# Today is the tomorrow we should have worried about yesterday: a proposal for an Italian law regulating usage, retention and deletion of georeferenced and chronoreferenced automatically collected data containing unique user identifiers.

**Gianni Bianchini**
Department of Information Engineering
University of Siena
<giannibi@dii.unisi.it>

**Marco Calamari**
The Winston Smith Project
<marcoc@winstonsmith.info>

**Andrea Glorioso**
Binary Only Consulting
<andrea.glorioso@binary-only.com>

**ABSTRACT**

The necessity of regulating automatic data collection is incredibly urgent today. A large part of data collections, even though they do not directly contain personal or sensitive data, allow for their inference through cross-referencing of other data bases, usually anagraphical or commercial information.

Current examples of such data collections are web server logs, GSM positional cell data and RFID data. More generally, all georeferenced or chronoreferenced data collections that contain UUID (unique user identifiers) easily allow for inferring personal and/or sensitive data using one or more of those features as "master keys".

These data are usually collected for specific purposes but can be easily cross-referenced, and as such they are destined to multiply themselves as information technologies deeply enter the most common spheres of our everyday life.

The serious dangers that such data collections pose to the right to privacy of individuals are doomed to rise exponentially. Therefore, a regulation regarding this kind of data collections is desirable to counter the impact of new technologies on personal privacy without negatively affecting their diffusion and positive effects. [Brown2004]

A possible approach to such regulation would be the definition of fair but mandatory data retention terms [Calamari2004], with the additional requirement that collected data be used for their primary goal only. Exceptions to the above requirements should be allowed but should be reported to the national Privacy Authority. Moreover, suitable standards concerning data deletion procedures should be formalised [Calamari2003].

Such a regulation would thus cover all data collections obtained through RFID [Bianchini2004], GSM cell data, web logs and all types of potential data collection means, such as wireless networks. This would allow for the anticipation of several kinds of problems, and avoid "post facto" interventions on passively accepted situations which every new technology necessarily creates.

This paper discusses a law proposal [WSP2004] developed by the Winston Smith Project[1] which will be submitted to the Italian legislative bodies in a forthcoming future. The data retention issues that this law proposal will consider are investigated, as well as the relationships of the proposal itself

1 http://www.winstonsmith.info/pws/index-e.html

with the existing Italian law on privacy.

**INTRODUCTION: A TECHNOLOGICAL PANOPTICON**

It is a common and accepted belief that the age we are living in is an "information age". A stunning set of technological achievements have allowed humankind, or at least a subset of it, to have information of all kinds at its fingertips.

While it is unquestionable that such technological achievements have a series of advantages — in everyday life, as well as in the context of the political and democratic participation of citizens, who can (at least in theory) exercise an unprecedented level of control on activities of their leaders — it is also necessary to recognize the negative effects that this possibility of "information at your fingertips" presents.

Paradoxically, the same technology which allows people unprecedented freedoms to communicate with each other, search for information and keep up to date with the most recent events in social, political and economical arenas, also allows a massive collection and retention of personal and sensitive data.

Given the existence of such technology, the real question becomes not whether it is possible to collect personal and sensitive data (it is indeed possible, and in truth it has been happening for a long time) but rather who controls such data, to which extent it can be used to achieve goals which are potentially illegal — and, even if formally legal, most of the time completely different from what was initially envisioned by the owners of collected and retained data — and what are the legal instruments which citizens possess to counter this phenomenon, which has been made possible by technological progress and is still not fully understood by legislators.

The English philosopher Jeremy Bentham (1748-1832) was famous for designing a new (for the time) kind of prison: the *panopticon* (from the greek words meaning "all" and "observe"). In his writings [Bozovic1995] Bentham defines the *panopticon* as an instrument to lower the total cost that society as a whole had to pay in order to maintain the prisons of the time. Thanks to an architecture which

> "incorporates a tower central to an annular building that is divided into cells, each cell extending the entire thickness of the building to allow inner and outer windows. The occupants of the cells [...] are thus backlit, isolated from one another by walls, and subject to scrutiny both collectively and individually by an observer in the tower who remains unseen. Toward this end, Bentham envisioned not only venetian blinds on the tower observation ports but also mazelike connections among tower rooms to avoid glints of light or noise that might betray the presence of an observer." [Barton1993],

Bentham envisioned that the prisoners would have been unable to understand whether a guardian was actually present or not — thus making the presence of the guardian completely unnecessary.

