Analysis of the Legal Challenges required for the Deployment of Network Robot Systems in European Urban Areas

Alberto Sanfeliu[1], Albert Punsola[2], Yuji Yoshimura[2], Maria Rosa Llácer[3],
Maria Dolors Gramunt[3]
[1]Institut de Robòtica i Informàtica Industrial (UPC-CSIC),
[2]Barcelona Urban Ecology Agency
[3]Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT-UB)

Abstract—**In this article we present a study of the legal challenges that must be solved in order to deploy robots and sensors in urban areas. We start describing urban issues and robot deployment problems that can derive in legal aspects. Then we identify the main challenges and then we focus in the privacy issue, discussing the concept, the European laws concerning these topics and its approach in networking robots in urban areas. Moreover, we describe some of the problems with cameras and wireless communications systems and we describe one solution for the privacy issue in the case of Bluetooth. Finally we present some open problems in the privacy issue.**

I. Introduction

The ethics in robotics has been studied for some authors, for example Asaro's article [14] argues that many of the issues regarding the distribution of responsibility in complex socio-technical systems might be best addressed by looking to legal theory, rather moral theory. In [13], Asaro analyses how legal theory might be applied to robots. Schweitzer in the article "Robotics - chances and challenges of a key science" [16], discusses what are the challenges in the development of robots into intelligent machines and describe some examples in several fields, for example medicine, service and education. Solum in [17], argue if an artificial intelligent (a robot) become a legal person and McNally and Inayatullah [15] discuss about the rights of the robots.

In this article we are more pragmatic, instead of trying to find how far a robot can be compare to a human being, we try to analyze what are the legal challenges that we will find deploying robots in urban areas, and more specifically we will analyze the impact of the networked robots in the privacy issue.

The idea of a network of robots circulating in the streets and performing different tasks emerges as a foreseeable contribution to the improvement of quality of life in urban areas. Now it is at an experimental stage, but it could become reality in the near future. In order to navigate and interact with humans, the networking robots need to get data from the environment. They can do that by themselves or with the help of some infrastructure placed in public space, for example trough cameras or sensors. The use of environment sensors and robots in private and public spaces in presence of people open the issue of privacy. If a robot captures the image of traffic light or a bench nothing happens, but if the camera captures people's face then it becomes personal data that should be treated by country laws. This example –that could be extended to other sensors-shows that networking robot deployment in cities involves not only technical or social challenges, but also legal ones.

II. From private to public sphere

For decades, the application of robotics has been limited to the industrial field. Mass production and the need to increase productivity to compete in the market have encouraged the incorporation of robots in the factories. They have been used for multiple tasks, for example assembling, painting, transporting, packaging and others, where the speed and precision is required. Recently, domestic robots have appeared in our lives and they are used for household cleaning and maintenance. Although their sales are not still massive, they have reached a high popularity in some countries as Japan or South Korea. Lack of time and the demands of leisure society can help domestic robots to become more widespread in the near future.

Industrial and domestic robots have different designs and functionalities, but they have in common, the fact that they can do tasks in the private sphere. As we have mentioned, the next step for robots development and presence in society will be the public space. Several reasons can explain this trend and they can be summarized in one sentence: there are high expectations of improving the urban management due to the increase of live complexity. Moreover, the mankind is becoming more urban than ever before. According to UN statistics in 2008 and for the first time in history, more people are living in urban areas than in rural areas.

The need for a more rational and efficient management of cities is linked to solving everyday problems like waste management, pollution monitoring or mobility co-ordination. It also has a strong economic and ecologic dimension. City Councils want to show the efficient use of the taxpayer's money and a clean city with less pollution and healthy environment. It cannot be forgotten that in many countries the ageing population might need more assistance in private and public spaces. Considering this context, the following issue arises: the potential contribution of robots to enhance city management and to improve live style require changes in the present laws.

III. Legality as a determining factor

From the technical point of view, there are many topics that still need to be solved in order to have networking robots in our lives, but we have no to forget that these robots and sensors will interact with people and objects, and that legal issues must be considered. For example, in the case of a robot hurting or injuring a worker in a factory, a question of responsibility arises. This is a case of industrial accident and every country has a specific labour law for it. This situation has happened in the past, prior to any perspective of robots becoming engaged in public service.

