the data subject is clearly defined by Art. 145 and 146 of the DP Code. Secondly, the (oral, written or digital) answer needs to be clear and exhaustive on the gathering, management and deletion of personal data, when the data subject requires further explanations on his/her personal data collected in certain databases (Art. 7 of the DP Code).[20] As a result, the judgement found that data controllers were tightly bound by the legislative codes of data protection procedure and were expected to respond to access requests in a strictly legally compliant manner.

3. *TAR*[21] *Sardegna, Sez. II, 02.08.2011, Sent. n. 865* – data access right and right of personal data protection when the access to public documents involves the personal data of third parties (employee vs. INPS-*Istituto Nazionale Previdenza Sociale*).

This case concerned an employee/partner in a cooperative society. This society had been wound up and the employee did not receive the total amount of his salary because the INPS-*Isituto Nazionale di Previdenza Sociale* (National Insurance Institute) collected some evidence against this employee from other colleagues which affected the final salary amount payable to the employee.This evidence included the amount of his pension contributions and national insurance contributions whilst employed with the cooperative society.. The employee, therefore, brought INPS to the administrative court, as he requested access to the documents belonging to the National Insurance Institute, containing the evidence of his colleagues, in relation to his salary payment. INPS always denied access to those documents, reasoning that it was an infringement of the personal data protection right of third parties in the judicial proceedings (in fact the documents contained the name, surname and other sensitive data of the employee's colleagues).

[19] TAR: *Tribuanle Amministrativo Regionale* (Administrative Regional Tribunal). It is the first instance of the administrative justice in the Italian judicial system.

[20] Cass. Civile, Sez. I, 09.01.2013, Sent. n. 349, in www.ilsole24ore.com/pdf2010/SoleOnLine5/Oggetti_correlati/Documenti/Norme%20e%20Tributi/2013/01/corte-cassazione-sentenza-349-2013.pdf

[21] TAR: *Tribunale Amministrativo Regionale* (Administrative Regional Tribunal). It is the first instance of the administrative justice in the Italian judicial system.

The TAR of Sardinia granted the employee's application, forcing INPS to let the employee have access to the documents containing his colleagues' evidence against him. From a juridical perspective, in fact, the magistrates reasoned that this judgment underlined that, in this case, there was an evident contrast and discrepancy of two (primary legislation)[22] principles: i.e. the "right of personal data protection" (in the Italian juridical system it is defined as "*diritto alla privacy*"), namely the identity protection of the two witnesses, and on the other side the "right of access data", namely the employee's right of obtaining access to the evidence of his colleagues to develop an effective defensive judicial strategy for protecting his right in obtaining his salary payment ("right of defense").[23]

To balance the two primary rights involved in the case (i.e. the "right of personal data protection" and the "right of data access" with the extension and further aim of "defense right"), the TAR judges decided to grant access to the INPS witnesses documents to the cooperative society employee. At the same time, they also required INPS to "censure" the sensitive data contained in those documents (i.e. name, surname and identification data of the witnesses), which were of no interest to the employee to develop his defensive judicial strategy. In fact, the interest of the employee in accessing the documents was always strictly in relation to the content of the evidence in order to define the total amount of his salary, and not to the identity of either of the two witnesses.[24]

4. *Consiglio di Stato,*[25] *Sez. V, 28.09.2007, Sent. n. 4999* – right of access to data and personal data protection rights, the problem of balance in cases of public administration official document access when third parties are involved.

This is the case of an NGO which aimed to protect stray dogs. The NGO requested access to data from TAR of Milan (first instance), namely documents belonging to the public dog kennels of Milan regarding the suspected illicit trade of stray dogs from Italy to Northern European Countries. The kennel denied access to those documents, assuming a clear infringement of the personal data protection right (the s.c. Italian "*diritto alla privacy*"). In fact, the association required a list of documents, including the temporary adoption certificates of dogs to third parties (namely, individuals), definitive adoption certificates of dogs, certificates attesting the restitution of the animal to the legitimate owners, data referring to the adoption of dogs by third parties, etc.

The TAR judge allowed access by the association to the public kennel archives, reasoning on the basis of the necessity to balance two primary legislation rights: i.e. the "personal data protection right", namely the sensitive data referring to the identity of third parties in the judicial proceeding on one side and, on the other, the "right of access data" extended to the "right of information" from the animalist association perspective. To balance the two juridical recognized rights, the judge of the first instance allowed access to the documents belonging to the dog kennels, with the limit of censure (by the substitution with the word

[22] In the hierarchy of the Italian legal sources the Italian Constitution and its fundamental rights is part of the "primary legislation".

[23] Ferrucci A., *Diritto di accesso e riservatezza. Osservazioni sulle modifiche alla L. 241/1990*, in www.giustamm.it/new_2005/ART_2005.html (last accessed 15 June 2013).

[24] TAR Sardegna, Sez. II, 02.08.2011, Sent. n. 865, in www.giustizia-amministrativa.it/DocumentiGA/Cagliari/Sezione%202/2011//201100270/Provvedimenti/20110865_01.XML (last accessed 15 June 2013).

[25] *Consiglio di Stato*: it is the last instance (Supreme Court) of the administrative judicial system.

"*omissis*") of the sensitive data content in the documents or, as an alternative, the public kennels should ask the data subjects' permission to transmit the documents and their related identities to third parties.

The animalist association, in fact, obtained those documents from the public kennels, but the use of the word "*omissis*" did not allow the association to investigate the subjects involved in the suspected illegal trade of stray dogs. Therefore, this association made an application to the Administrative Supreme Court, namely *Consiglio di Stato*, to reformulate the first judgment (made by the TAR of Milan). The *Consiglio di Stato* turned down the animalist association application, assuming that the TAR judge found the right balance between the two legitimate rights ("right of personal data protection" and "right of data access"), and the access to the documents was properly allowed. Regarding the fact that the censure ("*omissis*") of sensitive data (identities of third parties) hampered the investigation of the association, the *Consiglio di Stato* explained that the suspicious activities run by the public kennels would be the subject of an *ad hoc* criminal proceeding, through an *ex officio* procedure, automatically transmitting the judicial documents, as the judges of the criminal court would be legitimate in also having access to the sensitive data for investigative and judicial reasons.[26]

National exceptions to the EU Data Protection Directive and to the right of access to data

The right of access to data, mentioned in Title II (data subject rights), Art. 7 (data access right and further rights) of the DP Code[27] has some exceptions, described in Art. 8 of the DP Code, entitled "exercising the rights".[28] Data access required by the data controller or processor or by the DPA for certain categories expressed in Art. 8 of the DP Code is excluded, as they represent an exception to the rights expressed in Art. 7, *primus inter pares* the data access right. Therefore, data access is excluded when personal data are gathered:[29]

"a) on the basis of the legislation on money laundering;
b) when the personal data are referred to the legislation on the victims of extortion;
c) when the data are gathered by the Parliamentary Commission of Inquiry (*ex* Art. 82 Italian Constitution);
d) when a public authority gathers the data according to the law on monetary and currencies policies, payment systems, control of brokers' activity and financial markets control, as well as regarding the protection of their stability (e.g. it is not possible to exercise the data access right according to Art. 7 of the DP Code on the databases managed by the Bank of Italy and the Risk Center);
e) during defense investigations or during a proceeding before a Court, when there could be a prejudice for an individual from the data access rights exercise;

[26] Consiglio di Stato, Sez. V, 28.09.2007, Sent. n. 4999, in www.altalex.com/index.php?idnot=38736 (last accessed 15 June 2013).
[27] D.L.gs 30 June 2003 n. 196, in G.U. 29 July 2003 n. 174 – Supplemento Ordinario n. 123, implementation of the EU Directive 95/46/EC.
[28] DPA, *Cosa è il diritto alla protezione dei dati personali?*, www.garanteprivacy.it/web/guest/home/diritti/cosa-e-il-diritto-alla-protezione-dei-dati-personali (last accessed 15 June 2013).
[29] DPA, *Limitazione all'esercizio dei diritti (articolo 8 del Codice)*, www.garanteprivacy.it/web/guest/home/diritti/cosa-e-il-diritto-alla-protezione-dei-dati-personali (last accessed 15 June 2013).

f) when the access right is exercised by the suppliers of electronic communications services, accessible to the public, regarding incoming telephone communications, with the exception in cases of prejudice during defense investigations[30];
g) for justice reasons, involving judicial offices, included the Supreme Magistrate Council (CSM – *Consiglio Superiore della Magistratura*), or the Minister of Justice or similar authorities;
h) for the Police databases, but not including the Ced[31] database held by the Minister of Interior (L. 1 April 1981 n. 121)".

However, the DPA is not covered by these exclusions and the DPA, when necessary, can conduct inspections on all the archives where the personal data are stored. In any case, it is forbidden:

-to require any modification or integration of personal data referring to a personal evaluation, i.e. assessments, subjective opinions or personal appreciations (e.g. a subjective evaluation on the basis of a coroner's expertise);
-to access information about behaviors to adopt or decisions to take referring to the data subject (e.g. the necessity or not to take legal action).

Compatibility of national legislation with Directive 95/46/EC

The EU Directive 95/46/EC has been implemented in Italy with the D.Lgs. 30 June 2003 n. 196, the s.c. Data Protection Code.[32] The authority in charge of guaranteeing the application of this law is the DPA, created with the L. 31 December 1996 n. 675,[33] in line with the Schengen Treaty, enforced in May 1997, entitled "On the protection of the individuals and other subjects concerning personal data protection".[34] As far as the EU Directive 95/46/EC is concerned, the Italian DP Code has been inspired by the European Directive, as demonstrated by the fact that the basic definitions of several concepts related to the personal data issue reproduce the concepts expressed in the EU Directive 95/46/EC: i.e. the definitions of "personal data", "data controller", "data processor", "data subject", "data access", "processing system", etc. (see 2.1 and 2.2).

Surveillance and access rights: codes of practice at a national level. (CCTV and credit rating)

[30] The right of defence implies that the lawyer or the accused person can access the data referred to incoming telephone communications when they are fundamental evidences for an effective defensive strategy during a trial.
[31] Ced - *Centro Elaborazione Dati Interforze* (i.e. interforce data elaboration centre): it is a central database managed by the Minister of Interior, aimed at gathering data shared among the several security forces (i.e. national police, carabinieri, guardia di finanza, judicial police). The collected data refer to people involved in judicial police investigations and/or criminal proceedings, http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_della_polizia_criminale/scheda_16059.html

[32] Testo Unico sulla Privacy (T.U. Privacy)
[33] Art. 30, L. 31 December 1996 n. 675, in G.U. 8 January 1997 n. 5 – Supplemento Oridnario n. 3
[34] Garante per la protezione dei dati personali, *Accordo di Schengen. Audizione parlamentare del Presidente del Garante – 12 luglio 1999*, 12 July 1999, wwww.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/48005 (last accessed 15 June 2013).

