MIAUCE report 2008 : ethical, social and legal issues

Cornelis, Mathieu; Darquennes, Denis; Lobet-Maris, Claire; Poullet, Yves; Grandjean, Nathalie; Rouvroy, Antoinette

Publication date:
2008

MIAUCE

Multi modal Interaction Analysis and exploration of Users within a Controlled Environment
IST Call 5, FP6-2005-IST-5
www.miauce.org

Deliverable
D5.1.2
Ethical, legal and social issues

Title:	**Ethical, legal and social issues**
Author(s):	M. Cornélis, D. Darquennes, N. Grandjean, C. Lobet-Maris, Y. Poullet, A. Rouvroy
Status – Version:	
Period:	Month 24
Confidentiality:	**PP**: Restricted to other program participants (including the Commission Services)
Code:	MIAUCE_D5.1.2_200708_V1.0.pdf
Partners:	University of Amsterdam, CNRS, University of Glasgow, University of Namur, Sylis, Tilde, Visual Tools.

HISTORY

Author	*Version*	*File name*	*Remarks*
CITA and CRID; UNIVERSITY OF NAMUR	*1.0*	MIAUCE_D5.1.2_200708_V1.0.pdf	

EXECUTIVE SUMMARY

The MIAUCE (Multi-modal Interactions Analysis and exploration of Users within a controlled Environment) project is part of the sixth Framework program. The University of Namur (UN), through the involvement of both the Interdisciplinary Centre for Technology Assessment (CITA), and the Research Centre for Computer and Law (CRID), as leader of the WP5 of the Miauce project, is in charge of the ethical, legal and sociological aspects and plays many roles all along the project. The two axes of the University of Namur's involvement in the project focus on the internal aspect of governance (how to design Miauce applications taking into consideration the ethical, legal and societal aspects) on the one hand, and on the external aspect of governance of the project (How to integrate legal, ethical, sociological issues in the European technological policies).A major challenge of this project is to integrate human values (legal social and ethical aspects) as central design criterion along with more classical or traditional criteria of usability, economy, reliability and correctness.

In this second period, we have achieved two main research results regarding the internal aspect of the MIAUCE governance.

First of all, we have developed a methodological frame enabling collective deliberation about the ethical, legal and social issues involved in the design of MIAUCE technologies. This methodology is supported by two crucial options we had to define. The first one consists in the moral and the legal value from which one would assess these technologies and their application scenarios. In this report, we held that respect for, and encouragement of individual autonomy (self-determination) and collective autonomy (the vitality of deliberative democracy) are the two most sustainable reference principles or values that "value sensitive design" should strive to reinforce. The second option relates to our role and responsibilities, as researcher in human sciences and humanities, as partners in the MIAUCE project. Considering that ethics is not a theoretical knowledge that can be learned and appropriated by hearing experts, but is rather an attitude or a posture in life and work, the role we have held in the project, with reasonable success, consisted in enabling our partners to acquire a reflexive and ethically enlightened posture, which allows them to both understand and reflect on the ethical, legal and societal impacts – both actual and potential – of industrial and technological choices. Our methodology therefore always promoted a participative and deliberative determination of the ethical, legal and social constraints and values to be implemented through technological design and industrial orientations. This was a mutual learning process through which we, as human scientists, have learned to better define our position (or posture) and interventions and through which our scientific and industrial partners have had the opportunity to better understand their ethical, legal and social responsibilities in an increasingly technologized world.

The second result of this WP5 second year consists in the actual introduction of value sensitivity as a guiding criteria for the design of the scenarios as they are now described, adopting changes that have been considered necessary not for industrial nor scientific reasons, but for ethical, legal and societal reasons justifying the adaptation of the initial specifications of the technologies or in the organizational arrangements supporting their deployments (blurring faces, clear specification of the finalities of the technology, sensible data to be

protected, responsibility and liability constraints …)

Table of Contents

1. INTRODUCTION

1.1. OBJECTIVES OF WP5

The University of Namur (UN), through the involvement of both the Interdisciplinary Centre for Technology Assessment (CITA), and the Research Centre for Computer and Law (CRID), as leader of the WP5 of the Miauce project, is in charge of the ethical, legal and sociological aspects and plays many roles all along the project. According to the first review recommendations, UN has two main objectives to achieve in the MIAUCE project. Those two objectives of the University of Namur's involvement in the project focus on the internal aspect of governance (how to design Miauce applications taking into consideration the ethical, legal and societal aspects) on the one hand, and on the external aspect of governance of the project (How to integrate legal, ethical, sociological issues in the European technological policies).

The major challenge of this project is to integrate human values (legal social and ethical aspects) as central design criterion along with more classical or traditional criteria of usability, economy, reliability and correctness.

1.2.RESEARCH TASKS REPORTED IN DELIVERABLE D5.1.2

During this year and based on the recommendation of the reviewers, the SHS team has carried on and reinforced its role of 'intermediary' making the dialogue between industrials and scientists more efficient and workable in order to design technological scenarios compliant with the human values sustaining our democratic society and its legal organization.

A succession of research steps has guided the SHS team during this 2d year.

First step: epistemological and governance considerations

This second year was first devoted to question the status and responsibilities of the SHS intervention into technologically applied projects like MIAUCE. This epistemological questioning was a necessary first step to consolidate our role and intervention methodology in this project, taking into account both the expectations of our partners and our contractual mandate.

Next steps: construction and deliberation of the scenarios

The next steps achieved during this second year were devoted to the social construction and the collective deliberation of the three scenarios supported by the MIAUCE technologies. At the end of the 1st year of the MIAUCE project, the scenarios weren't yet fully developed. By way of scenarios, we had, at that time, basic hypothesis (escalator safety, supermarket marketing and interactive webTV) in which the foreseen technologies could find rewarding applications. But in order to design these technologies and be able to debate about and work on the 'societal' requirements constraining available organizational, technological and informational choices, transforming these basic situations into detailed and realistic scenarios was a crucial step. The scenarios have thus been built following a collective learning and discussion process allowing each team to question its own and its partners' choices and to gradually acknowledge the non neutrality, from the 'societal' point of view, of the choices - either technical or organizational - to be endorsed. In order to sustain the

dynamic of this collective learning process, the methodology described in Chapter 5 of the deliverable 5.1. has been implemented and adjusted as to make it more pedagogical and accessible to all the involved teams.

1.3. SCOPE OF WP5 WITHIN MIAUCE SCENARIOS

During this year and based on the recommendation of the reviewers, the SHS team has carried on and reinforced its transversal role of 'intermediary' making the dialogue between industrials and scientists more efficient and workable in order to design technologies compliant with the human values sustaining our democratic society and its legal organization.

To support an efficient dialogue between the teams involved into the design of the technologies supporting each scenario, we define and apply a similar methodology of scenario building for the three considered domains. This methodology can be considered as a collective learning process. (see the next point for the presentation of the methodology)

1.4. SUMMARY OF PROGRESS

A summary of progress towards objectives and details for each task

This second year was first devoted to question the status and responsibilities of the SHS intervention into technologically applied projects like MIAUCE. This epistemological questioning was a necessary first step to consolidate our role and intervention's methodology in this project taking into account both the expectations of our partners and our contractual mandate.

The next steps achieved during this second year were devoted to the social construction and the collective deliberation of the three scenarios supported by the MIAUCE technologies. At the end of the 1st year of the MIAUCE project, the scenarios weren't yet fully developed. By way of scenarios, we had, at that time, basic hypothesis (escalator safety, supermarket marketing and interactive webTV) in which the foreseen technologies could find rewarding applications. But in order to design these technologies and be able to debate about and work on the 'societal' requirements constraining available organizational, technological and informational choices, transforming these basic situations into detailed and realistic scenarios was a crucial step. The scenarios have thus been built following a collective learning and discussion process allowing each team to question its own and its partners' choices and to gradually acknowledge the non neutrality, from the 'societal' point of view, of the choices - either technical or organizational - to be endorsed. In order to sustain the dynamic of this collective learning process, the methodology described in Chapter 5 of the deliverable 5.1. has been implemented and adjusted as to make it more pedagogical and accessible to all the involved teams.

This methodology consists in three major methodological steps.

In the first one, we develop a methodology helping the partners to move from basic use cases (as they were developed in the deliverables of the 1st year) to detailed scenarios, inciting all the involved teams to fully specify the use cases foreseen in their detailed

technico-organizational dimensions or arrangements. This was an important step forward, which also eased the integration of work among Miauce partners by forcing them to debate about their visions and constraints in a kind of collective scenario building process. As this exercise is important, it needs to be well organized and supported by relevant framework in order to support an efficient deliberation.

In this process, the SHS team had a role of 'facilitator', organizing this collective process and supporting it with a questionnaire helping efficient deliberation between the teams involved.

The second step of this scenario building process can be considered as a 'translation procedure' consisting in articulating the detailed specifications collected in step 1 within a meaningful context of the 'future' generated by those technologies pointing out the major social, ethical and legal issues at stake. The lead of this step was the SHS team even if it was achieved through the confrontation with all associated teams.

The ambition of the third step is to clearly point out the societal choices raised by the scenarios and the technologies at work in order to enable collective deliberation and ethical learning. So the figure endorsed by SHS scientists during this step is not the figure of the expert but the one of a situated advisor enlightening the technicians and the industrials about the problems and the questions raised by the technologies supporting each scenario. Since The MIAUCE scenarios presented in the three domains of application were obviously centered on the bright impacts of technologies, it was difficult for the MIAUCE partners to clearly figure out exactly the scope of the socio-technical choices they faced. Moreover, the technologies are not merely 'introduced' into society, nor do they conform, in their existence and evolution, to the designers' preconceptions. In every technology resides a possibility of misuse. For these two reasons, we decide to use the methodology developed in the SWAMI[1] project and consisting in broadening the scope of inquiry, from the bright scenarios described, to more realistic, and darker versions of application scenarios epitomizing the potential dangers and misuses of the same technologies. The process highlights vulnerabilities and threats. These dark versions of scenarios are very valuable to unveil internal limits and potential risks carried by scenarios. In our deliberative approach, these dark scenarios, even fictional as they are at this stage, have helped the various partners to better understand the importance of issues at stake.

This collective exercise leads the MIAUCE team to re-design some aspects of the technologies involved in the scenarios and to re-consider their contexts of implementation in order to make them respectful to human and democratic values and compliant with the legal frame that organizes our society**.**

Interim Milestones for WP5

[1] Punie, Y., Delaitre, S., Maghiros, I. & Wright, D. (eds.) "Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities". SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507, November 2005. http://swami.jrc.es

Month	Id	Milestones	Measurable results	WP	Lead contractor
20		Methodology for scenarios deliberation - Analysis of the issues raised by the MIAUCE technogies	- Full methodological roadmap developed - Recommendations regarding the role and responsibilities of Human scientists in technological project - First analysis of the issues raised by the technologies at work in the scenario	WP5	UN
24		Socio-ethical and legal assessment of the technological specifications at work in the scenarios and collective deliberation about their adaptation	Socio-ethical and legal requirements for the technologies at work in each scenario	WP5	UN

Table 1. Interim Milestones for WP5

Significant results

At the end of this 2d year, four significant results are achieved :

Table 2. An appropriate methodology to support the collective deliberation regarding the ethical, social and legal choices at stake in the design of a technology. This methodology is presented in the introduction of the deliverable and supports the structure of the deliverable

Table 3. An epistemological framework regarding the role, the responsibilities and the values that could support the implication of human scientists into technological design. This result is presented in chapter 1.

Table 4. A precise understanding of the most significant issues raised by the technologies at work in MIAUCE. These issues are explored in the chapter 2 and in the conclusion.

Table 5. The design of the technologies supporting each scenario as they are not only a technical product but also a social result of the ethical deliberation animated by the University of Namur.

.

Reasons for deviations

No deviation.

Reasons for failing to achieve objectives

None

Deliverable Summary

<milestones at M24>

Del. N°	Deliverable Name	WP N°	Lead Participant	Nature	Dissemination Level	Due Delivery date from Annex 1	Delivered Yes / No	Actual / Forecast Delivery date	Comments
D5.1.2	Ethical, legal and social issues	5	UN	Document and Annex	**PU**	September 1st 2008	No	September 13st 2008	none

Table 6. Deliverable summary

1.5. STRUCTURE AND PURPOSE OF THIS DOCUMENT

In the first chapter, we question the status and responsibilities of the human scientists intervention into technologically applied projects like MIAUCE. This epistemological questioning was a necessary first step to consolidate our role and intervention methodology in this project, taking into account both the expectations of our partners and our contractual mandate.

Three crucial questions were debated and analyzed in this regard during this 2d year.

The first one relates to the 'figures' or 'postures' social scientists can endorse when participating into a technological project. This first question concerns the 'roles and responsibilities' of SHS in such an applied context, and the 'values' that should guide their contribution and cooperation with the other stakeholders.

The second question challenges the status of the human sciences' discourses when they take part in the design of a technological artefact.

Finally, the last question concerns the possibility to widen the scope of the SHS intervention as to address societal issues at stake on a wider scene, and, in this way, foster democratic debates about the relevant ethical, legal and societal issues.

As such, these epistemological considerations contribute to shape a sound democratic internal governance for the project.

Epistemological and Governance considerations are presented in **Chapter 1** of the deliverable 5.2

The next steps achieved during this second year were devoted to the social construction and the collective deliberation of the three scenarios supported by the MIAUCE technologies. At the end of the 1st year of the MIAUCE project, the scenarios weren't yet fully developed. By way of scenarios, we had, at that time, basic hypothesis (escalator safety, supermarket marketing and interactive webTV) in which the foreseen technologies could find rewarding applications. But in order to design these technologies and be able to debate about and work on the 'societal' requirements constraining available organizational, technological and informational choices, transforming these basic situations into detailed and realistic scenarios was a crucial step. The scenarios have thus been built following a collective learning and discussion process allowing each team to question its own and its partners' choices and to gradually acknowledge the non neutrality, from the 'societal' point of view, of the choices - either technical or organizational - to be endorsed. In order to sustain the dynamic of this collective learning process, the methodology described in Chapter 5 of the

deliverable 5.1. has been implemented and adjusted as to make it more pedagogical and accessible to all the involved teams.

A series of steps have supported this methodology of scenario building.

Table 7. In the first one, we develop a methodology helping the partners to move from basic use cases (as they were developed in the deliverables of the 1st year) to detailed scenarios, inciting all the involved teams to fully specify the use cases foreseen in their detailed technico-organizational dimensions or arrangements. This was an important step forward, which also eased the integration of work among Miauce partners by forcing them to debate about their visions and constraints in a kind of collective scenario building process. As this exercise is important, it needs to be well organized and supported by relevant framework in order to support an efficient deliberation.

Major results of this step are the **questionnaire (annex 1)** and the scenarios narrations (see for a complete version: the **industrial deliverable** – and for an **executive version the chapter 2** of the deliverable 5.2)

Table 8. The second step of this scenario building process can be considered as a 'translation procedure' consisting in articulating the detailed specifications collected in step 1 within a meaningful context of the 'future' generated by those technologies pointing out the major social, ethical and legal issues at stake. The lead of this step was the SHS team even if it was achieved through the confrontation with all associated teams.

Major results of this step are presented in the **Chapter 2** of the deliverable 5.2.

Table 9. The ambition of the third step is to clearly point out the societal choices raised by the scenarios and the technologies at work in order to enable collective deliberation and ethical learning. So the figure endorsed by SHS scientists during this step is not the figure of the expert but the one of a situated advisor enlightening the technicians and the industrials about the problems and the questions raised by the technologies supporting each scenario. Since The MIAUCE scenarios presented in the three domains of application were obviously centered on the bright impacts of technologies, it was difficult for the MIAUCE partners to clearly figure out exactly the scope of the socio-technical choices they faced. Moreover, the technologies are not merely 'introduced' into society, nor do they conform, in their existence and evolution, to the designers' preconceptions. In every technology resides a possibility of misuse. For these two reasons, we decide to use the methodology developed in the SWAMI[2] project and consisting in broadening the scope of inquiry, from the bright scenarios described, to more realistic, and darker versions of application scenarios epitomizing the potential dangers and misuses of the same technologies. The process highlights vulnerabilities and threats. These dark versions of scenarios are very valuable to unveil internal limits and

[2] Punie, Y., Delaitre, S., Maghiros, I. & Wright, D. (eds.) "Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities". SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507, November 2005. http://swami.jrc.es

potential risks carried by scenarios. In our deliberative approach, these dark scenarios, even fictional as they are at this stage, have helped the various partners to better understand the importance of issues at stake. This collective exercise leads the MIAUCE team to re-design some aspects of the technologies involved in the scenarios and to re-consider their contexts of implementation in order to make them respectful to human and democratic values and compliant with the legal frame that organizes our society**.**

Major results of this step are presented in **Chapter 2 and Chapter 3** of the deliverable 5.2.

In the conclusion, we explore the critical issues still remaining with regard to the general epistemological, cultural and political paradigm supporting the design and deployment of such multimodal observation technologies. Particularly, we address these most critical issues, which no adaptation or change in technological design or industrial organization can solve, since these questions concern the broader epistemological, cultural and political bases on which these emerging technologies are grounded.

ABSTRACT

This abstract provides an overview of the main research activities carried on by Social and Human Scientists (SHS), i.e. University of Namur (WP5), during this 2d year of the MIAUCE project.

During this year and based on the recommendation of the reviewers, the SHS team has carried on and reinforced its role of 'intermediary' making the dialogue between industrials and scientists more efficient and workable in order to design technological scenarios compliant with the human values sustaining our democratic society and its legal organization.

A succession of research steps has guided the SHS team during this 2d year.

FIRST STEP: EPISTEMOLOGICAL AND GOVERNANCE CONSIDERATIONS

This second year was first devoted to question the status and responsibilities of the SHS intervention into technologically applied projects like MIAUCE. This epistemological questioning was a necessary first step to consolidate our role and intervention methodology in this project, taking into account both the expectations of our partners and our contractual mandate. Three crucial questions were debated and analyzed in this regard during this 2d year.

The first one relates to the 'figures' or 'postures' social scientists can endorse when participating into a technological project. This first question concerns the 'roles and responsibilities' of SHS in such an applied context, and the 'values' that should guide their contribution and cooperation with the other stakeholders.

The second question challenges the status of the human sciences' discourses when they take part in the design of a technological artefact.

Finally, the last question concerns the possibility to widen the scope of the SHS intervention as to address societal issues at stake on a wider scene, and, in this way, foster democratic debates about the relevant ethical, legal and societal issues.

As such, these epistemological considerations contribute to shape a sound democratic internal governance for the project.

Epistemological and Governance considerations are presented in **Chapter 1** of the deliverable 5.2

NEXT STEPS: CONSTRUCTION AND DELIBERATION OF THE SCENARIOS

The next steps achieved during this second year were devoted to the social construction and the collective deliberation of the three scenarios supported by the MIAUCE technologies. At the end of the 1st year of the MIAUCE project, the scenarios weren't yet fully developed. By way of scenarios, we had, at that time, basic hypothesis (escalator safety, supermarket marketing and interactive webTV) in which the foreseen technologies could find rewarding applications. But in order to design these technologies and be able to debate about and work on the 'societal' requirements constraining available organizational, technological and informational choices, transforming these basic situations into detailed and realistic scenarios was a crucial step. The scenarios have thus been built following a collective learning and discussion process allowing each team to question its own and its partners' choices and to gradually acknowledge the non neutrality, from the 'societal' point

of view, of the choices - either technical or organizational - to be endorsed. In order to sustain the dynamic of this collective learning process, the methodology described in Chapter 5 of the deliverable 5.1. has been implemented and adjusted as to make it more pedagogical and accessible to all the involved teams.

A series of steps have supported this methodology of scenario building.

Writing the scenarios: from domains to detailed scenarios

In the deliverable 5.1., we have approached 'scenario' as a 'meaning making exercise' that stimulates exchange of ideas and sound deliberation about the choices of potential foreseen futures. In order to underline the social and epistemological dimensions of the concept of "scenario", we have adopted L.B. Rasmussen's definition as the focal point of our methodology. According to L.B. Rasmussen,

> Scenarios are flexible means to integrate disparate ideas, thoughts and feelings into holistic images providing context and meaning of possible futures[3].

Achieving this 'meaning making' exercise required us to move from basic use cases to detailed scenarios, inciting all the involved teams to fully specify the use cases foreseen in their detailed technico-organizational dimensions or arrangements. This was an important step forward, which also eased the integration of work among Miauce partners by forcing them to debate about their visions and constraints in a kind of collective scenario building process. As this exercise is important, it needs to be well organized and supported by relevant framework in order to support an efficient deliberation.

In this process, the SHS team had a role of 'facilitator', organizing this collective process and supporting it with a questionnaire helping efficient deliberation between the teams involved.

Each scenario (safety, marketing and WebTv) has been targeted by a specific questionnaire answered by the industrials and technicians directly involved in the development of the application foreseen. The questionnaires were very factual and pragmatic in addressing :

- *The 'process vision' of each scenario (a full description of all the processes supported by the foreseen application). This textual description had to be made in very accurately and exhaustively for each concerned process, using the same sequential frame as the one used for a storyboard describing for each process the technical support expected from the foreseen applications.*

- *The 'actors vision' of the scenario (a full description of the actors involved by the foreseen application). This aims at deliberating about the roles and responsibilities of the various actors directly or indirectly concerned by this application.*

- *The 'data vision' of the scenario (a full description of the data collected and of the various uses made of these data). This description deals with the nature of the collected data, the organizational details of data storage, and a full description of their potential uses (analysis, decision, communication, disclosure…)*

[3] Rasmussen, L. B., The Narrative Aspect of Scenario Building. How Story Telling May Give People a Memory of the Future, Online publication 12-8-2005, Springer Verlag, London Limited, 2005.

- *The 'finality vision' (a full description of the main finalities envisioned for the application). This deliberation aims at rendering the intentionality behind the scenario explicit, and, as a consequence, to better identify responsibility issues involved by each scenario.*

This scenario building process was organized in two rounds. The first round resulted in a draft version of the scenarios. Based on additional questions raised by the SHS team, the partners were then invited to refine and enrich this first version in order to provide a more precise and accurate view of each application.

This exercise was most useful, providing a critical opportunity to each of the associated teams to express their visions, expectations and constraints with regard to the applications under development.

Major results of this step are the **questionnaire** (see annex 1) and the scenarios narrations (see for a complete version: the **industrial deliverable D.6.2.** – and for an **executive version the chapter 2** of the deliverable 5.2)

Situating the scenarios: from paradigm to legal context

This step of the scenario building process can be considered as a 'translation procedure' consisting in articulating the detailed specifications collected in step 1 within a meaningful context of the 'future' generated by the application. The lead of this step was the SHS team even if it was achieved through the confrontation with all associated teams.

To support this stage, three conceptual frames have been used.

The first one does consist in resituating the scenarios and the technologies at work within the relevant socio-technical and epistemic paradigm. This broader contextualization allowed for a better identification of both the societal and epistemic conditions and consequences of the project. We have called this configuration of societal, technological and epistemic frames, at least temporarily, the "multimodal observation paradigm". This paradigm combines multimodal capture of data "extracted" from human bodies (facial expressions, eye gaze, postures and motions) with an implicit understanding or interpretation of these data as valid and privileged sources of "truth" about the persons, their preferences, intentions etc. following the preconception according to which the 'body does not lie' whereas, *a contrario* anything transiting through the prism of individuals' consciousness is *a priori* suspect and unreliable. This paradigm and its related hypothesis decrease the subjects' self-determination (autonomy). The deterministic codes of intelligibility built in the multimodal observation paradagm does not allow individuals to impact on the "informational image" compiled of themselves nor on the interpretation thereof. Moreover the "informational" image of the subject has performative effects on the real subject's perceptions of what is expected in terms of attitudes, behaviours and preferences, with the result, already exposed in the previous deliverable, of increased democratically detrimental anticipative conformity in society.

The second frame used aims at better approaching the finalities of the scenarios and the technologies involved. These scenarios are marked by finalities of safety and marketing. To better approach these ones, we have used the typology developed by C. Müller and D. Boos (2004) about the surveillance technologies and a typology developed by ourselves regarding the major systems for marketing approach of individuals. These typologies have served as tools to clearly situate the foreseen applications and their finalities in order to consolidate the collective understanding about

the social meaning of these scenarios. In our learning process, working with those tools allows a first awareness about the major issues related to the scenarios under building.

This new paradigm and their related applications as the ones proposed in MIAUCE question urgently the traditional legal frame that organizes and supports the social order of our society. Many legal concepts and principles, as privacy, responsibility and human rights are particularly questioned by those technologies.

This new reading of the scenarios with these three frames gave the opportunity for all associated teams to clearly understand first of all that the scenarios and the technologies at work were not neutral from human and social points of view. This reading gave also a clear insight regarding the questions (legal, ethical and social) that have to be explored in order to **make these scenarios respectful of human values and by then acceptable in the broad sense defined in chapter 1.**

Major results of this step are presented in the **Chapter 2** of the deliverable 5.2.

Exploring and broadening the scenarios: social, ethical and legal issues

This step consists in analyzing the issues raised by the scenarios. This analysis is led by the SHS scientists and framed by the human values and legal principles defined in chapter 1. To support this scenarios assessment, we used the three levels of structuration defined by A. Giddens. According to Giddens any social construct, as the scenarios are, should be questioned and analyzed with regard to three main dimensions:

- *Meaning: what social organization (coordination between actors and between actors and devices) embedded into the scenario?*
- *Power : what is the implicit distribution of power suggested by the scenario in terms of distribution of responsibility and capacity between the actors involved?*
- *Norms and values : what are the implicit norms and values sustained by the scenario to justify it and to legitimate or regulate the behaviors of the actors involved?*

The ambition of this analysis is to clearly point out the societal choices raised by the scenarios and the technologies at work in order to enable collective deliberation and ethical learning. So the figure endorsed by SHS scientists during this step is not the figure of the expert but the one of a situated instructor enlightening the technicians and the industrials about the problems and the questions raised by the scenarios under discussions.

Since The MIAUCE scenarios presented in the three domains of application were obviously centered on the bright impacts of technologies, it was difficult for the MIAUCE partners to clearly figure out exactly the scope of the socio-technical choices they faced. Moreover, the technologies are not merely 'introduced' into society, nor do they conform, in their existence and evolution, to the designers' preconceptions. In every technology resides a possibility of misuse. For these two reasons, we decided to use the methodology developed in the SWAMI [4] project and consisting in

[4] Punie, Y., Delaitre, S., Maghiros, I. & Wright, D. (eds.) "Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities". SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission

broadening the scope of inquiry, from the bright secarios described, to more realistic, and darker versions of application scenarios epitomizing the potential dangers and misuses of the same technologies. The process highlights vulnerabilities and threats. These dark versions of scenarios are very valuable to unveil internal limits and potential risks carried by scenarios. In our deliberative approach, these dark scenarios, even fictional as they are at this stage, have helped the various partners to better understand the importance of issues at stake.

This collective exercise has led the MIAUCE team to re-design the technologies involved in the scenarios and to re-consider their contexts of implementation **in order to make them respectful to human and democratic values and compliant with the legal frame that organizes our society.**

Major results of this step are presented in **Chapter 2 and chapter 3** of the deliverable 5.2.

The whole process followed into the WP5 can be considered as a collective learning process :

- *For SHS, this second year of the project gave them the opportunity both to better define their position and responsibilities into the project and to adapt their methodology to make it more efficient and accessible to all partners;*

- *For the industrials and scientist in charge of the project design, this process made the issues and the values questioned by the technologies at work more tangible and then allowed a better understanding of the importance to question and to adapt technological design as to make it, from the very first stage of the conception, as compliant as possible with the human values and legal principles sustaining our deliberative democracy. This process has also reinforced all partners' awareness of their social responsibilities.*

under contract 006507, November 2005. http://swami.jrc.es

CHAPTER 1: HUMAN SCIENTISTS IN THE MIAUCE PROJECT

INTRODUCTION

This first chapter addresses the question of the status and of the responsibility of human sciences in technological project funded by European Commission, that aims at developing surveillance, detection and monitoring systems targeted at human beings. Besides technological challenges, these technologies raise societal issues with crucial impacts on both the individual autonomy of the 'users' and the vitality of the democracy, two societal values we consider mutually productive of each-other, or "co-original"[5]. This first chapter gives an overview of the experience and reflections of the authors who, from their respective backgrounds in ethics, law and sociology, have now been committed in the MIAUCE project for a time sufficient to draw the first methodological conclusions regarding their interactions with scientific and industrial partners specialized in body recognition and tracking technologies, and their applications.