The novelty lies in the fact that robots that move in public space would multiply the number of opportunities in which law, surely, will be involved. This is because some of the tasks that the robots would be able to perform include interaction with citizens and the variability of the environment and it will lead necessarily to different situations which cannot be completely foreseen. This is something which is far away from machines performing the same repetitive movements, with the minimum change in their patterns (industrial and domestic robots). Networking robots in the street will be autonomous and will change behaviour according to changing circumstances, although they will rely on a basic pattern related to the work assigned to them. But, even so, the number of unexpected events in the street will grow high compared to a factory or a house. More uncertainty will lead to more conflict scenarios.

There are additional reasons why legal aspects increase their presence in the theoretical scenario we are depicting. For example, mobility in urban regulations has been designed for pedestrians, cars, motorbikes, etc., but not for all types of vehicles. In the city of Barcelona, the Segway's vehicles have banned momentarily its usage as it is unclear what kind of vehicle is and regulations cannot deal properly with it. This argument could be extended to robots.

Robots in the public sphere have to face legal challenges according to what they are and according to what they could potentially do. This is not just because they are robots, but because they are new unclassifiable moving objects and very little empiric knowledge of them is available to legislators. Consequently, as robot's elements and capabilities are better known and understood, it would become much easier to face properly legal challenges. It has to be underlined that it would be a mistake to consider legal challenges in relationship with the development of networking robotics as mere "obstacles to be removed". The right approach consists in considering how to introduce robots in the public sphere without interfering in the fundamental legal principles that European nations have given to themselves

IV. The key legal challenges

We have identified five key issues that are related to legal issues of robots in urban areas. These are:

Safety: It refers to the necessary technical regulations to avoid injuries to people who are in contact with the robots.

Security: It is necessary to determine the extent the robots can be used to carry out tasks of surveillance with the purpose of getting a higher protection level of the citizenship, to obtain higher degrees of citizen safety while respecting citizen's right to privacy. Moreover, it is necessary to determine the legal mechanisms that allow protecting the robots in the event of suffering attacks coming from people.

Urban regulations: We should know the norms (mainly, municipal norms) that robots incorporation in the urban context must submit to, considering that they may coincide with people and vehicles in such space.

Privacy: The way to guarantee the self control on the private data should be determined, especially when the personal information circulation mixes with the technical data circulation. It is absolutely necessary to know the norms to which the treatment and use of the citizens' personal data will be subjected, since these norms will constitute limits to the activities that the robots will be able to develop

V. Privacy: concept, debate, law

CONCEPT

The concept of privacy has a place in the history of ideas long time ago although not always with that name. Ancient Greeks distinguished clearly between the public and the private sphere and there lies the origin of privacy which is the ability or the right of an individual to prevent information about himself or herself from being known by others. The concept has evolved into a complex one, so rich in nuances and different visions, that no single definition has been established. In the academic world, privacy has been a subject of discussion even controversy. In spite of this ongoing debate, Privacy Law exists and keeps developing.

Privacy means self control on private data. This concept addresses directly to freedom. Data processing is an activity that places power in data controllers' hands. They obtain great amounts of private data by different means: traffic and navigation data (where do I link, at what hour and so on), locating data (where I am and where I go) and content data (images of my face or my body, my voice, what are my preferences, what kind of services do I ask for). Really, the knowledge of personal information gives others the capability to decide about our lives: for instance, who knows about us can use our profile to refuse automatically to supply a service.

THE LAW

With respect to privacy, the European Convention guarantees in article 8 the right to respect private and family life, home and correspondence. There is also jurisprudence on the right to privacy in the European Court of Human Rights in Strasbourg. In 1995 a European Directive was adopted by the Commission to protect personal data and its circulation. Member States have incorporated the Directive into their own legislation with slight differences among them. In this way data protection has become a common objective in the UE countries and special government bodies have been created to watch on this objective and enforce the law if necessary.

The main legal reference is the Directive 95/46/EC. As all directives this one has been adopted by national legislations which are quite homogeneous. The Directive and national legislations do not forbid the collecting and processing of personal data but this has to be done under specific conditions and sometimes under sectorial conditions. The Directive 2002/58/CE contains the specific regulation and the criteria to legitimate the data processing by electronic means.

The restrictive focus on personal data processing in Europe has its roots in the historic misuse of this type of data for criminal purposes by undemocratic regimes before and after World War II. In recent years the balance between security on one hand and freedom on the other has been altered by international terrorism in favor of security, but Europe retains strongly its principles of protecting individual rights.