In Italy CCTV is regulated through what has been defined by the DPA as "provision on video surveillance" which operates within the Data Protection Code. The last provision, issued in April 2010,[35] updated the provision issued in 2004 and the so-called "Decalogue" of 2000. However, it is worth noting that, in the national context, the processing of personal data through CCTV is not regulated by any specific legislation and therefore falls under the more general Data Protection Code. The 2010 provision focuses on general principles, obligations, specific requirements and specific sectors, public, private and profit-seeking bodies and sanctions. Pertaining to access rights, the provision makes reference to Art. 7 of the DP Code that outlines the right to be informed of the source of the personal data, the logic and purposes of the processing, the identification of the data controller and of the data processor as well as of entities to whom the data may be communicated (DP, Art. 7). Moreover, a data subject shall have the right to obtain updating, rectification, erasure, anonymization and blocking of a) unlawfully processed data and b) unnecessary retained data (DP, Art. 7). Art. 8, 9 and 10 outline respectively the exercise of rights, the mechanisms to exercise them and the response to data subjects. However, "it is factually impossible to exercise the right to have data updated, rectified and/or supplemented on account of the very nature of the data in question – which are real-time images of factual occurrences (see Art. 7(3)a of the DP Code). Conversely, any data subject has the right to have the data blocked if such data is processed in breach of the law (see Art. 7(3)b. of the DP Code)"[36].

In Italy the DPA has also issued a "Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments", published in the Official Journal no. 300 dated 23 December 2004 and subsequently amended by the notice published in the Official Journal no. 56 dated 9 March 2005.[37] The timing to answer the data subject's request to access his/her personal data is generally defined in Art. 8, clause 1, entitled "exercising the rights", which declares that the right *ex* Art. 7 (data access right) is exercised through a request, without any particular formality, submitted to the data controller or processor, also via a delegated person, and the feedback to the request has to be given to the data subject or his/her delegate "without delay".

The time limit for answering the data subject's request is more specifically defined in Art. 146, clause 2, where the standard timing is 15 days from the data access request. The DP Code also defines the exception in cases of complex personal data research or for specific reasons. In these cases, the data controller, or processor, can postpone the request for a short term but must give feedback to the data subject within 30 days, informing the person of the complexity and the reasons for which the data access requires longer research (Art. 146, clause 3). If the data subject's right of access is infringed, he/she can always file a petition to the Court or, alternatively, to the DPA (Art. 146, clause 1).

The promotion of access rights by DPAs and national authorities and their role in ensuring compliance to national norms

[35] Garante per la protezione dei dati personali,*Video Surveillance decision dated 8 April 2010*: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1734653 (last accessed 15 June 2013).

[36] Section 3.5, Provision on Video Surveillance

[37] Garante per la protezione dei dati personali, *Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1079077 (last accessed 15 June 2013).

The Italian DPA promotes access rights through its website[38] which provides information, both in Italian and in English, on access rights and how to exercise them. A sample form, for the purposes of making a subject access request, can be downloaded and clear information on how the data controller or data processor must handle the application is offered, along with information on lodging a complaint with the DPA and procedural costs. Moreover, the website provides contact details, including a telephone number, for citizens who may request information on data protection or making complaints.

In order to exercise their access rights, Italian citizens can download a form from the DPA website.[39] The data controller must handle the application: a) within 15 days from receipt b) within 30 days from receipt "if replying proves especially complex in terms of the steps to be taken or if there is any other justifiable ground".[40] If the application is not handled in time or if citizens are not satisfied with the reply, data subjects may claim their rights either before a judicial authority or before the DPA.[41] The case-handling fee is 150 Euro and this must be paid when making the complaint. The procedural costs must be paid by the losing party (which one may argue represents a significant disincentive for individuals to undertake legal proceedings). The DPA must communicate the complaint to the data controller within 3 days. He or she may be assisted and has to reply within 60 days (100 days if enquires are complex). Art. 150 of DP code reads as follows: "if no decision on the complaint is rendered within sixty days of the date on which the complaint was lodged, the complaint shall have to be regarded as upheld". If a citizen does not wish to lodge a claim to the DPA, he or she may lodge a report (Art. 141 (1)b of the DP Code). Reports are meant to provide relevant information to the Authority who may decide to check compliance to the DP Code. In this case, neither formal requirements (i.e. a form) nor fees are needed.

The role of the Italian DPA in ensuring compliance to national norms can be inferred by analyzing the annual reports issued by the DPA focused, *inter alia*, on their activities. At the moment of writing (July 2013) there are 10 reports available online from 2000 to 2012.[42] From the annual reports a complex picture emerges which reflects both the changes that have occurred within the DPA and its role in ensuring citizens can exercise their rights.

Role of national DPAs in ensuring that data controllers allow citizens to exercise their access rights

This role is hard to assess through the information provided on the DPA website as there is no reference to a general code of practice for data controllers. However, each provision and/or decision (i.e. CCTV; the banking sector; genetic data, etc.) issued by the DPA includes, for instance, measures and precautions to be taken by data controllers on how to process data, etc. As mentioned in the previous section, the annual reports shed light -to some

[38] www.garanteprivacy.it (last accessed 15 June 2013).
[39] Modello esercizio diritti in materia di protezione dati personali: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924 (last accessed 15 June 2013).
[40] Garante Privacy , *How can you protect your personal data?* http://www.garanteprivacy.it/home_en/rights#how (last accessed 15 June 2013).
[41] Italian Personal Data Protection Code, Part III, Title I, III (Non-Judicial Remedies): http://www.privacy.it/privacycode-en.html#sect147 (last accessed 15 June 2013).
[42] Garante Privacy, Relazioni Annuali: http://www.garanteprivacy.it/web/guest/home/attivita-e-documenti/documenti/relazioni-annuali (last accessed 15 June 2013).

extent- on the role of the DPA at a national level.[43] However, these reports focus more on the DPA activities and on citizens' complaints than on the relationship between the DPA and data controllers. In other words, the annual reports do not address the role of the DPA in ensuring that data controllers allow citizens to exercise their access rights, but rather they address, *inter alia*, quantitative (e.g. number of complaints) and qualitative (e.g. the nature of complaints) data concerning citizens' complaints.

Three important aspects emerge from the analysis of the DPA reports:

1. the implementation of the DP Code in 2003 led to an increasing number of citizens' complaints: 169 in 2001, 390 in 2002 and 608 in 2003. While there is no clear reference to the number of complaints on access rights, it is argued that one of the reasons behind the above-mentioned increasing numbers is the right to make a subject access request.[44]
2. The number of complaints progressively declined from 2005 to 2010 (between 300 and 400 every year) and then significantly decreased in 2011 (257) and in 2012 (233). This is probably due to the fact that the Italian DPA has always fostered a direct relationship between data subjects and data controllers who, as outlined in the previous section, now handle the applications in due time.[45]
3. The large majority of the complaints deal with the banking sector, in particular the central credit register which is an "information system on the debt of the customers of the banks and financial companies supervised by the Bank of Italy".[46]

In some reports there are statistical data that show, *inter alia*, the number of inspections carried out by the DPA on data controllers. For instance, in 2012, 395 inspections were carried out. Overall, as specified at the beginning of this section, it is challenging to clearly assess the role of the DPA pertaining to the promotion of access rights. Inspections, for instance, may be carried out for reasons which are not limited to the role of data controllers.

[43] It is worth noting that the role of the DPA changed widely from 2001 to 2010 due to the implementation of the DP Code in 2003. Additionally, the word "complaint" here refers to part III, Title I, sections 145-151 of the DP Code, namely "Administrative Remedies" and "Non-Judicial Remedies".

[44] Garante per la protezione dei dati personali, Relazione 2003, p. 134 available here: http://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali.

[45] Garante per la protezione dei dati personali, Relazione 2011, p. 151, available here: http://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali (last accessed 15 June 2013)

[46] Banca d'Italia: http://www.bancaditalia.it/statistiche/racc_datser/intermediari/centrarisk

LOCATING THE DATA CONTROLLER IN ITALY

Introduction

This country profile summary concerns the experiences encountered whilst attempting to locate data controller contact details of 33 sites in Italy at varying levels (local, national and international). In particular, the examples below are illustrative of the individual researchers' experiences conducted within the limited sample and do not claim to reflect the practices of *all* data controllers in Italy. This report illustrates some general trends noted alongside examples of good and bad practices encountered during the course of this research.

Methodological thoughts

We attempted to locate 33 data controllers out of 35 for two main reasons:

1. there are no entry-exit systems at our place of work. We do not have to use badges either to enter the main University building or to go to our offices;

2. a nationally-held patient health record system has not been implemented in Italy yet. While there is a specific legislative framework to set up a centralized system, at the time of writing (July 2013), patient health records are only held locally or regionally.

We successfully identified 26 out of a possible 33 data controllers. The attempts to locate data controllers failed in the following cases:

- Passport service
- Leisure time/sports clubs
- Facebook
- Email data
- Search engine data
- CCTV in a transport setting
- CCTV in a small/local store

Firstly, we chose the sites closest to our place of work and then, after this, we selected domains we usually use or we are more familiar with as they were the closest to where we live (i.e.: the bank or the supermarket we use):

- ANPR
- Banking records
- Insurance records
- ID cards
- Membership of leisure/sports club
- Mobile phone data
- Search engine data
- CCTV in a public space / in a large supermarket / in a bank
- Loyalty card scheme for a national supermarket or similar
- Electoral register

With regards to CCTV, we picked up systems which are not all close to the place of work in order to ensure variety and to avoid being recognized. In doing so, we choose both a big city and a small town to assess whether there were differences between big and small contexts. Furthermore, a few years ago one of the researchers carried out a research focused on CCTV in the city of Milan and, in some of the domains, she would have been recognized.

While the experiences encountered whilst researching Italy-based sites should capture the experiences of a lay person, a methodological concern seems to emerge. The knowledge or familiarity with specific domains, in particular with CCTV, might have "skewed" the experience as, in contrast with a lay citizen, the researcher knew exactly what to look for. Yet, the variety of the contexts (i.e. large supermarket, public and private spaces) limited this risk as the researcher was primarily familiar with public spaces than with the use of surveillance cameras in private spaces, like banks or stores.