1. FROM TECHNOLOGY ASSESSMENT TO VALUE SENSITIVE DESIGN

Along the different framework programs (FPs) organized by the European R&D, the status and responsibilities of human sciences have evolved. Three major steps characterize this evolution, showing a gradual shift from a general policy advisory role to a more local and instrumental role inspired by the "value sensitive design" paradigm. At the very beginning of the FPs, human sciences were supposed to provide political guidance and recommendations regarding the

[5] The relationship between **co-originality**, in the sense given to the concept by Habermas against Rawls (co-originality of individual and collective autonomy, inseparability of individual liberty and deliberative democracy), and **co-construction,** in the sense given by Jasanof (co-construction of techno-science and society through the mutual reinforcement of the representational regimes carried by technology and in society.)

Maybe the concept of **co-generationality** may be misleading in the present context, if the reader tries to connect it to the known theories of co-originality and co-construction. We would opt for using "co-originality" here, as it situates our thought from the start in the habermasian theory of communicational action, which is quite relevant for our position.

For references, on the relation between private and public autonomy, here is the text of the footnote 19 of Antoinette Rouvroy's paper on « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », Studies in Ethics, Law and Technology , Berkeley Electronic Press, 2008. :

« The inspiration for the link between private and public autonomy (the idea that they are 'co-originated' or mutually productive of each-other) is to be found in Jürgen Habermas's discourse theory of law (especially in Between Facts and Norms, MIT Press, 1996) according to which "Just those action norms are valid to which all possibly affected persons could agree as participants in rational discourses". One could interpret as an application of this thesis of the co-origination thesis the defense of privacy on the ground of its structural value for society to be read, for example, in Paul M. Schwartz, and William M. Treanor, "The New Privacy", Michigan Law Review, 101, 2003, p.216. On deliberative autonomy, see James E. Flemming, "Securing Deliberative Autonomy", Stanford Law Review, Vol. 48, N.1, 1995, pp. 1-71, arguing that the bedrock structure of deliberative autonomy secures basic liberties that are significant preconditions for persons' ability to deliberate about and make certain fundamental decisions affecting their destiny, identity, or way of life. On deliberative democracy, see James E. Flemming, "Securing Deliberative Democracy", Fordham Law Review, Vol. 72, p. 1435, 2004. Endorsing the concept of a co- originality of private and public autonomy as developed by Jürgen Habermas in Between Facts and Norms. On the concept of co-originality, see Rainer Nickel, "Jürgen Habermas' concept of co- originality in times of globaliation and the militant security state", IUE Working Paper Law, 2006/27. »

Commission's technological policies and investments. At this stage, a major challenge consisted in providing an advisory body composed of human scientists with an institutional settlement that would guarantee their independence and autonomy, against various pressures and undue influences from political, technological and industrial spheres. Following criticisms motivated by the general advisory recommendations' lack of impact over projects at work, a second step in the evolution of the role of SHS in FPs was marked by the development of TSER programs which funded human sciences projects dedicated to societal aspects involved in R&D projects supported by the Commission. The results of this second step were also much criticized for keeping technical and societal projects separated and without interactions. In order to respond to the crucial necessity of interdisciplinarity and dialogue between SHS and technology, a further strategy has been deployed in FP6 and FP7, integrating SHS *into* technical R&D projects, with the specific responsibility to impact on technical designs as to make them, from the start, "socially compliant" or acceptable. This strategy, inspired by social constructivism and by the theories of the social shaping of technology, which all consider that technological artifacts are *socially* constructed by the actors involved in both their design and appropriation. At the methodological level, this theoretical position has given rise to the so-called "value sensitive design" oriented towards an enhanced integration of 'moral values' from the very starting stage of technological design.

During this project we have experienced different figures or roles from which to assess the ethical aspects the contemplated technologies. Two main objectives or considerations have shaped these figures.

The first objective pointed towards the "*internal governance*" of the project, the ethical scene being here restricted to the teams of industrials and scientists involved in the project. On that scene, our main task was to set up the conditions for a sound collective deliberation on ethical issues and dilemmas raised by the project. To work towards this objective, we have tried different figures or roles, and we feel the are worth discussing and assessing, to foster the potential to learn from this experience.

Our second objective was targeted towards the "*external governance*" of the project, aiming at including "society at large" into the deliberations about the technologies at work. At stake is the possibility to make a wider deliberation emerge from the restricted scene of one specific project and, in this way, to contribute to building the conditions for widening the democratic debate around these technologies and the societal issues they involve. This concern for external governance raises the difficult challenge – political and pragmatic- of widening the scene for the democratic deliberation, considering that the technologies at work into the project are bearing societal issues and projects that have to be deliberated on a larger scene. Both internal and external governance aspects of our contribution to the MIAUCE project could hopefully help the European authorities to better define and design the responsibilities and roles of human scientists in future R&D European programs.

This integration of human sciences within technological projects raises at least three major critical questions.

The first one relates to the 'figures' social scientists can endorse when participating into a technological project. This first question attests to the underdetermination of human scientists'

'role' and responsibilities in such a context, and of the 'values' that should guide their contribution and cooperation with the other stakeholders.

The second question challenges the status of the human sciences' discourses when they take part in the design of a technological artifact.

Finally, the integration of SHS within the technological design process raises the question whether and how the involved SHS teams should or could widen the scope of their intervention as to address societal issues raised by the project they are involved in on a wider scene, and, in this way, foster democratic debates on the relevant ethical, legal and societal issues.

2. THE FIGURES OF HUMAN SCIENTISTS

2.1. The limits of the expert status

Traditionally, discussions on ethical issues are circumvented by the acknowledgment of an ethics committee of any sort, in charge of providing, *ex ante*, all relevant recommendations for having ethical standards complied with. The figure endorsed by the ethics committee members is the figure of the expert. In the MIAUCE project, the SHS team does not consider that figure to be the most appropriate to endorse.

More than a set of standards to be complied with, ethics, Jean Ladrière suggests, is a "savoir-faire", a capacity to make moral choice when faced with situations raising unprecedented ethical dilemmas or challenges. In that frame, Ladrière[6] emphasizes that ethics is not the 'exclusive business' of experts in ethics: ethics cannot be transferred or learned as a theoretical knowledge but has to be practiced in order to be genuinely appropriated by those who face an ethically challenging situation. As a consequence, Ladrière explains:

> *... nobody has a privileged competency in ethics. This is why an ethical approach could only be a collective process through which the different positions have to be confronted, with the hope of a convergence of these positions justified by the believe of the universality of the human reason*[7].

Agreeing with Ladrière's position forces us to consider alternative figures we have and could endorse, as SHS scientists in the MIAUCE project, and to clearly identify our responsibilities and legitimacy into the project.

2.2. From learner to facilitator

Various figures have successively marked the participation of the human scientists into the MIAUCE project. These positions are much in line with what Ladrière suggests regarding the role of "accompanier" that human scientists should have into the ethical process. This role appeared difficult to play during the project since the explicit expectations of the scientific and industrial partners were more demanding for the figure of the expert, deciding for them on ethical issues,

[6] Ladrière, J., *L'éthique dans l'univers de la rationalité*, Artel / fides, Namur, 1997.

[7] Ibidem

giving them clear indications of what is socially acceptable and what is not, and of how to design the technology and its applications as to make them socially acceptable and compliant with legal requirements.

2.2.1. LEARNER

"Learner" is the first figure that human scientists have adopted into this project. In fact, this project confront human scientists to unknown technological devices that they have to deeply understand in their specifications and constraints in order to be able to dialogue with their scientific, technical and industrial partners in the project. This learning process does not only concern the technical bases and knowledge at work into the project but also the inherent or implicit societal assumptions guiding and shaping the design of these technologies. In that sense, being involved from the design stage of technological development gives us, as human scientists, an interesting opportunity to investigate the technology from an 'insider' point of view and to better approach technical choices and the related assumptions regarding human beings and societal meanings. Among other things, being directly involved into this project gives us the opportunity to better understand the technicalities and implications of devices supporting human body modeling and the 'interpretation' of patterns of human bodies'expressions through, for example, a 'grammar of emotions' designed to interpret facial expressions. Our 'insider' learner position also allows us to better understand the processes and rationales involved in the constitution and enrichment of users' profiles, their contribution to the individualization and contextualization of service and information delivery, and the societal implications thereof. Grasping the complexities of the profiling processes is indeed crucial for understanding what, exactly, and how, individualization and contextualization of services and information provision may raise societal concerns.

To support this learning process, we have organized visits to the associated laboratories and developed a questionnaire, which each associated team has filled, concerning the technology, its deployment into applications, its social meanings, from the point-of-view of each partner, and the related societal issues. This questionnaire and its analysis helps to better identify and understand the rationalities at work, as well as the motivations held by the technical and the industrial teams when working towards the development of these technologies and their related applications.

2.2.2. INVESTIGATOR OR TRANSLATOR

The second figure adopted by the human scientists in this project is the figure of the investigator or the translator. This figure consists in repositioning the technologies involved in the project within a broader technico-social landscape. Through this figure, the major societal trends and expectations that give rise to such project are questioned in order to clarify the societal background. This societal background can be approached through the analysis of both scientific literature and political discourses that compose the implicit or explicit frame of the project. At this stage, the role of SHS scientists consists in drawing this framing landscape, the cultural, social, economic, philosophical specificities of the time that encourage the development of such projects whilst also supporting the claimed legitimacy of its resulting applications. The investigator or translator figure is important, for it allows to better capture the rationality and the "claimed legitimacy" supporting this kind of

projects and the subsequent assumptions about the added value it brings to the society. In order word, this research aims at unveiling the regimes of justification (Boltanksi and Thévenot[8]) or the 'Cui Bono' framing the project. For instance, it appears obvious that the MIAUCE project carries and relies on an implicit set of assumptions articulating societal demands for increased security with specific preconceptions identifying observations about the human body (and its observable patterns of appearance and behaviours) as the ultimate source of *truth* about human individuals, and as having a privileged predictive value regarding the future actions, behaviors, preferences of these individuals. This is one of the tacit epistemological assumptions reinforcing the "legitimacy claims" of body tracking and emotion recognition technologies.

2.2.3. INSTRUCTOR

The third role adopted by social scientist is the instructor one. As instructors, social scientists have to explore and ease the understanding of ethical, legal and societal issues raised by the project. This role is exploratory and explanatory, and tends to prepare the collective ethical and societal deliberation to be held with all teams involved within the project. This task, as it will be explained in the next section, is not neutral. It consists in confronting what social scientists observe from their insider position in the project about its societal framing to the values and the principles coming out from our tradition and culture. This requires the human scientists to clearly set up the working or explorative principles and values from which they assess and analyze the project and the associated technologies, and thus, to situate their analysis and assessment. The working and explorative principles we adopted, and that we selected for the reason that they are among the very rare principles reaching a large consensus in social sciences, with conceptual translations across the various disciplines (especially across the disciplines of ethics, law and sociology), are the principles of autonomy on the one hand, and deliberative democracy on the other hand. These two principles or 'values' will serve as the ultimate ideals against which to assess and evaluate the ethical, social and legal implications of the MIAUCE project, and as guiding principles for identifying the objectives of "value sensitive" design.

This assessment obviously requires to understand the finality of the technology developed and to identify their potential applications, as to measure the impact they may have on 'users' autonomy and on the vitality of deliberative democracy.

2.2.4. FACILITATOR

The fourth role is the role of facilitator. This role implies the responsibility of setting a sound ethical deliberative process amongst the teams involved. It is supposed to remain neutral as much as possible, in order to keep a critical distance from the debates and the participants. It is a kind of intermediary, facilitating both negotiations consensus building. Michael Doyle (2007) characterizes the facilitator as:

[8] Boltanksi, L. and Thévenot, L., De la justification. L'économie de la grandeur, Gallimard, Paris, 1999.

> *An individual who enables groups and organizations to work more effectively; to collaborate and achieve synergy. She or he is a 'content neutral' party who by not taking sides or expressing or advocating a point of view during the meeting, can advocate for fair, open, and inclusive procedures to accomplish the group's work.*

Two remarks have to be made about the facilitator's role into the MIAUCE project. First of all, as will be explained later on, as facilitator we have encouraged and activated the collective deliberation by broadening the scope of current application scenarios first presented by the technical and industrial partners. Through this broadening process, we have drawn or designed 'dark versions' of the actual scenarios in order to emphasize societal issues virtually raised by the MIAUCE project and to bring 'empirical' evidences sustaining the necessity for a sound societal deliberation about the development and implementation of such technologies. Secondly, contrary to the neutrality imperative claimed by M. Doyle, we consider this requirement as a fiction since we, as human scientists, are also stakeholders of this MIAUCE project. Therefore we acknowledge our position as *situated* facilitators[9] bearing, just as every other stakeholders, moral and ethical values guiding our intervention and contribution to the project. This status of situated facilitators requires us to define and explain our ethical or moral background. This clarification will be made in section 3.

From expertise to situated speech

Our initial mandate into the MIAUCE project consisted for the most part in addressing the social, legal and ethical issues raised by the surveillance and observation technologies developed in the project, and to assess its social acceptability. Yet, the concept of "social acceptability" itself deserves some critical assessment.

3.1. Utilitarianism and relativism of the social acceptability concept

Inspired by a kind of preference utilitarianism maintaining that whatever satisfies the preferences or desires of an individual involved in an action is morally right (see, for instance P. SINGER), M.W. BRUNSON [10] defines acceptability as:

> *A condition that results from a judgmental process by which individuals 1) compare the perceived reality with its known alternatives; and 2) decide whether the real condition is superior, or sufficiently similar, to the most favourable alternative condition.*

According to BRUNSON, the term 'social acceptability' refers to aggregate forms of public consent whereby judgments are shared and articulated by an identifiable and politically relevant segment of the citizenry. In this perspective the norms emerge form a democratic exercise involving all the concerned actors.

---

[9] Beside this, one can say that the diplomat could be another valuable attitude, because of that figure facilities also interactions between opposite camps. But finally, we did not decide to choose that figure because of the risk of compromises that it contains. For a discussion about the diplomat figure, see the MIAUCE deliverable D.5.1., 2007.

[10] Brunson, M., W., « A definition of "social acceptability" in ecosystem management" in Brunson, M., Kruger, L., Tyler, C. and Schroeder, S., (Eds.), *Defining social acceptability in ecosystem management: a workshop proceedings*, General technical Report PNW-369, Portland, 1996.

Beyond the pragmatic problems (democratic representation, deliberative procedures, asymmetry of actors capabilities, etc) raised by a such an approach and well analyzed by M. MAESSCHALK 11 and beyond the critical aspects of a sound and practical methodology that could be applied in the restricted frame of the project, this social acceptability approach confronts us to two major problems.

First, the concept of social acceptability conveys us to a scene on which the technological project and its embedded social meanings cannot be refused nor contested but merely adjusted, re-shaped as to make it compliant to the 'public' judgment and settlement. Using this social acceptability realm forecloses any radical critique, opposition or contestation, and subtly engages us on the path of silent conciliation. In other words, this arguably narrows the margins of action or the latitudes we have, as social scientists, in this type of exercise. That is why, following the recommendation drawn by Marris and alii, we will not indicate

> *"how to improve the social acceptability [...] without changing the nature of that which is "accepted" (…) "Improving the social acceptability" of technology can be envisaged stereotypically either as rendering a proposed finished technology (or product, or decision) accepted by promoting change among the public or as rendering the technology acceptable, by promoting change in the technology development path. The first interpretation is the most commonly found, both in the expectations of those who promote (and fund) the public perception research, and in the work of some social scientists in the field. We do not believe that social science research can or should aim simplistically to improve the social acceptability of technologies, if it means to facilitate the smooth (uncontroversial) social uptake of a technology without making any changes in the technology development path. Instead, we suggest that social science research could be used by decision-makers to circumvent or reduce public opposition to technologies, but only to extent that decision-makers utilizing the results take on board that it is perhaps not so much the misguided public which needs to be reformed, but the institutional practice and technological objects which this public is reacting against. ".* [12]

The second problem inherent to this approach concerns the legitimacy of the norms produced by such utilitarian reflection since it postulates that what is acceptable for a majority is good for all. This raises questions regarding the soundness or the goodness of the norms that can emerge from such social acceptability exercise. In practice, this exercise threatens the non conditionality of the individual fundamental rights, and renders the pursuit of social justice dependent of the good will of the majority. Current public debates about the deployment of video surveillance epitomize the phenomenon as it exhibits a trade-off between liberty (and privacy) rights and aspirations to security by the majority.

---

[11] *See for example :* Maesschalk, M., "Quelle philosophie des normes aujourd'hui? Gouvernance et apprentissage social » in *Les Carnets du Centre de Philosophie du Droit*, n°138, 2008.

[12] Marris et alii, *PABE Final Report*, 2001, p. 14.

These threats to the non-conditionality and indivisibility of fundamental rights reinforce the need for a deliberative approach grounded in an ethically and morally informed theory of justice. (see Delivrable 5 (Chapter 4) of the 1st year's MIAUCE scientific report).

This raises complex questions with regard to these principles' status and definition.

3.2. From normative to explorative ethical principles

Let us first examine the status of these principles. This status must be defined according to the pedagogical aims we try to achieve into the MIAUCE project. By pedagogical aims, we mean a clear refutation of any expert approach in which human scientists would endorse the responsibilities of defining the good, the fair nor legitimize the MIAUCE project and its technological specifications.

According to Ladrière[13], as already pointed out, ethics is based on ability or capability. It is not a theoretical or normative abstract knowledge that one could define and transfer to others. But it is a *praxis*, an ability to face a situation ethically.

This position is very close to those ones developed by Dewey or Rorty who underline that the permanent research of universal and fixed norms into ethical approach can be compared to the quest of certainty in epistemology, which is at the source of so many problems badly defined and solved. In that sense and according to Ladrière, the role of the so-called expert is not to decide in place of the concerned actors but to make the deliberation possible and to enlighten it by clarifying the ethical questions raised by the situation at work.

According to Ladrière, the ethical approach can only be collective and democratic, based on the confrontation of different positions. In this collective deliberation, the responsibilities of the so-called expert are to explore the ethical issues involved by the technologies in progress, to elaborate methodologies to support a sound democratic deliberation and to inform this deliberation with his/her knowledge of the ethical tradition or cultural ethical heritage framing the deliberation.

Here, again this position is much in line with what Dewey[14] suggests when saying that we never affront an ethical problem from a "tabula rasa", without using some ethical references or principles transmitted by the tradition. But for Dewey as for Ladrière, these principles are not fixed rules that could, as in a cooking recipe, tell by themselves what to do, how to act, determining quasi mechanically the fair way or the ethical course for our decision and action. For Dewey, these principles are explorative or analytical tools useful to enlighten a situation and to assess the various points of view expressed by the concerned actors. Dewey admits that general ideas such as justice, dignity, or fairness are of value as tools of inquiry to question and forecast unknown ethical puzzles. They have no intrinsic normative force but constitute a sort of moral background that may help facing an unknown moral situation.

[13] Ladrière, J., *L'éthique dans l'univers de la rationalité,* Artel / fides, Namur, 1997.

[14] Dewey, J., *Démocratie et éducation*, Armand Collin, Paris, 1975.

3.3. In search of explorative principles: the ethical posture of the Parrhesiast.

In order to embrace these authors' views, and to implement them in practical situations, rendering explicit the moral background or the exploratory principles on which we, as social scientists, are engaged within the MIAUCE project is crucial.

To do this exercise, we have adopted the concept of parrhesia developed by Foucault (1983). According to Foucault:

> *"Parrhesia is a verbal activity in which a speaker expresses his personal relationship to truth, and risks his life because he recognizes truth-telling as a duty to improve or help other people (as well as himself). In parrhesia, the speaker uses his freedom and chooses frankness instead of persuasion, truth instead of falsehood or silence, the risk of death instead of life and security, criticism instead of flattery, and moral duty instead of self-interest and moral apathy [15]."*

This attitude appears to be very critical in order to first situate the social scientists' speech into the MIAUCE project and secondly to make more explicit the implicit background we are using to explore the unprecedented ethical situation created by the technologies at work. As Foucault underlined, the major interest of the Parrhesiast figure consists in the non-performative characteristic of the expression of 'truth', that lets the situation clearly open and exposes it to an undetermined risk[16]. Parrhesia is defined by Foucault as the art of truth-telling courageously in the risky and free act [17].

This attitude is well explained by Carlas and Smircich[18] when underlining

> *" In Barbara Townley's[19] words, following Foucault, some of what this entails is for authors to specify the aspects of the world with which they are trying to engage and why; to situate knowledge and so de-reify it; to speak in a way that takes ownership of their arguments, and to be accountable for the choices made."*

3.4. The collective us: the shared explorative principles of the social scientists

Two main principles or values appear to be shared by us, as social scientists when endorsing this parrhesiast attitude. These principles shape a sort of community of understanding of the situation experienced, as social scientists, into the MIAUCE project.

---

[16] Foucault, M., *Le gouvernement de soi et des autres, Cours au Collège de France 1982-83*, Gallimard, 2008, p. 60.

[17] Idem, p. 64.

[18] Calas, M., B. and Smircich, L., "Past Postmodernism? Reflections and Tentative Directions" in *The Academy of management Review*, Vol. 24, Issue 4, 1999

[19] Townley, B., "Writing in Friendship" in *Organization*, Vol.1, Issue 1, 1994

The first principle relates to the autonomy of the subject and the second, to democracy, these two terms being intrinsically related by a process of co-originality each being a necessary (but not sufficient) condition of the other.

These principles have a twofold role in our approach: an explorative role helping us to face and explore unknown ethical situation related to the MIAUCE project but also a supportive role since these principles define the basic conditions for a sound deliberation about ethical situations.

Let us examine those two principles.

3.4.1. FROM AUTONOMY TO CAPABILITY

The autonomy of subject can be approached in a very broad and protectionist way of thinking defining the rights, the privacy and the liberty to be protected. Our concept of autonomy refers to a person's capacity for self-determination in the context of social or moral choices. This definition is very broad and difficult to work with since it remains very abstract and universal. To develop this concept and to make it more tangible and workable into the project, we adopt the concept of capability developed by Nussbaum based on Amartya Sen's concept of substantial freedoms[20]. Nussbaum[21] defines the concept of capability by raising the Aristotelian question "*What activities characteristically performed by human beings are so central that they seem definitive of the life that is truly human?"*. Her answer consists in the identification of the ten fundamental capabilities that make the life human.

***1.* Life.** *Being able to live to the end of a human life of normal length . . .; not dying prematurely . . .*

***2.* Bodily health** *. . . Being able to have good health, including reproductive health; being adequately nourished . . .; being able to have adequate shelter . . .*

***3.* Bodily integrity**. *Being able to move freely from place to place; being able to be secure against violent assault, including sexual assault . . . ; having opportunities for sexual satisfaction and for choice in matters of reproduction*

***4.* Senses, imagination, thought**. *Being able to use the senses; being able to imagine, to think, and to reason--and to do these things in . . . a way informed and cultivated by an adequate education . . . ; being able to use imagination and thought in connection with experiencing, and producing expressive works and events of one's own choice . . . ; being able to use one's mind in ways protected by guarantees of freedom of expression with respect to both political and artistic speech and freedom of religious exercise; being able to have pleasurable experiences and to avoid non beneficial pain*

***5.* Emotions**. *Being able to have attachments to things and persons outside ourselves; being able to love those who love and care for us; being able to grieve at their absence, to experience longing, gratitude, and justified anger; not having one's emotional developing blighted by fear or anxiety. . . .*

***6.* Practical reason**. *Being able to form a conception of the good and to engage in critical reflection about the planning of one's own life. (This entails protection for liberty of conscience.)*

[20] Both the concept of capability and substantial justice have first been developed by the Nobel Prize Amartya SEN in Inequality Re-examined, Oxford University Press, 1992 and in the book published in collaboration with Martha NUSSBAUM, Quality of Life, Oxford Clarendon Press, 1993.

[21] This part is based on the synthesis made by J. Garret : Martha Nussbaum : on Capabilities and Human Rigths, www.wku.edu/~jan.**garrett**/ethics/**nussbaum**.htm

***7.* Affiliation**. *Being able to live for and in relation to others, to recognize and show concern for other human beings, to engage in various forms of social interaction; being able to imagine the situation of another and to have compassion for that situation; having the capability for both justice and friendship. . .*
***8.* Other species**. *Being able to live with concern for and in relation to animals, plants, and the world of nature.*
***9.* Play**. *Being able to laugh, to play, to enjoy recreational activities.*
***10.* Control over one's environment**. *(A)* Political*: being able to participate effectively in political choices that govern one's life; having the rights of political participation, free speech and freedom of association . . . (B)* Material*: being able to hold property (both land and movable goods); having the right to seek employment on an equal basis with others . . .*

Table 1. Martha Nussbaum's capability concept

Source : List elaborated by J. Garret (op. cit.) from Martha Nussbaum, ***Sex and Social Justice****, Oxford University Press, 1999*

According to Nussbaum, those capabilities define life as human and are the necessary conditions for the human autonomy. This means also that any changes being technological or political treating critically one of those capabilities treat at the same time the humanity of the life. By this concept of capabilities, Nussbaum contributes to give a more pragmatic view of what makes possible the human autonomy being not only the capacity of self-determination but also conditioned by a set of capabilities that make this autonomy possible and human.

This way of defining capabilities concept agree with our previous definition of autonomy ast stated in deliverable of the 1st year[22] which includes both autonomy as "freedom from unreasonable constraints (from the state or from others) on the construction of one's identity" and autonomy as "control over (some) aspects of the identity one projects to the world."

3.4.2. FROM AUTONOMY TO DEMOCRACY

The second term or explorative principle of our "collective us" consists in democracy, considered as critical social organization that guarantees the possibility of constant renegotiation of the basic rules of fairness and justice. This concept of democracy is very central in our exploration of MIAUCE project and as such needs to be clarified.

Along with Sen we agree about the three critical ways in which democracy enriches the lives of the citizens.

> *« First, political freedom is a part of human freedom in general, and exercising civil and political rights is a crucial part of good lives of individuals as social beings. Political and social participation has intrinsic value for human life and well-being. To be prevented from participation in the political life of the community is a major deprivation . Second… democracy has an important instrumental value in enhancing the hearing that people get in expressing and supporting their claims to political attention (including claims of economic needs). Third…the practice of democracy gives citizens an opportunity to learn from one another, and helps society to form its values and priorities… In this sense, democracy has*

[22] Cfr. Delivrable MIAUCE D5.1.1. , p. 134-135

constructive importance, in addition to its intrinsic value for the lives of the citizens and its instrumental importance in political decisions.» [23]

According to this approach, democracy is at the same time the condition for the autonomy of human individuals and conditioned by this autonomy. But the value of democracy also concerns its constructive role since, as well underlined by Sen, as a process, democracy plays a critical role in the formation of values and in the understanding of needs, rights and duties [24].

In our project, democracy as presented above will serve as explorative principle but also as constructive principle to shape the deliberative exercise with the partners about the ethical and social issues raised by the MIAUCE technologies.

4. EXTERNAL GOVERNANCE: CITIZENS' JURIES AND THE STRENGTH OF WEAK LINKS

This external governance issue relates to the necessity to open the democratic deliberation process about the technologies at work to the society at large. Set like that, this aim or ambition appears quite unrealistic since 'society at large' remains a very abstract and fuzzy concept.

In the present deliverable, we will not develop the approach that will be mobilized to support this democratic process, which will be fully specified and applied during the 3d year of the project. We will merely briefly consider the two main orientations that will be explored in this regard. The first one consists in the "citizens' jury" methodology as an attempt to hear people's voices. This methodology is clearly an alternative to most common quantitative surveys based on large samples of people and to qualitative consultation of experts. The second orientation we would like to explore regards the composition of the jury. According to the general methodological guidelines supporting the citizens' juries approach, the panel has to be set on a 'best fit' (demographic) sample of 12 to 16 members of the public. Within the MIAUCE project, we intend to explore two types of panel: the first one, classic, based on a demographic sample of the general public and the second one, less traditional, and composed on a demographic sample of the population (or their representatives) most critically targeted by the considered technologies since they express or live situations that are at the margins of the dominant paths of the society. This confrontation between two panels should help balancing the needs for security and safety of the ones against the risks inherent to observation technologies as perceived by the others. This approach and its results will be fully developed in the deliverable 5.3.