The concept of *panopticon* was brought out of architectural discussions on the best structure for prisons to the realm of social relationships by the seminal work of the French philosopher Michel Foucault (1926-1984) [Foucault1975]. In "Discipline and Punish", Foucault argued that the power relationships which the architectural structure of the *panopticon* allow are a reality in most parts of society, and especially in those parts of it that are able to exert a strong disciplinary structure on its members — the Army, hospitals, schools.

Foucault's analysis of power relationships is incredibly apt to describe the current situation of our information age. What we are faced with is an incredibly asymmetric distribution of power, in which few agents have access to vast collections of information — related to every single aspect of our life — and the vast majority of people, like Bentham's prisoners, have few or no ways to know whether they are under surveillance or not. And while in democratic systems "punishment" can not be inflicted at the whim of those who have access to such information, we should ask ourselves — and our leaders — whether it is not already punishment enough that our actions and preferences (political, religious, sexual) can be traced, analyzed, potentially used in assessing our perceived ability and possibility to perform certain actions.

If the "panopticon" as a concept is inherently terrifying, the current situation is even worse; Bentham (and also the Big Brother of Orwell's "1984") described a situation of "synchronous surveillance", but the ability to store and retrieve massive databases of log data allow for a form of surveillance *a posteriori* — an "asynchronous surveillance". Being able to infer, from a database of GSM cell data, who was attending a given meeting held on a given date in a given place ten years ago is not only possible with the technology we have today, but is rapidly becoming so economical that in the near future it will be possible to achieve such depth of "data mining" with just a common personal computer.

The situation today — again, "thanks" to technology — is a vast archipelago of archives of personal and sensitive data, physically dispersed in different locations. But, as we argue throughout this paper, the mere possibility of cross-referencing such dispersed data could have potentially fearful effects — and such possibility must be explicitly regulated by the legislator, even in the case that such archives do not contain, in and by themselves, sensitive data. This is the focus of the law proposal by the Winston Smith Project.

**SOME EXAMPLES OF TECHNOLOGIES CURRENTLY USED FOR DATA COLLECTION AND RETENTION**

**RFID-** RFID is an acronym for RadioFrequency IDentification. An RFID system is composed of a transponder tag (usually a very small microchip with a built-in antenna and some amount of persistent memory) and a reader device, whose task is to remotely query one or more tags in order to read the information stored in the memory and to transfer it to a computer [Finkenzeller2003]. In low-end RFID systems, the tag and the reader must be very close to each other (up to a few centimetres), while high-end systems may operate at larger distances and process several tags at once.

Recent years have witnessed a great interest in the RFID technology due to a wide range of applications which are becoming more and more cost-effective as technology develops and the price of individual tags reduces. Application contexts vary from logistics and supply chain automation to security tracking for access control, from inventory management to tracking goods in supermarket shelves and trolleys.

RFID has often been referred to as the natural evolution of the bar code, with basically two major improvements over its forerunner.

Radiofrequency interaction allows for the identification of tags which are far away and "out of the sight" of the reader.

An RFID tag can store enough information to identify uniquely the single item or product it is attached to, while two items of the same kind and with the same origin are usually indistinguishable by the bar code. The Electronic Product Code (EPC) has been developed for the purpose of assigning such unique product

identifiers.

Forthcoming applications of RFID include tracking of airline luggage, performing measurements in critical environments, and identification of bank notes in order to track unlawful transactions. There is a renewed rumour that European Central Bank has plans to start embedding RFID tags in Euro notes.

Several privacy issues have been raised on the extensive use of RFID technology [RFIDMIT2003]. Such issues involve both technological and non-technological questions and basically stem from the simple argument that objects carrying RFID tags can actually "speak about us".

From the technological point of view, one major problem is that tags can easily be hidden or placed out of reach, and so can tag readers. Moreover, tags that have not been properly inactivated may be queried by "rogue" readers outside the environment in which they were originally supposed to be operated. The result is a potential information leak through which unique identifiers may be obtained. Such identifiers may then be linked to the identity of the consumer and cross-referenced with other information by means of the common practices outlined this paper.