Overall impressions

Data controller details were located either through official websites or through personal visits. The use of emails was not necessary as –in most cases- we found the information on official websites. However, we rarely found an online query form which may be easier to use for lay citizens as opposed to email. The phone was rarely used or used only when a first attempt (via website or in person) failed. Contrary to our expectations, in the case of public CCTV we had to speak to members of the staff as the CCTV signage did not include any details for data controllers. When we spoke to members of staff, in all but one site (CCTV in a transport setting), the conversations proved easy and we were given contact details. It is difficult to infer if the relatively good level of openness with regards to contact details for data controllers is due to a good level of expertise or it simply reveals the willingness to give this particular piece of information to the public given that the CCTV signage is inadequate. We never spoke to data protection experts but rather with employers who, when we asked for guidance (i.e. CCTV in a large supermarket), were able to help us despite their low level of knowledge as far as data protection is concerned.

We used the phone to identify nine data controller details and we were successful in five cases. Three out of the nine cases (passports service, email data and membership to a political organization) can be considered as "second round" attempts after we failed to identify data controller details online. Overall, phone calls proved to be more challenging than visits in person as suspicion seemed to arise merely by the use of the phone. Conversations on the phone proved more difficult than personal visits, especially in two cases: 1) the passport service and 2) a primary school. As explained in the following pages, the member of staff of the passport service had a very low level of knowledge while the employer of the primary school was suspicious and not willing to give the piece of information we asked for unless we proved our identity or had children who attended that school.

The overall impression of phone conversations and personal visits is that, despite the level of knowledge not being high, members of staff or employers are willing to assist. We had problems only in one significant domain – CCTV in a transport setting – as described below. As previously mentioned, CCTV signage in public spaces is heterogeneous and, more often than not, contact details are missing. The reason for this may be some changes that occurred over the last decade as far as the general provision on CCTV is concerned. From 2000 to 2013, in fact, a decalogue and two provisions on CCTV were issued by the DPA.

A numerical summary of the findings is shown in the table below:

Data controller contact details successfully identified in first round of visits	25 of 33 (76.8%)
Data controller contact details unable to identify in first round of visits	7 of 33 (21.2%)
Total number of data controller contact details successfully identified after second round of visits	26 of 33 (78,8%)
Total number of data controller contact details unable to identify after second round of visits	6 of 33 (18,2%)
Contact details identified via online privacy policy	14 of 26 (successful) cases
Contact details identified after speaking to member of staff on phone/via email	5 of 26 (successful) cases
Contact details identified after speaking to member of staff in person	7 of 26 (successful) cases
Average rating given to visibility of privacy content online	2 – Adequate
Average rating given to the quality of information given by online content	2 – Adequate
Average rating given to visibility and content of CCTV signage	1 – Poor
Average rating given to quality of information given by staff on the telephone	1 – Poor
Average rating given to quality of information given by staff in person	1 – Poor

Online content

We attempted to use official websites to identify 19 data controller details. The attempts were successful in the majority of cases except for the passport service, Facebook, email data, search engine and membership of a political organization. As such, only 14 data controllers were successfully identified using the privacy-related information located on their organisations' websites. In the case of the passport service, email and political organization we also used the phone which proved to be successful only in the last case (political organization). It should be noted that the use of the phone was a personal choice of the researcher rather than a specific suggestion on the official websites. Moreover, we used generic phone numbers as we did not find any specific numbers for inquires on privacy. The passport service seems to be of particular interest as the official website of the Ministry of the Foreign Affairs does not provide data controller details, nor is there any guidance on how to make a subject access request. There are FAQs about several issues but not about privacy. There is a general inquiry form but no specific access request form on data access.

With regard to the successful cases, privacy policies that included contact details were generally located at the bottom of web pages in small fonts. The location is where one might reasonably expect to find a privacy policy online and the small size of fonts is quite common too. These two features, thus, do not allow for negative generalizations on online content. The depth of information varied greatly across the domains but, as mentioned above, a common feature is the lack of an online query form except for driving license records, credit reference

and police records. The lack of a template can be considered as a negative practice that might prevent citizens from making subject access requests. While this approach does not facilitate users, it might be culturally explained as, in Italy, the relationships between the public/private sectors and the citizens have historically relied on direct interactions (i.e. by phone or in person). This holds true for the adoption and the diffusion of many practices and technologies which started later when compared with other European countries, for the same reasons. Indeed, the use of query forms has also only recently been used by the Italian DPA who, until a few years ago, did not provide any forms on its official website.

Another common aspect relates to the fact that usually the term "privacy policy" refers to the use of information collected through the website *only* and not to *all* the information collected by and/or shared with third parties by a specific organization. Once again, this does not facilitate the user who has to read all the information provided at the bottom of web pages carefully in order to assess whether the policy refers to the information collected via the website or to data collected by the organization.

The quality of information was reasonable for the majority of the websites, however we would not argue that –overall- the information given was particularly good. One domain which proved particularly difficult was Europol as it took us approximately 20 minutes to identify the Italian DPA as the data controller. Additionally, this piece of information is in English. Unless a citizen is familiar with the DPA activities and aware of its role as data controller for Europol, it seems problematic to find contact details. It also took us also a long time to identify details for border control. Public government websites (i.e. Ministry of the Foreign Affairs and/or Ministry of Infrastructure and Transport) tended to be less specific about their privacy policies than private organizations, such as national children's charity organizations or banks. Furthermore, the costs for making a request were never provided and the FAQ sections, on the majority of the websites, included generic information on privacy rather than templates and/or detailed guidance.

Public sector

Good practice

The political organization showed the best practice, despite the lack of information online. On the website we found the phone number of the local office, closest to where we live. The first person we spoke to gave us the data controller details without asking anything. Unlike other experiences, we did not have to explain why we wanted to know this piece of information and who we were. The quality of information was good.

The driving license records and the police records are also worth mentioning as the websites of the Ministry of Infrastructures and Transport and the Ministry of the Interior respectively provide templates to make a subject access request. These domains are thus two notable exceptions as compared to a large majority of websites where the lack of a query form is, as mentioned above, a common feature. However, we would not argue that they show "best" practices as, for instance, in the case of police records, the template helps a citizen who wants to update, delete or anonymize his or her data rather than simply access the data. While in the case of the Ministry of Infrastructures and Transport the template is specifically focused on the subject access request, the letter needs to be signed by a legal representative and this does not ease the process. Nevertheless, the template *does* provide full data controller details.

Bad practice

The most difficult domain was the primary school. This is perhaps due to standard precautions whenever minors are involved. After picking the school closest to where we live, we called and explained what we were looking for. The conversation was difficult as we were asked a) why we wanted to know these details, b) if we had children who attend that school, c) if we planned to enroll a child in the school, and d) where we lived. Notwithstanding distrust and hesitancy, it took us a relatively short time to obtain data controller details.

In contrast, the secondary school proved easier and the quality of information was reasonable. We spoke to a member of staff who did not understand the meaning of our inquiry but told us that, if we were willing to give an email address, someone else would write to us within a few hours which was exactly what happened. We received an email two hours later with all the requested details.

As mentioned in previous pages, the passport service was also more difficult than other sites. Initially we thought that a call to the police headquarters would be sufficient but, after we spoke to a member of staff with a very low level of knowledge, we searched online. The conversation on the phone was problematic as this person was obviously not trained for privacy-related issues and after a few minutes told us to check the Ministry of Foreign Affairs website which, as stated above, did not help. Once again, the language used ("data controller") seemed particularly obscure to the majority of the people we had a conversation with.

Finally, the personnel file at our place of work seems worth mentioning as, even if we found data controller details, the quality of the information given was rather poor and we were asked to explain a) why we wanted to know this information and b) our job position within the University. When we maintained that we were just curious, both skepticism and suspicions arose.

Private Sector

Good practice

The insurance company was an interesting domain as we obtained the information but the employer seemed quite concerned about the final aim of our question and asked whether we had any troubles with the company and if she could be of help. Yet, the reaction of the employer shows that data protection specific queries are not only infrequent but also raise concerns as they might imply "something else" or, as the employer put it, "troubles".

Two examples of good practice in the private sector were the banking records and the credit referencing. Despite the lack of a template, the quality of information given on the data collected and on how to make a subject access request was good. In particular, on the bank website there is a two-page document that explains, *inter alia*, which third parties your personal data might be shared with, both at a national and at an international level. This document, in comparison to other examples in the private sector, such as the pressure group/NGO or the mobile phone company, provides clear and detailed information.

Bad practice

The case of the email data is also worth noting as we attempted to identify the data controller details of our University email account, managed through the cloud service of Microsoft Office Exchange. Since no information is provided on the Microsoft Office Exchange

website, we called the university helpdesk who not only asked for details we were not supposed to give (i.e. why we are interested in such a specific information, who we are and where we work), but did not help us find the data controller details and told us that "no one ever asked for such information". This statement was reiterated by members of staff of other domains.

In the case of Facebook, while the privacy policy is explained in detail, the only contact detail address which is provided is in Ireland and it is for general inquiries on privacy. One might argue that non-English speakers are clearly disadvantaged. In the case of the search engine, similar considerations can be drawn as the privacy policy of Google is fully described but the lay citizen would not find any contact details.

CCTV

We went, in person, to 11 sites. 5 out of the 11 are settings and/or spaces where CCTV is used. We successfully identified data controller details in all but two cases, namely CCTV in a transport setting and CCTV in a small store. Success relied on the strategies of facilitation that can be described as follows:

a) CCTV signage included postal contact details for data controllers and comprehensive information about privacy (i.e. a large supermarket and a bank);
b) Despite the fact that staff members were not always familiar with our requests, they were willing to help us and directed us to someone who was knowledgeable (i.e. CCTV in a public space);

As far as CCTV is concerned, as stated above, the signage did not always include details and we had to ask for guidance. In one significant case, the strategy of denial seems worth mentioning. For the CCTV in a transport setting, we choose Cadorna Station which is one of main railway hubs and underground station in the city center of Milan. We went to the underground station where there are a significant number of cameras. The underground network is managed by a company which also operates the cameras at the stations. The first thing we noticed is that the signage is not immediately visible and it took us a few minutes to spot it. Secondly, it does not fulfill the basic requirements of the general provision on video surveillance issued by the DPA as it does not give enough information about the contact details for data controllers.