[23] Sen, A., "Democracy as Universal Value" in *Journal Of Democracy*, 10.3, 1999

[24] See also on this approach : Sunstein, C., R., *Why Societies needs Dissent*, Harvard University Press, 2005.

CHAPTER 2: SURVEILLANCE TECHNOLOGIES: VISION, TYPOLOGY AND LEGAL CONTEXT

INTRODUCTION

This second chapter aims at situating the technologies at work into the MIAUCE project in their broader context. This exercise is critical to understand the issues raised by these technologies regarding the autonomy of the individuals and the vitality of democracy. The first section questions the epistemic settlement of these technologies showing their specificities especially the primacy given to the body as privileged source of 'truth' about the persons, their preferences and their intention. The second section aims at situating the major finalities currently supported by those technologies. Those finalities regard first the security and the surveillance and secondly the marketing and the people profiling. To better explore those finalities, two typologies are drawn showing the critical elements articulating such systems in these two domains. In the next section we present the application's context of the MIAUCE technologies. This application's context does concern security or safety finalities with the scenario 1.3. and the marketing finalities with the scenarios M.1.1. and TV.1.1. The current scenarios as they are currently designed are very positive or benevolent in their intentions. In order to improve the collective understanding regarding the risks raised by those technologies for the autonomy of individuals and the democracy and because the same technologies can be deployed in other more risky contexts, we will broaden their scope drawing dark versions of the proposed scenarios. The last contextual exploration regards the social and the legal contexts. Regarding the social contexts, we explore the major changes and risks raised by those technologies for the autonomy of people and the democratic organization of the Society. In the last section of the chapter, the legal frames challenged by these technologies are presented and discussed showing that some traditional legal concepts and norms are particularly difficult to apply when facing the technologies at work.

1 EPISTEMOLOGICAL CONTEXT: FROM MULTIMODAL OBSERVATION PARADIGM TO SURVEILLANCE SOCIETY

As explained in the general introduction, the "multimodal observation paradigm" combines multimodal capture of data "extracted" from human bodies (facial expressions, eye gaze, postures and motions) with an implicit understanding or interpretation of these data as valid and privileged sources of "truth" about the persons, their preferences, intentions etc. following the preconception according to which the 'body does not lie' whereas, *a contrario* anything transiting through the prism of individuals' consciousness is *a priori* suspect and unreliable. This paradigm and its related hypothesis decreases the subjects' self-determination (autonomy). The deterministic codes of intelligibility built in the multimodal observation paradigm do not allow individuals to impact on the "informational image" compiled of themselves nor on the interpretation thereof. Moreover the "informational" image of the subject has performative effects on the real subject's perceptions of what is expected in terms of attitudes, behaviours and preferences, with the result, already exposed in the previous deliverable, of increased democratically detrimental anticipative conformity in society.

These technologies are in line with a larger context that many authors, belonging to the so-called surveillance studies, have characterized as a surveillance society. There was a crucial question to debate in the case of MIAUCE: is the intentionally of surveillance necessary to define the

surveillance, or is it sufficient to think that the simple presence of CCTV marks the location as monitored? In the case of the MIAUCE scenarios, can we define them all as surveillance scenarios? Beyond the risk to appear paranoiac, one can think that we cannot accept the term of surveillance to define the MIAUCE scenarios, because of the precaution of the intentionality. For example, the M.1.1 scenario is not devoted to surveillance, but to marketing purposes. The "multimodal observation paradigm" is more neutral about the intentionality of the scenario.

Moreover, one thinks important to situate these multimodal observation scenarios in a broader context. In order to better analyze the major societal issues and questions raised by the MIAUCE project, it is important to resituate this project in the broader context that spawns its socio-political significance. As Murakami and Wood underline in *A report on the surveillance society* (2006), this also provides a perspective from which to approach and understand the technologies involved.

So when looking at the technologies and at the related scenarios, even if they are not oriented only by towards security applications, they are nevertheless deeply rooted in and inspired by a worldview and an epistemology typical of the 'surveillance society'.

> *To think in terms of surveillance society is to choose an angle of vision, a way of seeing our contemporary world. It is to throw into sharp relief not only the daily encounters, but the massive surveillance systems that now underpin modern existence. It is not just that CCTV may capture our image several hundred times a day, that check-out clerks want to see our loyalty cards in the supermarket or that we need a coded access card to get into the office in the morning. It is that these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living.* (p. 1)

According to C. Norris and alii [25] the growing presence and deployment of surveillance technologies can in part be explained by what they called 'the globalised trends of the late modernity':

> *There has clearly been an expansion of CCTV surveillance around the world, especially in private sector surveillance, and there appears now to be an accelerating diffusion into the public realm. The globalised trends of late modernity have accelerated this growth. Increasing urbanisation has exacerbated the trend towards anonymity, leading to concerns over establishing and verifying identity. Increasing mobility, both locally and internationally, have given rise to a global 'stranger society', where social control and governance based on intimacy and face-to face knowledge are increasingly less viable. Risk management has also become the dominant mode of reasoning for both international corporations and governments alike. In the realm of criminal justice, reformist ideals have given way to more modest preventative responses that focus on 'opportunity reduction',*

[25] Norris C. and alii, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", In *Surveillance and Society*, 2 (2/3), pp. 110-135, 2004.

'situational prevention' and 'risk management', and CCTV can be seen as part of the trend towards a New Penology based on actuarialism (c.f.: Feely and Simon, 1994).

So, even if the MIAUCE scenarios have not, as such, surveillance and prevention of insecurity as explicit finalities, they nonetheless rely on purposeful, routine, systematic and focused observation of persons, for the sake of control, entitlement, management, influence or protection. These elements, according to Murakami and Wood, are definitional of surveillance (Murakami & Wood, 2006, p. 4).

2 TYPOLOGIES: FROM OBSERVATION TO MARKETING

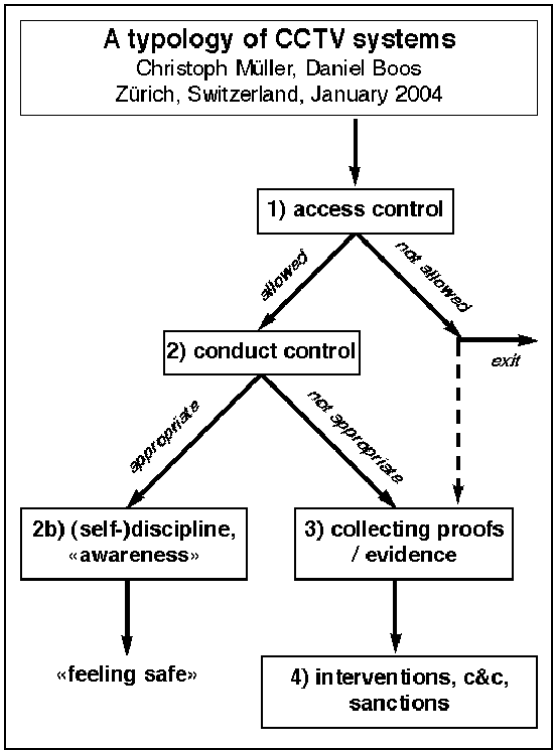
The MIAUCE scenarios develop two main finalities, which are (1) surveillance purposes, controlling public space -S.1.3.- and (2) marketing purposes – M.1.1 and TV.1.1.

2.1. A typology of surveillance

Surveillance systems, or rather, observation systems, as we prefer to call them in the context of Miauce applications, can work towards different goals and be supported by various technico-organizational arrangements. To better approach these technologies, it is important to clarify the various arrangements and intentions that may support and motivate these systems. C. Müller and D. Boos (2004) have identified a series of criteria relevant to establish a typology of surveillance (or observation) systems:

- false or real cameras?
- targeted at private or on public space?
- for prevention or for interventions?
- visible or hidden?
- recording or not recording observed events?
- real-time observation or not?
- isolated cameras or networked systems?
- focusing on individuals or on groups?
- with systematic analysis or not? (i.e. 'filtered' or not?)
- records cross-matched with other data bases or not?
- People as individuals or as a collective / crowd?

Based on these criteria, Christoph Müller and Daniel Boos draw a typology of surveillance systems. The typology consists in four main types:



2.1.1 ACCESS CONTROL

The first type of 'surveillance' system consists in systems aimed at filtering access of persons to restricted zones or locations. This filtering may be based on behavior, appearance or identity markers (such as passport, cards, badges…). This type of systems assists the personnel in charge of entrance control in 'objectifying' admission or restriction decisions. The system functions just as an 'additional eye', with no retention or further analysis or computation whatsoever of the observed data. The filtering finalities may even sometimes be fulfilled by the mere presence of fake cameras, which may have satisfactory dissuasive impact on those without a valid ID, badge, or whatever allowing them to enter the restricted area or location.

According to C. Müller and D. Boos (2004), such 'access control system'

> *act partly (a) as a tool to support some monitoring personnel in their decisions to allow or to deny access, and/or mainly (b) as a symbol for a self-selection of access. The cameras may indeed have a dissuasive function, which is deterrence: most observed cameras are visible, their presence is marked by signs.15 The effect may be a self-selection of who is entering an area and who is not. The message of these cameras-as-signs is: 'Watch out: If you are not allowed to enter this area, you better leave...'16 The main function of this type of access control is a symbolic one: These cameras are symbols and signs. For this purpose, however, they could be dummies as well.* (p. 166)

2.1.2 CONDUCT CONTROL

The second type in the typology consists in technological surveillance (or observation) systems aimed at regulating (influence, constraint), disciplining, and/or control the conduct of persons in a given environment. The presence of cameras, reminding people that they are watched, act as incentive or disincentive with regard to certain behaviors and attitudes, irrespective of whether the cameras are real or fake, or whether images are being recorded and stored or not. Cameras function as symbolic signs making people feel either constrained and observed or safe and secure. Yet, this disciplinary, or panoptic role of the camera is, as well underlined by C. Müller and D. Boos (2004), based on a series of hypotheses or assumptions:

> *Cameras only work as a means of conduct control as long as people believe that the cameras are real (and not dummies), that they are working properly, that they are being monitored by someone, that this 'someone' would organize an intervention, if necessary, or at least that the images would be recorded and could be used as evidence for ex-post sanctions."* (p.168)

To enforce discipline and good behaviour, three conditions are needed: true cameras, data registration and analysis and human monitoring and intervention.

2.1.3 REGISTERING EVIDENCE

The third type of surveillance or observation system implies images recording and data analysis. The role of this type of systems is to collect proofs or evidences regarding hazardous or other events, conducts, etc. This type of systems belongs to another universe than the two previous ones. In the previous onest, cameras, as explained, acted more as symbols or signs that you have to not enter, nicely behavior…. With the present type of registering system, cameras play a significant role in triggering interventions or sanctions.

Regarding the use of recorded data and of analytical results, two finalities must be distinguished: the first one is supported by real-time data (images) analysis and allows for immediate intervention. The second one does not rely on recorded an stored data by default, except when such use is necessary to react to hazardous events (accidents, crimes, fraud, vandalism…). In that case, the recorded data are used for prosecution, law enforcement and judicial evidence purposes.

Two of the three scenarios contemplated in the MIAUCE project belong to this third type of system even though, in the Miauce project, their deployment is not finalized towards security applications. These scenarios are the M1.1. and the TV1.1. , serving marketing goals and rationales.

2.1.4 FLOW CONTROL AND INTERVENTION PLANNING

The main objective of this fourth type of systems is intervention planning. In that sense, this type of system has some characteristics that differentiate it from the others. First of all the objects that are surveyed are not human subjects as such, but the fluidity or obstruction of human or vehicle flows. Data analysis must be in real time in order to allow for quick intervention. The system has to be fine tuned as to respond to the occurrence of the relevant parameters attesting of any 'abnormal'

situation. This detection again can either rely on human assessment, based on experience and professional heuristic, or automatic or autonomic, relying on logical programs and algorithms.

As underlined by the authors, the system can be seen

> *...as a command and control tool for planning intervention and sanction. Once incidents are detected, the cameras may be used to coordinated police response* (p. 170)

Muller (2002) points out that there is currently an important drawback associated with this type of system: it may inspire excessive public expectations with regard to the systems and personnel's in charge of surveillance and security. This may result in a dramatic increase of professional pressure on those in charge of control, surveillance and law enforcement, with a correlative decrease in the feeling of collective responsibility of people present on the observed scene.

This fourth type of surveillance technology corresponds quite well to the S1.3. scenario, which is motivated by the wish to fasten intervention in cases of escalators' failures (due to excessive crowding, or other physical or human obstruction).

2.2. A marketing typology

Marketing strategies have evolved during the last decades. This evolution is marked by the technological progress regarding the individual data capture, retrieval and analysis. In order to understand some of the social trends that shape the technologies currently at work in the MIAUCE project, the exploration of this marketing evolution is sensible. The marketing typology presented hereafter is based on different criteria as the definition and constitution of profiles, the marketing actions, the subjects aimed, the technical devices engaged, the types and time of the marketing feedback and the visibility of the strategies. Those criteria as staged in the third type of this marketing typology are also present into the observation technologies deployed in MIAUCE even if only two of the considered scenarios, i.e. the M1.1. and the TV1.1.scenarios can be classified as marketing oriented scenarios.

Type	Type 1	Type2	Type3
Profiles definition	A priori	Ex post	Continuous
Profiles constitution	A priori sorting (A-B-C-D life style sorting)	Ex post sorting based on habits of consuming	Continuous sorting based on dynamic data retrieval related to the attitudes of consuming
Marketing action	Mass marketing based on classes of consumers (segments)	Personalized marketing	Pervasive and personalized marketing
Subject	Classes or a priori	Semi-conscious	Un-conscious Bodies

	categories - volunteers	Individuals	
Technical devices	Marketing studies and surveys	Computerized data retrieval (loyalty card, plurality of traces left by his buying and consuming actions)	Computerized and video monitoring of moves and actions
Type of marketing feedback	Campaign	Personalized messages	Environment's modification
Time of marketing feedback	Planned	Ex post - deferred	Immediate
Visibility	Visible	Identifiable	Invisible

3 MIAUCE SCENARIOS: FROM BRIGHT TO DARK VERSIONS

In this section, we present the scenarios currently drawn into the MIAUCE project. Those scenarios aim at giving life and market to the technologies developed for the project. In their current vision, those scenarios present a benevolent version regarding the future use of the considered technologies. As currently sketched, those scenarios do not show clearly the critical issues for the autonomy and for the vitality of the democracy related to these technologies and their future deployment for other purposes than those considered by the current scenarios. By drawing dark version of those scenarios sketching those technologies in non benevolent context of use, we discover the non neutrality of the technologies and the potential challenge they raise for the autonomy and for the democracy.

3.1. Description of M.1.1

The general meaning of M1.1. consists in better assess the effectiveness or the attractiveness of a shelf inside a shop. To do this assessment, the scenario has to establish statistical relationships between data collected on individual body detection, head pose estimation and gaze tracking on one hand, and on the other data concerning the shelf.

The scenario contains three main steps of deployment:

- Statistical counting of individuals passing in front of the shelf
- Statistical counting of individuals stopping more than 5'' in front of the shelf
- Statistical detection of the visual field covered by the individual in order to make hypothesis regarding the zone of the display visualized by the person.

To get the exact measure, the system has to work on an individual basis, calculating and parametering each body stopping in front of the shelf. Actually, people watch for a special product on the shelf. So they move in the front of the shelf, look at many products, select one of them and take it. During the first stage of the scenario, it takes place in an experimental environment. A shooting workplace has been set up; it is composed of four shelves hanged on a white wall. They

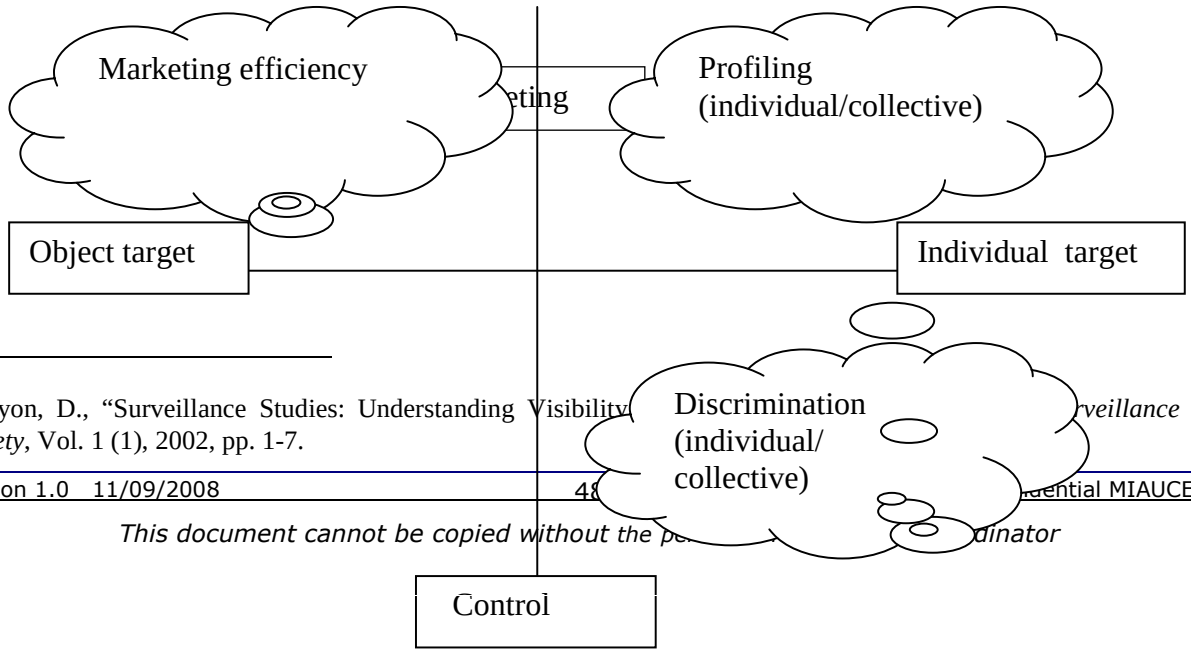
present different cereals boxes. Two cameras are needed: one for shooting the face and gaze fixation of the different persons of the shelf; and one for shooting the shelf and detect gaze fixation location on it. In a second stage of the scenario, it will occur in real conditions, mainly in supermarkets.

3.2. Towards a darker M.1.1 scenario

M.1.1. can be considered as one use case of a defined technological system. The utility of this use case is currently supported by two main hypotheses: liability (performance) and marketing or rather merchandising display (intention). In order to assess its acceptability, it is worth moving form those two hypotheses and questioning this observation system in another contextual frame. Because a performance failure, in that case, has only material incidence, we won't analyse this hypothesis in the frame of this scenario to concentrate only on intentional changes.

The current scenario addresses a shopping display hypothesis. The target of the system is people looking at a shop window. What interests the scenario knows **what is looked** into shelves, in other terms the question regards the effectiveness of the shop display. Let us change, based on the same technological system, the target of this surveillance system. So the target is no more what is looked but **who is looking** the shelves. This 'who' question can consider a **'collective who'** regarding particular social groups that could roughly being approximated by the system in terms of size, weight, dressing style, peel coloration, hair dressing, etc. It can also consider a **'personal who'** if the system is inter-operated with personal databases concerning for instance the usual customers of the shop.

These changes in the intention of the scenario open the door to crucial questions regarding the design and the use of such technologies to discriminate people and to profile them. In both cases, these new intentions of the system raise clearly the issue of the phenetic fix explained before which "*describes this trend – to capture personal data triggered by human bodies and to use these abstractions to place people in new social classes of income, attributes, habits, preferences, or offences, in order to influence, manage, or control them*"[26].



[26] Lyon, D., "Surveillance Studies: Understanding Visibility [illegible] *Surveillance and Society*, Vol. 1 (1), 2002, pp. 1-7.

It is worth rising some questions regarding the social acceptability of these technologies when being placed in this broaden context.

- Technically, is the system able to produce some discrimination effects on particular social groups based on their physical characteristics? If yes, do we, as designers, accept this 'evolution' of the system under development? If we do not accept, what can we do to protect this system against this evolved use?
- Technically, is the system interoperable with other personal databases and as such able to produce sorting and profiling of people? If yes, do we, as designers, accept this 'evolution' of the system under development? If we do not accept, what can we do to protect this system against this evolved use?

3.3. Description of S.1.3

The S.1.3 scenario aims to detect people mass blocking escalator exits to provide information for optimal response. The MIAUCE multi-modal technologies will capture images and analyse images and results. The analysis will be able to report the detection of events (mainly normal / abnormal situations) and also events logs (motion detection, highly crowded areas, blocking in escalators, etc). Practically the general idea is to record escalator exits, cameras are placed on the ceiling pointing at the escalators, both escalator entrance and exit. A real-time analysis is needed, even if some videos are kept in order to be annotated. The expected output of the analysis is raising an alarm that indicates when escalator is collapsed.

3.4. Towards a darker S.1.3. scenario

The scenario as it is presents a use-case of the technology in a specific safety context. But the same technology can be deployed in less benevolent environment. It is the reason why it is important to broaden the scope of the current scenario in order to better catch the implicit dangers or risks of this technological system for the autonomy of people and for the vitality of our democracy. This broadening process should clarify the human requirements to be incorporated into the technological design of the system. In order to provoke the questioning, imagine that this system is deployed in a non-democratic country that is well known for its active and violent repression against human rights. This situation is not futuristic; the same system can be at very good use for repressive matter.

We can imagine a strong and repressive intervention during a protest, for example. The same system could be deployed, but the purposes of intervention are oriented to the protection of the national security. The video streams are recorded in the database, and could be used as legal evidence. The context is not semi-public, like the airport, with a lot of security rules; but the context is the city centre, where the protests usually take place.

In that case, the scenario will not intervene to repair, but to repress people whose behaviours are considered as abnormal, suspicious. The system is coded with criteria [27], based on opaque parameters that sort out what is suspicious to what is not. If privacy is the most frequently discussed point, individual autonomy, transparency, consent and information are the major critiques that we can address to this system. A very important problem of categorisation, and thus of social sorting and normalisation could appear in this case.

The cameras and the related networked system become a tool of normalisation. The problem resides in the legitimacy of that normalisation: how to legitimize a system where there is no transparency and debates in the choices of criteria? This situation questions at least the responsibilities of scientists and those who are concerned by the design and the trading and implementation of this type of system. As designers, how do you intend to guarantee it, that individuals will be aware of the personal information is being collected, who seeks and why? As designers, do we accept that the designed system could serve to repress the human rights of people? As designers and industrials, what should we adopt as preventive agreements and measures to avoid this type of non-democratic use of the developed system?

3.5. Description of TV.1.1

The TV.1.1 scenario consists in developing an adaptative and interactive web TV site with audiovisual content from local producers and channels. While the previous two scenarios aimed at analysing the recordings of surveillance cameras, this scenario mainly targets the TV programs and other video contents that can be watched through an interactive Web TV application. As such, it will investigate the analysis of user behaviour with his personal environment and will concentrate

[27] We note here the obscurity related to the definition of a normal or abnormal behaviour. The social norms are usually tacit. Nevertheless, there is studies, asked by the UK home office about the anti-social behaviour: www.homeoffice.gov.uk/crimpol/antisocialbehaviour/. The collective responsibility and the social control are infringed and restricted to the definition given by the home office.

on different modalities to deliver personalized information to this user. Since the size and diversity of video contents available is increasing on the Web, it has become more difficult for the end-users to find relevant materials effectively. Therefore, there is a growing need to develop an effective system to support the end-users in accessing the video contents. The scenario concentrates on two specific aspects: recommendation of possible interesting material and summarization of material of interest for a particular user. In a first stage, the scenario will be tested in an experimental context before be inserted in a real application. A volunteer places his faces in front of the camera and the computer. The volunteer expresses his preferences actively and/or by metalogs, and the expressions of emotions are analysed. Thanks to the users' expression of preferences and the capture of the expression of emotions, the multi-modal technologies focus on the constant adaptation of the users' preferences and desires. The multi-modal technologies build profiles.

3.6. Towards a darker TV.1.1 scenario

If the cursor changes the intentionality of the scenario, some potential main issues can be encountered for the users. Imagine that the profile that you have permitted to build by expressing your preferences is stolen or misused. Your privacy's protection is not guaranteed anymore.

Secondly, the building of an honest profile can be seriously damaged by a trick and/or a misuse of preferences; one cannot promise that your preferences are followed by the system. For example, a 'pre-profiling' can exist intentionally from the designers and providers of the interactive WebTV, in order to influence the users' choices. In the same line, some advertisers can be imposed to the users' consent, because of that pre-profiling.

Another threat resides in the fact that the providers sell your profile to marketing agencies, that can abuse of the users' personal data by sending advertisers, spamming the email box, sending some viruses. The users' web identity does not depend of their own, but is controlled by anonymity.

As designers, how do you intend to guarantee it, that individuals will be aware of the personal information is being collected? As designers, do we accept that the designed system could serve to stole and/or trick with users' preferences? As Web TV providers, what should we adopt as preventive agreements and measures to avoid this non-autonomic use?

4 SOCIO-ETHICAL CONTEXT: SURVEILLANCE, AUTONOMY AND DEMOCRACY

The technologies developed in MIAUCE are not neutral. On one hand they do participate to the gradual setting up of the so called 'surveillance society'. The 'surveillance society' is characterized, on the one hand, by a mode of governance rooted in, and relying on 'gaze' or observation architecturally structured. The most famous figuration of that surveillance architecture is of course Jeremy Bentham's 'Panopticon', popularized by Michel Foucault: a model prison exposing each individual prisoner to the possibility of being watched at any moment by the guards, but where none of the prisoners can ever know with certainty when he is actually watched (section 4.1.). On the

other hand, these technologies may challenge personal autonomy and democracy in unprecedented ways. These issues will be addressed briefly in section 4.2. before being more developed and illustrated through the scenarios' analysis in chapter 3.

4.1 The Panopticon and the Information Society

To approach the concept and the sense of the "surveillance", the metaphor of Panopticon remains very valuable, as D. Lyon pointed out (Lyon, 1994), as well as the major part of the sociological literature about the surveillance. The Panopticon, an architectural system of social discipline proposed by Jeremy Bentham in 1787, invites naturally comparisons with CCTV observation. Without entering into the details of the Panopticon, we can simply remind its main characteristics:

> *The design of the Panopticon consisted of a central inspection tower surrounded by a ring-shaped building composed of cells, each housing an inmate. Control was maintained by the constant sense that prisoners were watched by unseen eyes. Not knowing whether or not they were under supervision, but obliged to assume that they were, conformity was the individual's only realistic option. In this respect, the architectural design of the Panopticon created a state of conscious and permanent visibility that assured the automatic functioning of self-control and self-discipline.* [28]

The *Panopticon* became for Foucault in *Discipline and Punish* (1975) a powerful metaphor to denote the meanings of institutional spaces. This type of 'power through the means of gaze' can spread in non-institutional spaces, especially in the urban spaces in the case of CCTV. The phenomenon of over-accumulation of digital information associated with the powerful computerization of our Information Society, ensure the **efficiency** of the observation through the collection, storage, treatment, extraction, sorting and cross-matching of data captured in CCTV networks.

Beside this, for D. Lyon, surveillance consists in *"any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered."* 29 This definition involves the *"computer power, which allows collected data to be stored, matched, retrieved, processed, marketed and circulated."* 30 Lyon insists on the fact that the so-called Information Society is intrinsically surveillance society. Thus, every location with CCTV systems involves a social ordering influenced by surveillance characteristics. The social ordering is divided into four key themes:

[28] McCahill, M. and Norris, C., "On the Threshold to Urban Panopticon, Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts", *Urbaneye Project, Working Paper n°2*, 2002.

[29] Lyon, D., *Surveillance Society. Monitoring Everyday Life*, Open University press, Birmingham/Philadelphia, 2001.

[30] Ibidem.

coordination of social activities in time and space, the growing perception and production of risk, the role of privacy in generating as well as trying to contain surveillance, and the question of how power is redistributed in surveillance societies 31.