Prior to the Directive 95/46CE, the OECD gave some nonbinding principles that have to be taken into account for the treatment of personal data and the protection of privacy:

- Notice: data subjects should be given notice of data collection
- Purpose: data should be used for the purposes stated and not for other purposes
- Consent: data should not be disclosed without the data subject’s consent
- Security: data collected should be kept secure from potential abuses
- Disclosure: data subjects should be informed about who is collecting their data and for whom
- Accountability: data subjects should have the possibility to hold data collectors accountable for following the above principles

All these requirements have been incorporated into the Directive 95/46CE. This Directive gives green light to personal data collecting and processing but at the same time establishes that these operations must be done under precise principles, mainly three: transparency, legitimate purpose and proportionality. The Directive also says that there must an authority that supervises all the operations.

Given the importance of these issues, and according to the Directive 95/46CE the European Commission has set up a work group of experts known as the Article 29 Working Party whose purpose is to study the subject, write reports and give advice about the level of protection of personal data and its evolutions in the European Union, country by country and on the whole.

The Directives and the transpositions at national level state the criteria of lawfulness of data processing. But above all, they return to citizens the control on their lives. This is, in fact, the aim of the legal framework. It draws three important points of reference: the structural obligations or legal guarantees of the processing (security of personal data filing systems, confidentiality, objective quality of data to be processed), the citizens’ rights and means of pro activity (information about the processing, possibility to consent it; access, opposition and claim rights) and, finally, the exceptions to freedom or the legal possibility to allow a public or private processing without the consent of citizens (always based on public interest valued in a democratic society). The deployment of networking robots in urban areas states those questions. In European areas the data processing is controlled by law: a correct processing is a lawful one. This premise guarantees the citizenship acceptance and will avoid claims and sanctions (which are really strong when they come from public Administration).

The application of national legal provisions can register different levels or intensities:

- No legal limits: this happens when data are anonymous, so they are not personal data. It this case, technical options work, apparently, without submission to legal limits.
- Submission to legal criteria. Data processing involves, normally, the constitution of a filing system. The processor must create the database according to law and he must fulfill legal obligations, specially the duty to inform about the processing. If there is not a legal exception, he must obtain the citizens’ informed consent to collect ant process their personal data. Exceptionally, the simple recording of image or voice in real time, without storage, does not involve a filing system and obliges only to inform the citizens about the recording.

NETWORKING ROBOTS IN URBAN AREAS: LEGAL APPROACH

The deployment of networking robots in urban areas implies the processing of different kinds of data (image or voice data, and traffic or locating data) which can be used for two very different goals: public services (including surveillance) and requested or private services. Those goals are really important to legal approach and we must separate the general use (submitted to general law or to the Directive 95/46/CE incorporation) and the surveillance use (regulated by national provisions applying to video surveillance).

a) Image and voice are personal data if they identify a person without disproportionate efforts.

> - On the hand of requested services, law handles them as normal data and does not build a special system. The processing of image, voice or biometric data is completely submitted to general law (for instance, they are useful to identify people, when they ask for a service requiring a previous authentication).
> - But on the hand of public services, we can consider two situations: surveillance and other utilities on public areas.
> - Surveillance deserves a special regulation because it risks private freedoms.
> - Other utilities (for instance, estimation of the number of pedestrians in a fixed area) are submitted to legal guarantees and, really, need to make data anonymous.

b) Traffic or locating data allow connections between the networking robots and the engines or sensors of pedestrians. The goals of those data may be very different. If pedestrians ask for some e-service (information about recommended routes, restaurants or stores in neighborhood), the data processing is similar to any service provided by a private operator or an e-communications server (submitted to the Directive 2002/58/CE and the Directive 2006/24/CE). If those data are after public surveillance, the situation is closer to the video surveillance and needs a specific legal framework.

We will pay attention to public services and, especially to the surveillance question, which leads us to the field of legal exceptionality. The purpose of surveillance can justify data processing with a lower level of guarantees. But, obviously, the whole situation must fulfill the legal criteria that support the exceptional treatment of the fundamental right of privacy. When law does not support a data processing, it is clear that data must be anonymous. And if networking is to be used for surveillance purposes, a very high level law must provide the channel to do it. In our society, with a permanent feeling of insecurity and where technical resources can be unlimited, this is not mainly a juridical question.