Picture 1: CCTV signage at a metro station

Furthermore this CCTV signage looks "old-fashioned" compared to signage generally used both in public and in private spaces. We went to the closest helpdesk to ask for information and spoke to one staff member who did not understand our question. In the second round of visits, we went to the same helpdesk and attempted to speak to another member of staff who appeared to be immediately suspicious (" I do not know what you are talking about and even if I knew I wouldn't share this piece of information with a passer-by") and extremely reluctant to help us. When we mentioned our legal right of access, he changed his attitude and we were advised to go to the Duomo station and ask there. We went to the Duomo underground station which is the most important station right in the heart of Milan. We spoke to two staff members who were less suspicious but nonetheless did not give us any details for data controllers. The people we spoke to did not have any data protection expertise and failed to understand the meaning of "data controller".

Attempting to locate contact details at a small store was a similar experience albeit in this specific case, the employee was neither suspicious nor reluctant but simply did not have adequate training as apparently she had been hired recently.

With regards to other contexts (i.e. CCTV at a supermarket and at a bank), the signage included contact details. At the supermarket we did not see the signage immediately and, therefore, had to ask a member of staff who pointed it out to us and actually read it *with us* as she "has never read the signage before". At the bank, the signage was right at the entrance and contained all the details and comprehensive information about privacy. We would thus argue that the supermarket and the bank tended to show best practice as far as CCTV signage is concerned. However, the lack of interest and/or training of the employee at the supermarket is also worth taking into account when assessing best practices.

Picutre 2: CCTV signage at a bank

Picture 3: CCTV signage at a supermarket

CCTV in the public space and ANPR proved extremely easy as it took us less than 5 minutes to have details of the data controller. However, as mentioned in the methodological thoughts, we choose a small urban context in order to ensure variety and to avoid being recognized. This might have made a difference in terms of the quality of interactions with staff members who have to deal with relatively "minor issues" in comparison to the complex dynamics of a big city.

Concluding remarks

Overall, the exercise of access rights, in the Italy-based sites we researched, both in the public and in the private sectors, seems to depend on *subjective* rather than on *objective* aspects or best practices. Namely, in the absence of online forms, the level of knowledge and/or training of members of staff significantly impacted on the success or failure in identifying data controller details. This is particularly true in the case of CCTV signage that does not meet the basic requirements.

It seems also worth considering that that some private bodies (i.e. banks, supermarkets, political organizations) seem more compliant with the law than public bodies (i.e. passport service). Albeit this is perhaps due to a great amount of bureaucracy within the public sector and consequently leads to more difficulties and rigidity compared with the private sector, the inability to find contact details in the passport service is of particular concern. This in fact shows either an essential incapacity to deal with big data or a lack of training which, in the public sector, is highly problematic if not unacceptable. The process of exercising one's right is at stake here. Moreover, the "opaqueness" of the public sector seems to be in contrast with the "transparency" required from the citizens. Despite sensitive data being disclosed on a daily basis, a lay citizen interested in data protection is perceived as someone who has some underlying issues with it. The aim of our request was often asked for and, more often than not, even the original question was considered peculiar or "odd".

Additionally, the websites of some public bodies appear to be more disorganized than those of some private entities. A concerning common feature is the lack of an online query form with a few exceptions. This is another problematic aspect as it does not facilitate those who look for information online in the first instance. The adequate quality of information given by online content, thus, is tempered by the lack of a facilitation strategy, namely an online form.

Overall, five important aspects emerged from our research:

1) The "language issue". The expression "data controller" is either unknown or confused with other more generic privacy-related words. Rarely did we speak to people who immediately understood our question.
2) Recurrent statements such as "no one ever asked for this piece of information" suggest that access right is perhaps seldom exercised through visits in person.
3) "Privacy policies" at the bottom of webpages are sometimes misleading as they refer only to the information collected through the website.
4) Despite the fact that exercising this right should not require a detailed explanation on "why" and "who" is wanting to know this piece of information, the reasons behind our inquiry were often asked for by the majority of the people we spoke to.
5) We never found any details of the costs of making a request.

SUBMITTING ACCESS REQUESTS IN ITALY

Introduction

This country report describes the experiences of submitting subject access requests to 18 organizations[47] in the public and private domain[48]. The results outlined below reflect the emerging trends of the main sample. To date, individual subject requests have been submitted both by researchers and by third parties. While we limited the use of third parties, fear of being recognised as researchers led us to rely on two individuals who have never been involved in similar research before. Hence, the opportunity of being recognized by data controllers was almost non-existent. However, this did not prevent data controllers from checking online who was submitting the request or, at least in one case, from recognising the researcher. To some extent this probably impacted on the overall result without, we would argue, skewing the sample. In order to reduce this risk, we submitted subject access requests to organizations which are located in different contexts (e.g. big city and small urban contexts in different regions). It is also worth noting that today, the blurring lines between online and offline are common to the experiences of all citizens whose names can easily be "googled" to find out information. Thus, while acknowledging the methodological limits of this research, the trends may be indicative of the experiences a layperson may have to deal with when submitting a subject access request in Italy.

Overall summary

To date, 18 individual subject access requests have been submitted.

	Site	**Data controller**
1	Public	CCTV in open street
2	Public	CCTV in a transport setting
3	Public	CCTV in a government building
4	Private	CCTV in a department store
5	Private	CCTV in a bank
6	Public	Local authority
7	Public	Vehicle licensing
8	Public	Europol

[47] Of these 18 sites, one was approached twice (for banking records and CCTV footage).
[48] An additional 16 CCTV-based sites were investigated as part of the CCTV side study.

	Site	**Data controller**
9	Private	ANPR
10	Private	Loyalty card (supermarket)
11	Private	Loyalty card (supermarket)
12	Private	Mobile phone carrier
13	Private	Banking records
14	Private	Credit card records
15	Private	Amazon
16	Private	Twitter
17	Private	Microsoft
18	Private	Google

We have received 16 responses ranging from partial to full disclosure of personal data. Only in two cases were the responses complete and respondents gave correct information along with full disclosure of personal data. Five[49] cases have been referred to the Italian DPA as "reports" or "informal complaints" due to either a non-response from the data controller or partial and unsatisfactory replies. The Data Protection Code lists three options when sending complaints[50]:

1. "circumstantial claim pursuant to Section 142" which entails specific infringements of the Data Protection code. This procedure leads to a formal investigation by the DPA;
2. "reports", which are more "informal" complaints that consequently imply a less formal procedure
3. "complaints with a view to establishing the specific rights referred to in Section 7".

[49] These were credit card records; banking records; mobile phone carrier records; Microsoft; Google
[50] Personal Data Protection Code, Title I, Administrative and Judicial Remedies, Section 141 (http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf).

In the case of a formal investigation, the case-handling fee is 150 Euro and must be paid when making a complaint. We decided to send informal complaints to the DPA. Communication with the national DPA has been more complex than we had expected and we have experienced excessive delays as well as dismissive responses which we had not anticipated. Having deemed five cases to be sufficiently non-compliant to warrant a complaint to the DPA, we made a 'collective' complaint to the DPA which was submitted on 16/12/13. At the end of January, we received a response from the DPA claiming that the authority considers only "circumstantial claims" which lead to formal investigations. Indeed, we were informed that this holds true for all the complaints we made, except for the one made regarding Google (as shown below in the Google case summary). However, the response of the DPA addressed only three of our five complaints (mobile phone carrier and banking records were not addressed). As such, two of our complaints were not mentioned whatsoever and we have effectively received no response from the DPA on these matters. Generally speaking therefore, reports or informal complaints are not enough for the DPA to intervene. This can be deemed as a restrictive practice for at least two reasons: first, circumstantial claims are expensive. As mentioned in the overall summary, the case-handling fee is 150 Euro. It is therefore likely that only citizens who can afford this fee will be able to use the formal complaint mechanism which will presumably enhance their ability to exercise their democratic rights. Second, the authority did not show any interest in our numerous complaints. We received a letter mentioning our complaints and access rights but failing to "go beyond" mere bureaucratic features (e.g. description of access rights and lists of documents to provide with the circumstantial claim). We had different expectations pertaining to communications with the Italian DPA. Given that our complaints featured a range of poor practices and behaviours from different data controllers, the general lack of interest and assistance received from the DPA was disappointing in the extreme and raises significant questions as to the fulfilment of their duties as mediators in disputes between data subjects and data controllers.

As per the methodological design of the research, we approached all multinational organizations (Amazon, Microsoft, Google and Twitter) in our native language in order to a) test their ability to deal with non-English subject data access requests and b) reflect the knowledge of the average Italian citizen who may not have a high level of written English.

The two satisfactory responses mentioned above refer to the private sector. Interactions with members of staff in the private sector have proven more professional than those with public employees. Despite variable levels of knowledge, the respondents in the public sector, especially when dealing with access to CCTV footage, failed to give correct information even after follow-up correspondence and/or phone calls in which we were asked to clarify our request. More often than not, respondents had not received proper training in data protection issues and this resulted either in delays or in answers which reiterated that we were not entitled to access our data or in answers that hardly ever disclosed with whom our data were shared with. In the majority of the cases, replies were not given within the statutory 15 days time limit, not even when the data controller itself was the Italian DPA (as in the case of Europol data).

While it is challenging to highlight common trends due to enormous differences across the domains, a few distinctive aspects seem to emerge. First, accessing CCTV footage is particularly problematic for the data subject. This is perhaps due, as specified in the section on CCTV, to specific agreements between private organizations such as banks and law-enforcement agencies and to common practices of deleting footage after 24 hours.

Additionally, as we were often told, subject access rights are rarely exercised. Data controllers are more accustomed to dealing with police asking for footage rather than with citizens doing so. Second, restrictive practices were experienced with multinational organizations, except in one notable case, as detailed in the analysis below. Third, facilitative practices both in the public and private sector often rely on subjective aspects (i.e. the availability of the data controller) rather than on objective aspects (i.e. the legislative framework).

Case by case analysis

Public – Facilitative Practices

We found no examples of clearly facilitative practices in the public sector in response to our requests for personal data.

Public – Restrictive Practices

Local Municipality

We made a request to access our data from the local municipality. The data controller's details were located online. Fifteen days later, we received a phone call from the Office for Relations with the Public, acknowledging our request and explaining that they would send us a letter. The person we spoke to emphasized that they had never dealt with such a request and that our documents were ready for us to check. The responded sounded anxious and asked whether we were looking for a specific document. We received a timely response which enclosed basic information which was, however, too generic ("*the demographic office holds data on you, as it holds data on every resident*"). The organization failed to disclose any specific information on data sharing with third parties and only partly disclosed information on automated decision-making. Moreover, we were asked to go, in person, to the Office for Relations with the Public.