**HTTP**— HTTP (Hyper-Text Transfer Protocol) is the protocol currently used on the Internet to transfer hypertext pages (i.e. web pages, although HTTP can in principle transfer any kind of data) between two different endpoints. The most common case in which HTTP is used is when a browser requests one or more web pages from a web server. What most people are not aware of is that every single time they view a web page, their browser's request to the web server is recorded in so-called "log files". A typical entry for a log file might look like this:[2]

> 66.196.90.79 - - [28/Feb/2005:14:51:43 +0000] "GET /pipermail/copywhat/2004-April/000561.html HTTP/1.0" 304 - "-" "Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)"

It takes some time and practice to understand what the cryptic characters above actually mean (there are computer programs which can automatically parse and dissect the information contained in such log files and present a much more understandable report). But just by reading one line of a log file, whoever has access to such file can know:

1. The Internet Protocol address — similar to a telephone number — of the computer who made the request to the web server;
2. The date and time of the request, with a very high precision;
3. The precise web page which was requested;
4. The web page from which the requester was directed to the requested page, if any;
5. The type of program which the requester was using

Although in and by itself none of this information is particularly sensitive (the web page requested could very well be, though) the possibility of cross-referencing many single lines of a log file with each other, and with other information coming from other sources, is potentially dangerous.

Almost all other Internet applications (such as e-mail, news reading, etc) and

---

2 The precise formats of log files can differ between different types of web server or even between different instances of the same type of web server, according to the configuration. The general principles outlined above, and the amount of information that can be obtained from a log file entry, however, are valid no matter which particular web server type or web server configuration is being used.

protocols produce similar logs, whose level of detail varies, but is usually more than sufficient to pose serious privacy risks when cross-referenced with data coming from other sources.

**GSM Data Cells**— The cell phones most of us always carry in our pocket rely on a technology (cell transfer) by which each cell phone "binds" with a GSM cell. A GSM network contains thousands of GSM cells.

When powered on [GSMBASICS2000], cell phones bind to the nearest cell of the GSM network. The GSM network control devices write in a log file the identification number (IMEI — International Mobile Equipment Identity, a unique number given to every single mobile phone, typically found behind the battery) of the specific mobile phone which is binding, the cell position and the time of the event. When you walk away from the original cell, the telephone disconnects from the original cell and binds to the next one; also this change is logged in the same manner.

In this way the GSM network continuously logs in a database the position of each phone also if it is not currently in use, but simply powered on.

Since the GSM provider usually knows the name of each person who owns a phone with a given IMEI, in practice it is not only phones which are tracked, but people too.

This database that records and maps in the time and space dimensions everyone who carries a phone, can later be queried to know:

- where a single person was at a certain time;
- a list of people who were at a given meeting, held in a given place at a given time;
- a list of people who are meeting one person (or at least who were near that person) in a given period of time;
- the path and movements of a given person in a given timeframe;
- [insert your worst privacy nightmare here]

In fact, the analysis of GSM positional cell data is rapidly replacing phone eavesdropping as the most common method to perform criminal investigations in Italy [PI49026]. This would be not a bad thing in itself (assuming, of course, that a specific criminal investigation is actually useful and conducted in a legal manner) but the real point is that data collected through these investigations, if not suitably protected, can be quite easily abused, violating basic privacy rights of people.

**THE LEGAL AND POLITICAL LANDSCAPE IN ITALY**

The field which the law proposal by the Winston Smith Project is going to address (if ever it is accepted) is regulated by two recent laws:

1. "Codice delle comunicazioni elettroniche - Dlgs 259/2003" (Law on Electronic Communications)

   This law mainly regulates radio frequencies and their usage for radio and television broadcasting. However, this law contains the only time limit on mandatory data retention, regarding user connections to Internet Service Providers (ISP), phone traffic data and GSM cell data. The mandatory retention term is three years. All other data retention terms in Italy are not mandated by law, but extrapolated from old police or court regulations.

For example, the five years usual term for generic data retention is deduced from the retention term of hotel registration data (yes, in Italy people must identify themselves to sleep in an hotel); such term is a consequence of the statutes of limitation of civil and criminal prosecution.

