# AMBIENT INTELLIGENCE AND DATA PROTECTION. CHALLENGES AND OPPORTUNITIES AFTER THE LISBON TREATY

by Shara Monteleone

## Introduction

There is an increasing need for legislation to keep apace with the technological developments, which have proved to both support and threaten individuals' fundamental rights.

The paper considers the impact of '*Ambient Intelligence* (AmI) and of profiling techniques on the right(s) to privacy and data protection. It approaches the topic of AmI technologies – which create a daily environment completely computerized and responsive to people's needs - under two main perspectives. On the one hand, the increasing 'security emphasis', that characterizes major initiatives of the current European policy and that allows us to foresee the advance of unexplored '*AmI detection scenarios'*. On the other hand, the consequences of the entry into force of the Lisbon Treaty in this field, including the existence of a legal basis for a new comprehensive legislative framework, the binding value of the Charter of Fundamental Rights and the new role of the European Parliament.

After a brief overview of AmI applications and of the 'Internet of things', the first part of the text focuses on the profiling technique, as one of the key elements of AmI environment, thanks to which computers can process large amounts of previously collected data in order to extract recurrent patterns and make decisions in an automated way. These techniques have been recognized in recent years as major threats to privacy and data protection rights, due to the risks of unauthorized accesses and misuses of these data. Profiling techniques are increasingly used also for security purposes in counter-terrorism activities (i.e. new *detection technologies*), without receiving, so far, the due legal attention, despite the serious issues that may arise, such as the risks of false positives, overlapping of profiles, unfair decisions, indirect discrimination.

The second part concentrates on the consequences of the entry into force of Lisbon Treaty. A new legal basis for data protection as fundamental right, the abolition of the pillar structure and the binding nature of the Charter (which contains a specific provision for data protection) are the most evident and direct effects, which allow us to hope for a better enjoyment of this right and for a more comprehensive legislative framework. This framework will include areas traditionally not covered by Data Protection directives, such as police and judicial cooperation in criminal matters. Although this is not the main focus of this paper, it is worth mentioning that indirect effects of the Lisbon Treaty on data protection legislative agenda include the new role of the European Parliament (EP) firstly in the law-making process and, secondly, in both the European external relations and its enhanced collaboration with other European bodies (among which FRA and EDPS).

Finally, the legal-technical approach adopted by the European Digital Agenda will be also considered.

## 2. The AmI environment: a new *habitat*

When the computer revolution started some decades ago, probably nobody could expect that the capabilities and intelligence, only imagined in science fiction films, would become a reality. Technologies, which were used until now in a passive way, are becoming active and personalized in order to respond to individual specific needs or desires.

The expressions Ambient Intelligence, or ubiquitous or pervasive computing, created by computer-science researchers around the world, indicate a quite recent discipline that, taking the advantage of important changes in the Information Communication Technologies, aims at **bringing** ‘intelligence’ to our everyday life environments, making them responsive and sensitive to us (Aarts E. - Marzano S. 2003)·.

While we are becoming accustomed to sensors that control temperature or lighting in modern houses, the possibilities of Ambient Intelligence go much further than that, allowing the combination of several electronic devices in order to interact in an ‘intelligent’ way with the users, that is, to be adaptive and responsive to features, behaviour and acts of users, thus. People are surrounded by micro sensors and electronic devices incorporated in daily objects (fornitures, clothes, vehicles) distributed in the space and linked each other through networks. These technical tools, with reasoning capability create a new *habitat* (Santosuosso 2011), recognizing and interpreting features, intentions, emotions of people living in, assisting them according to preferences, i.e., providing personalized services and anticipating their needs. The AmI perspective, object today of significant investments by governments and that seeks for an increasing role of computers in our life, is the fruit of the development since the ‘80s of the ‘Light Artificial Intelligence’, the movement which abandons the idea to imitate the human brain and adopts a more funcionalistic and pragmatic approach for ICT solutions (Santosuosso 2011)

The legal relevance of these technologies, their invasive nature and the fact that they rely on the collection and processing of personal data make privacy right safeguards and data protection rules, undoubtedly applicable. What is more difficult to say is to what extent and in which manner they should be applied.