We went to the Office and we met the person that we had spoken to over the phone who made us sign a document declaring that we had submitted the data access request. This person also showed us a folder with our name on it and reiterated that no one had ever submitted such a request. Clearly, the data controller representative was not trained to process data access requests and had no previous experience of doing so. We sent a second letter asking for clarification as far as data sharing and automated decision-making are concerned. Again we received a phone call, two weeks later, from someone we had never spoken to before. She asked for more time in order to respond properly to our requests. Since then, we have not heard from the municipality and therefore made a complaint to the DPA. As per the outline given in our overall summary, our complaint to the DPA was dismissed due to its informal nature.

Europol

The national data controller or, as it is detailed on the website, the national competent authority for Europol data in Italy, is the Data Protection Authority. It took us a long time (20 minutes) to locate the data controller on the Europol Joint Supervisory Body website. We made a data access request to the DPA and received a phone call from them after more than one month. The Office for the Relations with the Public acknowledged our request but argued that the letter was not "*accurate*". Specially, we had failed to mention a specific article of the

data protection law which refers to Europol data. We were advised to resend the data access request which we did a few days later (October 2013).

Since then, we have not heard anything from the DPA. It may be the case that this is because no data is held about us by Europol and therefore the DPA has nothing to disclose to us. However, it is nevertheless poor practice to fail to respond to our request and if no data is held about us, we should be made of this. Overall, the procedure seemed quite rigid and might discourage citizens from making a request. Citizens not familiar with the legislative framework might find the overall procedure too complex. In spite of the fact that the member of staff was courteous, the organization is un-responsive to the request and did not respond at all to the second letter, which we had in fact been advised to send in order for us to submit a correct access request.

Vehicle licensing

We made a request to the Ministry of Transport and Infrastructures to access data both on vehicle and on vehicle licensing. We received a letter three weeks after the request which failed to disclose any data but specified that only the law enforcement agencies can access the database. Moreover, due to the complexity of searches within the database, we were advised that it was necessary to include a timeframe for our request (no more than 12 months). However, it is unclear whether this is legally correct and if data controllers are in fact allowed to restrict requests in this way. Nevertheless, following this response, we sent a second letter which included a limited timeframe: from January to June 2013.

We received a letter three weeks later which disclosed data on our vehicle and on vehicle licensing. We were also informed that "*it cannot be excluded that your data have been shared with law enforcement agencies but, due to the great amount of data shared with them on a daily basis, we are not able to tell you whether this has occurred*". Therefore, the data controller seems unable to give a proper answer and cannot track how personal data is shared. Moreover, the reply we received appeared to suggest that the organisation's daily administration and organisational practices involve sharing so much data with third parties that they are completely incapable of tracking this. This is of particular concern given that this effectively means the organisation is inherently unable to answer data subjects' queries regarding data sharing in anything other than very general terms.

From January to June 2013 there are no data on our vehicle licensing in the database. However, we were informed of some correspondence between the local municipality and the Ministry of Transport and Infrastructures which included a list of residents and, consequently, our vehicle licensing details. The response seems accurate and transparent and the organization, despite excessive delay, gave clear guidance (e.g. time frame). More information on automatic decision-making would help to clarify how the database actually works.

<u>Private – Facilitative Practices</u>

Twitter

We checked the privacy policy through our Twitter account and quickly found an email address to send requests to and/or to ask for information about privacy.

We sent our subject data access request in Italian to privacy@twitter.com on 28/10/13 and received a response within a few hours from a contact person within the company's Trust & Safety department. The email we received is shown below:

> *Hello,*
>
> *If you are requesting your own Twitter account information, please fax us a signed request providing consent to disclosure for specific information (e.g.,IP logs), including the username (e.g., @Safety or twitter.com/safety) and email address on the account, along with a scanned copy of your valid, government-issued photo ID to 1-415-222-9958.*
>
> *We will send a request-for-consent email to the email address of record for the account, to which you will have to respond affirmatively. Receipt of an appropriate request and an affirmative response to the request-for-consent email will authorize us to release your information.*

We therefore obtained an answer in English to an email sent in Italian. We replied in English asking for a confirmation of the fax number and we received the exact same email from Twitter Trust and Safety on 31/10/13. Hence, we surmised that the email was an automatic reply. We sent a fax on 11/11/13 and, since we did not receive any correspondences, we sent a second fax on 16/12/13. We insisted on writing in Italian for the reasons explained above.

On 10/01/14 we got an email from Twitter Trust and Safety with a copy of the fax sent on December 16th attached and asking us to confirm our lawful consent to the disclosure of data regarding our Twitter account. Once again, the email was sent in English and this time we replied in English in order to avoid further delays. We immediately confirmed our consent and subsequently received, on the same date, an email with the following files:

- "basic information about Twitter account"
- "Any records of changes of the email address on file for your Twitter account"
- "Tweets of your Twitter account".
- "Favorites of your Twitter account"
- "Direct messages of your Twitter account"
- "Any contacts imported by your Twitter account"
- "Accounts followed by your Twitter account"
- "Accounts that follow your Twitter account"
- "Any lists created by your Twitter account"
- "Any lists subscribed to by your Twitter account"
- "Any public lists that include your Twitter account"
- "Any searches saved by your Twitter account"
- "Logins to your Twitter account and associated IP addresses"
- "Any records of a mobile device that you registered to your Twitter account"
- "Any records of a Facebook account connected to your Twitter account"
- "Any records of changes to your Twitter username"
- "Images uploaded using Twitter's photo hosting service (attached only if your account has such images)"
- "Your avatar and background image, if uploaded"

- "Links and authenticated API calls that provide information about your Twitter account in real time"

Moreover, they specified in the email that "No records were found of any disclosure to law enforcement of information about your Twitter account" and that additional information that Twitter may collect, use and "the limited circumstances in which your private personal information may be shared" are written in the privacy policy.

Therefore, our data were fully disclosed but the issues of a) automated decision-making and b) data sharing with third parties were not addressed. While this strategy cannot be deemed as *completely* "restrictive" as data were fully disclosed, some restrictions of rights seem to emerge. First, the linguistic rigidity which might discourage non-English speaking data subjects from submitting a data request. A good level of English is taken for granted: emails from the Twitter Trust and Safety are written in English only and files attached to emails are in English[51]. The procedure is not *per se* complex although the use of fax in the digital age can be disputed. Once again, this indicates a certain level of rigidity as it entails that Twitter users rely on fax and/or own a fax machine while the use of emails and scanners would probably simplify the procedure. Second, it is worth noting that it took us more than two months to access our data and, third, the response was not complete. We contacted the organization again (on 28/01/2013) asking them to clarify the issues of automatic decision-making and data sharing with third parties. On 06/01/2014 we had an email from Twitter Trust and Safety. The email we received is shown below:

> *As you are aware, Twitter helps users share information with the world, and the vast majority of the information on our service is public. We make the public nature of our service clear to users in our Privacy Policy, and it is readily apparent from Twitter's operation and design. As a result, much of the information that users submit to Twitter, including their Tweets, who they follow, who follows them, and what Tweets they've "favorited," is public and readily accessible to each user through the service.*
>
> *Twitter does not process any personal data about our users without first obtaining their consent through agreement to our Terms of Service and Privacy Policy. We do not engage in any automated individual decision-making about our users that produce legal effects or significantly affects him, as set forth under Article 15 of the EU*

[51] However, it should be noted, that the language setting of our account is English. This may partly explain why we received files written in English and not in our mother tongue.

Data Protection Directive.

Twitter does not disclose your private personal information to third parties except in the limited circumstances described in our Privacy Policy, and set forth below for your convenience:

User's Consent: We may share or disclose the user's information at the user's direction, such as when they authorize a third-party web client or application to access their Twitter account.

Service Providers: We engage service providers to perform functions and provide services to us in the United States and abroad. We may share the user's private personal information with such service providers subject to confidentiality obligations consistent with our Privacy Policy, and on the condition that the third parties use the user's private personal data only on our behalf and pursuant to our instructions.

Law and Harm: We may preserve or disclose the user's information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter's rights or property. However, this is not intended to limit any legal defences or objections that a user may have to a third party's, including a government's, request to disclose a user's information.

As we explain in our Guidelines for Law Enforcement, available at http://support.twitter.com/articles/41949-guidelines-for-law-enforcement, Twitter requires a subpoena, court order, or other valid legal process to disclose information about our users to law enforcement authorities. Before making that disclosure, we notify users of the request for their information from law enforcement authorities where possible and unless we are prohibited from doing so by law. In addition, if a user making a data access request asks whether their

information has been disclosed to law enforcement authorities, we also include that information in our response.

Twitter is largely a public service and therefore the vast majority of the information a user creates on Twitter is readily accessible to each user through the service. We make every effort to provide users with access to their personal information except in certain instances, as set forth below:

We are careful to respect the privacy of our other users and want to ensure that the individual making the request is actually the individual operating the account whose information is being requested. As a result, it is our policy not to provide information requested by a user (other than information that is readily accessible to each user through the service) unless we have been supplied with sufficient information to allow us to confirm the identity of the user making the request.

It is also our policy not to provide information requested by a user that reveals the non-public information of another user or of Twitter. For example, to respect the privacy of our other users, Twitter does not supply data subjects with the private lists created by other accounts that include the account of the data subject. We also do not provide Twitter's confidential commercial information that we have taken steps to protect from disclosure as its disclosure would help our competitors.

Consistent with standard industry practice, we do not provide our log files to users in response to data access requests, largely due to the extremely high volume of log entries that are generated daily by our hundreds of millions of users. Additionally, the manner in which our logs are recorded would require extensive customized engineering work to separate the log entries for a user that has submitted a data

access request from the entries of all of our other users, which would

be necessary in order to respect all of our users' privacy.

This email shows a partial facilitation of rights. Unlike other organizations, Twitter addresses the two issues, however a lack of clarity seems to emerge as far as third parties are concerned. They explain that they "may share" information with service providers but they did not disclose the list of providers. The question of data sharing is thus addressed in generic terms while automatic decision-making is more clearly explained. However, this might raise the suspicion: how do advertisers target audiences on the social network without automatic-decision making? That said, it should be noted that the data controller replied adequately from a strictly legal standpoint despite the questions not being answered as we wished.

Amazon

We made a request to access our data to Amazon on 28/10/2013. Amazon Service Europe is located in Luxembourg and the contact details of the data controller can easily be found in the privacy policy on the Amazon website. Given the reasons specified above, we sent a letter in Italian. At the end of November we received two letters (dated on 21/11/13) and an encrypted CD-ROM from the Amazon Legal Office. For security reasons, the CD-ROM was sent separately from the letter which had contained the passwords to access the data.