2. "Codice in materia di protezione dei dati personali — D.L. 196/2003" [DL196] (Law for the Protection of Personal Information). This is the most comprehensive Italian law regulating the recording and usage of personal data. It is heavily bent towards citizens' rights; consider, for example, how D.L. 196/2003 states that every person is always the owner of his personal data, even if a part of such data is physically owned by others; this means (at least in theory) that everyone can obtain a copy of his personal data from any organization that has it at a given time, and mandate correction or cancellation of them at will. However, several exemptions from this rule are possible due to (more or less understandable) principles of public interest. All in all, the main defect of D.L. 196/2003 is that it is rooted in an old "*paper record and database*" concept and does not truly assimilate the modern concept of automated collection, retention and dissemination of information via electronic instruments.

3. Special anti-terrorism laws of the late seventies and early eighties [DL625] [L1980-15] which are still fully valid today even though they were supposed to be "emergency laws" (and the general Italian attitude with regards to the power of "power" over individuals [Mereu2000]) pose other indirect but heavy limitations on privacy rights when preliminary criminal investigation are performed for a wide range of law violations.

4. In Italy the Privacy Authority (created as per art. 28 of European Directive 95/46/EC [EC9546] is the "Ufficio del Garante per la Privacy" (Bureau of the Ombudsman for Privacy). The Privacy Authority has (at least in theory) the power to ask for corrections to laws, to audit the application of D.L. 196/2003, and to prosecute directly for privacy violations. In fact, the current approach of the Privacy Authority is to regulate the consequences of new technologies for the individual privacy *a posteriori*. This approach does not try to anticipate problems, but only to correct them when they become evident (and often too large to be corrected). Some sign of a change in this approach has arisen in the present attempt to regulate RFID (Radio Frequency Identification Devices) and prepaid digital TV smartcards [GP2004]. In addition this year the head of the Privacy Authority will change. The highly respected professor Stefano Rodotà, who headed the Privacy Authority from the beginning, will leave, and rumors suggest that this change risks to undermine (at least in some extent) the independence of the Privacy Authority from the government.

The main problem which the law proposal of the Winston Smith Project tries to address is that the continuous and widespread collection and retention of data in different data bases, even when not directly linked to a specific person through anagraphical means, can lead to huge privacy risks if coherent measures to stop cross-referencing between such data bases are not put into place.

Article 1, commas 8-10 of the law proposal help framing the problem:

> Comma 8. "*User profiling*" is any operation which, by treating data coming from automated collections of personal data, produces derived data that highlight or collects information on users or on behaviour, which can be associated with specific persons.

> Comma 9. A "*Unique User Identifier*" (UUID) is any item of data which allows to group a collection of data and attribute it to a specific user (who is not identifiable through anagraphical means), such data not being necessarily personal or sensitive and having been previously collected in an anonymous form.
> Examples of such data collection are GSM cells data, where the UUID is the IMEI code, or data collected through an RFID, where the UUID is the device serial number.
>
> Comma 10. "*User identification*" is any operation which implies computing or cross-checking automated collections of personal data, either with each other or with other kinds of data, which can achieve, possibly through the usage of a UUID, the anagraphical identification of a user as a physical person.

Once data is collected in one or more data bases, the action of cross-referencing such data ("*User Profiling*" in the text of the law proposal) can lead not only to the "identification of a user as a physical person" (text of the law proposal) but to the reconstruction of the overall life of someone – what a person has done, what he bought, where he went to, etc. Since in and by itself the collected and retained data is not necessary personal and/or sensitive, the provisions of D.L. 196/2003 do not necessarily apply.

This is a case of over-zealously analysing the trees, but missing the forest; or rather to miss the fact that in the information society, it is not only information *per se* which is important, but the relationships between such pieces of information and the ease with which these relationships can be created, analysed – possibly through more and more powerful automated tools – and used for purposes and goals which are often neither the same for which data was collected, nor have a particularly relevant social value. The general trend seems to consist in such cross-referenced information to be used for commercial purposes: if you are using a mobile phone in a shopping mall and you happen to walk beside an RFID reader which recognizes your new [put a random brand name here] shoes, maybe you could be a potential buyer for receiving harassing phone calls from the sales department! Or this "logical inference" can be stored in a database, to be used later on – even years later.

Besides commercial usage – which is in and by itself rather disputable anyway – this cross-referencing possibilities pose serious risks for our social and political life, too. If you tend to visit shopping mall X but never buy brand Y, preferring brand W which just launched a massive "Help Africa" campaign, and you happen to have visited web site Z (maybe the website of an environmental organization?) several times in the past year, are you a "good" citizen or are you on the borderline of antisocial behaviour?