4.2. Surveillance, autonomy and democracy

Three major trends related to those technologies are worth being underlined, as they directly question individual autonomy and therefore the capacity of individuals to democratically contribute to the Society : first, regarding image capture, the considered technologies are characterized by their *invisibility* and the fact that they apply directly *to the bodies rather than to the subjects* or to the persons. Second, regarding data analysis, information technologies, subjecting individuals to the unilateral 'power' of information systems, generate or reinforce *power asymmetries* between individuals and bureaucracies. That is what D. Lyon usefully suggested through his Phenetic Fix metaphor. Finally, surveillance technologies have an 'implicit impact': observations show that they reinforce a sort of *social ordering fostering both the conformity and the individualism*. Let us examine these three dimensions.

4.2.1 INVISIBILITY, BODY AND IDENTITY

The first element striking observers of the MIAUCE project is that the developed technologies capture personal information by direct tracking of human bodies. This deserves three remarks. First, targeted directly at human bodies the project denotes a kind of over-valorization of information 'emanating' directly from the human body, and a correlative distrust and disregard for whatever may emerge from the subjectivity, intentionality and narrative of the observed individuals. To a certain extent, *bodies* are considered as more objective, more reliable and informative than *persons* and as more revealing of personal identities, personalities and lifestyles than whatever the individuals may tell or express. In other words, this type of project provides evidence of a certain distrust in persons and in their subjectivity.

The second remark relates to the status of the body. Without developing too long philosophical reasoning, one may observe that an observation project based on CCTV transforms the status of the body from 'something' very private and personal or individual into a sort of expropriated public body approached as a mathematical object or a data set which is calculated and retrieved in order to inform the observers.

This is well expressed by Ceyhan (2008)[32] when underlining that this type of surveillance technology or project

moves the site of identity from the Self (in relation to the other) to the body itself. This is the body that becomes the very source of identity. However this body is not about the body as the site of subjectivity (Ricoeur) and humanity (Arendt, Bauman) but a reified body without

[31] Ibid., p. 5.

[32] Ceyhan, A., "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics" in *Surveillance and Society*, Vol. 5 (2), pp. 102-123, 2008

any reference to the Other. Moreover, as Salter[33] contends, within its storage in databases the individual becomes a mobile body and through the interconnection of databases, the passport and the visa system within the institutions of customs and immigration control, the body becomes an internationalized body which has lost control over its subjectivity

The last remark targets this ambition to capture the identity in its most objective and reliable way. In order to achieve this, the observers must remain invisible in order not to influence the observed persons or their bodies' motions and expressions. Invisibility of the surveillance systems is clearly correlated with the wish to capture the body in its most *natural* state in order to get objective data about individual identities, risks etc. This leads to sly systems capturing images of persons without clear notice, even if a general notice has to inform the public of the fact that the place is controlled by CCTV or surveillance system. But to be efficient, these systems must remain as hidden as possible.

These three aspects impact on individual autonomy, and on the individual capability to live and express oneself freely. Freedom in that sense may be incompatible with individuals being reduced to physical data related to their bodies and being, as a consequence, deprived of a portion of their subjectivity. This reduction or deprivation raises also questions about democracy since this system can entail the freedom and the power necessary to be a democratic actor in the society.

4.2.2. MEANINGS, NORMS AND THE PHENETIC FIX

The second element related to these surveillance systems relates to the analysis performed out of data about the body motion or expression. In other words, it concerns the meaning given to these data. First of all, as already underlined here above, this meaning is no more the fact of the observed person and its subjectivity but is externalized and produced through mathematical models and calculus. This production of meanings is made by statistical sorting, clustering and profiling. As well pointed out by D. Lyon[34] :

Categorizing persons and populations – or 'social sorting' (Lyon, 2002) – is now a key to understanding surveillance. This was noted in some important studies in the 1980s (Gary Marx, 1988, on 'categorical suspicion') and 1990s (Oscar Gandy, 1993, on the 'panoptic sort') and today it is unavoidable.

For G. Marx[35], this capacity to create meanings regarding persons and populations is at the very root of modern surveillance systems

---

[33] Salter, M., B., "The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics" in *Alternatives: Global, Local, Political*, Vol. 31 (2), pp. 167-189, 2006

[34] Lyon, D., "Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix" in *Surveillance and Society*, Vol. 1 (1), pp. 1-7, 2002

[35] Marx, G., T., "What's New About the "New Surveillance"? Classifying for Change and Continuity" in *Surveillance and Society*, Vol. 1 (1), pp. 9-29, 2002

> *A better definition of the new surveillance is the use of technical means to extract or create personal data. This may be taken from individuals or contexts. In this definition the use of "technical means" to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Many of the examples extend the senses by using material artifacts or software of some kind, but the technical means for rooting out can also be deception, as with informers and undercover police. The use of "contexts" along with "individuals" recognizes that much modern surveillance also looks at settings and patterns of rela tionships. Meaning may reside in cross classifying discrete sources of data (as with computer matching and profiling) that in and of themselves are not of revealing.*

This leads implicitly to the shaping of normative profiles or statistical identities that serve to control, convince or influence individual persons and to take decisions about them. For Ericson and Haggerty[36], this growing need for classification and for profiling is very in line with what they call the **'**risk society':

> *Risk society is fuelled by surveillance, by the routine production of knowledge of populations useful for their administration. Surveillance provides biopower, the power to make biographical profiles of human populations to determine what is probable and possible for them. Surveillance fabricates people around institutionally established norms – risk is always somewhere on the continuum of imprecise normality.*

Moreover, these authors argue that such observation system helps building a social ordering, "as clean as possible", excluding persons unable to conform to what is defined as normal or acceptable behaviors.

The second point regards the intelligibility or the transparency of this meanings' construction and its related process of people normalization and classification. This issue has been very well approached by Lyon[37] when speaking about the 'Phenetic Fix' phenomenon.

> *If the modern world displayed an urge to classify, today this urge is endemic in surveillance systems. What I call the 'phenetic fix' (see also Phillips and Curry, 2002) describes this trend – to capture personal data triggered by human bodies and to use these abstractions to place people in new social classes of income, attributes, habits, preferences, or offences, in order to influence, ma nage, or control them. Thus it is not merely that new information technologies have made everyday actions and communications routinely visible as never before, or that networked technologies have helped to turn the rigid top-down apparatus of surveillance into a flexible assemblage (Ericson and Haggerty, 2001) of pulsating, undulating observations, but that the phenetic drive has been raised to a new level. Categorizing persons and populations – or 'social sorting' (Lyon, 2002) – is now a key to understanding surveillance. This was noted in some important studies in the 1980s (Gary Marx, 1988, on 'categorical suspicion') and 1990s (Oscar Gandy, 1993, on the 'panoptic*

[36] *Ericson and Haggerty,* Policing the risk society, *Oxford : Clarendon Press, 1997, p. 450, quoted in McMahill and Norris, (2002),* On the threshold to urban panopticon, Analysing the Employment of CCTV in European Cities and Assessing its social and political impacts, ***Urbaneye Project**, Working Paper n°2, p. 9.*

[37] Lyon, D., "Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix" in *Surveillance and Society*, Vol. 1 (1), pp. 1-7, 2002

> *sort') and today it is unavoidable. One of the clearest signs of the phenetic fix is in the new surveillance initiatives following September 11 2001. Several tacks have been taken to try to plug the gaps in intelligence and security made poignantly evident by the success of the notorious attacks. They include the use of biometrics, new 'smart' ID systems, CCTV with facial recognition, and upgrading communications interception techniques (Lyon, 2002a; Webster and Ball, 2003). In each case the primary goal is to obtain data to classify persons in terms of potential risk – the most obvious being profiling of those with 'Arab' features or of 'Islamic' convictions.*

What is questioning with this phenetic fix strategy is that it directly undermines the people capabilities for self determination since first of all it places people into categories and secondly it does not make clear how and why those categories are elaborated. By doing this, it creates a dramatic unbalance of power between the observed people and the observers raising very critical questions regarding the basic human rights that are at the settlement of the modern democracy (see the next section about the legal context). At last, as well demonstrated by many authors, those systems make the discrimination easier based on statistical sorting and profiling. So what is at work with those surveillance systems is the creation of a social ordering based on non explicit and transparent norms, which can move according to the events or/and to the political intentions of the observers. This raises question regarding the democratic control the society can have on the building up of this social ordering.

4.2.3 CONFORMITY, RESPONSIBILITY AND MOBILITY

The anticipatory conformity is another issue directly related to the deployment of those systems of observation. This anticipatory conformism has been very well approached by Norris and Armstrong:

> *an anticipatory conformity may be a strictly temporal and spatial phenomenon, with those individuals with deviant intentions shifting the time and space of their activities to outside the camera's gaze.*[38]

This phenomenon is one of the most worrying consequences of those observation systems for the autonomy, the self-determination, the self-respect of people and therefore their sense of freedom.

The question of the social responsibility is also raised when analyzing those surveillance systems. The question raised here does concern the impact of the surveillance systems on people reactivity and sense of responsibility when facing some dangers or accidents needing for their human assistance. In line with this question, many authors underline that it is not surprising that those systems are first deployed into the airport, in rail stations or in large shopping malls. Those places are characterized by a certain individualization or anomy of the social ordering due to the fact that people just pass through those transitory places and do not life there. Those places of high mobility and therefore low normativity and social responsibility are by excellence places where those surveillance systems are applied. Due to the globalized trends that affect our Society, one can

[38] Norris, C. and Armstrong, G., *The Maximum Surveillance Society. The Rise of CCTV*, Berg, Oxford, 1999.

question if what happens currently into those transitory places is not a microcosm of what would come, in a foreseen future, in the wider Society

5 LEGAL CONTEXT

5.1 Introduction: the scope of legal enquiry

As already mentioned in our first deliverable, multimodal observation technologies have the potential to increase the 'visibility' of the wide range of daily experiences that compose the fabric of everyday life and that, for a significant part, we never even had to think of as 'private' or 'anonymous',[39] as there were no reasons to fear being 'watched', recorded and interpreted by others, either because the technical capabilities to do so were lacking, or because we thought those experiences were so trivial and meaningless that nobody would ever pay attention to them, or memorize them for more than a very short time (allowing the 'practical opacity' of things said or done even in public).

A useful question to ask is, in the context of multimodal observation: what aspects of our life are protected when we 'have' privacy? Spatial, informational, emotional, relational, communicational privacy are various 'aspects' of privacy with which multimodal observation technologies may interfere.

Communicational privacy is explicitly acknowledged in Article 8 of the European Court of Human Rights and in Article 7 of the European Charter of Human Rights, and suggests the enjoyment of a certain level of intimacy when one communicates with others, even in the public space, as well as a guarantee of some confidentiality of the content of our communications with others.

We can moreover feel 'privacy' when we have our 'spatial' territory, such as our home, protected from unconsented intrusions by others. Protection of the home is indeed explicitly acknowledged in Article 8 of the European Court of Human Rights and in Article 7 of the European Charter of Human Rights. Ubiquitous and pervasive computing easily crosses walls, and has the potential to interfere with our *spatial privacy.*

We also share the notion that our own body should be protected from intrusive gazes. The reason why we wear clothes is not exclusively the need to protect ourselves from the cold or from the sun. There is something more: *physical privacy* (in the American Constitution, protection against unwarranted searches and seizures protects, to a certain extent, the physical privacy of the citizens). In this regard, protection of the legitimate interests of individuals may require reconsidering the "boundaries" of the subject. The European Group on Ethics of Science and

[39] Anonymity has been described famously by Alan F. Westin as a form of privacy "that occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance" (*Privacy and Freedom*, Athenaeum, 1967.) Anonymity is certainly something most people expect to have even in public places, although, as it will be argued, because expectations of privacy and anonymity are indeed inversely proportional to the intensity of surveillance, those expectations are probably prone to decrease in the coming years, if the 'security state' further develops.

Technologies suggested, in its 2005 report on ethical aspects of ITC implants in the human body, a broader conception of the individual endowed with the right to claim the total respect of a body, which is at the same time physical and virtual. The idea has been suggested, for a few years already, (and especially in feminist and post-structuralist scholarship), that the person, the subject deserving legal protection, is irreducible to the spatially situated and physically circumscribed subject.[40] Disembodied informational samples gathered in databanks, in that view, constitute 'informational identities'[41] parallel to – but interacting with - the physically embedded identities, and independent from the personal biographies through which individuals construct and maintain their self-perception. How 'physical privacy' interacts with the potential legitimate interests that a person has in the protection of his or her 'digital' or 'virtual' identity would be an interesting field of research.

Informational privacy is a notion that appears quite obvious to most people, although they are not necessarily conscious that images, sounds, movements 'emanating' from their body are indeed at stake when they think of informational privacy. The usual way to protect informational privacy is by empowering the subject with (legal and/or technical) means to control the collection and use of personal information.

Privacy may also be conceived as protecting one's "thoughts, emotions, and sensations"[42] and thereby one's "right to inviolate personality". The tracking and analysis of facial expressions in order to derive information about "users"'emotions obviously interferes with the enjoyment of *emotional privacy.*

As has already been mentioned, the European Court of Human Rights acknowledged that the right to privacy is not something that must necessarily be lived in isolation: the right to enter in relationships with others, or the right to *relational privacy*, is part of the right to privacy. This is not surprising if indeed one understands the right to privacy as the right to construct one's personality free from unreasonable constraints. Relations with others are essential to the construction of an individual's personality. Respect for relational privacy may require others to abstain from interfering with the personal relationships.

That legitimate interests of privacy may be acknowledged in those, and many other, diverse dimensions of human existence does not necessarily imply that those interests always trump competing interests of others (the government, enterprises, other individual). It is the law's business to balance these legitimate interests of the subject against the competing interests of others to interfere with his 'privacy'. The methods for doing so have been explained in our first deliverable.

---

[40]See Haraway, D. J., *Modest_Witness@Second_Millenium. FemaleMan_Meets_OncoMouse: Feminism and Technoscience*, Routledge, 1997, p. 247) : 'Most fundamentally,(…) the human genome projects produce entities of a different ontological kind than flesh-and-blood organisms (…) or any other sort of "normal" organic being (...) the human genome projects produce ontologically specific things called databases as objects of knowledge and practice. The human to be represented, then, has a particular kind of totality, or species being, as well as a specific kind of individuality. At whatever level of individuality or collectivity, from a single gene region extracted from one sample through the whole species genome, this human is itself an informational structure.'

[41] See Katja Franko Aas, "The body does not lie' : Identity, risk and trust in technoculture",in *Crime, Media, Culture*, 2(2):143-158,2006.

[42] Warren, S., and Brandeis, L., "The Right to Privacy", *Harv. L. Rev.* 1890, p. 193.

Beside privacy though, multimodal observation may also infringe on other fundamental rights and freedoms. These will be explored in the next section. The following section will then be dedicated to the more specific data protection issues raised by multimodal observation technologies. A third section will, very briefly introduce the potential responsibility issues raised by the technologies.

5.2 Reminding of the applicable legal framework

5.2.1. THE HUMAN RIGHTS FRAMEWORK.

Human rights, pursuant to the Universal declaration on Human Rights, the European Convention on Human Rights and to the Charter of Fundamental Rights of the European Union, constitute a first layer of general constrains applicable to all scenarii.

Among Human Rights, the following are particularly relevant in the hypothesis of safety, security, profiling and marketing scenarii such as those pursued in the MIAUCE project:

1. *Human dignity* is inviolable. It must be respected and protected (Article 1 CFREU).

The principle of human dignity attests to the fundamental and guiding role occupied, in our western legal culture, by the ethical imperative of conceiving and dealing with human beings always as *ends in themselves* and never as *means to an end*. This obviously anti-utilitarian orientation guides the interpretation of the whole Human Rights framework.

2. Right to respect for one's *physical and mental integrity* (Article 3 CFREU).

Following from the fundamental imperative of respect for human dignity, the right to respect for individual physical and mental integrity makes it illegal and, in most countries, also anti-constitutional, except in exceptional cases, unconsented medical or other intervention on an individual's body, as well as unconsented manipulation of a person's mind.

e.g. Respect for mental integrity may be particularly at issue in any scenario involving monitoring of emotions, and/or excessive marketing impacting on consumers' choices.

3. Respect for *private and family life, home and correspondence* (Article 8 ECHR). The scope of the right to privacy, from the intimacy of the home, has been gradually extended by the European Court on Human Rights to portions of peoples' lives that are not necessarily "intimate" strictly speaking, and may be relevant to personal behaviours, attitudes, held outside personal homes and private premises.

In its decision in the P.G. and J.H. v. the United Kingdom case (Application no. 44787/98) of 25 September 2001, the European Court of Human Rights held the following reasoning:

> *There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable*

expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method (see Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V). The Court has referred in this context to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2) (see Amann v. Switzerland [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, where the storage of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted)… the Commission previously had regard, for the purpose of delimiting the scope of protection afforded by Article 8 against arbitrary interference by public authorities, to whether the taking of the photographs amounted to an intrusion into the individual's privacy, whether the photographs related to private matters or public incidents and whether the material obtained was envisaged for a limited use or was likely to be made available to the general public … Where photographs were taken of an applicant at a public demonstration in a public place and retained by the police in a file, the Commission found no interference with private life, giving weight to the fact that the photograph was taken and retained as a record of the demonstration and no action had been taken to identify the persons photographed on that occasion by means of data processing … (See Peck v. The United Kingdom, 28 January 2003)

In Von Hannover v. Germany, 2004[43], the Court held that:

> *…a person's physical and psychological integrity; the guarantee afforded by Art.8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life*

The scope of privacy is thus not limited by the non-intimate nature of personal information or acts concerned, nor by their public occurrence. That individuals enjoy a right to privacy even with regard to behaviours, attitudes and communications in public spaces like streets, shopping malls,

[43] ECHR, Von Hannover v. Germany (2004) 40 E.H.R.R. 1 at [50].

airports...or even at work,[44] means that, recording, storage and use of information relating to individuals in these various places constitutes an invasion of their privacy that must, in order to be lawful, comply with the conditions set at article 8§2 of the European Convention of Human Rights:

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The « horizontal effect » doctrine of the European Court of Human Rights results in making those requirements valid for private interferences as well.

Recently, the German supreme court[45] acknowledged, as part of the right to privacy, a « basic right to the protection of confidentiality and integrity in information systems », that is, the right not to have one's information technological systems searched by government, law enforcement officials and intelligence services except, after approval by a judge, in the rare circumstances of « factual indications for a concrete danger » in a specific case, for the life, bodily integrity and freedom of persons, for the foundations of the state or the existence of humans. The mere probability that the danger will materialize in the near future is insufficient to authorize such online searches, which can thus not be used for normal criminal investigations or general intelligence work. Information technological systems are defined by the German court as systems, such as laptops, PDA, mobile phones etc. which

> *alone or in their technical interconnectedness can contain personal data of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality.*

The decision was grounded on the following :

> *From the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and from the dangers for personality that are connected to this use follows a need for protection that is significant for basic rights. The individual is depending upon the state respecting the justifiable expectations for the integrity and confidentiality of such systems with a view to the unrestricted expression of personality.*

This is but an example of how the judicial interpretation right to privacy might evolve as to adapt to the new circumstances of the advanced information society.

---

[44] See ECHR, Copland v. United Kingdom, 62617/00 [2007] ECHR 253 (3 April 2007). As for the applicability of the Directive 95/46/EC, Article 29 Data Protection Working Party explicitly explained in its Opinion 8/2001 on the Processing of Personal Data in the Employment Context, Sept. 13, 2001 (5062/01/EN/Final WP 48), at 24.) that "[t]here should no longer be any doubt that data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, internet access, video cameras or location data. »

[45] *BVerfG, 1 BvR 370/07 vom 27.2.2008.*

4. freedom of *thought, conscience and religion* including freedom, either alone or in community with others and in public or private, to manifest one's religion or belief, in worship, teaching, practice and observance (Article 9 ECHR) ;

5. freedom *of expression including freedom to hold opinions* and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Article 10 ECHR) ;

6. freedom of peaceful *assembly and to freedom of association* with others, including the right to form and to join trade unions for the protection of his interests (Article 11 ECHR) ;

7. freedom of *movement* (Article 2 of Additional Protocol N°4 of the ECHR, Article 45 of the Charter of Fundamental Rights of the EU), *including the right to move without being constantly traced*. In its Opinion 4/2004, the Article 29 Working Party noted explicitely that freedom of movement does not only mean that one must be free to move in the physical space, but also that one must be free to move withouth inevitably leaving continuous and/or fréquent traces of one's movements for the benefit of systems enabling permanent Optical observation and grassing out.[46] Being seen without seeing may indeed constrain the person in her movements and trajectories.[47]

8. the right to enjoy these freedoms *without discrimination* on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status (Article 14 ECHR);

9. the right of *persons with disabilities* to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community (Article 26 CFREU).

The principle of respect for human dignity, for physical and mental integrity, may be said absolute: they allow no exception at all[48], whereas the rights to privacy, to freedom to manifest one's religion

[46] See also the European commission for Democracy through Law (Venice Commission), Opinion on vidéosurveillance in pubic places by public authorities and the protection of Human Rights, adopted by the Venice Commission 16-17 March 2007, CDL-AD(2007)014.

[47] See our first Deliverable on legal issues, identifying the risk of anticipative conformity as one of the uprecedented challenges raised by the implémentation of Miauce scenarii and my reflections in Rouvroy, A., « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence » in *Studies in Ethics, Law and technology*, Berkeley Electronic Press, 2008.

[48] This is not absolutely non controversial though. See Carmi, G.E., "Dignity versus Liberty: the two western cultures of free speech", (August, 22 2008). Available at SSRN: http://ssrn.com/abstract=1246700.

or belief, to freedom of expression, to freedom of association, are not absolute rights: they can be interfered with in exceptional cases, provided that the interference is in accordance with the law, and only on the condition that interference is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

A crucial requirement is thus – for any scenario one can imagine – that it complies with that general principle of proportionality, which is much 'broader' than, for example, the data protection requirement that personal data collected and processed be non-excessive: "the very installation of a surveillance system is unlawful if other types of control allow attaining the purposes to be achieved without making use of personal data."[49]

The peaceful enjoyment of privacy requires that everyone be able, at certain times and in certain activities, to shield themselves from observation by unauthorized third parties. This requirement entails the non observability of many aspects and acts of daily life by unauthorized partie, even using automated means and without the data subject being identifiable, as well as the inviolability of the home conceived not only as a physical space but also from a virtual standpoint.

As a matter of fact, anyway, one may anticipate that whenever a scenario does not comply with the proportionality requirement as defined in Human Rights instruments, it will also lack social acceptability and infringe on ethical values. The opposite would also be true : scenarii that would not meet the criteria of social acceptability and ethical validity would most probably also fail to comply with the proportionality requirement and thus be considered contrary to Human Rights.

Human Rights principles (or the specific conditions of their exceptions) must be complied with unconditionally, unlike data protection requirements, which only apply in the hypothesis specified in the relevant EU Directives: in cases involving the processing of personal data. One objective of this section, besides helping the partners to the Miauce project to identify the means to ensure that application scenarii ensuing from the Miauce project will not infringe upon Human Rights, is to ascertain when the applications contemplated fall within the scope of the European data protection framework and when they are clearly outside that scope. It should thus be noted right away that even when an application scenario clearly falls outside the scope of the data protection regime (because the processed data are unambiguously anonymous, for example) it may nevertheless be questionable from the broader point-of-view of other fundamental rights, such as privacy (the right to data protection does not exhaust what privacy is about[50]), freedom of movement, freedom of

[49] Buttarelli, G., "Surveillance in Public Paces and Protection of Personal Data" in *European Commission for Democracy Through Law*, Study No. 404/2006, Strasbourg, 14 February 2007.

[50] See the part addressing legal issues in our first deliverable, where we listed, among the 'facets' of privacy, and besides informational privacy (data protection), attentional, physicial, emotional, relational, spatial privacy, …

expression, non-discrimination etc. Identification issues (data protection) do not exhaust all potential issues arising from what one may broadly call surveillance, monitoring and profiling.

e.g. safety scenario (escalator) : besides potential data protection issues, and even when all data protection law requirements have been complied with, the mere presence of cctv systems embedded in the infrastructure de facto decreases the level of privacy enjoyed when using these infrastructures ; whenever the system's functioning results in individuals feeling compelled to avoid using the infrastructure at all, as to avoid being "recorded" by a CCTV system, their freedom of movement and right not to be discriminated against may also be an issue.

e.g. interactive web-TV scenario : besides potential data protection issues, emotional privacy is obviously interfered with as the user's emotions are to be scrutinized.

e.g. marketing scenario (shop window) : besides potential data protection issues, attentional and emotional privacy are at issue when individuals' gazes and facial expressions are recorded and observed.

5.2 Data protection issues

Data protection issues are obviously involved, in the three prototype scenarii, and in any context of implementation one can imagine.

An unavoidable question is to what extent the Miauce scenarii must comply with the restrictions and obligations imposed by the European Directive, and, a contrario, to what conditions, or in which cases, compliance with the data protection principles are dispensable, from a legal point-of-view. It remains that two kinds of legislations must be taken cumulatively into account in that context. Directive 95/46 EC has enacted the main legislative principles applicable to all processing of personal data and definitively most of the scenarii chosen by the MIAUCE consortium will be subject to these personal data protection legislation to the extent that they are dealing with personal data. Beyond the directive one may underline that the Council of Europe Convention n. 108 on the protection of individuals with regard to the automatic processing of personal data dated from 1981 had fixed the major principles of data protection that inspired the Directive, but that the principles of the Council of Europe Convention are more extensively applicable since they are covering all kinds of personal data processing and not only, as does the Directive, data processing falling under the first pillar, the exclusion of processing operated by enforcement agencies or intelligence services.

Moreover, in the future, technologies developed in the MIAUCE project may be used for other purposes and ignore the severe constraints (controlled environments, safety rather than security purposes, exclusion of profiling in the marketing scenario, etc.) the MIAUCE partners have wished to impose through their drafting of the scenarios. By instance the pure safety scenario (Scenario 1) which proposes to work only with blurred faces may evolve into a scenario in which faces and movements of people will be collected and analyzed for identifying among them either persons in need of help or suspect persons. In that case, personal data protection will definitively be applicable.

But even if no personal data is processed, the mere capture of even non personal datais subjected in most of the European countries to specific legislations dealing with videosurveillance, "Videosurveillance Acts",[51] applicable even when no personal data is collected.

The main principles enacted in these legislations are more or less the same as those proposed by the Data Protection legislations: it means the principle of t**ransparency** which renders mandatory the obligation for the users of these videosurveillance systems to take measures in order to ensure the information of the persons whose data are captured and the purposes of these collection. That is the sense of the message "Smile you are filmed" affixed at the entrance of the supermarket. The other principle is the **legitimacy** and **proportionality** principle which limits the data to be captured only to the data needed for the accomplishment of a legitimate purpose and just for the duration of the accomplishment of the data. If as manager of a store, you want to use data for determining the appropriate location of your shelves, you do not need to keep the images for a long time but just a while for calculating the number of persons attracted by a certain product. Finally one mentions the additional, principle of security which implies the obligation to take appropriate security measures for ensuring that no illegal usage of the captured data may happen.

Just a word about the e-communications and Privacy Directive 2002/58: this directive is not applicable to private networks even though this been considered sub-optimal by the article 29 Working Party. However certain provisions enacted in the Directive are applicable to private networks, like the article 5.3 about terminal equipment. This article forbids any intrusion into a terminal equipment connected to a network without withdrawable consent of the terminal user. This article may receive application in the context of the MIAUCE scenario Interactive Web-TV

In the next lines, we will develop the consequences of the application of the personal data legislations. We take as reference the European Directive 95/46 already mentioned which has been implemented in all European countries with only minor divergences.

5.2.1 APPLICABILITY OF DATA PROTECTION LAW

5.2.2.1 Applicability of Personal Data Protection legislation to the scenarii.

Definition of "personal data"

Data protection principles apply to the processing of "personal data" that the directives define as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to

[51] Videosurveillance is an ambiguous concept since it covers systems of capture of images in order either from one part to detect abnormal or deviant behaviours of people (videosurveillance in the strictest sense) and either from the other part to detect the presence and follow the behaviour without intent to control people but only for detecting their attitudes in order to better marketing strategies. It might be clear that the same technology might be used for both purposes.

an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

The notions of "identification or identifiability" reflect situations where a person may be recognized among a small group of individuals by using means reasonably available either to the data controller or by a third party (for instance by law enforcement officials matching faces captured by a CCTV camera and a data base containing pictures of suspected criminals). No data protection issues arise whenever captured images are blurred immediately and original, clear, images are immediately discarded, and where no other means exist to re-identify the persons who have been filmed.