On the CD-ROM there were several files, all protected by two different passwords: one to access folders and another to access single documents. The documents, all written in Italian, fully disclose data on:

- payments and credit cards
- addresses
- promotional codes
- wish lists
- order history (digital and non-digital)
- registered e-readers
- memberships
- correspondence

The "language" issue seems to be of particular importance to Amazon. In putting together information on correspondence, in fact, they noticed an email sent, via Amazon, to our email account in German. This email referred to an item bought from a German seller. The person who put together the document for the correspondence wrote a comment which is, presumably by mistake, still visible in the "track changes". The author of the comment wonders why there is something written in German. This seems to corroborate our hypothesis of language as an important facilitation strategy of this multinational organization when dealing with subject access requests.

The letter mentions the online privacy policy and the laws of the Grand Duchy of Luxembourg that governs the terms of use. Additionally, the letter partly addresses the fact that "personal data has been shared with Amazon's European subsidiaries and American subsidiaries which participate in the Safe Harbour Privacy principles developed by U.S. Department of Commerce and the European Union." Personal data is also shared with third party service-providers that perform functions on Amazon's behalf and they can release

account and other personal information to comply with the law or to enforce the condition of use "or protect the rights, property, or safety of Amazon.com, our users, or others". The security of information is protected by using Secure Socket Layer which encrypts information and, in the case of the credit card number for example, "when confirming an order only the last four digits are revealed".

However, the letter does not address in detail with which specific parties they have shared our data and what specific data they have shared. In this respect, it is framed in rather generic terms as it simply reports what it is written on the Amazon website. Therefore, it touches upon this issue without giving the answer that we had hoped for. It should be noted there that while the reply we received regarding data sharing with third parties was not what we had hoped for, the data controller nevertheless fulfilled the legal requirements by providing us with categories of recipients of our data, as per the legal terms in the EU Directive 95/45/EC. Having said this, the failure to go beyond the strictly legal requirements perhaps demonstrates a lack of willingness by the data controller to go the extra mile in their response by answering our query comprehensively.

The last line addresses the automatic decision-making process: "we do not take decisions on clients based on automated decision-making". However, consumers' profiling seems one of the key strategies used by Amazon, therefore the failure to disclose any information on this aspect suggests a lack of transparency and accountability. Amazon seems transparent as far as the disclosure of personal data but it seems reluctant to reveal how automated decision-making works. We contacted the organization again and received an answer on 07/02/2014.

In this letter Amazon provides a list of third parties divided into three categories specifying for each the "purpose" of sharing and which data is shared. The first category is affiliated Amazon Businesses. With some of them (e.g. Amazon.co.uk) personal data (name and full contact details) are shared to fulfil orders while with others, like Amazon Media Eu Sàrl, data are shared when ebooks are downloaded. The second category includes third-party service providers who perform functions on their behalf, such as Bartolini or SDA which deliver packages. As for Amazon Businesses, full contact details are shared. Interestingly enough, an Italian law firm is mentioned: Orsingher Ortu. The law firm "manages subject access data requests". The third category is sellers on Amazon Marketplace in order to fulfil Marketplace orders.

Furthermore, Amazon reiterates that they do not take decisions on clients based on automated decision-making". We would argue that this response is more transparent than the first response and that Amazon did disclose relevant information on third parties in a timely and clear manner. Indeed, in their second reply, Amazon in fact disclosed not only categories of recipients of our data but also provided us with lists of these recipients, demonstrating a willingness to disclose information to us beyond that which is legally required.

Loyalty card (supermarket)

This case concerned a small organic supermarket chain. It took us just one click to find the privacy policy on the main website. As suggested online, we sent an email asking for the name of the data controller on 11/09/13. The day after, we received a reply with the name, phone and fax numbers of the data controller. The data access request was sent by email on 13/09/12. On 27/09/13 we received an email from the data controller with a pdf document attached containing disclosure of data along with information on data sharing and automated decision-making. Moreover, the data controller specified that "*the original document will be*

sent to you via recorded delivery letter" (received one week later) and that he was keen to answer to any further questions and/or give clarifications. The legal timeline during which data controllers must respond is 15 days, therefore the company demonstrated an acceptable response time. This is a notable exception as all the other organizations, both in the public and private domains, failed to respond within the statutory term.

The letter discloses both personal data (name, address and email address) and what costumer data they collect when we use the loyalty card, namely information about purchases made using the loyalty card:

- type of product and price
- location of the retail outlet and date of the purchases
- points card

The above-mentioned information is collected "*only when you use your Loyalty card"* and data are processed by more than one data controller. For instance, database administrators can process information.

Additionally, the letter we received lists five third parties with whom our data is shared. The list includes names and address of third parties' data controllers and provides full contact details. It is worth noting that, once again, this is an exception and reflects a considerable degree of facilitation as not only were third parties identified, but also the contact details of the data controllers were provided. No other organization provided us with a list which was not generic (e.g. "your data might be shared with"); in the majority of cases the question was ignored or incorrectly addressed.

They also informed us that the data are both paper-based and electronically stored. The address of the "datacentre" is fully disclosed along with information on who has access to the database and how. In particular, only data controllers have access, all data are password protected and passwords are changed periodically. We have not been subject to automated decision-making processes and customers are not profiled. In other words, they do not use database marketing which, in our personal experience appears to be true as we have never received targeted advertising from them. Yet, the company is a small chain and apparently consumer profiling is not crucial compared with the bigger groups. The database, thus, stores data "*only to assign points per purchase.*"

Overall, a few distinctive strategies of facilitation seem to emerge. First, the simplicity of the procedure and the readiness to respond within the statutory term. Despite there not being a form on the website which may further simplify the request, clearly such requests are dealt with, via email, as a matter of priority. Second, the organization is responsive to requests and is well informed about citizens' rights. All questions were addressed in a timely and unambiguous manner which reflects familiarity with the procedure and also fulfilment of citizens' expectations. Third, and perhaps more notably, responses are comprehensive, transparent and accurate.

Private – Restrictive Practices

ANPR

With regard to ANPR, we submitted our subject access request to access any data (including CCTV footage) captured by ANPR cameras placed at a motorway exit. In this case it was

difficult to locate the data controller as it was not immediately clear who was in charge of the ANPR system. We expected that ANPR systems at motorway exists were managed by traffic police but this was apparently not the case. We received a response after more than a month from a private company responsible for the operation of the ANPR system. The letter explained that cameras record only if something occurs, e.g. drivers who fail to pay at the motorway toll at the booths at the exits. Moreover, CCTV footage is shared only with debt collection and law enforcement agencies.

Credit card records

We made a request to access our credit card records from our credit card provider. Due to the sensitivity of the data, we did not write our credit card number on the subject access request but we specified the name of the credit card holder. The data controller's contact details were located online and we did not have to log in to the client/members-only section. We wrote to the data controller on 13/09/13. We did not receive any response from them. We thus sent a second letter on 28/10/13 explaining that we wished to have a response within 7 days, otherwise we would make a complaint to the national DPA. This time we sent a registered letter which ensured that it would be received within 24 hours.

We received a phone call three weeks later. The person called from the customer service department and told us that they did receive the second letter but not the first. We were advised to send a fax as "*letters can get lost and you don't know who is going to handle the request"* We then asked if we had to send the fax to the data controller and she said, "*it's better if you send it to customer service. Someone is going to read the fax while, with letters, you never know where they end up*". The person we spoke to was clearly not familiar with the procedure and told us that our letter was unclear. When we asked her to tell us what was not clear, she answered "*it is not clear what you want from us. Framed like this it is difficult to understand. If you write a fax describing exactly what you want from us, it would be better. The letter you sent is too generic; you should list exactly what you want to know"*. We replied that we thought it was clear enough and explained that we simply submitted a data subject access request and that we had the right to do so. We also reminded her of the national legislation. After our explanation her reply was *"It is fine, but I think you still have to write a fax to speed things up and clarify what you need so that we can deal with more a specific request"*. She also asked why we wanted to access our data and we explained, once again, that it was our right to access our credit card records. She was kind but reiterated the lack of clarity of our letter.

We sent a fax on 26/11/13. In the fax we mentioned both letters that had been sent before and the conversation we had had with the customer service representative. We resubmitted our data access request via fax and emphasized that we wished to have a detailed response within seven days otherwise we would make a complaint to the national DPA.

To date, we have not received any response and, therefore, we made a complaint to the DPA (as part of a number of other informal complaints). Moreover, we have never had the opportunity to speak to the actual data controller and we have not received any correspondence from the legal office. Instead, it seems that our request was handled through the general customer service department. The data controller was mentioned only once and even then, this was mentioned by us, over the phone. As described in the overall summary above, our complaint was dismissed by the DPA.

In summary, returning to this specific case, the credit card's customer service demonstrated restrictive practice. While it did not *completely* ignore our requests, the data controller failed to respond to our correspondence at least twice. The person we had a conversation with was kind but was not able to offer guidance and was probably incompetent at dealing with such requests. We were not viewed with suspicion but, rather, we had the impression that our request was not understood or worse, that they pretended not to understand what was unmistakably written and explained over the phone. The representative we spoke to was probably not trained and not familiar with data subjects' rights and it was not clear to us what they did not understand. The strategy of denial reflects a lack of accountability which is of particular concern, given the sensibility of the data involved. Moreover, the organisation clearly demonstrated an inefficient administrative and procedural approach, failing to provide an unambiguous format through which we could make our request.

Banking records

We made a request to access our banking records from our bank, one of the largest banking groups at a national level. The data controller's details were quickly located via its official website in just one click without the need to log in. We received a response within the statutory time which fully disclosed personal data but completely failed to address automated decision-making. The document also included the bank's privacy policy and a six page list of data controllers described as "*third parties who are data controllers on behalf of the bank*". We found this sentence particularly confusing as it is unclear who owns or is in charge of the data. In particular, it is not clear if only the bank is responsible for the data. The letter, thus, enclosed clear guidance on privacy policy but did not answer our questions directly. We sent a second letter and received a timely response but the document did not cover all aspects despite the second being more precise than the first. We made a complaint to the DPA but, as described above, the specific aspects of this case were not addressed in their response. In effect, we received no response from the DPA to our complaint.

The legal office of the bank seemed competent in dealing with data subject requests and the organization is responsive but there is a lack of preparedness in dealing with specific questions which are answered in rather generic terms.

Mobile Phone carrier

We made a request to access our mobile phone records from our mobile phone carrier. We received a phone call two weeks later from the customer service department acknowledging our request and inquiring if we had any problems with the contract. Interestingly enough, the staff referred to our subject access request as "*a complaint*". Moreover, we were asked to explain exactly "*what we expected from them as it was not very clear*". She also highlighted that the company provides location data only to law-enforcement agencies and for very specific reasons (e.g. phone tapping in mafia cases). A week later we received a letter which was incomplete but for one piece of information: data are not disclosed to third parties because we indicated this as our preference when were signed up with the service a few years ago (2008).