The scenarios for possible applications and activities that these technologies are expected to provide are manifold and involve private as well as public spaces. Some examples are the smart homes (e.g. for the intake of proper food), hospitals (for the intake of medicines/health monitoring and assistance), transportation (for increased safety, e.g. controlling the driver’s dangerous behaviour), smart office or campus (for information services or use of remote facilities).

AmI technologies and pervasive computing can impact the individual’s life, changing his/her habits, and manner of relating to the environment: sensors, Rfid tags, cameras or other advanced devices can track items and persons’ movements to collect, match and re-elaborate data in real-time in order to promptly provide individuals with suggestions or other information services. Pervasive computing’ is defined by the Centre for Pervasive Computing, www.pervasive.dk, as next generation computing environments with information and communication technology everywhere, for everyone, at all times”, inspired probably to the Microsoft CEO Stave Ballmer’s statement of 1999 on the future of computing as “anybody, anywhere, anytime, connected to Internet, on any device”.

In the scenarios imagined in computer science many of these reasoning and informative capabilities of the pervasive computing are presented as an innovative way to amplify and facilitate individual choice: the system will offer a range of possible solutions (roads, stores, items to buy), but you ‘choose’ the one with the best rate.

The limitation to freedom of choice is, though, one of the main issues at stake when considering the impact on privacy by AmI technologies (beside the fact that tracking movements in a pervasive computing environment is considered already as invasion of user’s privacy, since the system is always aware of the user’ location and activities). Since everything in an AmI world tends to be automated, the choice of individuals tends in parallel to be reduced: he will decide among packaged possibilities, suggested on the basis of his (supposed) preferences and profiles, without having the occasion to change tastes and opinions (Rouvroy 2008a) . The idea of Mark Weiser, pioneer of pervasive computing, was that pervasive computing will exist when it become so natural that people do not even realize they are using computers and technologies: for that reason devices need to rely on global networks that emphasize wireless technologies, large databases and profiling capability (http://www.ibiblio.org/cmc/mag/1995/apr/last.html).

We still do not know how the world will look in a full AmI, "when everything becomes connected" (Ridges 2008), but 'the situation seems alarming if we put together these visions of AmI (therefore, not yet completely realized) with the already proved experience of data collection and exchange among government agencies and private companies De Hert (2005).

It is possible to notice that, while the main concern of computer scientists is to make the AmI systems as widely accepted for society as possible (Cook 2009), the main concern of the jurists is to verify, on the one hand, the legitimacy of these technologies according to the existing values deriving from the fundamental rights protection and, on the other, to find out legal responses, in order to 'balance' the apparently opposite values (security and predictability, on one side, privacy and self-determination, on the other). In the next sections it will be also discussed how these challenges for privacy right(s) are issued by a particular kind of new technological scenario, what we have called the *AmI detection* (or *security*) *scenario*.

Some steps have been taken in this direction, in order to enhance privacy while developing automated technologies, as shown by the 'privacy by design' approach (i.e. data protection principles embodied into the same architecture of the technical tools, *infra*), but several legal issues remain to be addressed. If, in the AmI space, radio frequency identification devices, incorporated in objects or even in human bodies, allow to wireless gather information and to render the defferent environments interoperable (home, workplace, vehicle, public spaces), could, in this space, fundamental rights – as enshrined in national constitutions and in the Charter of Nice - develop and be enjoyed? In other words, is it a "rights and liberties friendly ambient" (Santosuosso 2011)?

While it is not possible at the international level to find a uniform approach and different regulatory regimes are currently available of public, private or co-regulation nature (from the intergovernmental Convention n.108/1981 to the Network Global Initiative), one answer could be the adoption, within an improved general framework, of relevant sector-based rules, more adaptive to AmI contexts and privacy needs.

At European level, a renewed legal framework for data protection is already *in fieri* as the Commission announce the intention to adopt in the course of 2011 a proposal for a new legal framework (EU Commission 2010a).