Except when the data is anonymous or automatically anonymised from the start (it will not be the case if the images are blurred only after their transmission to the central security office) then, any collection, storage and use of coded or personal data relating to human subjects must comply with the 1995/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. When, in addition, that information is about the user's communications over the internet (as in the interactive web-TV scenario), the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) must be complied with.

The *finality of the data processing* – although a fundamental criteria to assess the legitimacy of the processing - is not a relevant criterion for the applicability of the data protection regime. In the safety scenario, for example, although the aim of the image capture is not to identify, control or monitor individuals, the captured images are nonetheless personal data if, on the basis of these images, individuals are or can be identified.

The necessary condition for excluding the application of the data protection directive is that the data be anonymous (that is, that it cannot be traced back to an identified or identifiable person). In other words, if one wishes to avoid the obligation to comply with the requirements of the data protection regime, relevant technical measures must be implemented that ensure reliable anonymization of the processed data. Except when the possibility to identify the individuals involved is an absolute necessity for achieving the purpose of the scenario, data must be irreversibly anonymized. Due attention should be paid to the fact that, given recent technological developments in the field of biometrics, which, for example, may allow identification and recognition of unique features that characterize each person's walking, writing and other patterns and attitudes, even blurred images of individuals (whose faces are not 'visible') may become considered as personal data the processing of which requires compliance with data protection laws. **The conditions to be met as to comply with this 'anonymity requirement' cannot be fixed once and for all, especially considering the fast evolution of biometric identification technologies.**

Moreover, due attention must be paid to the possible evolutions of the legal definition of the concept of personal data. In view of the difficulties raised by RFID systems (which, although not necessarily carrying 'personal data' endanger users' privacy in a myriad of ways) and of the still unclear status of 'profiles', the concept of personal data has recently received a broadened

definition by the Article 29 Working Party[52] on the protection of personal data. Personal data refers, according to the WP29 opinion, to:

- "any information", either objective (such as the substances in one's blood) or subjective (such as opinions or assessments), either correct or incorrect, about individuals, regardless of their position or capacity (as consumer, patient, employee, etc.), and regardless of the format or medium on which that information is contained (numerical, graphical, photographical, acoustic,…).
- that relates, even indirectly, to individuals (information on the functioning of a machine where human intervention is required and allowing to ascertain the productivity of the person working on that machine, or information about the length and pace of a queue, allowing to ascertain the productivity of an employee in an office or a shop)[53] either because it contains information about a particular person and/or because that information is processed for the purpose of evaluating, treating in a certain way or influencing the status or behaviour of an individual, and/or because the processing of that information is likely to have an impact on a certain person's rights and interests (the mere fact that the individual could be treated differently from others as the result of the processing of the data counts as "impact" in this regard), taking into account all the circumstances surrounding the case.

In an example, the Article 29 Working Party asserts that in case of videosurveillance, when the purpose is finally to have the possibility, not necessarily immediately but perhaps in the future (in order to identify the person responsible of an incident on the escalator, for example, in the Safety scenario) the captured data are personal data. The ultimate criteria to decide whether a specific data is personal data or not would then be the possibility that, thanks to the processing, action could be taken vis à vis the subject.

This broad understanding of the concept of personal data is not unanimously endorsed in all the countries of the European Community though. How the interpretation by the Group 29 will impact of future interpretation of the applicability of the directive remains to be seen.

That data are not personal data does not mean that no specific legislation remain applicable. As previously said, the so-called Videosurveillance Acts remains applicable with the consequences described above, notably the obligation to make the system transparent and to notify the existence of it. Administrative requirements may also be legislatively also exist such as the obligation to register the videosurveillance system. Furthermore certain specific legislation are dealing with the question of videosurveillance employed for controlling employees. The main additional principle

[52] WP 136,Opinion 4/2007 on the concept of personal data, adopted on 20th June, available on the website of the EU Commission

[53] The WP29 had previously noted, in the context of its discussion on the data protection issues raised by RFID tags, that "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated." (Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005, p. 8.)

laid down in these legislations is the obligation imposed to the employer to hold prior consultations with employees representatives before installing such a powerful instrument of 54.

Sensitive data.

Some types of personal data may never be processed or may only be processed under severe and strict conditions. Article 8 of the Directive 95/46/EC makes it in principle illegal to process **personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life**.[55] This raises particular questions with regards to some of the potential Miauce applications, as the intervention of information technologies may alter the 'nature' of the data involved (not sensitive a priori, but metamorphosed into sensitive data as a result of the processing). Images of persons unavoidably provide information about their racial or ethnic origin, and may also in certain cases provide indications of their religious faith and health status; profiling of persons on the basis of their preferred entertainment programs in a context of interactive web TV may generate indications about these persons' political opinions, religious or philosophical beliefs; tracking of potential consumers' gazes through a shop window may reveal sensitive aspects of their private life. These data are however not, from a technical point-of-view, under current data protection framework, considered sensitive data at least as long as it remains demonstrated that the purpose of the processing is not to identify these sensitive characteristics. So the simple recording of people among whose persons with disabilities might be recognized will not lead to the application of the more severe provisions of the Directive except if the processing is aimed at identifying individuals belonging to the category of, say, impaired individuals as to, for instance, analyse their consumer's preferences.

Definition of "data subjects"

The "personal data" at issue may relate to either the simple "user" of the infrastructure (people using the escalator, individual watching interactive web-TV, potential customer watching through a shop window), or the airport or shop employees, or to anyone who happens to appear on the video-stream. The obligations and rights ensuing from the data protection regime must be identified and complied with in relation to the different categories of data subjects, whatever their "role" may be in the scenario.

e.g. –In the escalator scenario: potential data subjects include any individual using the infrastructure (escalator); employees of the airport each time they cross the area covered by the camera; employees of the airport whenever the captured image might be are used to assess their productivity or to control the quality of their work or service (if the broad definition of "personal data" adopted by Group 29 is complied with);...

---

[54] About the question of videosurveillance and privacy, see Art. 29 WG, Opinion 25 nov. 2002, WP 67 on personal data processing by videosurveillance, available at the website of the EU Commission

[55] Article 8 The processing of special categories of data:

- In the supermarket shelf scenario: potential data subjects include not only the any passer by who happens to be filmed customers but also the; employees of the shop;...

Definition of "processing"

Any "operation" (collection, storage, use,…) involving personal data is considered a "processing" under the EC Directives and relevant national laws. Any collection, or storage (including in images repositories) of texts, images, sounds, etc. is considered "processing". It must be underlined that the simple fact to collect, through CCTV, clear images of persons, even though these images are blurred immediately *after* they have been recorded, is sufficient to consider these captured images personal data (at the capture stage). The anonymisation is in that context a second operation applicable to the personal data collected .

Definition of the "data controller"

The data controller must be identified taking into account all types of delegations of service provision that may happen. So, in the safety scenario for example, the data controller may be the airport authorities, the provider of technical services, or third parties having been made responsible for the data processing, or all of these actors simultaneously. (Art. 6) Due account must be taken of the fact that the scenario involves a network of actors, and of applications, and therefore complexities regarding the ascription of responsibilities among actors.

Besides the category of data controller, the Directive mentions the possibility to have processors when the processing is carried out by a third party on behalf and under the control of the data controller. For instance, we might imagine that a supermarket not having the technical or human means to operate the CCTV system would request the furnisher of the system to process the data and disclose the main results to the supermarket manager. Other example: a company specialized in security would manage all security measures of an airport, including the videosurveillance system described in MIAUCE scenario on safety. Certain obligations are enacted by article 17 §3 of the Directive to data controller and data processor in these cases. Firstly it is the duty of the data controller to assess the quality of the data processor and his ability to provide adequate security measure. Furthermore the data controller has to define precisely, in a written contract, the missions of the data processor, and to check if the data processor does respect entirely the limits of his contractual duties. Precisely it is the data processor's obligation not to infringe his contractual duties and not to process data for other purposes than those assigned by the contract. The processor shall act only under instructions from the controller. If he exceeds his mission (defined contractually) - for example, the security company sells the processed 'safety' data to marketing companies- he will be acknowledged as controller himself and therefore, in case of illegitimate processing, may be sued in civil and criminal courts.

5.2.2.2 Principles relating to the lawfulness of data processing: duties of the data controller

A typology of purposes ascribable to the technological devices and systems developed in the MIAUCE project includes the (not exhaustive) following list: safety, security, efficiency, marketing. Data protection law requires that the purpose of data processing be legitimate. Whenever a processing is in the scope of data protection law, it must comply with a series of requirements. Article 6 of the Directive 95/46/EC specifies the requirements relating to the lawfulness of the data processing.:

1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
c)....

It shall be for the controller to ensure that paragraph 1 is complied with.".

Let us describe each condition of this lawfulness.

1. ***Fairness:*** the processing must be lawful and the data must be collected in a transparent way. The right of the data subject to data protection must be constantly weighted against the interests both third party or parties in obtaining personal data. Conversely, the right to process personal data about data subjects must be accompanied by effective means to allow data subjects to defend their interests, especially to be kept adequately informed
2. ***Legitimacy:*** The processing must be according to article 6 of the Directive legitimate. Article 7 of the EC Data Protection Directive 95/46 defines a list of cases which makes a priori the data processing legitimate. We do insist about the fact that to comply with this list does not mean automatically that the processing is legitimate but creates a presumption of legitimacy.

5.2.2 PRINCIPLES RELATING TO THE LEGITIMACY OF DATA PROCESSING

Whenever a processing is in the scope of data protection law, it must comply with a series of requirements. Article 7 of the EC Data Protection Directive 95/46 lists those basic principles as follows:

(…) personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Whereas safety and security (detection and intervention) scenarios will most probably rely, to establish their legitimacy, on either « the vital interest of the data subject », or the « public interest or exercise of official authority vested in the controller », marketing and convenience (profiling) scenarios will more probably rely on « consent » or the « legitimate interests of the controller ».

The vital interest of the data subject may be difficult to establish though, as indeed society has so far coped with the vital interests of individuals without the sophisticated surveillance systems proposed in Miauce. “Vital interest” has to be interpreted in the strictest sense. A vital interest is at stake when the situation threatens a person’s life.

The public interest may only be invoked when the data controller is vested with official authority, which would probably not be the case in most business cases contemplated so far but which might be the case if the videosurveillance system is coupled with the information system of law enforcement authorities occasionally or on a permanent basis. Another question might be raised regarding the storage of records by the data controller in order to allow access to these data by law enforcement agencies upon their request. In our opinion, data storage for the purpose of responding to such “potential requests” is not legitimate absent explicit legal obligation to proceed to such storage. The 2006 data retention directivewhich precisely imposes such an obligation to keep specific data, called “traffic data”, is not applicable to CCTV. Notwithstanding this principle, some EU legislation requires the data controller to inform the law enforcement agencies about their CCTV systems and their characteristics and make it compulsory to grant an access to these authorities when their request is based upon a judiciary mandate...It must be underlined that the question of access by these authorities to the data processing operated by private parties is not covered by the Directive 95/46 since this access clearly falls under the third pillar.

The unambiguous consent of the data subject is thus hardly avoidable as a necessary condition for the whole system to be legitimate. For the consent to be unambiguous, it cannot be merely implicit. Therefore, whenever possible, « opt-in » systems should be preferred to « opt-out » systems. True consent presupposes a real possibility of choice, a precondition which would not be met if a data controller conditions the delivery of a service (e.g. the access to the TV channels) to, for example, the user consenting to be observed and tracked through a webcam. The fact that a financial advantage be offered to the person who accepts to have her data processed may also challenge the validity of consent.

The last possibility is often advanced by marketers to justify their processing: “processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the

interests for fundamental rights and freedoms of the data subject...” They argue that their interest as marketers is legitimate and that the prejudice they cause to the data subject is minor in comparison with the benefits the data subjects will get from the publicity and with their own legitimate interests. As the value behind data protection is the fundamental right to privacy, including the right not to undergo excessive pressures and constrains in the autonomous development of one’s personality, and that individualized marketing and advertising may come to be so effective that it may indeed exercise such an excessive pressure, the marketers’ argument does not appear sufficient to justify in all cases such data processing.

The legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed may legitimize the processing as long as these interests are not overridden by interests for fundamental rights and freedoms of the data subject. A balance must therefore be made between the data controller’s and the data subject’s interests. The more the processing infringes upon the data subject’s fundamental liberties and freedoms, the less probable it is that the processing will appear legitimate.

Information must be provided, in adequate form, to all potential data subjects. This includes all employees working in any considered infrastructure. Consent must be explicit, and revocable. Therefore « opt-in » solutions should be preferred to « opt-out » solutions.

e.g. In the safety scenario, as well as in the shop-window scenario, the classical pictogram must be present at both ends of the escalator.

e.g. In the interactive Web-TV scenario, comprehensive information, in an understandable form, must be provided to the users, about what type of information is being collected and processed, with what aims etc. Rather than an « opt-out » system allowing users to refuse interaction, an « opt-in » system must be technically put in place, allowing users willing to do so, to enter in the interaction. The user must be empowered with technical means allowing him or her to reset his or her profile (that is, to erase any information relating to him or her stored in the system). Refusal to participate in the interaction must not result in any disadvantage for the user. The potential incentives for inducing user to enter in the interaction must not be excessive.

Prior Determination of the purposes: The data controller has the duty to define precisely the purposes of his processing and to make them explicit. It means that he has not to use vague wording but definitively to enunciate in a document the purposes in a way which might be understandable by a reasonable data subject and apart from which the data subject will envisage the reason why the data are collected. For example: if in case of marketing usage of the data collected through a web camera installed on a TV, I say to the customer that I collect the data for marketing purposes. It might be for this people to know exactly if they are using profiles for one to one marketing or just having statistical information about the audience. It is impossible for the data subjects to know if the data controllers are selling the data to third parties or just keeping the data for their own marketing purposes.

Compatibility*:* This requirement is very important in evolutive system like most of the automated processing since it is very easy apart from an original application existing at the moment of the data

collection to imagine a new one that will allow new purposes. For example, I am collecting data in a supermarket only for security reasons but at a certain moments I can imagine that I will couple the data so collected with a automated recognition of the faces (matching the images recorded in real time with the images collected at the moment of the creation of the shopping cards) in order to propose to the persons so recognized individual marketing offers. This usage is new and has not been announced at the moment of the data collection (the moment of the delivery of the shopping card). The question is then the following: Is that a new usage or might this usage be considered as compatible with the former one? The criterion to distinguish the compatible use versus the incompatible use has been defined by the criterion of the reasonable expectation. In other words, would the data subject have had the possibility at the initial moment of the data collection to imagine this future usage as included in the purpose of the processing. If yes, the processing is deemed compatible and is legitimate without new formalities. If not the processing is a new one and has to find a basis for its legitimacy and the data subject must be at least informed or even agree to this processing.

Data minimization is another legal requirement implying that only the personal data that is necessary for the implementation of the system should be collected, processed and/or stored, and that the data must be deleted when no longer necessary and after the legal conservation requirements.

The data controller is, moreover, responsible for ensuring that the processing complies with the data quality requirements.

5.2.3 OBLIGATIONS RELATING TO THE PRINCIPLES OF "DATA QUALITY"

Article 6 of the Directive 95/46/EC specifies the requirements relating to the data quality:

1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

Among the data protection principles that must be complied with in any scenario involving the processing of personal data, whatever the finality of the processing, the following are particularly important:

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Beyond the stage of prototype scenarii, finalities (or purposes, or business cases) may obviously be diverse and combine or shift from one to another over time.

e.g. The “collapsed escalator” scenario is presented as a safety rather than as a security scenario to the extent that the purpose of the technological system implemented is not to control or monitor peoples' behaviours, but merely to monitor occurring events, and characterize them according to their potential to result in situations unsafe for the users. Yet, if the video camera happen to capture images suggesting that some individual might be on the point of causing degradation to the infrastructure, or of committing a crime of any sort, the system put in place could well be used for security rather than merely for safety purposes. This is not unimportant, as criteria of legitimacy vary depending on the finality pursued.

Given the dynamism and plasticity of the systems at issue, constant monitoring should be exercised as to ensure that the conditions of legality (compliance with human rights as well as data protection requirements) are always met. The whole system's legitimacy should be reassessed each time a shift in the variables involved occurs. The legitimacy and proportionate character of a given surveillance system, for example, may well be established in specific circumstances when those circumstances involve a higher than usual risk level, but disappear (along with their legality) in ordinary times. Measures must be taken in that case as to ensure that the whole system be disabled (when implemented through CCTV and other technological devices, surveillance is usually carried out in a steadier fashion compared to other forms of – more occasional and/or irregular in nature – human control).

The criteria of legitimacy are unavoidably contingent on non-legal factors, such as the processing’s societal acceptability and its compliance with ethical principles. Legal, societal and ethical assessments are thus, de facto, interdependent and complementary.

The proportionate character of an application with a legitimate purpose must be demonstrated taking into account all existing technical and non-technical solutions that provide an alternative to the processing of personal data. The processing of personal data may be considered proportionate only when no such alternative is available at reasonable cost. The fact that data subjects (the ‘users’) have consented to the data processing does not per se absolve the data controller from his obligation to guarantee that the data processing complies with that proportionality requirement. No justificatory cause absolves a surveillance system from complying with the proportionality requirement. Consent, especially, is never by itself a sufficient justification to do away with the requirement that the system put in place be proportionate to the legitimate finalities pursued.

Moreover, a technological system put in place for a given purpose may well, over time, and as technology and circumstances evolve, be used for additional or different purposes: replacing the whole system would make no economic sense in that case. An acceptable way of dealing with the apparent contradiction between the requirement of purpose-specificity of personal data processing

and the need for incremental adjustment of whatever system is in place may be continuous monitoring.

5.2.4 RIGHTS AND PRIVILEGES OF THE DATA SUBJECT

5.2.4.1. Information

A central notion of data protection regimes is the notion of the data subject's informed consent to the processing of « his » data. A first issue is then : what kind of information should be provided to the data subject in order to comply with the legal requirement? Article 10 and 11 of the European Directive 95/46/EC address that issue.

> Article 10 - Information in cases of collection of data from the data subject :
>
> Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
>
> (a) the identity of the controller and of his representative, if any;
>
> (b) the purposes of the processing for which the data are intended;
>
> (c) any further information such as
>
> the recipients or categories of recipients of the data,
>
> whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
>
> the existence of the right of access to and the right to rectify the data concerning him
>
> in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

> Article 11 - Information where the data have not been obtained from the data subject :
>
> 1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
>
> (a) the identity of the controller and of his representative, if any;
>
> (b) the purposes of the processing;
>
> (c) any further information such as

the categories of data concerned,

the recipients or categories of recipients,

the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

5.2.4.2. Access and rectification

Another right of the data subject is the right to access « his » processed data, have incorrect information rectified or have personal data erased from the system. Article 12 of the EC Directive 95/46 describes the modalities to be complied with in this regard :

Article 12 - Right of access

Member States shall guarantee every data right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred .to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

5.2.5 ADDITIONAL REQUIREMENTS: SECURITY OF PROCESSING

The security measures to be implemented by the data controller rely on section VIII, with its articles 16, concerned by the "confidentiality of processing" and 17, concerned by the "security of processing", of the directive 95/46/EC.

According to these articles, "the controller must implement appropriate technical and organizational measures to protect personal data" (articles 17, §1) and these measures "shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected." (article 17, §1, second part).

The controller "must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures." (article 17, §2). Furthermore, "Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law" (article 16).

Following paragraph 3 of article 17, "the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

the processor shall act only on instructions from the controller,

the obligations set out in paragraph 1 of article 17, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

Following paragraph 4 of article 17, "for the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."

The ten points for implementing a security plan may thus be summarized as follows:

1) The security policy must describe the risk analysis, the priorities to be encountered by the security plan, the duties and responsibilities of anybody concerned by security, the incidents management process, the elected measures to keep up to date the security system after its activation. This point is relevant to the previous article 17, §1, concerning the appropriate organizational measures.

2) A security counsellor must be appointed by the data controller, to whom he will directly report. He must have enough means, information, training and abilities to fulfil his work. Mainly he must justify the entire security policy. This point is relevant to the previous article 17, §1, concerning the appropriate organizational measures.

3) The human security requires that every person implied in the process of personal data will be constantly and correctly informed and trained about its specific duties and responsibilities to fulfil his work. In particular they will be informed that any infringement of the rules can give rise to

disciplinary actions, and that an oath of confidentiality may be required. Those two points are relevant to the previous article 17, §1, concerning the appropriate organizational measures.

Furthermore, any delegation to a third party must be clarified in a contract. This contract must incorporate the same obligations of security than those in effect inside the data controller organisation. This point is relevant to the previous articles 17, §2, article 17, §3 and article 16, concerning the confidentiality of processing.

4) The physical security requires to install the storage medium and the computer systems in identified and well protected places. In case of service continuity constraint, prevention, detection and processing systems of physical danger must be installed and regularly maintained. Regular back up must be recorded in order to block accidental lost or corruption of personal data. Finally, the access must be restricted to the authorized persons only, at the hours justified by their function. Those measures are relevant to the previous article 17, §1, concerning the appropriate organizational and technical measures.

5) The network integrity requires to protect the network implied in the processing of personal data, against any unauthorized access (interference, malware, etc…). This measure is relevant to the article 17, §1 concerning the appropriate technical measures.

6) The logical security of access requires a list of the authorized persons entitled to access and to handle personal data, with their respective rights (create, read, modify, erase). The access authorizations must be translated in technical systems taking part into the processing of personal data. Identification can be completed by authentication. Those measures are relevant to the previous article 17, §1, concerning the appropriate organizational and technical measures.

7) Activity logging, tracebility and analysis of access must be foreseen in order to find the identity back of any actor having accessed or processed the personal data (physical access, or the logical access, or both). Furthermore, data for tracebility being personal data, their processing must be done with appropriated security measures. Those measures are relevant to the previous article 17, §1, concerning the appropriate organizational and technical measures.

8) The surveillance and maintenance of processing, evolution of resources and analysis of activity logging must be planed. Regular checks (at least once a year) of the objectives and the applied security rules must be planed in order to correct or improve them in case of necessity. Finally every reorganization or modification of the organisation structure must imply an updating of the exiting security measures. Those measures are relevant to the previous article 17, §1, concerning the appropriate organizational and technical measures.

9) The management of security incidents will describe the procedures to be followed when security incidents are detected, as well as the persons responsible to handle those incidents. The

circumstances of any incident must be analyzed in order to infer the preventive or corrective measures. In case of service continuity constraints, recovery and continuity measures must be planed in order to face security incidents involving an interrupted service for an unacceptable delay.

Those measures are relevant to the previous article 17, §1, concerning the appropriate organizational and technical measures.

10) A documentation must be written, with the following characteristics:

- exhaustive, formalized, proportional to the needs in security,

- constantly updated,

- accessible in due course to whom it may concern.

In particular, this documentation must list at least:

the identity of the counsellor in security;

the policy of security;

the plan for implementation of security measures;

the inventory of the processed personal data, their localisation and the executed processing;

the name list of the agencies, employees and officials able to access those data;

the technical configuration of the systems and networks;

the technical documentation concerning the effective security measures;

the timetable of operations planning;

the policy of traceability;

This measure is relevant to the previous articles 17, §4, and article 17, §1, concerning the organizational measures.

5.3. Responsibility and accountability issues

« Complex and confusing systems enable users and designers to blame the machine, but with improved designs responsibility and credit will be properly given and accepted by the users and designers." [56] The effective realization of that wishful prediction may be more difficult though. Information systems built on multimodal observation typically rely on a "post-modern" epistemology where prediction of events, behaviours etc. relies decreasingly on methods of reasoning centred around the *explanation* of phenomena in terms of *causality* and increasingly on a logic that does not try to *explain* phenomena in terms of *causes and consequences*, but that merely *observe* correlations between phenomena, and, from that observation, establishes and enriches

[56] Shneiderman, B., "Human Values and the Future of Technology : A Declaration of Responsibility" in Shneiderman, B., (ed.), *Sparks of Innovation in Human-Computer Interaction*, Ablex Publ., 1993.

population wide and individual profiles. Identification of causes formerly used in order to predict consequences is increasingly replaced by observation of correlations in order to predict risks and opportunities. This epistemological shift is far from unproblematic for the law. The notion of causality is indeed central in any legal regime of responsibility. The relevance of all this is of course hypothetical, but would be undeniable if the technologies developed in Miauce were to be used in law enforcement applications, for example.

At the stage of technology implementation beyond the experimental context, additional issues must be considered, such as those relating to the still unclear ascription of responsibilities for the damages arising from a potential failure of the system. Potential responsibility for the failure (designers; operators; data controllers;...); responsibility for bad decisions induced by the automatic system (designers; operators; data controllers;...) must be carefully addressed before the implementation of any scenario. From a legal point-of-view, however, the technical intermediation may be a challenge for the legal ascription of respective share of responsibility in the actors network involved. Further studies are therefore needed to address the very troubling consequences, and to assess whether current legal rules for the establishment of causality should be reworked as to fit the needs for compensation arising from potential malfunctioning of these complex human-technological networks.

CHAPTER 3:

SCENARIOS EXPLORATION: SOCIOLOGICAL, ETHICAL AND LEGAL ISSUES

INTRODUCTION

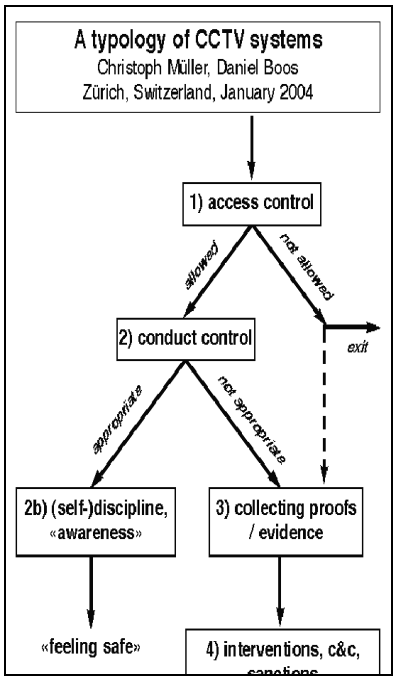
This third chapter of the deliverable is dedicated to the scenarios analysis.and to their progressive consolidation around a sensible ethical, legal and social design. The whole approach has been supported by a true participation of all the teams involved into the MIAUCE project. According to what we have developed in the previous chapters regarding the limits of the experts' figure and our approach of ethics as a pragmatic know-how, this participation is a critical requirement to foster the learning ability of all the involved teams to make sensible choices when facing unknown ethical situation.

In this chapter we will first assess each scenarios as they have been proposed by the scientists and the industrials and raise the major issues (social, ethical and legal) questioning them. This process of analysis and prospective has given raised to a collective deliberation about new requirements for the design of the technologies. These agreed requirements are formulated at the end of the analysis of each scenarios.

1. SAFETY SCENARIO (S.1.3)

1.1 Situating the scenario

The first analysis of this scenario consists in well situating the role and the responsibility of the technologies at work into the scenario. To do that we use the typology drawn by, Christoph Müller and Daniel Boos and presented in Chapter 2. According to this typology, the S.1.3. can be considered as belonging to the Flow control and deployment (intervention planning) system. (the 4th Type)



Let us remind the role of this type of systems. The main role of this system is to plan an intervention. In that sense, this type of system has some characteristics that differentiate it to the others. First of all the objects that are surveyed are not the individuals or the space but flow of individuals, of cars. The recording and the analysis of data (being human or not) have to be in real time in order to support quick intervention. The system has to be very reactive according some parameters to detect normal and a-normal situation. This detection again can be human based on experience and professional heuristic or automatic based on logical programmes and algorithms.

Based on this definition, it appears quite clearly that the scenario S1.3 belongs to this fourth type of system that means systems considered as instrument to collect in real time evidences that are used to plan intervention. In this type of system the collected images do not consider individuals but flow of moving people (crowd) or moving objects (traffic) in order to survey the normality of the flowing, to detect every breaks or a-normal situation (collapse, running panic, etc.) and to react in 'real time' : intervention.

The general meaning of this S1.3 scenario is to fasten the coordination between images collection – problem detection - human decision – human intervention. The two first processes are automated even if based on human choices in designs and parameters; the two last belong to the human intelligence and reactivity. In this coordination chain, the system designed by MIAUCE plays a role of warning to detect and identify a-normal situations.

The main objective of S.1.3. is the detection of anomalous situations in airport escalator exits through the capture, analysis and recording of movements and trajectories on the escalator. The exemplar hazardous situation depicted in the scenario is an escalator collapse resulting in people being trapped in a crowd.