We sent a second letter and received another phone call but not from the same employee. This person asked for more time as "*they were double checking the legislative framework".* A second letter from Tim arrived a few weeks later but the document failed to address automatic decision-making. Therefore, we made a complaint to the DPA as part of our collective complaint. As described above, this case was not addressed in the DPA's response

and we therefore have received no response on this matter to date.

Microsoft

At our workplace, we use a Microsoft Exchange iCloud email account (Office 365-Exchange online). Locating the data controller was not as quick or easy as we had expected. We checked the pdf document on cloudmail provided by the University but this did not include the privacy policy. We therefore made a request to Microsoft Italia. However, we provided only our email account without further details (e.g. password) as we felt uncomfortable in disclosing sensitive information. They failed to reply within the statutory term and therefore we sent a second letter explaining that we wished to have a response within seven days, otherwise we would make a complaint to the national DPA. Microsoft Italia received our registered letter 24 hours after we sent it. Since then (end of November 2012) we have not heard from them. We therefore had no option but to make a complaint to the DPA as part of our collective complaint. As described above, this complaint was effectively dismissed.

The lack of response from this multinational organization gave us the impression that our request was simply ignored. Not only did they not reply but they did not even attempt to contact us via email or phone. This strategy of denial certainly discourages citizens to make such requests.

Google

We made a request to Google Italia in November 2013. After two weeks, we received an email from "Google Italy Legal" saying that Google Italy was not able to fulfil the request as "*all is managed by Google Inc. California*". We were advised to check the privacy policy and the account data on the Google Mail dashboard, as far as Gmail was concerned. The email, signed by the Google Italy Team, did not include comprehensive guidance but instead discourages citizens from making data subject requests as it emphasises that users can control account information and/or can read the privacy policy online. However, this was not what we asked and also the email did not address data sharing with third parties and automated decision-making at all.

We decided to send a fax, in Italian, to the US headquarters. We sent two faxes but, to date, the organization has been non-responsive. The last fax was sent at the end of November. We made a complaint to the DPA and received an email from the national authority on 04/03/2014. The attached document had been sent to a Google privacy lawyer and we were copied in to this email. The DPA asked Google to provide our data access to the national authority by 07/04/2014. This seems of particular interest as, for the first time and despite the fact that we sent an informal complaint to the DPA, the authority wrote directly to a lawyer, on our behalf, in order to exercise access rights. Moreover, we were somewhat confused by the DPA's order to disclose our data to *them* rather than to us. No explanation was provided for this procedure. To date, no response has been received from the DPA or the data controller.

Loyalty card (supermarket)

Information on the data controller was located after we went in person to the supermarket. However, the contact name we obtained for the data controller was not considered "right" by the staff we spoke to and we were advised to go online where we found a phone number for inquires. Therefore, it took us more time and effort than we had originally expected to

identify the right data controller whose contact details were given to us over the phone. We had to send two letters in order to obtain a response. After a considerable delay, (more than 30 days), we received a letter disclosing data and only partly addressing automated decision-making and data sharing.

In particular, third parties are not clearly identified ("your data can be shared with the postal service and other parties") and there is very little on automated decision-making. Apparently the company uses automated decision-making but the document does not include, for instance, details on the logic of this process. We contacted the organization again and the case is still pending at the time of writing.

CCTV

We submitted subject access requests to five different domains: open-street CCTV, public mass transport, a government building, a department store and a bank. As mentioned in the introduction, we used a third party in two cases for fear of being recognised. All subject requests were unsuccessful for a variety of reasons. CCTV has proven to be the most challenging domain in which the balance of power between citizens and data controllers seems to be particularly problematic. The provision on CCTV issued by the DPA in 2010 is rarely enforced and it is hard for the citizen to understand why access to CCTV footage is almost impossible. In all cases, our feelings were that the request was deemed illegitimate or not welcomed. The imbalance of power is, not only between the data subject and the data controller, but also between the citizen and the police. More often than not, only law enforcement agencies are entitled to access the footage, notwithstanding the clarity of the provision as per data subjects' rights. Conversations with members of staff in all the domains were difficult since they had not been trained or had not been informed about a) citizens' rights and b) the name of the data controller. The variety of signage is also noteworthy. While signage was displayed in all locations and it was, in the majority of the cases, visible, information on the signs varied widely.

CCTV in a bank

The information notice at the bank was immediately visible and clearly displayed all the information we were looking for. Regarding the signage, this was the best information notice we encountered during our research for at least three reasons: a) the color of the signage made it easy to spot; b) its location was at the entrance to the bank and c) it displayed comprehensive information.

Picture 1: CCTV signage at a bank

It is also worth noting that the colour also makes the information notice immediately visible and that the sign is big enough to display all relevant information, including contact details of the data controller at the bottom and in bold. The data controller of the bank showed perhaps the best practice but the response received still seemed legally inaccurate and we were denied access to the footage. The response was received without delay and we were also sent a copy of the signage which clearly informs costumers that the footage is stored for seven days and that, as specified above, can be accessed only by law-enforcement agencies. However, this last point can be disputed as there is no mention about this in the general provision on video surveillance issued by DPA. Broadly speaking, data subjects should be able to exercise their rights and according to Italian law, "Any identifiable data subject must be enabled to actually exercise their own rights in pursuance of the DP Code, in particular the right to access the data concerning them, check the purposes of the processing as well as the relevant arrangements and the underlying logic (see Section 7 of the DP Code)"[52].

CCTV in a transport setting (metro station)

The CCTV signage was quite difficult to spot and the information notice looked very old-fashioned and unusual.

[52] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1734653

Picture 2: CCTV signage at a metro station

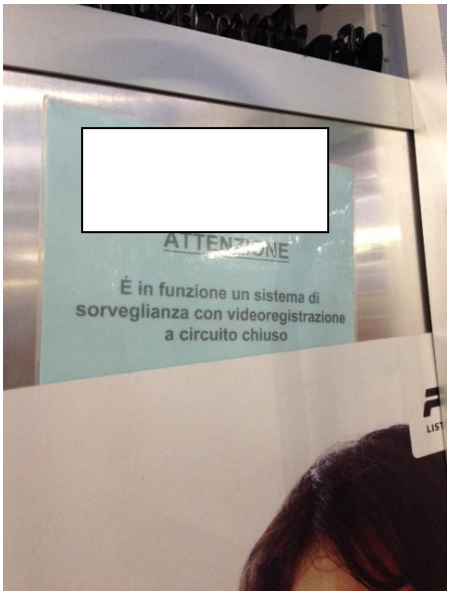
It was even more difficult to engage in conversations with members of staff who were neither trained nor particularly interested in helping us. In contrast with the signage used in Picture 1, in Picture 2, the signage is more difficult to spot despite the presence of many cameras across the entire location. Additionally, it does not provide full contact details of the data controller. It was also difficult to read it as it was far above the ground and written in small font. This demonstrated poor practice, given the centrality of the location and the amount of citizens captured by surveillance cameras on a daily basis.

We were discouraged from making the request by them pointing out that we did not have the right to access the footage. They were clearly unmoved by our request and, when we insisted, we were directed to other people and had to go to a different metro station in order to find the data controller details. The people we spoke to were incompetent and ignorant of citizens' rights.

We sent our request and the response we obtained from the company who manages public transport raised some suspicion. Signed by a lawyer, the document highlights that "*the CCTV cameras do not always record. When the cameras do record, the footage is deleted within 24 hours and the footage is not shared with third parties. We do not hold any data on you*". While it is true that CCTV systems do not always record, it is unlikely that surveillance cameras located at metro stations do not record on a regular basis for security reasons.

CCTV in a department store

We went to store which is a relatively small department store, located close to where we live.



Picture 3: CCTV signage at a department store

The CCTV signage at the department store (Picture 3) was at the entrance but not immediately visible as it was located in a corner. This information notice is probably the worst in the sample and was in breach of the law. The minimum standard for CCTV information notice is, in fact, that it should provide: the data controller's details and the purpose of the processing, neither of which is provided on that signage.

We asked for guidance as the name of the data controller was not provided on the information notice. The member of staff was very suspicious and asked us twice why we were interested in the CCTV footage. The person did not have a clue about how the CCTV system worked and reluctantly gave us the contact details of the director of the store who was also the data controller. We submitted a request but received no reply in the first instance so we sent a second letter. We received a reply after two letters, claiming that the cameras do not record. Both the data controller and the staff person we had contact with seemed incompetent in dealing with data access requests. Moreover, we had the impression that the request was not legitimate and, indeed, "odd".

CCTV in a government building

We went to the a government building in Milan, but the signage at the entrance of the office didn't provide us with any relevant information. Therefore, we checked the website but we couldn't find any further details. As a result, the day after, we sent a registered letter directly to the office's postal address. We received an answer to our footage access request and the employee of the public administration office explained to us, in a very detailed and clear manner, that the CCTV system complied with the DPA Provision on video surveillance and with the DP Code (*ex* art. 11 D.L.gs n. 196/2003). The data controller happened to be the same office that we had addressed the letter to and they explained that footage is not shared with third parties as the CCTV system isn't connected with any external company or entity. CCTV is used only for security purposes as sensitive data about citizens and the city of Milan (i.e. public and private buildings, etc.) are stored in their office. In fact, *in extremis*, footage is accessible only by the police or judicial authorities when a crime has occurred. The footage is stored for 24 hours and then deleted so they couldn't provide us with our footage.

CCTV in open street

We went to Piazza della Scala which is a square located right in the heart of Milan. Palazzo Marino, the city hall, is located in the square, therefore there are many surveillance cameras in the area and several police officers on patrol. In fact, we asked one of them who was stationed at the entrance of the building explaining that we were interested in the CCTV footage of the cameras that we had spotted in the square, not of those on the building. He told us that "no one can have access to the footage" and directed us to the local main police station where we asked other local police officers. We were viewed with suspicion and were directed to yet another member of staff who gave us two addresses to which we could submit the request. It took us more than half an hour and three separate attempts to speak to someone who could be of help. We received a response more than month later claiming that the footage was erased and it is only shared with law enforcement agencies. Overall, we experienced a restriction of rights as: a) the guidance was completely absent; b) the staff were not competent in dealing with such requests and displayed non-collaborative behavior.