While all of this might seem science fiction, Italy has a long history of collection of personal data for political purposes, both during Fascism and throughout the life of our young Republic – even though our Constitution clearly states that no one can be discriminated on the basis of his or her political beliefs.

The "better safe than sorry" attitude – collecting data and not using it, except in cases of (supposed) need – is dangerously colliding with the old latin saying "Quis Custodiet Ipsos Custodes?" (who guards the guardians?). It is not acceptable to let collection of data continue indiscriminately, not in a technological environment which allows refined and deep analysis on such data – even more so when these data collections are not formally protected by law, not being "sensitive enough", that is, as far as we know, the current attitude of the Italian Privacy

Authority towards log data.

**A LEGAL SOLUTION: THE LAW PROPOSAL BY THE WINSTON SMITH PROJECT**

The Winston Smith project is an organization of people concerned with issues of privacy in the context of new digital technologies. The project was founded in 1999 with two different goals in mind:

1. Promote a privacy culture in the Internet, producing and distributing documents and HOWTOs[3] for users who need or want privacy and/or anonymity and for people who want to volunteer time and resources to build servers for privacy (i.e. Anonymous Remailers [Poli2004] and Freenet [Clarke1999] nodes);
2. Be a living proof-of-concept and a test of feasibility in building and operating an anonymous organization through technological instruments. Anonymity can be seen as the strongest embodiment of privacy: being technically able to remain totally anonymous, an individual can freely choose his or her "grade" of anonymity, and consequently the extent of privacy he or she needs.

This last point has interesting consequences; the public members of Winston Smith Project are not physical people but two main kinds of entities, virtual identities that are used by the Winston Smith Project to interact with the rest of the world.

The names used by the group come from George Orwell's novel "1984"; "Winston Smith", the visionary (the "1984" protagonist) and "Emmanuel Goldstein", the number one public enemy of the Big Brother.

Both identities use technological, well-established instruments to interact in a normal (but totally anonymous) way via the Internet. E-mails are signed with pgp keys [Menezes1996] which guarantee the identity of the sender; such e-mails are sent via anonymous remailers [Chaum1998] and/or pseudonym server [Mazières1998] which guarantee the non-traceability of messages. Web pages are published on Freenet [Clarke1999], guaranteeing the anonymity both of their publishers and of their readers. Last but not least, the process of accepting new members in the Winston Smith Project is done by Winston Smith himself, by signing the pgp key of the new member. Of course, all the members of the Winston Smith Project usually publicly declare their association to the project, because in this project anonymity is just a proof-of-concept - all their activities are, of course, fully legal.

The law proposal was "engineered" (yes, we come from the *Dark Side,* most of the members of the Winston Smith Project are engineers!) considering the current Italian situation.

Since creating a completely new regulation, with new roles, procedures and sanctions would be extremely onerous and complex, the general idea of the law is to frame its regulations into the existing law infrastructure for protection of personal and sensitive data. In Italy (but this applies to most E.U. Countries) such infrastructures are embodied in the Law "Codice in materia di protezione dei dati personali — D.L. n. 196/2003" (from now on "D.L. 196/2003").

The key points of the law proposal are:

---

3 An HOWTO is a "an informal, often short, description of how to accomplish some specific task. They are generally meant to help non-experts, and may leave out details that are only important to experts, and may be greatly simplified from an overall discussion of the topic. See procedural knowledge for a discussion of what sort of knowledge is imparted, and how far it can be imparted, in how-tos." (see http://en.wikipedia.org/wiki/HOWTO).

1. Mandate a general data retention term which is coherent with invoicing/administrative/technical needs – but not more than that (art. 2, comma 2 and comma 4);
2. Mandate the deletion of automated collected data after the retention term has expired, and define procedures, roles, duties and sanctions if the data is not deleted (art. 2, comma 2);
3. Prohibit, with some specific and regulated exceptions, any handling of data for different reasons or goals for which than it has been collected (art. 3);
4. Generally permit for any data retention and use of automatically collected data, provided that detailed information about this exception is communicated to the Privacy Authority, as for the collection of highly sensitive personal data [DL196];
5. Allow certain predefined and common types of data treatment to be performed in a predefined way, even without communication to the Privacy Authority (i.e. ISP can retain logfiles containing modem access data for one month in order to bill users);
6. Give roles and responsibilities to those subjects which have already been created within the D.L. 196/2003;

**CONCLUSIONS**

The law proposal was first shown to the representative of the Privacy Authority, that represent it at the E-Privacy 2004 Conference[4] (incidentally, the representative's speech during such conference focused on the attempt of the Privacy Authority to shorten data terms for mandatory retention of phone traffic and GSM cell data, from 5 to 3 years)

The general reaction to the law at the time seemed to imply that it was of some interest, even though the proposal seemed to be somewhat "extreme" and it had the big drawback of imposing extra burden on the already quite-stretched capabilities of the human resources of the Garante.