The scenario comprises several phases, that may be qualified as:

A-Image capture;

B-Interpretation: application of algorithm allowing interpretation of images as either normal or abnormal or unexpected, potentially hazardous situation;

C-Action taken either by human employee in charge of security or by the system itself (autonomic decision) to stop the escalator, leaving the human employee to restart it after the cause of disturbance has been remediate.

As it is presented by the scientists and the industrials, this scenario is

1.2 Socio-ethical analysis

1.2.1 TECHNOLOGICAL PATERNALISM AND SOCIAL RESPONSIBILITIES

Regarding the social acceptability of the system and moreover the related question of the responsibility enacted by the system, it is important to raise the question of risk management embedded into the system.

The first issue raised by this question of responsibility concerns the definition of the exact finality of the developed system. This definition is critical to capture the exact responsibility of this system regarding risks of accident and of injured people. Does this system play a role of anticipation in order to warn monitoring team about a risk of accident and of injures or, does this system play a role of reparation helping to manage and to prevent accidents and injures? This question is directly related to the question of the real time considered into this scenario and has to be clearly positioned in order to well define the sharing of responsibilities in case of accident.

The second issue raised by the scenario as it is concerns the complexity of the cooperation chain between human and non-human actors. The map of the involved actors and their responsibility in the chain of coordination has to be clearly defined. This question is analyzed later on in the legal analysis part. From a socio-ethical point of view, the clear definition of each involved actor is a strong requirement for the social acceptability of the system.

Actors	Status

Airport society	Owner/legal chair person
Public	Citizens
System Designer	Conceiver
Commercial	Vendor
Monitoring team	Employees or private group
Airport team	Employees

Again, this clarification of the respective power and responsibilities of human actors versus non-human actors is critical if one would avoid risks and dangers for the involved actors. This issue is particularly important to assess in case of lack of liability or defection of the system. Let us imagine a technical failure,, a problem of capture or of retrieval of data which leads to the non-detection of a problematic situation. This defection has as consequence that a group of travellers collapses in an escalator and is seriously injured.

This situation obliges us to raise two main questions:

- Who is responsible in case of a failure of the observation system?
- What is the tolerance to risks that has to be embedded into the system?

But the failure or the defection can also be human. In that case the monitoring team does not consider a signal of the system and does not warn the intervention team in order to avoid fatal consequence of a collapse. Here again, travellers are seriously injured into the accident.

This situation obliges us to raise two additional questions:

- Who is responsible in case of a human failure of the observation system?
- How to avoid this type of human failure?

The third issue regards what we could call the technological paternalism inspired by this scenario. By technological paternalism, we mean, along with S. Spiekermann and F.Pallas (2006)[57], the fact that people become both more dominated by and confident in ever more complex and autonomous technology. This questions directly the capability of people for self determination and then the vitality of our Society. In the scope of the concerned scenario, three risks related to this 'technological paternalism' should be avoided.

The first one well described in the literature does concern the increase of stress that this 'technological eye' could bring on the monitoring professionals in charge of the airport

[57] Spiekermann, S. and Pallas, F., "Technology paternalism. Wider implications of ubiquitous computing" in *Poiesis Prax*, vol. 4, *2006*, pp. 6-18

surveillance. This is very in line with the implicit control those technologies can make on the professionals. Thus, security agents could cope with more stress and a more controlled work, due to the recording of the video streams in the database. But this stress could also be related to the over-expectation of the public, due to the presence of this technological system, for rapid and efficient intervention. This has well been demonstrated by C. Müller and D. Boos (2004) noting that ,

> *There is an important drawback of such CCTV systems working as 'additional eyes' for police forces: While allowing them to plan their interventions, these systemsmay at the same time increase the public's expectance that the police will intervene every time when the public believes that there is a necessity for an intervention. This may result in an increased pressure on police forces to intervene (otherwise, they may loose credibility) .*

The second one still regards the professionals and do concern the risk of de-skill of a decrease of vigilance of the human operators due to the presence of this technological eye. That means, for instance, if the security agent or a monitoring staff member detects *de visu* something wrong on an escalator, must he intervene or not if nothing is detected by the system? This raises the question of the 'confident technology' and has to be clearly defined and explained to the concerned actors in order to avoid non-responsible attitude

The third risk regards the decrease of the collective or social responsibilities of the concerned public due to the presence of this technological eye. This is even more critical when the technology is implemented in a space marked by a high mobility of people and then by a very low level of sociality. This observation has to be well taken into account for the information displayed to the public when such technology is implemented.

1.2.2 PUBLIC SPACE VERSUS PRIVATE SPACE: BLURRING AND RESPONSIBILITY

For D. Lyon (2003) airports are filters to the mobilities that pass through them. Those places of high mobility, cultural diversity and then low sociality and shared normativity are by excellence places where surveillance systems have chance to be developed.. But those places are also marked by a sort of a tied and complex blurring between private and public, even if for the people they appeared as public space.

The question raised by this blurring regards mostly the organisational and social impact that could have the deployment of the technology at work.

First of all, as already underlined before, the deployment of this technology raises questions about the sharing of responsibility between private society acting those surveillance systems and the public forces in charge of public order. As underlined into the literature, in many cases, the deployment of this type of surveillance system reinforces the blurring between private and public by a sort of privatization process of public space. As the *Report on the Surveillance Society* underlines, this question goes beyond the limits of the space:

> *Whilst both public sector and private sector share information, boundaries between state and private sector interests are blurring, as more tasks of government are carried out through a sometimes complex combination of public, private, voluntary-sector and market mechanisms.*

> *Increasingly, a variety of local partnership arrangements bring together a variety of agencies and professions so that their skills can be better focused on providing services to individuals in a more integrated way. Where state information is available for private use, as has been suggested with the National Identity Register (NIR), concerns have to be raised about the limits to the consent of people as citizens and as consumers, and where those boundaries lie. Questions will continue to be raised with the privatisation of telecommunications, border management (IBM's Project Semaphore, the UK's e-borders programme) and local security (e.g. Citizen Corps in the US who 'look out for unusual activities').* [58]

We can note another intrinsic danger residing in that blurring: personal data, contained in video streams, could overflow from one purpose or one sector to another one. It is critical to design the technology in order to limit the risk of this overflow. This issue will be developed in the next section devoted to the legal requirements.

This privatization process of the so-called public space - or of what is perceived as a public space by the lay people- raises many issues that overstep the strict frame of the scenario at work. But it seems important to point them out in order to better understand the major societal changes that could generate the deployment of these observation systems in our Society. Many urban geographers soicologists have underlined the fact that a new observation or surveillance system in the public spaces, for instance pedestrian streets, malls, airport, implies a new organization of urbanism.

> *The privatisation of urban space has raised concerns among many commentators, as a process that systematically sorts the privileged or compliant from the undesirable or disobedient (e.g.: Caldeira, 1996a, 1996b; Davis, 1998; Abaza, 2001), while subjecting those who patronise these forms of 'mass private property' (Shearing and Stenning, 1981; 1983) to forms of surveillance and social engineering so pervasive that conformity to their rule systems is induced unthinkingly (see for example Shearing and Stenning's (1987) vivid recollection of a trip to Disney World)…* .
>
> *Moving from the ethics of surveillance to the ethics of exclusion, there is a growing danger that the social orders will come to be defined by the conservative requirements of the popular majority, closing off access to those who challenge these conventions"*[59]

One can note that the blurring between private and public space are very close to what Giorgio Agamben develops in *Homo Sacer, II* (2003): the *State of Exception* describes a transitory and extraordinary status in which the fundamental rules of the democracy are evicted, invoking security and necessity reasons.

---

[58] *A Report on the Surveillance Society*, *For the Information Commissioner* by the Surveillance Studies network, Full Report, September 2006, p. 26.

[59] Wakefield, A., "The Public Surveillance Functions of Private Security" in *Surveillance and Society*, Vol. 2 (4), 2005.

It is firstly obvious that we frequently can no longer differentiate between what is private and what public, and that both sides of the classical opposition appear to be losing their reality(…) The state of exception consists, not least, in the neutralization of this distinction. Nonetheless, I think that the concept is still interesting. Think only of the multitude of organizations and activities in the United States that, at present, are devoted to the protection and defense of "privacy" and attempt to define what belongs within this realm and what does not. [60]

1.3. Legal issues.

1.3.1. APPLICATION OF HUMAN RIGHTS FRAMEWORK

The application of the international legal norms to the airport scenario leads to the following observations. Regarding the international regulation, i.e. the Human Rights frameworks, there will be no serious threats against the human dignity, as against the freedom of movement, for the users of the escalator as well for the security employees using the system, as long as we consider a safety purpose, with no specific will of people identification.

Nevertheless, for the airport scenario, as for any other Miauce scenario, we have to remember that even if the data legislation does not apply to it, it might be questionable from the broader point-of-view of other fundamental rights, such as privacy, freedom of movement, freedom of expression, non-discrimination among others. For the airport scenario, as explained before, the mere presence of CCTV systems embedded in the infrastructure de facto decreases the level of privacy enjoyed when using these infrastructures; whenever the system's functioning results in individuals feeling compelled to avoid using the infrastructure at all, as to avoid being "recorded" by a CCTV system, their freedom of movement and right not to be discriminated against may also be an issue.

In order to prevent any significant infringement against the right to move without being constantly traced, we recommend to blur the faces on the images. This technical measure will allow the system to be adequately proportional in respect of a safety prevention, offering a real improvement regarding non technical devices, but not allowing any response to a secondary security purpose. However, in that last case, the decryption of the blurred faces could be possible only in the context of application compliant with article 8, §2 of the European Convention of Human Rights.

1.3.2. EUROPEAN DATA PROTECTION REGULATION

After this application of the Human Rights Convention, we will study the application of the European data protection regulation. As already noticed, the user of the system will have also to take into account more specific legislation as Videosurveillance Act which might cover also the capture of non personal data. Within the frame of the Data Protection Legislation, as previously

[60] Raulff, U., "Interview with Giorgio Agamben – Life, a Work of Art Without an Author: The State of Exception, the administration of disorder and private Life" in *German Law Journal*, n°5, 2004. *Special Edition, available on* http://www.germanlawjournal.com/article.php?id=437

developed, we have to consider, different definitions within the specific context of the airport scenario: “personal data”, “data subjects”, “processing”, “data controller”. In a second step, we have to consider the principles relating to the lawfulness of data processing, i.e. the duties of the data controller, as the obligations imposed to him relating to the principles of “data quality”. In a third step, we will analyse the rights and privileges of the data subject, e.g. the right to be informed, and the access and rectification.

1.3.2.1. Personal Data at stake

As introduction, a very important point to be remembered is that the finality is not a relevant criterion for deciding the applicability or not of the data protection regime. Concerning the airport scenario, even if its finality is not to identify, to control or monitor individuals, the fact that the captured images identify or can identify individuals, will be the real criterion to decide or not the applicability of the european data protection regime. The only way to avoid application of this legal regime is then to implement technical measures that ensure reliable anonymisation of the processed data, and if compatible with the purpose of the scenario, an irreversible anonymisation will be the best.

So as first conclusion to the analysis of our airport scenario, the captured images constitute well personal data, as they are information that concern individuals identified or identifiable, and that are not irreversibly blurred at the very start by the system.

1.3.2.2. Data subjects

Having noted that we are in presence of personal data, we will focus our attention to their relation with the people they concern. This lead us to identify the different categories of those people, so called “data subject”, such personal data are related with. At this level, we may quickly discuss the sensitive nature of those data. As our scenario purpose is not based on those physical peculiarities, and so, the provisions about sensitive data will not be taken into account.

The data subjects represent the different categories of people submitted or related to the technical system in place. For the airport scenario, this includes the passengers or common travellers, or their relatives, familiars or friends since all these people are using the escalators, but also the employees of the airport each time they cross the area covered by the camera, and the employees of the security team, watching the control since the system will permit to the airport company or the security company in charge of the data processing to monitor indirectly their activities. The personal data could be different, depending on the concerned data subject categories. So the personal data of the two first categories will be the captured images. For the employees of the security team, any data produced during the performance of their work and related to them will constitute their personal data.

1.3.2.3. Data controller and data processor

Those personal data will be processed in order to fulfil some purposes, depending of the categories they concern. Those purposes are fixed by the data controller. He must be identified taking into account all types of delegations of service provision that could happen. In our airport scenario, this

role will be played by the airport authorities, together with the provider of the technical services or the third parties responsible for the data processing (so called, according to the Data Protection Directive, the "data processor"). We are then in presence of a network of actors, and of applications, involving a certain level of complexities regarding the ascription of responsibilities among actors.

Besides privacy and data protection issues, this 'airport' scenario raises a series of potential difficulties in cases of human or system failure.

In principle, the airport is in principle responsible towards the public for the correct functioning of the infrastructure put at their disposal. The notion of infrastructure includes the escalator and the ICT system embedded therein. On the contrary the airport is not responsible as regards the wrong behaviour of passengers using the infrastructure.

The technological intermediation may, in such a configuration, impact on responsibility and liability in the following ways:

1. Recorded images will, in certain cases, facilitate the demonstration, by airport authorities, of the responsibility of a passenger or user for the malfunctioning of the escalator. Faults and negligence that would otherwise have been ignored will be more easily assignable to individuals. .

2. The airport would be responsible for informing the users and customers of the exact functionalities of the observation and reaction system in order not to generate unrealistic expectations in terms of safety, for example..

3 .The airport should keep the original or traditional system functional as to be able to face a dysfunctioning of the ICT system.

4. In cases where the airport authorities would have been recognized responsible for the damages resulting of a technical failure of the ICT system, or for inappropriate or delayed reaction to an alert emitted by the system,

• 1st situation: the ICT warning system has functioned correctly: the image captured might be used as a « prima facie » proof of the employees' lack of care if the collect has been achieved lawfully, it means according to privacy regulations. This conclusion is founded on the principle that nobody might be received by a Court if the means of evidence have been illegally collected. .

• 2nd situation: the ICT warning system has not functioned correctly (e.g. the system has not detected the hazard it normally had to detect according to the description of the functionalities of the system). The airport will be liable towards the public but …

–may in turn involve the responsibility of the information system integrator whenever the system does not match the airport authorities' expectations**,** whereas

–the information system integrator may, in turn, if acknowledged responsible, sue the information system designer. How all this will be settled may depend on whether specific provisions regarding liability have been established by the contract between the I.S integrator and the airport company.For our airport scenario, as previously explained in chapter two, it is the duty of the data controller, if he decides to make recourse to a company for operating the security system, to assess the quality of the data processor and his ability to provide adequate security measure. Furthermore the data controller has to define precisely by a written contract the missions of the data processor and to check if the data processor does respect entirely the limits of his contractual duties. Precisely it is the data processor's obligation not to infringe his contractual duties and not to process the data for other purposes than those assigned by the contract. The processor shall act only under instructions from the controller. If he exceeds (for example, the security company sells to marketing

companies the data collected through the airport's CCTV), he will be designated as controller and since his processing are not legitimate might be suited before civil and criminal courts.

1.3.2.4. Lawfulness of the processing

The data controller has many duties to respect, in order to guarantee the lawfulness of the data processing. As a very first condition, the data must be collected in a transparent way and processed fairly and lawfully. There is a need for a balance of interests, weighting constantly the right to confidentiality of the data subject versus the interests of third party or parties in obtaining personal data. The right to process personal data about data subject must be accompanied by effective means for this later to defend his or her interests, especially to be kept adequately informed. So, in our airport scenario, there is an important obligation of information and transparency for the data controller, with respect to the data subject, about the purposes, about a permanent evaluation of the balance of interests and about the possibility for the data subject to always be able to defend his or her interests.

As second condition, the processing must be legitimate. Among the list of cases which makes a priori the data processing legitimate, those following are the most relevant: the processing is necessary in order to protect the vital interests of the data subject or to answer to a prominent interest of the airport company (ensuring the security of the passengers) considered as more important than that of the data subject to confidentiality. Exceptionally, we might envisage that the processing would be necessary for the performance of a task carried out in the public interest or by the exercise of official authority vested in the chief of the data controller. As previously explained in chapter two, the vital interest has to be interpreted in the narrowest sense, it means when the body of a person is seriously endangered. The public interest may only be invoked when the data controller is vested with official authority, which would probably not be the case in most business cases contemplated so far but which might be the case if the videosurveillance system is under a specific legal obligation coupled with the information system of the law enforcement authorities timely or on a permanent basis.

As third condition, the data controller has the duty to define precisely the purposes of his processing and to make them explicit. It means that he has not to use vague wording but definitively to enunciate in a document the purposes in a way which might be understandable by a reasonable data subject and apart from which the data subject will envisage the reason why the data are collected This obligation is also part of our technical recommendations as presented at the end of this analysis.

As fourth condition, the compatibility is a very important requirement in a system characterised by the possibility of evolutive applications. It is quite easy to imagine new applications linked with the CCTV surveillance system with new purposes. The question to know if this is definitely a new usage not compatible with the prior purpose existing at the moment of the collection, or, at the contrary, a usage compatible with the former one, can be solved with the criterion of “reasonable expectation”. This one raise the question to know if the data subject has had the possibility at the initial moment of the data collection with the information given by the data controller to imagine this future usage as included in the purpose of the processing. If the answer is yes, the processing is deemed as compatible and is legitimate without new formalities. If not, the processing is a new one and has to find a basis for its legitimacy and definitively the data subject must be at least informed or even agree to this processing. Through this fourth condition, and as with the balance of interests,

we find here again the necessity of a constant evaluation, meaning that no final judgement regarding privacy and data protection can be reached with such dynamic systems. This is then an important responsibility of the data controller to be aware of such obligation and to comply with it! In general, given the dynamism and plasticity of the systems at issue, constant monitoring should be exercised as to ensure that the conditions of legality (compliance with human rights as well as data protection requirements) are always met. The whole system's legitimacy should be reassessed each time a shift in the variables involved occurs. This idea of permanent legal assessment due to permanent technical evolution is also part of our technical recommendations, presented further in this analysis.

1.3.2.5. Data quality

Apart from those obligations concerning the lawfulness of the data processing, the data controller has also to fulfil obligations related to the principle of "data quality", ie no more concerning the processing but the data processed. In that case, the data must be adequate, relevant and not excessive, in relation to the purposes for which they are collected and/or further processed. They must be accurate and kept up to date, and if not, must be erased or rectified. They must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. For our airport scenario this implies not to conserve data if no incident happened. The data minimization implies that only the personal data necessary for the implementation of the system should be collected, processed or stored, and that the data must be deleted when no longer necessary and after the legal conservation requirements. For the airport scenario, all those requirements imply to decrypt the blurred images only if there is an accident, and to the extent strictly necessary to review the images of the accident's moment. Furthermore, just these images might be kept, the others have to be deleted insofar they are no more necessary considering the purpose of the recording.

1.3.2.6. Rights of the data subject

The directive 95/46 affords different rights to the data subject. We have already discussed some of these in our previous explanations about the application of Human Rights framework. One central notion of the data protection regime is the notion of transparency. Apart from this principle, legislation imposes to the Data controller to deliver information about the main characteristics of his processing to the data subject. This will depend on the situation where the data are obtained or not from the data subject. In both cases, that information enlightens the data subject about the purpose, the identity of the different actors in presence and the existence of his rights he can exercise. This information must be given in adequate form, ie for our airport scenario, in the form of a clear and visible pictogram, at both ends of the escalator. The concrete meaning of this obligation of information is also detailed in the technical recommendations that follow, as responsibility of the security officer (or counsellor).

Another right of the data subject is to access his processed data, to have incorrect information erased or rectified, to have illegally collected or processed information deleted from the system. In the airport scenario, this seems difficult to be guaranteed. We believe that a special effort of information to the public must be done, in order to convince him that no personal data are kept longer than necessary, that data are most of the time encrypted and that only useful data are decrypted if an accident is reported. This is essential to obtain and keep the public confidence. In that case one might consider that right of access is no more necessary insofar the exercise of this

right of access would oblige the data controller to keep a record of the data and so to create a risk to data protection interest greater than the interest pursued by granting the access.

The second main European legal instrument, the directive 2002/58, concerning the processing of personal data and the protection of privacy in the electronic communication sector, is not applicable in this scenario.

1.4. Recommendations

Applied to the specific context of the airport scenario, we finally recommend some additional requirements regarding security of processing.

The context – an airport - of use for such technology is not clear from a legal point of view. Are we in presence of a private or public space? That needs to be clarified even in both cases the data protection and Privacy requirements are applicable. Following the security recommendations that have been presented at Nantes meeting, from a general point of view, we will recommend a clear definition of the security policy, by proceeding with a deep risk analysis, by clearly specifying the priorities of the security plan, by describing the duties and responsibilities of every stakeholders, by clearly describing the incidents management process and the measures taken to keep up to date the security system after it has been activated. This policy must clearly specify on which bases the legitimacy is established. The principle of data minimization must be respected, in the sense that only the necessary data for the implementation of the system should be collected, stored and processed, and that those data may not be conserved for a period exceeding the legal requirements.

According to article 9 of the Directive, a clear information about the purpose of the processing, the nature of data and the data controller's identity must be given to the data subjects, that should be present at both ends of the escalator.The quality of the security depends not only on technical measures, but also on organizational measures, implying human responsibilities and obligations, giving rise to disciplinary and legal actions in case of infringement by the persons in contact with personal data.From the technical point of view, we agree with the limited time of image storing in data base, in respect of the legal obligations in that matter. We recall that any storing of data in a data base implies for the data processor to secure those data bases against any unauthorized access. We agree also with the complete separation of the TV circuit used for this safety purpose, from any public network. This measure meets the requirements to protect the network implied in the processing of personal data, against any unauthorized access.

Furthermore, we agree with the access restriction to the video or to be more precise to personal data collected through the CCTV system, inside the intranet, by the control centre operator only. This measure must be included in a global access policy, defining the rights of access and the rights of action of each employee and the time where this access is made possible. Regarding the capture of images, we recommend the use of anonymization techniques, in order to forbid any identification of any person in the observed crowd. This measure is valid not only for the videos captured on line, but also for the videos used for training and validation. Regarding the source of input images, we require attention in case of use of the video stream for security purpose, but duplicated for safety purpose.

From the organizational point of view, there is a necessity to designate a security officer in charge of the global supervision of the safety system in operation. It has to be remembered the necessity for the security officer (or counsellor) to act independently, to report directly to the management team and to have enough means - time, human, material, financial resources, abilities and training

resources and access to any relevant information - to perform his work in normal conditions. From a legal point of view, this security officer is clearly liable for the entire security policy.

It has to be clearly recalled that any other person – internal or external – implied in the processing of personal data will be constantly and sufficiently informed about its specific duties and responsibilities, and will be sufficiently and correctly trained to practice his work and his responsibilities in the domain of security. Finally, this system can indirectly control its own users and monitor workers. Any data like activity logging, traceability or resulting from an access analysis are personal data and must be processed with appropriated security measures.

2 MARKETING SCENARIO (M.1.1)

2.1 Situating the scenario

The M1.1. scenario exhibits mainly marketing orientations. We can identify the finality of the system as collecting evidence (which is very close to the type 3 defined in the typology of Müller and Boos) as to measure the efficiency of a specific shelf display, which involves data recording and analysis. The finality of the system is not to collect evidence or proofs of specific or general human attitudes or conducts. Regarding the use of recorded data and of analytical results, two situations have to be differentiated: the first one is supported by real-time analysis and devoted to on time intervention. The second one does not use the recorded data except in case of problems (accidents, crimes, fraud, vandalism…). In that case, the recorded data are use as proof of evidence for an ex-post sanction or trial. In the case of M1.1., the use of the recorded data is differed since it serves for merchandising re-arrangement. M.1.1. aims at collecting data for marketing purpose. In the described scenario, the marketing purpose is much more orientated towards merchandising that is to say to collect statistical evidences regarding the merchandising disposal on a shelf in a supermarket. Even if it is more merchandising orientated, it also belongs to the more general environment of marketing methods and it is worth locating the M.1.1. scenario into this broad environment.

Type	Type 1	Type2	Type3
Profiles definition	A priori	Ex post	Continuous
Profiles constitution	A priori sorting (A-B-C-D life style sorting)	Ex post sorting based on habits of consuming	Continuous sorting based on dynamic data retrieval related to the attitudes of consuming
Marketing action	Mass marketing based on classes of consumers (segments)	Personalized marketing	Pervasive and personalized marketing
Subject	Classes or a priori categories -	Semi-conscious Individuals	Un-conscious Bodies

	volunteers		
Technical devices	Marketing studies and surveys	Computerized data retrieval (loyalty card, plurality of traces left by his buying and consuming actions)	Computerized and video monitoring of moves and actions
Type of marketing feedback	Campaign	Personalized messages	Environment's modification
Time of marketing feedback	Planned	Ex post - deferred	Immediate
Visibility	Visible	Identifiable	Invisible

Regarding the three types of marketing methods, it seems clear that the M1.1. belongs to the third one. Some characteristics of this third type can be applied without difficulties to the scenario M.1.1. : continuous – un-conscious bodies – computerized and video monitoring – Environment modification and invisibility. Others are not applicable into the strict frame of M1.1. but could help us to draw some prospective or alternative scenarios. According to the typology of MULLER and BOOS and the typology of marketing method, it appears quite clearly that the scenario M1.1. aims at collecting evidences regarding the attractiveness of shop window display in order to better manage the display of the products.

This particular scenario aims to capture the multi-modal behaviour of people who look at a shop window, to determine the effect of product displays. Such analysis can be applied to a shop window of a little store or in a pedestrian street. As such, the end-user of this application can be the shop owner, store manager, or those who are responsible for display arrangements. Since there is little existing technology that can evaluate the effectiveness of product displays based on people's behaviour, the multi-modal interaction analysis is a promising technology to apply to such problems.

The environmental context of the cameras installed will be an important aspect for optimisation of the detection algorithms of multi-modal interaction analysis. The contextualised presentation of the outcome of the analysis should also improve the understanding of the relationship between the product displays and people's behaviour.

The general meaning of M1.1. consists in better assess the effectiveness or the attractiveness of a shelf inside a shop. To do this assessment, the scenario has to establish statistical relationships between data collected on individual body detection, head pose estimation and gaze tracking on one hand, and on the other data concerning the shelf.

The scenario contains three main steps of deployment:

- Statistical counting of individuals passing in front of the shelf
- Statistical counting of individuals stopping more than 5'' in front of the shelf
- Statistical detection of the visual field covered by the individual in order to make

hypothesis regarding the zone of the display visualized by the person.

The main intention of this system is to measure the attractiveness of a product displayed into a shelf. To get the exact measure, the system has to work on an individual basis, calculating and parametering each body stopping in front of the shelf.

For legal reasons, the scenario is presented in an experimental environment working only with volunteers. But this raises other questions regarding the liability of such system since this type of observation requires that people behaviour naturally, that is to say without knowing that they are observed. We will come back on this point in the sections devoted to socio-ethical and legal analyzes.

The scenario suggests that the system is auto-sufficient, that means that it is not connected with other databases as for instance data concerning the customers. This prevents the current scenario from more intrusive application regarding the privacy of people. As it is, it is presented as a guarantee for non-misuse of the developed system in terms of sorting, profiling and discriminating.

But here again, this argument has to be questioned:

- First of all, without any connection to other data bases, the proposed scenario appears a bit weak regarding its added value for marketers and shop owners;
- With connection to other databases, the system becomes more attractive but at the same time more risky and dangerous regarding its effect in terms of privacy and discrimination.

2.2. Socio-ethical analysis

2.2.1. BODY, TRUTH AND HUMAN CONSENT

Based on the third marketing paradigm, this scenario shares a central principle that “a body does not lie”. Into the marketing frame of the scenario, this argument promises ‘natural data’ not corrupted by the human reasons and the subjective analysis of the situation.

This supremacy given to the body as the unique access to authenticity and truth present in the M1.1 has to be questioned. In fact, translating human identity into information patterns not only provides more information, it also creates new conceptions of identity. Techniques of biometrics are presented as the guarantee of an authenticable and non-falsifiable identity, because of the intrinsic value of naturality that resides in the human body.