VI. Cameras, Wireless Sensors and Privacy in Public and Private Areas

In relationship with privacy, there is an interesting challenge because this legal aspect is not connected with errors or robot malfunction but just with capabilities that are included in a correct performance of a task. A good example is networking robots navigation which depends on cameras that get people's images and this poses a privacy problem, a delicate subject in European Law, which is extensively regulated and watched. The same could be said in the case or other personal data like codes or personal numbers that can be captures with sensors.

A first step towards identifying the limits in the privacy field is to analyze the two mentioned elements that *work* with networking robots: cameras and a specific type of wireless sensors.

6.1 Cameras

A picture of someone is undoubtedly a personal data, because the definition of this concept includes information about a person that could lead to identification of that person. Definition of personal data in article 2 of the Directive 95/46CE (3) is as follows: "any information relating to an identified or identifiable natural person, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

Image and sound devices can be very sophisticated and they considered useful and justified under circumstances of real or potential danger. Naturally, there is a danger for citizens too, because they become massively identifiable, not only by the image of their face. New devices permitting the automated acquisition of body movement or facial traits can detect strange or suspicious conducts or identify a person by a specific part of his face or body. They can connect those data with elements of personal identity, as passwords. This is an automated processing, very easy and quick because it doesn't involve any human activity. The control on citizens by these kinds of data represents a restriction on human freedoms ant is only justified if it is necessary in a democratic society and proportionate to the achievement of specific purposes. Member States have developed national provisions to channel the resource to private data (image and sound) to surveillance goals. The Opinion 4/2004 of Article 29 Data Protection Working Party shows a list of national provisions applying to video surveillance.

The image, the voice or physical characteristics, as personal data, are under the national laws that incorporate the Directive 95/46/CE. But the installation of cameras to surveillance purposes needs some exceptions (especially to exempt the processing of the consent of citizens), that is why some Member States develop special laws. For instance the French Law n° 95-73 (art. 19 ant 10-1), in relationship with the general Law n° 78-17 (10) ; or the Belgian law in relationship with the general Law. Some countries prefer to develop other kind of instruments, like codes of conduct or special provisions from National Authorities. For instance, in United Kingdom, the Information Commissioner (http://www.ico.gov.uk/) published a CCTV data protection code of practice in 2000, used to help ensure that the use of CCTV complies with the Data Protection Act 1998. In Italy, the *Provedimento generale sulla videosorveglianza* specifies the applications of general principles and recognizes the limitation of consent.

These laws or special instruments are not an incorporation of a European Directive. Of course, the principles of the general Directive are essentials, but distinctions and requirements can be quite different. For instance the Belgian Law regulates the complete possibilities of installation of cameras: in open public places, in closed places open to the public and, finally in closed places not opened to the public. In those three cases, there must be an official visa by the official authority. The Spanish law, on the contrary, divides the consideration of cameras into two legal frameworks: the installation of cameras for the purpose of surveillance in public spaces (open or closed) by Organic Law 4/1997, and the installation in private spaces, only by a private company (Law 23/1992).

The submission to law of the cameras handled by urban robots will strongly depend on national regulations. Certainly, principles are common, through the Directive 95/46/CE, but the details (system, authorizations) will not be uniform.

There is a previous distinction between the installation of equipment in public areas and in private areas.

a) Surveillance in public areas (open or closed areas)

There is not a specific Directive on this question. But art. 13.1 of the Directive 95/46/CE expresses that Member States may adopt legislative measures to restrict some obligations and rights when such a restriction constitutes a necessary measure to safeguard public security or the prevention, investigation, detection and prosecution of criminal offences.

We can summarize that data processing for surveillance in public areas is reserved to police or State security forces. Law drafts the measure of the processing according, first, to general principles. Data must be adequate, relevant, not excessive, not further processed in a way incompatible with the purposes of the special law, and kept for a limited period. The purpose of the installation of cameras must be specific and lawful and the recourse to video surveillance proportional and adequate to the foreseen goals (cfr art. 2 of the *Provedimento generale sulla videosorveglianza*). The prerequisites applying to the engines, verified before the public authorization, become the elements to safeguard the rights of citizens. But the surveillance goal justifies the absence of consent: the obligation to inform citizens about the presence of the engine is compatible with the processing without consent. This statement is valid for static cameras (prior authorization and obligation to inform on their existence) but must be rectified indeed for mobile cameras (implicit information if they support static cameras; and installed even without previous authorization if urgency). Law limits the rights of access and the right to cancel data too. Citizens' capability to control the use of their data decreases in this context. On the other hand, the control on the processor of personal data is very strict.