In order to build a more general support for the law proposal, the Winston Smith Project submitted it to senator Fiorello Cortiana (Green Party). In February a formal meeting was asked and organized, during which three representatives of the Winston Smith project (Gianni Bianchini, Marco Calamari, Lorenzo Cipparrone) presented the project and the law proposal, asking for support in submitting the law to the Italian Parliament during 2005. Unfortunately, no reply was heard from the office of the Senator until now – but it should be noticed that the Senator, as a strong supporter of the "No Software Patents" movement,[5] has been quite absorbed by the political consequences of the Council decision on the matter.

The Winston Smith Project will continue to work on the law proposal, refining it where necessary, either through internal analysis or thanks to external contributions, suggestions, criticisms, and trying to find a political and civil consensus broad enough to submit the law in the Italian Parliament (and hope for it not to get killed in the tar pits of the Italian legislative processes).

---

4 http://e-privacy.firenze.linux.it/ .

5 http://www.nosoftwarepatents.com/ (amongst others).

**APPENDIX: THE LAW PROPOSAL**

LAW PROPOSAL (version 6 of Feb 8, 2005)

on “Regulations for the collection, usage, retention and deletion of georeferenced or chronoreferenced data, containing unique user identifiers, through automatic devices”

*PART I — GENERAL PRINCIPLES*

*Art. 1*
*(definitions)*

Comma 1. A “computer program” (software) is a program for an electronic computer (either an operating system, or an application program)

Comma 2. A “device for the automatic collection of personal data” is any physical device or computer program which automatically stores or transmits, on a temporary or permanent basis, data regarding its own functioning or the functions of other devices and computer programs, which can potentially contain personal or sensitive information (as per D.L. n.196/2003) or from which such information can be found or obtained.

Examples of such personal data collection devices are GSM networks, RFID devices, World Wide Web servers and video surveillance systems, and all the devices which automatically store, in digital files or analogue media, information produced by individuals' activities, like short text message, GSM terminal positio, visited web pages, locations and times of presence, biometric data.

All data collections related to individuals' activities which are either georeferenced (i.e. contain data on geographical position) or chronoreferenced (i.e. contain data on time) and contain Unique User ID (UUID) are a part of such category.

Comma 3. A “*manager of automatic data collections*” is the person/entity with responsibilities for data management (as per D.L. n.196/2003) or, lacking such person/entity. the person/entity in charge of the organization of data collection devices, or, lacking such person/entity, the person/entity who is responsible for operating the data collection devices.

Comma 4. An “*automated collection of personal data*” is any archive or data flow generated by a device performing the automated collection of personal data.

Comma 5. A “*log file*” is any collection of information gathered through a physical device or a computer program which is useful or necessary for its functioning, but is not its main function.

Comma 6. A “*data flow generated by a device for the automated collection of personal data*” is the transmission of data through a device for the automated collection of personal data, towards other devices or subjects who can potentially use or store it.

Comma 7. A “*backup procedure*” is the set of administrative procedures, computers, computer peripherals and data storage supports which are used to guarantee the temporary conservation of data archives copies, in order to allow for archiving or restoring such data in case of necessity.

Comma 8. "*User profiling*" is any operation which, by treating data coming from automated collections of personal data, produces derived data that highlight or collects information on users or on behaviour, which can be associated with specific persons.

Comma 9. A "*Unique User Identifier*" (UUID) is any item of data which allows to group a collection of data and attribute it to a specific user (who is not identifiable through anagraphical means), such data not being necessarily personal or sensitive and having been previously collected in an anonymous form.
Examples of such data collection are GSM cells data, where the UUID is the IMEI code, or data collected through an RFID, where the UUID is the device serial number.