## 3. Increasing security emphasis and data protection instance.

### 3.1. A preface.

As it has been observed (Liberatore 2005) we have been assisting in the last decades to a special emphasis for security issues in the political and legislative agenda. It is possible to find many traces of the increasing concerns for public security in the current international and regional policies. The Convention of Budapest on Cybercrime and the Data Retention Directive 24/2006/EC are some examples. Regarding EU policy, these trends are becoming very 'strategies,' as we can observe in several hard- and soft-law legal documents (e.g., European Council Stockholm Program, *infra*).

Although the issue of possible conflict between fundamental rights and security is not new (Zucca, 2008), the post-09/11 effects have tremendously sharpened it (Francioni F.- Ronzitti N (eds) 2011), especially as far as privacy and data protection are concerned (De Hert, 2005). Some of the counter-terrorism measures already adopted by the U.S. as well as by the EU raised several doubts about their 'constitutional' legitimacy (Sheinin et al., 2009) and about the balancing principle as a proper approach for such a dilemma. Amongst them, particularly interesting, for their possible and predictable connection with AmI scenarios, are the new types of 'detection technologies', the aim of which is to empower the practices of the fight against terrorism. Privacy issues seem to arise not only from the increasing resort during the last decades to these mechanisms but mainly from the invasive character of the new technologies (Leenes et al. (2008), that enables them to penetrate more deeply into the private sphere of the individuals than ever before (e.g., body scanners).

The situation could become thornier with the future development and use of AmI technologies for these purposes (Maghiros, 2003). Some authors (Friedewald et al. 2007) argue that AmI technologies tend to go beyond the currently existing privacy guarantees, but also that they are changing our expectations of privacy, in terms of its diminution, given that these technologies become a common part of our life. In other words, we are becoming costumized to see our privacy limited and, worst, to be commonly considered as potentially 'suspicious,' as demonstrated by the increasing use of detection technologies.

As has been argued, there are no simple solutions to reach the right balance between privacy and security, just as there are no simple solutions to ensure that AmI is beneficial for citizens, industry and governments as well. The only alternative seems to be to address those (emerging) threats one by one and to make everyone involved in safeguarding his/her privacy, identity and security (Wright et al., 2008). Surenly, a new legal-technical literacy is unavoidable. Legal and philosophical debates in the context of balancing privacy and security have been lit up (Liberatore 2005); (Francioni F. 2007). Against the advocates of the so called "I've got nothing to hide" argument, it is sustained here that it is necessary to recognize that the issue at stake is not to fully accept or to totally renounce the relative security and surveillance policies, but to verify the related oversight procedures that governments are expected to put in place (Solove, 2007).

Considering the legal instruments available at the moment in Europe, it might be useful to evoke here that the European Data Protection (DP) Directive does not apply to data processing carried out for the purposes of public security, defense and activities in the area of criminal law (the so called 'third pillar' of the pre-Lisbon Treaty). After several debates on the opportunity to extend data protection also to these areas of action, the European Council has adopted a Framework Decision in 2008 (2008/977/JHA), defining the data subject's rights in the context of criminal investigation and other police practices (including profiling): the right to be informed, the right to access, rectify or erase data, activities that should also be made known to third parties to whom the data have been disclosed and a specific obligation to ensure a high quality of data is also provided for, in order to guarantee the correctness of the consequent profiles (Wright et al., 2008). Nevertheless, as stressed by the EDPS (EDPS PressNews, 2008; Opinion 2009/C 128/02), this decision only covers police and judicial data exchanged among Member States or EU authorities and not to domestic data, leaving the level of protection unsatisfactory.

In the last part of the paper it will be discussed how this situation is likely to change with the recent entry into force of the Lisbon Treaty. Before acknowledging the opportunities and challenges issued by the Lisbon Treaty, the following sections will illustrate briefly some of the major AmI environment and techniques, potentially challenging privacy and data protection (e.g. biometric profiling) and those characterizing the security measures of post - 9/11 (the new ‘detection technologies’); the discussion will turn, after, on the legal instruments of HR law currently enforceable towards such measures (e.g. the Art 8 ECHR, in the *Marper* case), as well as on the need for reviewing the current legal framework.