The deployment of cameras by robots in urban areas, for surveillance purposes, must adequate to these legal premises:

- Competence to decide the installation of video surveillance engines is reserved to public security forces (verified by official Commissions). Its use would be, then, included in their activities to prevent crime and protect persons and their properties.
- The processing of images or voice is lawful when the authority authorizes the installation of cameras and checks the lawfulness of the measure. We can see that, in this moment, the general duty of consent disappears, because there is a legal permission of processing.

- The right of access and to cancel data could be denied to benefit enquiries and general security.
- Filing system that store images or sounds are databases depending on public authorities. Their holders are the public authorities who obtained the authorization to install cameras, and they must notify and register the filing system and fulfill the obligations of security suitable to the kind of data stored in database.

b) Surveillance in private areas

The surveillance in private areas, when it exceeds the personal or household activities, involves the processing of third persons' data. The surveillance, to protect the entrance or different activities in buildings, is decided by the owners (single owners or condominium). The circumstances and requisites of the installation must fulfill legal duties. Law becomes, again, the guarantee of a correct processing and the instrument to avoid the individual consent of citizens.

The owners of private areas are the controllers who determine the purposes and means of the processing of personal data, and responsible of the filing system. But the installation of cameras will be normally submitted to authorization, or as in Spain, reserved to companies of security, which competences are recognized by law. So there is a specific legal permission for those companies to install surveillance engines and who become processors (in the sense of art. 2.e of the Directive 95/46/CE: bodies who processes personal data on behalf of the controller). This legal permission considers the installation of video surveillance as a complementary and subordinated activity in relation to public security. This must be clearly explained in a separated law (Spanish case); on the other hand this function becomes obvious when law regulates the video surveillance as a whole (public and private areas).

Even a high protective provision, like the Italian one, recognizes that the exceptions to consent can be strong. Art. 6.1 *Provedimento generale* begins making differences between public and private processors of databases; private controllers only can process personal data if they have the consent of interested people. But the provision recognizes too that lawfulness without consent can be handled by law because exceptions are highly necessary when the processing purpose does not allow contacting previously with interested people. The duty of information on the other hand is essential (art. 10 Directive 95/46/CE, French Law n°95-73 art. 10.II).

We can see that the origin of data filing is absolutely private. Networking robots in private areas will always require the initiative of the private processor. Some countries reserve the installation of cameras to an authorized security company, through a legal recruitment (under conditions of legal principles) and, finally, it is submitted to the inspection of the Supervisory Authority.

6.2 Wireless communications systems: the case of Bluetooth scanning sensor for mobility management purposes

One of the services that could be provided by networking robots is mobility management. Mobility is a fundamental factor for the economic growth of cities and social sustainability [1]. However the poor management of mobility can transform people's necessity of travel into different problems: the collapse of the road system to a point that becomes unable to absorb more traffic (i.e. emergence of bottlenecks), the degradation of the environment as noise increases, air pollution which affect public health and the emissions that increase global warming.

On the other hand, successful traffic management can overcome apparent contradictions like achieving economic development and at the same time protecting the environment. In consequence, a variety of sensors and methodologies have been proposed in order to study vehicle's behaviors and understand their patterns. In most cases, the approaches rely on Electromagnetic loop, Ultra Sonic Sensor or Origin Destination Survey (OD Survey). In addition, different types of Video Cameras from the infrared camera to closed circuit television (CCTV) offer solutions to identify a moving object for traffic data collection.

The recent advances in wireless and mobile devices such as mobile phones, navigation systems, Pocket PC and PDA, opens new possibilities for data collection which could not be imagined just a few years ago. These wireless devices can act as sensors and be tracked to collect precise trajectory in space-time. For instance, the Floating Car Data Collection System can generate dynamic traffic information as traffic flow, congestion or micro weather conditions in real time through various sensors installed in the vehicle.