Comma 10. "*User identification*" is any operation which implies computing or cross-checking automated collections of personal data, either with each other or with other kinds of data, which can achieve, possibly through the usage of a UUID, the anagraphical identification of a user as a physical person.

*PART II — AUTOMATED COLLECTION OF PERSONAL DATA*
*(obligations for subjects doing automated data collections)*

Art. 2

Comma 1. Automated collections of personal data can be performed only to allow, control or ease the functioning of detection devices, computers or computer program.
Automated collections of personal data can not be used to achieve different goals from the ones for which they have been put in, with the exceptions contained in Art. 2, Comma 2.
Automated collections of personal data can be stored only for the time necessary to the technical goal for which they have been collected, and must be subsequently deleted, in an accountable way, from their original supports and from all the copies generated by any backup procedure.
During their existence, such collections will be subject to the norms and the regulations of D.L. n.196/2003 (and subsequent modifications).

Comma 2. In case the person responsible for the automated data collection wishes to treat the collected data to achieve different technical goals than originally intended, the data will be considered personal and/or sensitive information (as per D.L. n.196/2003, and subsequent modifications), depending on the kind of personal information that might be contained.

Comma 3. The person responsible for the automated data collection who wishes or must proceed to further treatment or storage in excess of the provisions of Art. 2, Comma 1, must give appropriate notice to the Privacy Authority.
The person responsible for the automated data collection must make public the collection, its modes of acquiring data, its goals, and the retention, copy and deletion procedures, both to the Privacy Authority and to all the subjects whose data can be potentially collected.
The methods for the communication and the individuation of the interested subjects will be detailed in the subsequent Implementation Rules.
The Implementation Rules will contain a list of types of data treatment which are excluded from notification to the Privacy Authority.

Comma 4. Where the law does not state otherwise, the maximum period of retention of data collected through automated collection of personal data or data derived from personal data is 60 days.

Comma 5. If the person responsible for the automated data collections does not comply with the deletion of data in the proper timeframe, or treats them, or stores them beyond the allowed timeframe, or transmits them to third parties, s/he will be subject to the sanctions for the same kind of violation, contained in D.L. n.196/2003 (and subsequent modifications)

*PART III – COMUNICATION OF PERSONAL DATA COLLECTED THROUGH AUTOMATED COLLECTION OF PERSONAL DATA*
*(access to automated collections of personal data on behalf of the judicial power or public security authorities)*

*Art. 3*

Comma 1. On request of the competent Judge and/or of the Authority for Public Security nominated by such a Judge, in the context of investigations related to pending penal actions or preliminary investigations, the person responsible for automated data collection must make the data coming from automated collection of personal data available only to the extent which fulfills the goals of the request.

Comma 2. In the text of the Implementation Rules, certain automated collections of personal data for which the timeframe of retention will be less than stated by Art. 2, Comma 2, will be listed.
The text of the Implementation Rules will determine the procedures for the retention and deletion of data and the procedures for their request on behalf of the authorities.

Comma 3. It is prohibited to request generalized disclosure of data which could be used to create personal data archives, related to entire groups of physical or juridical persons, which are not globally the subject of a court investigation.
The disclosure must be strictly limited to the data required by the procedures or investigations, and the data must be retained only for the strictly necessary time frame.

Comma 4. The data transmitted to the competent Judge and/or to the Public Security Autority must be used only to achieve the goals for which they have been requested, and shall not be used for different goals without a new and different authorization.
When the usage of data ends, all the copies of the data must be deleted, with the exception of data which the law obliges to retain.
In this case, data should be treated and possibly made public with the same provisions of the action and/or investigations that requested them.

*PART IV – FINAL DISPOSITION*
*(Implementation Rules)*
*Art. 4*

Comma 1. Within 180 days after this law becomes effective, the Government shall publish the Implementation Rules necessary to its full application.