First of all, this paradigm of naturality must be politically interrogated. That seal of naturality is fundamentally political: it argues that the body is the last instance of the truth and authenticity of the human being. In the post-modern context, when there is a fragility attributed to the human consciousness, human bodies become more and more synonyms of truth and authenticity, as the only remaining tangible reality of the subjectivity. It appears that the subject is no more trustful, but his body is the last rampart of truth, authenticity, because it is a “readable text” (Van der Ploeg, 1999) and understandable material. Bodies and faces are readable through a specific prism, and statistically computable.

The question raised by M.1.1 does also concern the reductionist approach of the body. R. Hall has

demonstrated that the body is the settings and the vehicle of social identity and communication. To a certain extent, people construct their bodies in order to feel conformed, marginal or recognizable amongst the others. So body is an intrinsic part of the social personality and identity of the people. That means also that this assertion that suggests that bodies do not lie to justify and legitimate more and more intrusive observation system has to be questioned. In particular, 'body can lie', can be disguised, distorted when knowing being observed as it is required by the legal requirements regarding the informed consent.

The informed consent is another problem raised by this scenario. The central principle of this type of marketing scenario is to remain invisible for people in order to capture a body that is supposed to not lie. Mark Andrejevic[61] explains very well the rationality and values of this major principle that supports modern system of surveillance:

> *...the goal is to surprise the real state of mind into revealing itself: to put it in positions where it doesn't have time to compose itself for the camera or the investigator. Such monitoring strategies promise to cut through an unreliable discourse, in order to reveal direct physical evidence: voice stress or unconscious "tells," electrical activity in the brain that correlates with a desired response to an advertising campaign. If the content of the words can't be trusted, perhaps physical traces can be.*

According to this author, this trend can be qualified as post-modern scepticism. In the scenario, cameras observe more bodies than people, and attach a great importance to special features of the body (eye gazes for instance in the scenario). Consequential problem raise from this prism of representations, as Lynsey Dubbeld (2003:151) underlines:

> *Body representations techniques such as CCTV produce constructions of the subject that involve judgmental, discriminatory processes of categorisation and are based on a asymmetrical relations between observers and observed.* [62]

2.2.2. BODY'S INTEGRITY AND "DIS-EMPOWERED" MODES OF SUBJECTION

David Lyon [63] (2001 : 16) explains in *Surveillance Society* the problem due to the widespread presence of CCTV in public space: a paradox of disappearing bodies occurs. Traditionally, observing and monitoring bodies were attained through the physical, by viewing individuals and their behaviours. Now the bodies remain the crucial site of observation, but with the paradox of transformation through the digital matter, with codes reducing to a virtual and symbolic matter.

A kind of primacy about the bodies as matter is observed in this type of observation system, but, nevertheless, their matter disappear in the digital codes, statistics, calculation.... The scope is oriented towards "digital bodies", bodies that the very matter is transformed into binary codes that serve the computerization.

---

[61] Andrejevic, M., "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance" in *Surveillance and Society*, Vol. 4, 2005

[62] Dubbeld, L., "Observing bodies. Camera surveillance and the significance of the body" in *Ethics and Information technology*, Vol. 5, pp. 151-162, 2003.

[63] Lyon, D., *Surveillance Society. Monitoring Everyday Life*, Open University press, Birmingham/Philadelphia, 2001.

An important question raised by this type of technologies regards the body as it is considered by the system. In this observation system, as well noted by A. Ceyhan[64] the body is reduced or reified, victim of a sort of de-subjection. This raises important questions regarding the status given to the body as captured by the algorithm under development and the interpretation of its motion, pose, gesture… for marketing purposes. This clarification of the body status is not only important for instrumental reason (the marketing purpose) but also for ethical and political reasons regarding the rights of people on their subjectivity and their identity. As D. Lyon has underlined it in different papers, many of those systems are operated and processed without the subject's knowledge and consent.

The present context of technologization of security [65] has increased the fact that the bodies undergo fragmentation, reduction and hybridization. Those transformations are accompanied with a high-value path of naturality devoted to the body. It means, at the end, that we can assess ontological changes in the philosophical representations of the body. In references to Bergson, we note that the body looses gradually his *supplement of soul*, technologies reducing it to fragments, organs, parts of flesh and machines...

First of all the body is fragmented, because of the extreme focus on certain visible parts of the body. In the M.1.1 scenario, some of the technologies used consist in body-tracking, eye-tracking and eye gaze tracking. It implies a kind of reductionism, because the human body is condensed into those visible and calculable parts.

But with these technologies, the body is also hybridized. Some technologies, described in MIAUCE, model the face in order to calculate eye gazes and to deduct the contents of what the user was watching. They use a virtual mask, which represents the visible modelling of the face. This virtual mask is a kind of frontier runner between the face and the whole system and hybridizes the skin and the algorithms. In this scope, the political fiction of Cyborg (Haraway, 1985) will be very useful to rethink a new ontology of hybridized bodies.

Along with Deleuze and Guattari (1987), in *A Thousand Plateaus*, we can develop standpoints that assume those transformations. The concept of *Body without Organs* (BwO) allows us to better understand the problematic of human bodies and human faces exposed in MIAUCE. It is very useful thinking order to better understand that fragmentation and reduction process. BwO, which was originally built as a tool of positive experimentation, endures a kind of perverse experience: the organs escape from the *organism*, but it is not from its own initiative, but under the constraints of the technologies [66].

The BwO *is not at all a notion or a concept but a practice, a set of practices (1987: 150).* It is a kind of experimentation, in the sense where it is conducted by the subject in order to slough the organs off, or to loose them. Organs must be understood as parts of organism, e.g. the organisation of strata as Family, State, Science...

---

[64] Ceyhan, A., "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics" in *Surveillance and Society*, Vol. 5 (2), pp. 102-123, 2008.

[65] Idem

[66] Idem.

Dismantling the organism has never meant killing yourself, but rather opening the body to connections that presuppose an entire assemblage, circuits, conjunctions, levels and thresholds, passage and distribution of intensity, and territories and deterritorialisations measured with the craft of a surveyor. (1987: 160)

The body is not understood anymore as a harmonious entirety, but as a whole of collected fragments that match together (or not). In the larger cases of the biotechnologies, converging technologies, AmI technologies, some parts of the body are reified, or overestimated. In the MIAUCE scenario, one concentrates the scope on particular parts of the body (eye gaze, head positions, silhouette...): the body is no more considered as usually, because one focuses on these parts in order to extract some crucial information for calculation and algorithms. The BwO, as a set of practices, where *only intensities pass and circulate (1987: 153)*, matches with the MIAUCE technologies. Moreover, the BwO includes the fact that there is no interpretation to make, because it is populated by intensities and because one does not reach it, it is experimentation.

The MIAUCE technologies applied in M.1.1, tracking the face and eyes gazes, makes a BwO to human bodies: new intensities pass on the virtual mask that models the face, there is no interpretation at a first level. Interpretations come later, but are conditioned by the virtual mask. There will be only the type of interpretations that the designers have previously thought and conceived.

The main problem, with the MIAUCE technologies, consists in the fact that the experimentation is not carried out by the users or the end-users. It is fulfilled by the designers, and the users have no control or power on the sytem that captures their faces and bodies and that interpret them. The BwO, as a flux of positive experimentation, becomes confiscated by the technologies, and the user is “dis-empowered”. This whole process influences the modes of subjection that become affected and over-embodied. An unbalance appears, due to the fact that the modes of subjection belong more to the technologies than to the users’ subjectivity.

2.3 Legal assessment

2.3.1. Application of Human Rights framework

For the supermarket scenario, a possible threat against human dignity depends on the final use of the process results. As long as they only concern the marketers in their researches of the goods best location within a shelf, no serious threat has to be feared, as no specific profile of customer is produced. However as for the first scenario we have to remember that even if the data legislation does not apply to it, it might nevertheless be questionable from the broader point-of-view of other fundamental rights, such as privacy, freedom of movement, freedom of expression, non-discrimination among others. But the construction of any individual profile could leads to a threat, mainly if its purpose is to manipulate the customer in its activity. In order to consider the people as ends in themselves (following the ethical imperative), and also to avoid a disrespect to mental integrity, we believe that there is a strong necessity of transparency and information about the processes and their purposes, precondition to a full autonomous consent.

It is important to remember that this principle of human dignity is absolute and will allow no exception but if the principle is absolute it is not obvious to determine the limits apart from the

human dignity is violated. A public debate has to be launched on that point. So the Data Protection authorities have at several times recalled (See particularly the so called London Declaration which closed the annual international meeting of the data Protection Commissioners held in 2006) that the multiplication of videosurveillance camera in public spaces could attempt to the citizens dignity since their behaviour might be greatly affected in the sense of a normalization of their behaviours.For the supermarket scenario, as long as we don't consider individual profiling, but only statistical information about the impact of goods presentation on their selling rate, no threats have to be feared concerning freedom of thoughts, conscience, religion, expression or hold opinions, of any customer analised by the device. It is not obvious that the conclusions would be the same if the data are used for profiling the people.

2.3.2. EUROPEAN DATA PROTECTION REGULATION

For the supermarket scenario, we have to remember that even if the data legislation does not apply to it, it may be nevertheless questionable from the broader point-of-view of other fundamental rights, such as privacy, freedom of movement, freedom of expression, non-discrimination among others. So, besides potential data protection issues, attentional and emotional privacy are at issue when individuals' gazes and facial expressions are recordedWithin the frame of the Data Protection Legislation, as previously developed, we have to consider, different definitions within the specific context of the supermarket scenario: “personal data”, “data subjects”, “processing”, “data controller”. In a second step, we have to consider the principles relating to the lawfulness of data processing, ie the duties of the data controller, as the obligations imposed to him relating to the principles of “data quality”. In a third step, we will analyse the rights and privileges of the data subject, eg the right to be informed, and the access and rectification.

2.3.2.1. Personal Data at stake

For the supermarket scenario, as explained before in chapter two, besides potential data protection issues, attentional and emotional privacy are at issue when individuals' gazes and facial expressions are recorded and observed. Anyway these personal data does represent more sensitive data than the data recorded in scenario one since certain deduction might be derived from these data to identify at least through statistical methods the psychology or the typical behaviour of a person. Other thing the precise recognition of faces might lead to reasoning allowing the discrimination in function of disabilities, ethnic characteristics, etc.

So as first conclusion to the analysis of our supermarket scenario, the captured images constitute well personal data, as they are information that concern individuals identified or identifiable, and that are not anonymous – that is, it cannot be traced back to an identified or identifiable person.

2.3.2.2. Data subjects

Now that we know that we are well in presence of personal data, we will focus our attention to their relation with the people they concern. This lead us to identify the different categories of those people, so called “data subject”, such personal data are related with. At this level, we may quickly discuss the sensitive nature of those data. It is in principle illegal to process personal data revealing

racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. It has to be demonstrated in the supermarket scenario that its purpose is not to identify these physical peculiarities. So, for instance, the simple recording of people among whose persons with disabilities might be recognized will not lead to the application of the more severe provisions of the Directive except if the processing is designed to retrieve that category of persons in order to analyse by instance their consumer's preferences.

The data subjects represent every categories of people submitted or related to the technical system in place. For the supermarket scenario, this includes the visiting customers as they stand in front of the shelf, searching for a specific product, but also the employees of the shop each time they cross the area covered by the camera. The personal data could be different, depending on the concerned data subject categories, but in this case, ie the supermarket scenario, for both categories, the personal data will be the captured images.

As introduction, a very important point to be remembered is that the finality is not a relevant criterion for deciding the applicability or not of the data protection regime. Concerning the supermarket scenario, even if its finality is not to identify, to control or monitor individuals (and the positions of the cameras are not adapted for a video-surveillance purpose), the fact that the captured images identify or can identify individuals, will be the real criterion to decide or not the applicability of the European data protection regime. The only way to avoid application of this legal regime is then to implement technical measures that ensure reliable anonymisation of the processed data, and if compatible with the purpose of the scenario, an irreversible anonymisation will be the best. A difference must be well established between the use of video for security and for marketing. We remind the existence of some specific national legislations regarding the use of cameras for employees surveillance.

If this technical system is connected to a public information network, then there is a strong necessity to very well protect the collected information against any intrusion, through encryption of the images and through severe protection of the data base of stored images. The information must also be kept only for the necessary duration. If some of them must be stored for a longer time, as they serve to feed the emotion algorithm and to improve its analysis capacity, their level of protection must be very high. It is under the responsibility of the security officer (or counsellor) to include that point in its global security policy.

2.3.2.3. Data controller and data processor

Those personal data will be processed in order to fulfil some purposes, depending of the categories they concern. Those purposes are fixed by the data controller. He must be identified taking into account all types of delegations of service provision that may happen. In our supermarket scenario, this role will be played by the shop owner, together with the provider of the technical services and the third parties responsible for the data processing (so called the data processor). We are then in presence of a network of actors, and of applications, involving a certain level of complexities regarding the ascription of responsibilities among actors.

For our supermarket scenario, as previously explained in chapter two, it is the duty of the data controller to assess the quality of the data processor and his ability to provide adequate security measure. Furthermore the data controller has to define precisely by a written contract the missions

of the data processor and to check if the data processor does respect entirely the limits of his contractual duties. Precisely it is the data processor's obligation not to infringe his contractual duties and not to process the data for other purposes than those assigned by the contract. The processor shall act only under instructions from the controller. If he exceeds (for instance, making statistical researches based on the sex or race origin), he will be designate as controller and since his processing are not legitimate might be suited before civil and criminal courts.

2.3.2.4. Lawfulness of the processing

The data controller has many duties to respect, in order to guarantee the lawfulness of the data processing. As a very first condition, the data must be collected in a transparent way and processed fairly and lawfully. There is a need for a balance of interests, weighting constantly the right of the data subject versus the interests of third party or parties in obtaining personal data. The right to process personal data about data subject must be accompanied by effective means for this later to defend his or her interests, especially to be kept adequately informed. So in our supermarket scenario, there is an important obligation of information and transparency for the data controller, with respect to the data subject, about the purposes, about a permanent evaluation of the balance of interests and about the possibility for the data subject to always be able to defend his or her interests.

As second condition, we have that the processing must be legitimate. Among the list of cases which makes a priori the data processing legitimate, we believe for our supermarket scenario that this following is the most relevant: processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject... As previously explained, they argue that their interest as marketers is legitimate and that the prejudice they cause to the data subject is minor in comparison with the interest the data subjects will get from the publicity and their own legitimate interests.As third condition, the data controller has the duty to define precisely the purposes of his processing and to make them explicit. It means that he has not to use vague wording but definitively to enunciate in a document the purposes in a way which might be understandable by a reasonable data subject and apart from which the data subject will envisage the reason why the data are collected This obligation is also part of our technical recommendations as presented at the end of this analysis.

As fourth condition, the compatibility is a very important requirement in evolutive systems, that permit through their natural evolution, to imagine new application with new purposes. The question to know if this is definitely a new usage, or always a usage compatible with the former one, can be solved with the criterion of reasonable expectation. This one raise the question to know if the data subject has had the possibility at the initial moment of the data collection to imagine this future usage as included in the purpose of the processing. If the answer is yes, the processing is deemed as compatible and is legitimate without new formalities. If not, the processing is a new one and has to find a basis for its legitimacy and definitively the data subject must be at least informed or even agree to this processing. Through this fourth condition, and as with the balance of interests, we find here again the necessity of a constant evaluation, meaning that no final judgement regarding privacy and data protection can be reached with such dynamic systems. This is then an important

responsibility of the data controller to be aware of such obligation and to comply with it! In general, given the dynamism and plasticity of the systems at issue, constant monitoring should be exercised as to ensure that the conditions of legality (compliance with human rights as well as data protection requirements) are always met. The whole system's legitimacy should be reassessed each time a shift in the variables involved occurs. This idea of permanent legal watch due to permanent technical evolution is also part of our technical recommendations, presented further in this analysis.

As previously said, in this scenario, the data are collected to evaluate how well the goods are placed on a shelf, in order to preferentially attract the gaze of the customers facing the shelf. In this situation, there are no purpose to profile the customers. But a shift in the scenario is still possible. Profiling is not a goal in itself but a technical means of achieving a particular result. Profiling may have much more significant consequences than simple statistical processing; it can help to take specific decisions likely to have varying degrees of impact on individuals, like exclusion of essential services. There is then an imperative necessity to allow individuals that are subject of automatic profiling decisions to have a right of redress via a non-automated channel, particularly when these decisions affect the exercise of a fundamental right. The lawfulness, transparency and proportionality, as pillars of personal data processing, must be applied at an early stage of any profiling operation. The threat of disproportionate processing lacking in transparency arises early on, at the warehousing and data mining stages. A risk prevention policy, based on the precautionary principle, must therefore be applied before profiles are applied to specific individuals.

2.3.2.5. Data quality

Apart from those obligations concerning the lawfulness of the data processing, the data controller has also to fulfil obligations related to the principle of “data quality”, ie no more concerning the processing but the data processed. In that case, the data must be adequate, relevant and not excessive, in relation to the purposes for which they are collected and/or further processed. They must be accurate and kept up to date, and if not, must be erased or rectified. They must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. For our supermarket scenario this implies not to process data in order to profile a specific client or to cross the information of the shelf with others, like the bank account or the credit cash facilities. The data minimization implies that only the personal data necessary for the implementation of the system should be collected, processed or stored, and that the data must be deleted when no longer necessary and after the legal conservation requirements. For the supermarket scenario, all those requirements imply to use the gaze information, but without keeping the image of each specific client. So, only the anonymous globalized results resulting from the statistical calculation must be stored, and not applied to specific customer.

2.3.2.6. Rights of the data subject

The directive 95/46 affords some rights to the data subject. We have already discussed some of these in our previous explanations about the application of Human Rights framework. One central notion of data protection regime is the notion information to be given to the data subject. This will depend on the situation where the data are obtained or not from the data subject. In both cases, that information enlightens the data subject on the purpose, the identity of the different actors in

presence and the existence of his rights he can exercise. This information must be given in adequate form, ie for our supermarket scenario, in the form of a clear and visible pictogram, standing on the shelf.

Another right of the data subject is to access his processed data, have incorrect information rectified or have wrong personal data erased from the system. In the supermarket scenario, this seems difficult to be guaranteed. We believe that a special effort of information to the public must be done, in order to convince him that no personal data are kept longer than necessary, that data are globalized and used only to help the marketers to better dispose the goods on a shelf, to increase their selling rate. This is essential to obtain and keep the public confidence.

The second main European legal instrument, the directive 2002/58, concerning the processing of personal data and the protection of privacy in the electronic communication sector, is not applicable in this scenario.

2.4. Recommendations

As very first recommendation, and with respect to the proportionality principle, an irreversible anonymisation of images is compulsory. Even if this scenario is out of the scope of the European data protection regulation, it will always remain questionable from the broader Human Rights perspective (emotional, physical and intellectual facets of privacy). It is necessary to clearly inform the customer about the presence of such cameras in the shelf, and about the purpose of their presence.

Applied to the specific context of the supermarket scenario, we finally recommend some additional requirements regarding security of processing.

The experimental scene has been described in details in report, and takes place inside the shop. In this context, the camera takes no more pictures from any space outside the shop. The goal is now to detect the orientation of the eye gaze of a customer, facing a shelf inside the shop, the camera being placed inside the shelf.

There is a necessity of anonymization of the videos used to calibrate the system, as of the videos taken on line. The videos must be proportionate, taking no other information that are necessary for the purpose. No sensitive data – like the colour of the skin – cannot be taken into account.

The images may not be stored for a longer period than necessary to achieve the stated finality. The legitimacy must be clearly established, based on the explicit consent of the data subject. An alternative should exist; offering to the data subjects an opt-out.

The principle of data minimization must be respected, in the sense that only the necessary data for the implementation of the system should be collected, stored and processed, and that those data may not be conserved for a period exceeding the legal requirements.

Any customer can exercise its right of access to those data, as the right to correct them or suppress them. The data bases used to store the video must be secured against any unauthorized access or uses.

We require attention about the re-use of videos initially captured for a security purpose. There is a need to clearly define the supermarket purposes and to respect the principle of proportionality in this process.

3. INTERACTIVE WEB-TV SCENARIO (TV.1.1.)

3.1 Situating the scenario

As previously explained supra, we sorted the MIAUCE scenarios into typologies. The TV.1.1 scenario belongs to three typologies, because of its very openness and porosity. It can be called hybrid, because of the mix of genres by which it is influenced. TV.1.1 is a marketing/ profiling, "dataveillance" and Ambient Intelligence scenario, which all involve different but interconnected issues.

3.1.1 TV.1.1. AS A MARKETING SCENARIO

The scenario TV.1.1 has clearly marketing purposes, in the building of an adaptive profile of the consumer, by collecting data through the Facial Recognition System of emotions. As in the M.1.1 scenario, this scenario belongs to the third type, with a continuous, pervasive, immediate and invisible sorting based on data retrieval made on computerized and video monitoring of moves and actions.

Type	**Type 1**	**Type 2**	**Type 3**
Profiles definition	A priori	Ex post	Continuous
Profiles constitution	A priori sorting (A-B-C-D life style sorting)	Ex post sorting based on habits of consuming	Continuous sorting based on dynamic data retrieval related to the attitudes of consuming
Marketing action	Mass marketing based on classes of consumers (segments)	Personalized marketing	Pervasive and personalized marketing
Subject	Classes or a priori categories - volunteers	Semi-conscious Individuals	Un-conscious Bodies
Technical devices	Marketing studies and surveys	Computerized data retrieval (loyalty card, plurality of traces left by his buying and consuming actions)	Computerized and video monitoring of moves and actions
Type of marketing feedback	Campaign	Personalized messages	Environment's modification
Time of marketing	Planned	Ex post - deferred	Immediate

feedback

Visibility	Visible	Identifiable	Invisible

This marketing characteristic can lead us to the potentiality of profiling, because of the 'adaptative user profile' implied by this scenario. Bohn et alii agree on the fact that profile generates issues such as : *Besides the obvious risk of accidental leaks of information, profiles also threaten universal equality, a concept central to many constitutions, basic laws, and human rights, where "all men are created equal"*. [67]

3.1.2 TV.1.1. AS A "DATAVEILLANCE" SCENARIO

Beside this, another threat consists also in the observation and analysis of personal and sensitive data, also called "dataveillance". The processes described by 'phenetic fix', 'dataveillance', 'consumption surveillance' and 'panoptic sort' are very similar. The borders between the observation and the marketing purposes are very tiny and blurred. Many authors have highlighted the danger of 'function creep', as understood as:

Personal data, collected and used for one purpose and to fulfil one function, often migrate to other ones that extend and intensify surveillance and invasions of privacy beyond what was originally understood and considered socially, ethically and legally acceptable [68].

The question resides in the guarantee that the declared purposes will be respected and followed, in order to avoid a 'function creep' of data flows. It is clear too that the end-user must be informed about the way that the personal data is exploited.

Even if the scenario is not presented with surveillance purposes, the processes described in the two next points seem very close to the scenario TV.1.1. and it motives this literature review.

Let us examine briefly the literature review. Firstly, it makes it closer to the 'panoptic sort', that Gandy [69] describes as "a complex discriminatory technology".

The panoptic sort, as a complex technology, includes not only the computers and telecommunications systems that facilitate the collection, storage, processing, and sharing of personal information, but also the analytic approaches that differentiate, classify, segment, and target individuals and groups upon the basis of models, assumptions and strategic orientations that demand the maximization of profit and the minimization of risk.

Secondly, the concept, introduced by Clarke, of '*dataveillance*' helps to contextualize our

---

[67] Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. and Rohs, M., *Ambient Intelligence and Ubiquitous Computing*, Institute for Pervasive Computing, ETH Zurich, Switzerland, p. 12

[68] *A Report on the Surveillance Society, For the Information Commissioner* by the Surveillance Studies network, Full Report, September 2006, p.13.

[69] Gandy, O., "The Panoptic Sort : A Political Economy of Personal Information", Boulder, Colo. : Westview , in Lyon, D. & Zureik, E. (eds) *Computers, Surveillance and Privacy*, 1993 and Gandy, O., "Coming to terms with the Panoptic Sort", in Lyon, D. & Zureik, E. (eds) *Computers, Surveillance and Privacy*, 1996, pp. 134-156

.

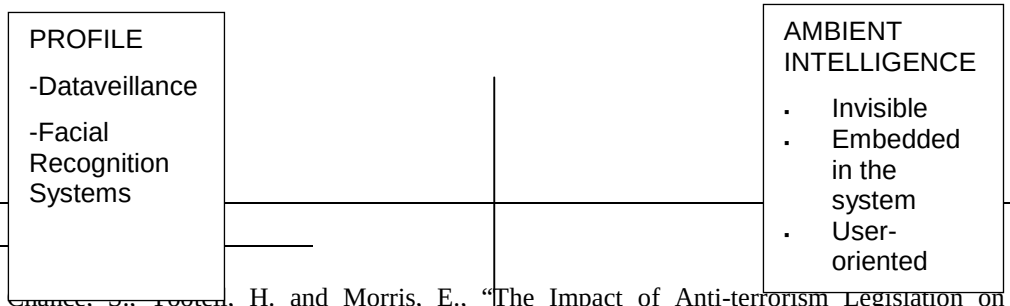
problematic of adaptive user profile on the WebTV. Dataveillance monitors people's activities or communications in automated ways, using information technologies.

Dataveillance is defined by Clarke (1988) as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons". The notion of dataveillance is supported by Flaherty (1989) who described the practice of dataveillance within the broader notion of surveillance as the "supervision, observation or oversight of individuals' behaviour through the use of personal data" (Davies, 1996). Other sources of contemporary literature, however, use a variety of terms to describe the practice of dataveillance. Langford (2000) has likened the concept of dataveillance to the practices of data-matching, data-monitoring and data-recording. In contrast, Bennett (1996) describes the concept of dataveillance as computer matching. He believes that it is this discrepancy in terminology that has attributed to the lack of effective regulation regarding dataveillance and related practices (Bennett, 1992). [70]

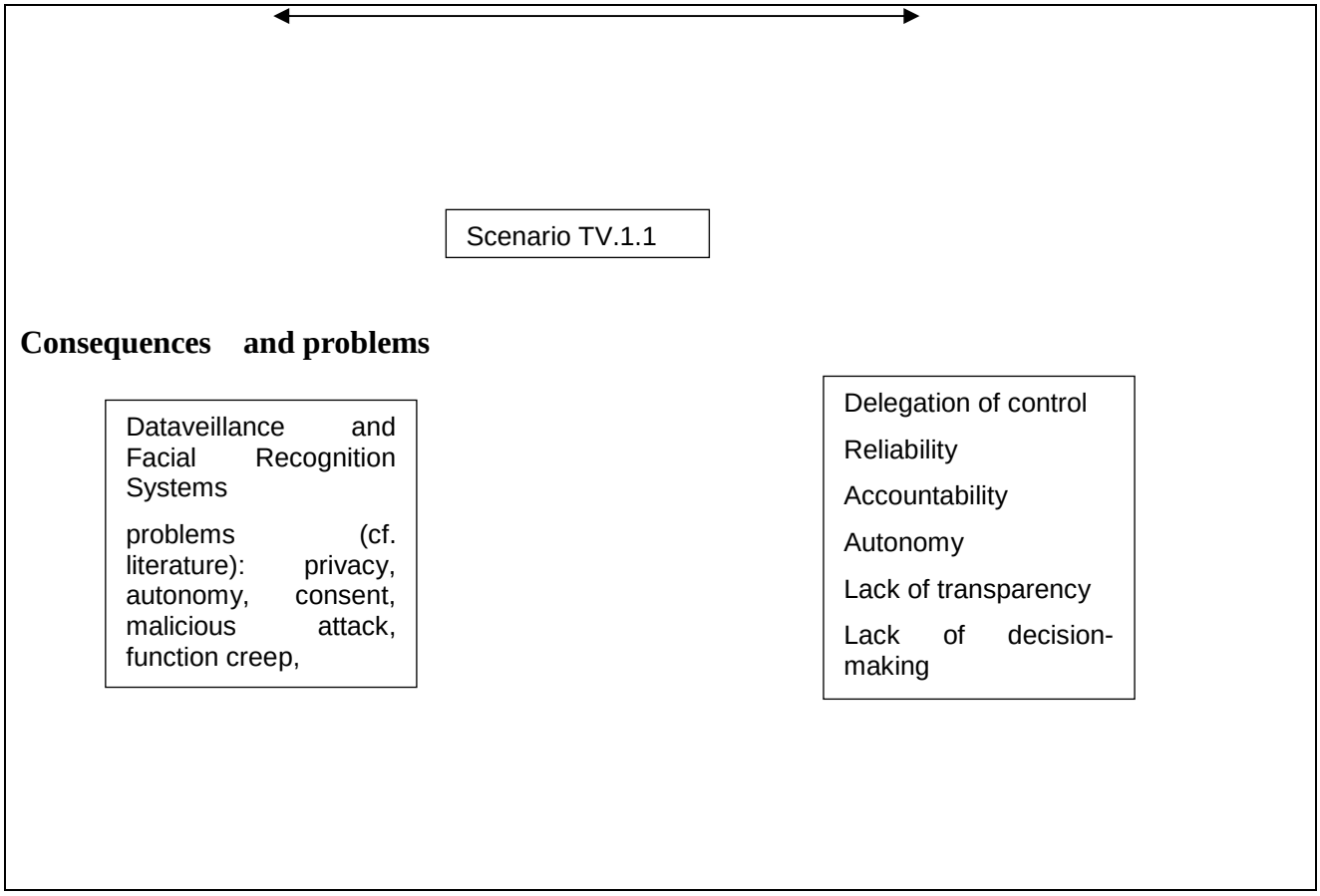
3.1.3 TV.1.1. AS AN AMBIENT INTELLIGENCE SCENARIO

Bohn et alii highlight the fact that the profiling is favourable to the ambient intelligence systems, and reciprocally: the ambient intelligence systems tend to surround people by intelligent and intuitive interfaces embedded in everyday objects around, and tend to build an environment recognizing and responding to the presence of people in an invisible way. What is proposed in the scenario TV.1.1 is very close to this vision of Ambient Intelligence, even if the system presents a visible interface (PC screen), the eye gaze capture and analysis are not visible (*de visu*) for the WebTV user, even informed. Problems around the privacy issues are commonly invoked, and those frequently related to AmI are reliability, delegation of control, accountability and autonomy

Technical view



70 Chance, S., Footch, H. and Morris, E., "The Impact of Anti-terrorism Legislation on Dataveillance" in *Proceedings CollECTeR 2004*, http://collecter.org/archives/2004_May/12.pdf



3.1.4. AN EXPERIMENTAL SCENARIO

For reasons due to the privacy regulations, the scenario is presented in an experimental environment working only with volunteers. This scheme can protect, at a first glance, from some privacy restrictions, but could not avoid the issues raised by the intentions of 'natural behaviour capture', which consists in a privacy and intimacy incursion.