Bluetooth and traffic management

These developments have enabled the ability to use of Bluetooth sensors (BT sensor) for vehicle and pedestrian localization. Bluetooth is the global standard protocol (IEEE 802.15.1) for exchanging information wirelessly between mobile devices, using 2.4 GHz short-range radio frequency bandwidth. Ericsson started to develop it in 1994 and released it in 1998. It was designed to reduce the communication cost between the fixed and portable devices with low power consumption. Nowadays, it allows devices to communicate without the physical line between devices from 10m to 100m range, even if there exist some obstacles between them. One of the characteristics of Bluetooth is the device-discovery ability which permits to collect information about nearby Bluetooth devices as Media Access Control address (MAC address), device name and device type.

Although a variety of other project have used Bluetooth detection, many of them exploited its proximity detection mechanism for measuring the social network relation of people indoors and outdoors [2,3,4]. For instance, the Cityware project[1] applied this technique in public space for detecting individuals [5]. The purpose of this application is to understand people's behaviour and social networks through the combination of several techniques: human observation and pervasive technologies. In another line of research, the Innovative Cities of Next Generation (ICING) project[2] proposed a traffic management system by identifying the trajectory of vehicle through Bluetooth signal [6]. In this case the goal was neither to count the number of passing cars nor to perform a precise count. The objective was to get the trajectory data and to validate both the methodology and the data obtained.

Based on this first experiment the Barcelona based firm, Bitcarrier[3] has developed and refined the techniques to come up with a patented technology that detects around 70 different devices per second. The immediate communication of these data to a centralized server enable allows visualizing them in real time on their web page[4]. This solution is effective for tracking vehicle and pedestrian movements and also for analyzing the patterns and trends of the movements of people across the city.

Privacy issues concerning this technology

The MAC address is a unique code that belongs exclusively to a specific device (PC, mobile, PDA, Car Navigation System), although exceptionally some makers release few devices with the same code not following the standard procedure. Nevertheless, this code can be considered as personal data because a link between the code, the device and the owner of the device is not impossible.

This code consists in the combination of 6 alphanumeric pairs (Hexadecimal). The first 3 pairs are allocated to the company through the Institute of Electrical and Electronics Engineers (IEEE) and the last 3 are distributed to each device by the service provider company. For instance, MAC address of the Car Navigation System TomTomGo700 would be like this: 00:13:6c:0b:d4:2f. The first 3 pairs, 00:13:6c, are assigned to the company TomTom NV by the IEEE. That means that all TomTomGo have their MAC address starting with this sequence, 00:13:6c. The last 3

[1] http://www.cityware.org.uk/
[2] http://www.fp6-project-icing.eu/
[3] http://www.bitcarrier.com/
[4] http://www.bitcarrier.net/map/, Password: mediatest

pairs, 0b:d4:2f, are attributed to this particular device (in this case a car navigator) by TomTomNV.

This information is useful to differentiate an individual Bluetooth device but rather ineffective to identify a specific person. Indeed, in order to know the owner, it needs to combine several datasets from different sources protected by service providers. Therefore, it is very difficult to achieve it practically and identify the owner. However, one can argue that there would be a possibility of uncovering personal data. The code which is, in principle, anonymous could become personal data if someone is able to establish the adequate connections between the different sources and obtain a link to a personal identity. But there is a technical solution that can avoid this to happen. A solution applied in some Bluetooth projects [7].

By using an adaptation of SHA (Secure Hash Algorithm) to BT sensor, it permits to generate anonymous trajectory data even if there is a record of these data in an archive without invading privacy. This happens as follows: when the sensor gets a MAC address, SHA algorithm generates an internal identifier with it. The original MAC address is erased at when the identifier is assigned. In consequence, it is not possible to retrieve the link between the generated number with the original MAC address as the identifier becomes anonymous with no possibility to make a link to any personal data. The advantage of hash algorithms is to be able to generate always the same output from a specific input. It doesn’t need to save any state data in the archive. This scheme permits to perform an anonymous logging and identify trajectories of people without invading their privacy.

Within this legal framework, more than 5,300,000 unique code at 11 points in Barcelona have been obtained during 8 months for the purpose of traffic and pedestrian management. Currently, several projects for mobility analysis are proceeding through collaboration with the Mobility Department of the Barcelona City Council, Technical University of Catalonia (UPC) and Massachusetts Institute of Technology (MIT).