The telephone number of the data controller was never displayed. In the best-case scenario, only the name and address were provided. This can be deemed as restrictive of citizens' rights who have just two options: writing down the address or asking for guidance. This was probably the most challenging part of our research as the people we spoke to either discouraged us from making the subject access request or did not have a clue about subjects' rights. Public transport, Milan Metro Station, proved more difficult than other domains. The staff were not trained and provided unclear guidance. The members of staff reiterated that we did not have the right to access the CCTV footage but – when reminded that we actually did- they simply directed us to other people or advised us to go to different locations in order to find out the details of the data controller. This represents a strategy of denial as – without a strong purpose - the lay citizen would more than likely be discouraged from the ambiguous, if any, guidance.

The variety of signage corresponds with the variety of replies that we received from data controllers. Two similarities seemed to emerge:

1. A considerable amount of delay - Except in the case of the bank, all responses were received after more than three weeks and in, the case of the department store, we had to write a second letter. In one case, the government building, we did not receive any response at all and made a complaint to the DPA which is pending.
2. The impossibility of access to CCTV footage - Even when we had sent registered letters delivered in 24 hours, we were advised that the footage had been already deleted or we could not access it for several other reasons. For instance, in the case of the bank, the footage is apparently shared only with the police and with the judicial authority. In the case of the open-street CCTV, the footage had allegedly been overwritten. It is worth noting that since our delivery methods ensured that our requests were received within 24 hours, the failure to obtain footage due to deletion is the result of the delay incurred while awaiting responses from data controllers and *not* the result of our requests being received too late.

Overall, submitting a data subject access request to view CCTV footage was regarded with suspicion. At the department store, staff asked us twice why we wished to know the name of the data controller and whether we had "any problems". The data controller of the

department store responded only after he received the second letter, to inform us that the cameras did not record while the signage says exactly the opposite.

This reliance on "access only by law-enforcement agencies" is an issue of concern which has become common practice both for public and private entities: more often then not, the legal position of the data subject is incorrectly framed and it is justified more on the basis of specific agreements between private organizations and law-enforcement agencies than on the provision issued by the DPA. Therefore, it is difficult for the data subject to understand whether his/her position is legitimate and whether he/she has to refer to the provision or to the above-mentioned agreements which are not always available for the data subject to look at. The picture that seems to emerge is therefore ambiguous and patchy.

As far as sharing images with third parties and automated decision-making, only the first aspect was covered in all responses. CCTV footage is claimed to be shared, if requested, only with law enforcement agencies and/or private security guards. It should be noted that often, especially in the case of private entities, there are specific agreements with law enforcement agencies which are the only subjects entitled access to footage.

Concluding thoughts

When submitting subject access requests to public and private organizations we had expected the same problems experienced during our attempts to locate data controller contact details. Indeed, the problems we encountered have proven to be quite similar. There are a few aspects or emerging trends which are worth considering. As briefly mentioned in the introduction, subject access rights seem to be rarely exercised. Many data controllers were genuinely surprised by our request and reiterated that they had never received such a request before. Therefore, one might argue that in addition to a general lack of training, they are not familiar with this procedure. This holds true for both the public and the private domains, even though private organizations displayed more strategies of facilitation than the public sector. Unfamiliarity with the procedure resulted in a variety of responses that ranged from formal letters to informal, if not incorrect, replies. In some cases, data controllers failed to refer to the legislative framework which is an aspect of concern. Moreover, both in the public and private sectors, conversations occurred with members of the staff, not directly with the data controllers. Moreover, we often spoke to people who lacked proper training and had little or no knowledge about privacy laws.

SIGNIFICANCE OF FINDINGS - ITALY

A number of key findings have emerged from the research. Firstly, we found that in the course of attempting to exercise informational rights, data subjects are regarded with suspicion, especially in the public sector where data controllers obviously deal with law enforcement agencies more than with citizens. This calls into question the issue of the balance of power. It seems challenging for the citizen to exercise her or his access rights in a landscape where special agreements between the police and the organization prevent the citizen from accessing their data. In the public domain, even if special agreements were not mentioned in the letters, we had been told, informally, that only the police are entitled to, for example, access CCTV footage. This aspect brings to the fore the crucial issue of the realistic possibility of data subjects in exercising their rights.

Another emerging trend, which is a common feature of public and private organizations, is the prevalence of subjective aspects over objective facts. In other words, accurate responses and/or disclosure of data seem to rely more on the willingness and/or training of the data controller than on the right of the citizen to access his or her data (objective dimension). While the subjective dimension is not *per se* a problem, subject access requests should not be determined by personal attitudes. This also relates to the lack of a common language. As specified above, responses varied widely across domains.

The language issue is another feature at stake when dealing with private multinational organizations. Except for one notable exception (Amazon), a good level of English is required. This is a strategy of denial which might discourage citizens from submitting an access request. Non-European headquarters are more difficult to approach without using the English language.

When submitting subject access requests we asked specific questions on data sharing and automated decision-making. These matters were almost never addressed by data controllers and we had to prompt them, seeking clarifications which were fully explained only in very few cases. Especially when dealing with the commercial sector (e.g. the shopping mall, multinational organizations), data controllers seemed unwilling to provide explanations on automated decision-making. While third-party data sharing was described more clearly, policies on data sharing, when disclosed, failed to answer to our questions directly. In the case of CCTV none of the data controllers addressed automated decision-making directly. In the majority of the cases, data controllers neither confirmed nor denied that we had been subjected to automated decision-making. In summary, both public and private organizations are less transparent when it comes to dealing with the two above-mentioned aspects than when disclosing data they hold on us. In a number of cases this issue is still ongoing and we will update this in the final draft.

Accessing CCTV footage had been very difficult across all domains. In this context, differences between information notices are indicative of a lack of homogeneity which makes it harder for the citizen to understand her/his actual rights.

When it comes to differences between the public and the private realms, perhaps the most notable aspect is that strategies of facilitations, such as timely responses, flexibility and competency, had been more often offered by private than public organizations. Surprisingly, public entities have been less responsive and even less competent in dealing with our requests.

Lastly, communication with the national DPA has been more difficult than we had expected. The DPA have been generally uninterested in our complaints (except for the Google case) and the only practical advice we received came in the form of one phone call from them in which we were advised to resubmit a request. Even in this case (Europol), having followed their advice, we were still unsuccessful in obtaining our personal data. Notwithstanding the considerable number of procedures the DPA has to deal with on a daily basis, we would argue that excessive delays or complete silence are restrictive of rights. When the DPA finally responded to our informal complaints, after lengthy delays, these were dismissed and it appeared that the case-specific concerns we had raised had not been closely considered. As such, the informal system of submitting complaints was plainly inadequate for our purposes. The more robust complaints procedure offered by the DPA is, as explained above, subject to high financial costs, which suggests that only those who can afford these fees are likely to receive comprehensive interventions from the DPA in disputes with data controllers. As a result, the exercise of democratic rights seems to be the preserve of only data subjects with sufficient financial resources.

References

Consiglio di Stato, Sez. V, 28.09.2007, Sent. n. 4999, in www.altalex.com/index.php?idnot=38736 (last accessed 15 June 2013).

Corte di Cassazione, Sez. III Pen., Sent. 01.06.2011, n. 21839, www.penale.it/page.asp?idpag=960; www.cortedicassazione.it/Documenti/21839_06_11.pdf (last accessed 15 June 2013).

D.L.gs. 30 June 2003 n. 196, in G.U. 29 July 2003 n. 174 – Supplemento Ordinario n. 123.

DPA, *Cosa è il diritto alla protezione dei dati personali?*, www.garanteprivacy.it/web/guest/home/diritti/cosa-e-il-diritto-alla-protezione-dei-dati-personali (last accessed 15 June 2013).

DPA, *Limitazione all'esercizio dei diritti (articolo 8 del Codice)*, www.garanteprivacy.it/web/guest/home/diritti/cosa-e-il-diritto-alla-protezione-dei-dati-personali (last accessed 15 June 2013).

European Parliament and the Council, *Directive 2006/24/EC of 15.03.2006 on the retention of data generated or processed in connection with the provision of public available electronic communications services or of public communication networks and amending Directive 2002/58/EC*, in OJ L 105/54-63, 13.04 2006.

European Parliament and the Council, *Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, in OJ L 281/31-39, 23.11.95.

Ferrucci A., *Diritto di accesso e riservatezza. Osservazioni sulle modifiche alla L. 241/1990*, in www.giustamm.it/new_2005/ART_2005.html (last accessed 15 June 2013).

Garante per la protezione dei dati personali, *Accordo di Schengen. Audizione parlamentare del Presidente del Garante – 12 luglio 1999*, 12 July 1999, wwww.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/48005 (last accessed 15 June 2013).

Garante per la protezione dei dati personali, *Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1079077 (last accessed 15 June 2013).

Garante per la protezione dei dati personali, *How can you protect your personal data?* http://www.garanteprivacy.it/home_en/rights#how (last accessed 15 June 2013 (last accessed 15 June 2013)

Garante per la protezione dei dati personali, *Relazione 2003*, http://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali (last accessed 15 June 2013)

Garante per la protezione dei dati personali, *Relazione 2011*, http://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali (last accessed 15 June 2013)

Garante per la protezione dei dati personali, *Video Surveillance decision dated 8 April 2010*: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1734653 (last accessed 15 June 2013).

Personal Data Protection Code http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf (last accessed 15 June 2013)

TAR Firenze, Sez. I, 12.05.2011, Sent. n. 80, in www.giustizia-amministrativa.it/DocumentiGA/Firenze/Sezione%202/2011/201101050/Provvedimenti/201300220_01.XML (last accessed 15 June 2013).

TAR Sardegna, Sez. II, 02.08.2011, Sent. n. 865, in www.giustizia-amministrativa.it/DocumentiGA/Cagliari/Sezione%202/2011//201100270/Provvedimenti/201110865_01.XML (last accessed 15 June 2013).

Tribunale di Milano, Sent. 04.02.2009 and Corte d'Appello di Milano, Sent. 11.05.2010. www.garanteprivacy.it (last accessed 15 June 2013).

List of Abbreviations

ANPR – Automatic Number Plate Recognition

ATM - Azienda Trasporti Milanesi which manages public transport in Milan

CCTV – Closed Circuit Television

CED - Centro Elaborazione Dati (Data Elaboration Centre)

CSM - Consiglio Superiore della Magistratura (Supreme Magistrate Council)

DP Code – Data Protection Code

DPA – Data Protection Authority

EU – European Union

FAQ – Frequently Asked Questions

INPS - Istituto Nazionale di Previdenza Sociale (National Insurance Institute)

NGO – Non-governmental Organisation

TAR - Tribunale Amministrativo Regionale (Administrative Regional Tribunal)