**BIBLIOGRAPHY**


[Barton1993] Ben F. Barton and Marthalee S. Barton. "Modes of Power in Technical and Professional Visuals." *Journal of Business and Technical Communication* **7.1**, 1993, 138-62

[Bianchini2004] G. Bianchini, "*RFID - Automatic RadioFrequency Identification: the impact on personal privacy*", Proceedings of E-privacy Italian Conference 2004 (in Italian)
http://e-privacy.firenze.linux.it/atti/ep2004-Bianchini-RFID.pdf

[Bozovic1995] M. Bozovic (ed.), "*The Panopticon Writings*", Verso, London, 1995

[Brown2004] I. Brown, D. Korff, "*Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime*", UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004
http://www.informationcommissioner.gov.uk/eventual.aspx?id=6840

[Calamari2004] M. Calamari, "*Privacy issues in electronic communication*", Proceedings of E-privacy Italian Conference 2004 (in Italian)
http://e-privacy.firenze.linux.it/atti/ep2004-Calamari-sfera_privacy.pdf

[Calamari2003] M. Calamari, "*E-Privacy and infosmog, an integrated approach to privacy protection of personal data*", Proceedings of E-privacy Italian Conference 2003 (in Italian)
http://e-privacy.firenze.linux.it/2003/atti/Ep2003_E-privacy_e_Infosmog.pdf

[Chaum1998] David Chaum, "*Untraceable electronic mail, return addresses, and digital pseudonyms*", Communications of the ACM, n. 2, 1981
http://world.std.com/~franl/crypto/chaum-acm-1981.html

[Clarke1999] Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong, "*Freenet: A Distributed Anonymous Information Storage and Retrieval System*", 1999
http://freenetproject.org/freenet.pdf

[DL196] "*Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali*", 2003
http://www.garanteprivacy.it/garante/doc.jsp?ID=1105372

[DL625] "*Decreto Legge 15 dicembre 1979 n. 625 — Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica*" ("*Urgent measures for the protection of democracy and public security*"), *Gazzetta Ufficiale 17 December 1979, n. 342*, 1979
http://www.giustizia.it/cassazione/leggi/dl625_79.html

[EC9546] "*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*", 1995
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

[Finkenzeller2003] Klaus Finkenzeller, "*The RFID Handbook*", J. Wiley & sons, 2003

[Foucault1975] Michel Foucault, "*Surveiller et Punir*", Gallimard, Paris, 1975

[GP2004] Ufficio del Garante per la Privacy, "*La protezione dei dati nell'ambito di quattro temi di attualità: gestione delle carte di 'fedeltà', tv satellitare e*

*interattiva, tecniche RFID e videotelefonini. La consultazione pubblica indetta dal Garante*", 2004
http://www.garanteprivacy.it/garante/doc.jsp?ID=1078227

[GSMBASICS2000] "*Basics of GSM*", http://www.pulsewan.com/data101/gsm_basics.htm

[L1980-15] "*Legge 6 febbraio 1980, n.15 — Conversione in legge, con modificazioni, del decreto-legge 15 dicembre 1979, n. 625, concernente misure urgenti per la tutela dell'ordinde democratico e della sicurezza pubblica (antiterrorismo)*" ("*Conversion to law, with modifications, of law decree 15 december 1979, n. 625, regarding urgent measures for the protection of democracy and public security (antiterrorism)*"), Gazzetta Ufficiale *7 febbraio 1980, n. 37, 1980*
http://www.giustizia.it/cassazione/leggi/l15_80.html

[Mazières1998] David Mazières, M. Frans Kaashoek, "*The Design, Implementation and Operation of an Email Pseudonym Server*", Proceedings of the 5th ACM Conference on Computer and Communications Security, 1998
ftp://cag.lcs.mit.edu/pub/dm/papers/mazieres:pnym.pdf

[Menezes1996] Alfred Menezes, Paul van Oorschot, Scott Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1996.

[Mereu2000] Italo Mereu, "*Storia dell'intolleranza in Europa*" ("*History of intolerance in Europe*"), Bompiani, 2000

[PI49026] Punto Informatico, "*Intercettazioni, Italia in testa*", 2004
http://punto-informatico.it/p.asp?i=49026

[POLI2004] Francesco Poli, "*An introduction to Anonymous Remailers*", Proceedings of E-privacy Italian Conference 2004 (in Italian)
http://e-privacy.firenze.linux.it/2004/atti/ep2004-Poli-remailers_printable.pdf

[RFIDMIT2003] *Proceedings of RFID privacy workshop @ MIT*, November 2003.
http://www.rfidprivacy.org/2003/agenda.php (not working at the time of writing this paper)

[WSP2004] The Winston Smith Project, "*A law proposal on collection, use, retention, and deletion of georeferenced, chronoreferenced data containing unique user identifiers*" (in Italian), 2004
http://www.winstonsmith.info/proposta_di_legge_rdp_v6.rtf