VII. Conclusions

We have presented key legal challenges that are required for deploying robots and sensors in urban areas. We have discussed mainly the privacy issue and show some examples where this issue is required. Some conclusions of the privacy issues are:

- The use of robot networking with data recording and storage devices for private purposes, including requested e-services, involves the general legal framework application, that is, the need to obtain or not the consent of those concerned. This consent is not needed when the law foresees exemptions (because the service is requested by user or the data are anonymous, for instance for statistics goals).

- On the hand of public purposes (not surveillance purposes), data must be anonymous or there must be an informed consent or a legal specific permission; otherwise the handling of such data will not be lawful.

- On the hand of the anonymous surveillance, there is a special legal framework. In this case, a decrease of individual guarantees happens because the public interest. This legal framework exists for video surveillance (cameras and sound recording engines).

- The legal framework foreseeing the use of sensors does not exist yet and we must conclude that, nowadays, the processing of personal data obtained by the means of sensors must be restrictive and not possible without making them anonymous (to obtain an informed consent doesn't seem easy in any situation, specially in public areas). However, there is the exception of data retention foreseen by the Directive 2006/24/CE allowing the disclosure of traffic and locating data to public authorities, if required, to follow criminal investigations.

Acknowledgment

This research was conducted at the Institut de Robòtica I Informàtica Industrial of the Technical University of Catalonia and Consejo Superior de Investigaciones Científicas. It was partially supported by CICYTproject DPI2004-05414 and IST-045062 of the European Community Union,

References

[1] Commission of the European Communities (2007). Green Paper Towards a new culture for urban mobility, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0551:FIN:EN:PDF, 26/02/2009

[2] Eagle, N., Pentland, A. (2006) Reality mining: sensing complex social systems. Pers Ubiquitous Comput 10 (4): 255-268..

[3] Paulos, E., and Goodman, E. (2004). The familiar stranger: anxiety, comfort, and play in public places. In proceedings CHI 2004, ACM, pp. 341-350.

[4] Nicolai, T., Yoneki,E., Behrens,N., Kenn, H. (2005). Exploring social context with the Wireless Rope. In: On the move to meaningful internet systems, 2006: OTM 2006 workshops, part I, LNCS, vol 4277. Springer, Heidelberg, pp 225-242.

[5] O'Neill, E., Kostakos, V., Kindberg, T., Fatah gen. Schieck, A., Penn, A.,Stanton Fraser,D., Jones,T. (2006). Instrumenting the city: developing methods for observing and understanding the digital cityscape. In: Ubicomp 2006: 8th international conference on ubiquitous computing, LNCS, vol 4206. Springer, Heidelberg, pp 315-332.

[6] Yoshimura, Y., González, E., Punsola, A., Andrés, D., Cárdenas, F. (2007). Tools for process modelling and decision-making, ICING document.

[7] Kostakos, V. (2008). The privacy implications of Bluetooth, arXiv:0804.3752.

[8] Rouvroy, A. (2008): Privacy, Data Protection, and the Unprecedented Challenges of Ambient InteligenceStudies in Ethics, Law, and Technology, Berkeley Electronic Press, 2008.

[9] Dumortier, Franck: "La vidéosurveillance sous l'angle de la proportionnalité : premières réflexions au sujet de la loi réglant l'installation et l'utilisation de caméras de surveillance" Revue du Droit des Technologies de l'Information, 2007, n° 29.

[10] Martínez Martínez, Ricard : "Videovigilancia y protección de datos personales: la Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos",

[11] Revista Aranzadi de derecho y nuevas tecnologías, Nº. 13, 2007

[12] Goulet, Jean: "Du logiciel traditionnel à la robotique fine : l'adaptation des règles du droit à la technologie de pointe", Cahiers de Propriété Intellectuelle, 2008, Vol. 20, n° 3

[13] P.M. Asaro, Robots and Responsibility from a Legal Perspective

[14] P.M. Asaro, What Should We Want From a Robot Ethic?, International Review of Information Ethics, Vol 6 (12/2006).

[15] P. McNally and S. Inayatullah, "The Rights of Robots: Technology, Law and Culture in the 21st Century," World Peace Through Law Center: Law and Technology (Winter, 1987.

[16] [S. Lawrence B., Legal Personhood for Artificial Intelligences(1992). North Carolina Law Review, Vol. 70, p. 1231, 1992.

[17] J G. Schweitzer, Robotics – Chances and challenges of a key science, 17th International Congress of Mechanical Engineering (COBEM 2003), São Paulo, Brasil, November 10-14, 2003