This procedure questions the liability of such a system since this type of observation requires that people behaviour naturally and following their common sense, that is to say without tricking or lying.

3.2. Socio-ethical analysis

3.2.1. FACIAL RECOGNITION SYSTEM AND PERVASIVE SYSTEM

The Facial Recognition System – FRS – used in the scenario, develops specially the facial recognition of emotions. Let us describe the procedure:

- "Mr Volunteer" places his face adequately just in front of the camera.
- The camera captures his face and models it with a virtual mask shape.

- This mask interprets the facial expressions due to coding points into the face, determined by the average of the occurring and articulating into the faces, and attributes facial expressions to basic emotions (anger, sadness, happiness, etc) categorised by Ekman.
- Then a statistical scale appears and shows, in percentage, what emotions are expressed.

We can observe that this procedure is shortening the sense of what represents socially and culturally an emotion, because it reduces the expression of emotion to the plain emotion. It will have some consequences on the interpretation made by the potential users or end-users, in the sense where they can confuse the two levels.

We can formulate two main remarks: firstly, those FRS technologies, specially when oriented to recognition of emotions, must be considered as what they are, that is to say that they can not edict truths about emotions, feelings, sensations... they can only tell about the connections of a set of basic emotions and their pretended expressions. They tell nothing about the personal story, the preferences, the intimacy, the choices of the person, which the face is captured and the facial expression of emotions is recognized. Every connection made is pure interpretation, and represents a hermeneutic danger.

The second remark concerns the debates in the Human Computer Interaction fields. The studies, showing the cogency of the accountability of the emotional intelligence in the HCI must not caution an instrumental or utilitarist approach. Indeed, as McCarthy & Wright (2004) underline, a newly approach, more holistic, considers that the users dealing with the ICT build a *personal, constructive and transformative "felt-life".*[71] It encourages the account of the emotional intelligence in the design of new systems of facial recognition system. We can observe a reversal in the links between human sciences and experimental sciences: what the human scientists tried to bring into past debates about the subjectivity is now reclaimed by the experimental scientists in an efficient and rational finality. The sphere of HCI is nourished with new debates and assumptions.

Furthermore, every facial recognition system increases the empowerment and the ambiguous confidence of a silent system. As well noted by M. Gray[72], the potential of facial recognition systems as a seamless integration of linked databases of human images and the automated digital recollection of the past – will necessarily alter societal conceptions of privacy as well as the dynamics of individual and group interactions in public space. Moreover, psychological theory linked to facial recognition technology (Ekman) holds the potential to breach a final frontier of surveillance, enabling attempts to read the minds of those under its gaze by analyzing the trace of involuntary micro-expressions that cross their faces and betray their emotions.

To conclude this point, we can assert that this silent and invisible technology is a pervasive micro-

[71] McCarthy, J. and Wright, P., "Putting "felt-life" at the centre of human-computer interaction (HCI)" in *Cogn Tech Work*, Springer éd., Vol. 7, pp. 262-271, 2005.

[72] Gray, M., "Urban Surveillance and Panopticism, Will we recognise the Facial recognition Society", In *Surveillance and Society*, 1/13, 2003

politics. As Introna and Wood underline, this micro-politics is a consequence of the black box character of its pervasive technology:

> *This obscurity is due to two factors. First, most of the software algorithms at the heart of facial recognition systems are propriety software objects. Thus, it is very difficult to get access to them for inspection and scrutiny. More specifically, even if you can go through the code line by line, it is impossible to inspect that code in operation, as it becomes implemented through multiple layers of translation for its execution. At the most basic level we have electric currents flowing through silicon chips, at the highest level we have programme instructions, yet it is almost impossible to trace the connection between these as it is being executed. Thus, it is virtually impossible to know if the code you inspected is the code being executed, when executed. In short, software algorithms are operationally obscure. Second, most of the algorithms in facial recognition are based on very sophisticated statistical methods that only a handful of experts can interpret and understand. Indeed it seems that even they have been surprised by the behaviour of their algorithms (Philips et al., 2003). Thus, for most ordinary members of society facial recognition systems are somewhat exotic and obscure 'black boxes'. After all they do well what we find difficult to do — identify faces. This obscurity together with their obvious sophistication may give them a legitimacy beyond that which they deserve. In moments of uncertainty they may be taken as more authoritative than the humans involved — this could have important implications as we will argue and show below.*[73]

3.2.2. EMOTION AND REDUCTIONISM S[74]

3.2.2.1.Emotions: an overview of different models

Many models have been built in order to render the density and complexity of the emotions. Traditionally, emotions are defined as obstacles to rationality or liberty, because they seem to perform a lack of control, and thus could be interpreted as a vector of determinism in the construction of the personality.

There are four general frames considering the emotional sphere. The first one consists in the Darwinian one, to which belong Ekman's theories. The Darwinian model considers the emotions as a process optimizing the survival, and as an universal phenomenon of alerts in a metaphoric jungle. In a situation of aggression, for example, emotions are the alert for the subject, for his community and for the aggressors, emotions are perceived as exterior signs aiming to anticipate the future

[73] Introna, L. D. and Wood, D., "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems" in *Surveillance and Society*, Vol. 2 (2/3), pp. 177-198, 2004

[74] HUMAINE European Project (Human-Machine Interaction Network on Emotion), has also tried to assess ethically the researches about the human-machine interaction and emotions. In this project, P. Goldie et al. have chosen to exploit the Beauchamp and Childress' ethical standards., *see* http://www.emotion-research.net

behaviours. The Darwinian characteristic resides in the fact that this interpretation implies that the individuals demonstrating the most receptive ability to emotions will be the strongest and the most resistant. The representatives of that school of thinking are William McDougall, Robert Plutchik, Paul Ekman, Carroll Izard, Sylvan Tompkins Joseph LeDoux.

A second perspective is enlightened by W. James. He develops the fact that one could be impossible to have emotions without somatic modifications, which comes always before the emotions. For example, because of a trigger (bear), there is a somatic reaction (sweating, tachycardia), therefore one can say that the perception of the change is the emotion (fear). This vision implies the interrogation about what comes first, emotion or perception? The most representative, after James, is A. Damasio.

A third perspective is the cognitive interpretation of physiologic change. Thought and emotions are indissoluble; emotions are understood as a consequence of a cognitive evaluation. For example, the bear has a collar, proving that it has been domesticated, so there is no reason to be feared. The most representatives of that school of thinking are Lazarus, Frijda, Scherer, Roseman, Ortony, Clore and Collins.

Another standpoint, at last, is the socio-constructivist vision that supports the fact that every physiologic change and its correlated interpretation as emotion is the result of a social shaping. Emotions are a cultural product, which are coherent and significant due to the social norms. It implies that emotions are not universal and they do not exist per se. Emotions are meaningful in relation with the otherness. The representatives are Averill or Despret.

3.2.2.2 Facial recognition of emotions and reductionism

With the facial recognition technologies, specially oriented to the reading of emotions, there is a tentative to reduce the complexity of emotions to the simple expressions of emotion; in that case those expressions are determined by a whole of points into the face. This reductionism is very close to the behaviorism, developed since the 18th century. Behaviorism means that one may confirm "hypotheses about psychological events in terms of behavioural criteria" (Sellars, 1963, p.22)[75]. There are different types of behaviorism which each represents a level of radicalism linked to their final uses: "methodological" behaviorism, "psychological" behaviorism and "analytical" (or "logical") behaviorism. *Methodological behaviorism* claims that mental state or internal events of information are not proper objects of empirical studies. In that sense, psychology is the science of behaviour, not of the mind.. *Psychological behaviorism* refers to an *explanation* of human and animal behaviour in terms of external physical stimuli. By this explanation, this type of behaviorism

[75] Sellars, W., "Philosophy and the Scientic Image of Man" in Science, perception, and Reality, Routledge and Kegan APul, New-York, pp. 1-40, 1963.

may be called a "radical" behaviorism which implies a reduction of mental states to physical states. *Analytical behaviorism* is about the philosophical aspect of the meaning and semantics of mental terms.

Methodological and radical behaviourisms are very close to the approach developed into this MIAUCE scenario. It is very inspired by the research made by P. Ekman, a psychologist who has calculated the points into the face[76] in order to determine what expression of emotions correspond to a basic emotion [77]. We can characterise this model as a methodological behaviourist because the psychological activities concern the behavior rather than the internal mental state. But it is also close to the "psychological" (or "radical") behaviorism since the emotions are explained in terms of FSR interpretations. It implies that a whole field of social, cultural significations is missed and denied.

This scientific model is linked to a methodological reduction of human beings and their emotions. As Despret and alii [78] underline, it is an invariant inside the human sciences to have exploited the scientific models to support a better understanding. The problem happens when, inside those stories of successive borrowing and co-learning of models, "authority effects" overstep the intelligence effects concerning a reality. It is correlated with a general focusing on the body, especially on its physical features, which confers a seal of authenticity to human bodies. The body becomes a matter of calculations, and thus can render averages and statistics as a site of truth.

That prevalence to the body as matter implies a general deny to the human subjectivity, and the ability of individuals to determine what constitutes themselves. It means that our body knows better than us. ,A kind of standstill about the subject appears, that we can assume as a lack of autonomy and a loss of auto-determination.

3.2.3. PREFERENCES AND PROFILING

In the MIAUCE scenario, the users are supposed to express their preferences concerning the videos they are watching. These preferences are deducted from the clicks and metadata, facial expressions and eye tracking, and they contribute to construction of the users' profile, called multi-modal profiling. Once the profile established, the system can send some recommendations to the users in correlation to the profiles. Express a preference requires knowledge about one's own personality. It is not sufficient to assume that a sum of choices can express a preference. Here again, there is a sort of reductionism in the approach of the concept of "preference" settled by this technology.

Moreover, the opacity of the system implies its lack of consistency and contents. We can imagine that the system can trick without the user's consciousness, or the system can lie if it is coded to lie. There is no way to ensure that the preferences of the user are followed, nor that the system understands precisely what their real preferences are.

---

[76] *More about Paul Ekman, see his personal website* http://www.paulekman.com/

[77] Ekman, P., "Basic Emotions", in T. Dalgleish and T. Power (Eds.) *The Handbook of Cognition and Emotion*, John Wiley & Sons, Ltd., Sussex /U.K, pp. 45-60, 1999

[78] Despret, V., Elkaïm, M. and Stengers, I., « Comment penser l'émotion ? », in *Cahiers critiques de thérapie familiale et de pratiques de réseaux*, n° 29/2, 2002.

This raises important issue regarding the autonomy of people if the possibility of retroacting, in relation to the preferences and choices, is not guaranteed by the technology, as well as the transparency and the verifiability of the process. It can involve a loss of autonomy and reflexivity: by delegating the control of the summarization and recommendation to the system, individuals are constrained to trust blindly to the system, with no guarantee of transparency and of respect of their preferences. In addition, building his own 'web-biography' into that kind of system could be very restrictive, because of the constant and successive closures along the Web surfing. There is a risk of disinterest and indifference, which threaten the social cohesion.

Finally, we say that choice and consent are assigned by the system, even if they are retrieved from the preferences and emotions of the users. The fact that the emotions are correlated to the preferences highlights shows an important reductionism and a very limited vision of the individuals and their subjectivity.

3.3. Legal assessment

3.3.1. APPLICATION OF HUMAN RIGHTS LEGISLATION

As regards the interactive web-TV scenario, some concerns might be raised concerning potential threats against the user's human dignity, and against its mental integrity since the system works more specifically in a one to one relationship with the user, using at last potential profiling techniques in order to send appropriate advertisements, even to select programmes according to the profile sketched apart from various sources. Emotional privacy will be obviously interfered with, as the user's emotions are to be scrutinized, and there is a real impact on cultural representations, with the risk of radicalization of thoughts and opinions.

It is important to remember that Human Dignity is of absolute value and will not allow any exception. Any attempt must be sanctioned without taking into consideration other interests (no balance of interests). For that reason, and in order to really permit the development of a useful tool respecting the self determination of the user and thus respecting his or her human dignity, we recommend first of all a very good level of information to the user, with a specific effort to provide him the technical possibility to edit, improve or even to suppress his or her profile and to forbid any use of it.

Beyond that and keeping in mind that the goal of the system must be to advise the user, the system conception have to confess its non neutrality regarding its cultural background, being then able to impose some cultural schemas against the thoughts, conscience, even religion representation of the user. A total transparency of the criteria used for operating the selection of the messages sent or the programming advices has to be ensured. We recommend a building up of the system that always offers the possibility to the user to consciously approve or disapprove the results of its interactions, allowing him never to be trapped in the cultural representations. Furthermore, the possibility for the user to edit, improve or delete his associated profile is a necessary tool to be implemented in order to guarantee the respect of his or her freedom of expression, of holding opinions and of receiving and expressing information and ideas without any interference by public authority – as well as

private interference, due to the "horizontal effect" doctrine of the European Court of Human Rights - and regardless of frontiers.

This technical possibility will also guarantee the right not to be discriminated apart from any criteria, such as sex, race, religion, political opinion or social origin. In a way, this technical capability will empower the user to keep more control over information regarding both himself and his environment, avoiding him to be reduced to a means, in place of being considered as the final beneficiary of this technological device. Furthermore, this empowerment will also insure the respect not only of the proportionality principle, but also of the social acceptability and of ethical values.

3.3.2. EUROPEAN DATA PROTECTION REGULATION

Within the frame of the Data Protection Legislation, as previously developed, we have to consider, different definitions in the specific context of the interactive web-TV scenario: "personal data", "data subjects", "processing", "data controller". In a second step, we have to consider the principles relating to the lawfulness of data processing, ie the duties of the data controller, as the obligations imposed to him relating to the principles of "data quality". In a third step, we will analyse the rights and privileges of the data subject, eg the right to be informed, and the access and rectification.

3.3.2.1. Personal Data at stake

As introductory remark, a very important point to be remembered is that the finality is not a relevant criterion for deciding the applicability or not of the data protection regime. Concerning the interactive web-TV scenario, the fact that the captured images identify or can identify individuals, that they serve to deduce personal emotional reaction, will be the real criterion to decide or not the applicability of the European data protection regime.

So as first conclusion to the analysis of our interactive web-TV scenario, the captured images constitute well personal data, as they are information that concern individuals identified or identifiable, and that are not irreversibly blurred at the very start by the system. In general with this scenario we have many others informations directly related to the user, in its one to one relation with the system. All those information must be considered as personal data, as they are related to an identified or identifiable user. Again, their level of protection must be adapted in consequence. As this scenario has for objective to create a profile, the drafted recommendation of the Council of Europe in that matter must be respected.

The data collected might be considered as very personal data. They encompass our TV preferences, our emotional reactions before the screen end definitively all the data about our consumption of such programmes (duration of the connection, time spent on each programme, etc.) It is quite clear that if they are collected and retrieved in an appropriate way they reveal our personality and definitively might be of great interest not only for the data controller but also for advertisers and other third parties who wants to enter the profile created apart from these processing for having a better cognizance of our psychology and eventually to discriminate the uses from different services or products on the basis of the profile. Let us add that these data might be also very easily considered as sensitive data since they might reveal our health conditions, our philosophical opinions etc and be treated as such for discriminatory purposes. That is why we are quite concerned

by these possible reuse of the data even in the context of the scenario chosen by the partners that kind of usages is up to now excluded.

As this technical device relies on Internet, we believe there is a strong necessity to very well protect the collected information against any intrusion, through encryption of the images and trough severe protection of the database. The information must also be kept only for the necessary duration. If some of them must be stored for a longer time, as they serve to feed the emotion algorithm and to improve its analysis capacity, their level of protection must be very high. It is under the responsibility of the security officer (or counsellor) to include that point in its global security policy.

3.3.2.2. Data subjects

Now that we know that we are well in presence of personal data, we will focus our attention to their relation with the people they concern. This lead us to identify the different categories of those people, so called “data subject”, whose such personal data are related with. At this level, we may discuss the case of the sensitive data. No global category or individual profile, based on the processing of sensitive data, ie data related to the sex, the race, the age, can be constructed. This must be very well explained and certified to the final user, ie the data subject. This does not exclude cases where the users would spontaneously and voluntarily include these characteristics in their own profile. This aspect is an open question for the lawmakers.

The data subjects represent every categories of people submitted or related to the technical system in place. For the interactive web-TV scenario, there is only one category, constituted by the final user, in front of its personal computer. The amount of data collected is high, and they are directly related to him.

This category includes children, which are more vulnerable then others to profiling and mental manipulation. For them, it will be necessary to develop as far as possible technical means to detect their session and to embed routines and filters preserving them from inappropriate contents.

3.3.2.3. Data controller and data processor

Those personal data will be processed in order to fulfil some purposes, depending of the categories they concern. Those purposes are fixed by the data controller. He must be identified taking into account all types of delegations of service provision that may happen. In our interactive web-TV scenario, this role will be played by the service provider, together with the provider of the technical services and the third parties responsible for the data processing (so called the data processor). We are then in presence of a network of actors, and of applications, involving a certain level of complexities regarding the ascription of responsibilities among actors.

For our interactive web-TV scenario, as previously explained in chapter two, it is the duty of the data controller, in this case the service provider, to assess the quality of the data processor and his ability to provide adequate security measures, organizational as well as technical, to guarantee against all forms of disclosure of users' data and profiles. Furthermore the data controller has to

define precisely by a written contract the missions of the data processor and to check if the data processor does respect entirely the limits of his contractual duties.

Precisely it is the data processor's obligation not to infringe his contractual duties and not to process the data for other purposes than those assigned by the contract. The processor shall act only under instructions from the controller. If he exceeds (for example, the security company sell to marketing companies the data collected through the airport's CCTV), he will be designate as controller and since his processing are not legitimate might be suited before civil and criminal courts. The users will be informed of the details of such contractual arrangement.

3.3.2.4. Lawfulness of the processing

The data controller has many duties to respect, in order to guarantee the lawfulness of the data processing. As a very first condition, the data must be collected in a transparent way and processed fairly and lawfully. There is a need for a balance of interests, weighting constantly the right of the data subject versus the interests of third party or parties in obtaining personal data. The right to process personal data about data subject must be accompanied by effective means for this later to defend his or her interests, especially to be kept adequately informed in order to ensure a fair processing. So in our interactive web-TV scenario, there is an important obligation of information and transparency for the data controller, with respect to the data subject, about the purposes, about a permanent evaluation of the balance of interests and about the possibility for the data subject to always be able to defend his or her interests. All technical possibilities of communication (messages, pop-up windows, internet link, etc...) must be exploited to provide the highest level of information to the data subject, at any time of its session.

As second condition, we have that the processing must be legitimate. Among the list of cases which makes a priori the data processing legitimate, we believe for our interactive web-TV scenario that this following is the only one relevant: the data subject must have unambiguously given his consent. As previously explained in chapter two, the unambiguous consent of the data subject is thus hardly avoidable as a necessary condition for the whole system to be legitimate. For the consent to be unambiguous, it cannot be merely implicit. Therefore, whenever possible, « opt-in » systems should be preferred to « opt-out » systems. The consent supposes a real possibility of choice. It would be not the case if a Data controller imposes as condition for the delivery of a service (e.g. the access to the TV channels) the consent to be traced through a webcam. The fact that any financial incentive is given to the person who accepts to see his or her data processed might put into question the reality of the consent. The technical possibility must be offered at any time to the data subject to withdraw his or her consent, without loosing any advantages (e.g. the gratuitousness of the access to the TV channels or the submission to longer advertisements). This also implies for him the possibility to delete any information and personal profile stored in the system, as he is leaving it. He must receive written confirmation by the data controller of that suppression. Finally, refusal to give such consent must not prevent the users to benefit from such interactive Web-TV service on the same terms as he had provided such consent (ie no financial penalties).

As third condition, the data controller has the duty to define precisely the purposes of his processing and to make them explicit. It means that he has not to use vague wording but definitively to enunciate in a document the purposes in a way which might be understandable by a reasonable data

subject and apart from which the data subject will envisage the reason why the data are collected This obligation is also part of our technical recommendations as presented at the end of this analysis. We insist on the necessity to clearly define and to explain the purpose to the data subject, and also the type of data that are collected, how they are processed, by whom and for whom, and what is their level of protection.

As fourth condition, the compatibility is a very important requirement in evolutive system, that permit through their natural or technical (by the addition of certain software or by coupling with other data bases) evolution, to imagine new application with new purposes. The question to know if this is definitely a new usage, or always a usage compatible with the former one, can be solved with the criterion of reasonable expectation. This one raise the question to know if the data subject has had the possibility at the initial moment of the data collection to imagine this future usage as included in the purpose of the processing. If the answer is yes, the processing is deemed as compatible and is legitimate without new formalities. If not, the processing is a new one and has to find a basis for its legitimacy and definitively the data subject must be at least informed or even agree to this processing. Through this fourth condition, and as with the balance of interests, we find here again the necessity of a constant evaluation, meaning that no final judgement regarding privacy and data protection can be reached with such dynamic systems. This is then an important responsibility of the data controller to be aware of such obligation and to comply with it! In general, given the dynamism and plasticity of the systems at issue, constant monitoring should be exercised as to ensure that the conditions of legality (compliance with human rights as well as data protection requirements) are always met. The whole system's legitimacy should be reassessed each time a shift in the variables involved occurs. This idea of permanent legal watch due to permanent technical evolution is also part of our technical recommendations, presented further in this analysis.

A specific attention must also be given to the profiling. Profiling is not a goal in itself but a technical means of achieving a particular result. It has much more significant consequences than simple statistical processing, since it may exclude individuals from access to essential services, or may reveal sensitive aspects of user's character, even elements this one doesn't know consciously about himself. The three pillars of personal data processing, ie the lawfulness, the transparency and the proportionality, must be applied at an early stage of any profiling operation, even if the human data being processed are not personal.

3.3.2.5. Data quality

Apart from those obligations concerning the lawfulness of the data processing, the data controller has also to fulfil obligations related to the principle of “data quality”, ie no more concerning the processing but the data processed. In that case, the data must be adequate, relevant and not excessive, in relation to the purposes for which they are collected and/or further processed. They must be accurate and kept up to date, and if not, must be erased or rectified. They must be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the data were initially collected. For our interactive web-TV scenario this implies to capture only relevant data. The data minimization implies that only the personal data necessary for the implementation of the system should be collected, processed or stored, and that the data must be deleted when no longer necessary and after the legal conservation requirements. If the storage duration must be permanent for the good functioning of the analysis algorithm, the data subject must be well informed about this, as about the protection level of those data.

3.3.2.6. Security measures

In conclusion, the interactive web-TV scenario has potentially the greatest impact on the user's privacy, due to the amount and quality of personal data collected and due to the connection to a public communication network. Following the principle of the balance of interests, we ask for this scenario a very high level in the measures of protection. This protection must be deployed at the level of the user, as well as at the level of the data controller and processor.. This last point implies for him to strongly secure any data base of collected data, and to permanently review the global security level of his system. Finally, in order to avoid any unlawful and disproportionate processing, the data controller will have to apply the precautionary principle. As an evidence, this scenario implies for him the highest responsibility level. The control of the threat related to the profiling relies also upon the rights of the user, mainly to be informed about the collected data and their purpose, but also about the logic of the global process.

The second main European legal instrument, the directive 2002/58, concerning the processing of personal data and the protection of privacy in the electronic communication sector, is applicable in this scenario, mainly through its article 5.3. This one declares that *"the use of electronic communications network to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller"*. As previously expressed, this clause assures the user to keep control on his informational environment, with respect to basic principles of dignity, mental integrity, proportionality and freedom of expression, thought and conscious, without discrimination of any ground.

3.4. Recommendations

Following the classification proposed by Glasgow University, among our three scenarios, the interactive Web-TV is the most interested in profiling. It implies a possible crucial impact on thoughts and cultural representations, with the risk of radicalization of thoughts and opinions.

We recommend to provide adequate information and technical means to the user as to allow him to keep control over information regarding both himself and his environment; the user must be able to « fool » the system, ie to furnish to the system a totally different image of himself.

Two kind of means can be used: the first one is the technical possibility to give feed back to the user, on the relevance of his own profile, and the second one is the technical possibility to edit, to switch off, improve, suppress, parts or totality of his profile.

Among the different users, children constitute a particularly vulnerable category. We recommend developing as far as possible technical means to detect children users and to embed routines and filters preserving them from inappropriate contents.
As the constructed profiles are of great interests for other companies, there is a necessity to take all appropriate organizational and technical measures to guarantee against all forms of disclosure of users' data and profiles.

There is a necessity to address by contract the respective responsibilities of the data controller and the interactive web-TV content provider with regard to the management of users' data and profiles. The users will be informed of the details of such contractual arrangement.

The user must provide a fully informed consent to the processing of his data and the profiling process at the time he subscribes to the interactive web-TV service. Refusal to give such consent must not prevent the user to benefit from such interactive web-TV service on the same terms as if he had provided such consent (ie no financial penalties).

Whenever the user wishes to withdraw from the system, he should be able to do so without any penalty. In such case he will receive a written guarantee that all data and profiles will have been irreversibly erased.

Whenever, for technical or other reason, data are used for new applications, these applications must be compatible with the original processing of the data, and comply with users' reasonable expectations.

Sensitive data (ethnic origin, religion, sexual preferences, political opinions, health and disability status) must in principle never be processed; our recommendation in this regard would be to avoid situations where the system would automatically enrich the user's profile with information inferred about such sensitive criteria. This does not exclude cases where the user would spontaneously and voluntarily include these characteristics in his own profile.

Finally, the data controller is obliged to notify to the relevant national data protection authority about the processing of personal data.

CONCLUSION AND FUTURE WORK

CONCLUSION

ACHIEVEMENTS OF WP5

In this second period, we have achieved significant research results.

First of all, we have developed a methodological frame enabling collective deliberation about the ethical, legal and social issues involved in the design of MIAUCE technologies. This methodology is supported by two crucial options we had to define. The first one consists in the moral and the legal value from which one would assess these technologies and their application scenarios. In this report, we held that respect for, and encouragement of individual autonomy (self-determination) and collective autonomy (the vitality of deliberative democracy) are the two most sustainable reference principles or values that "value sensitive design" should strive to reinforce. The second option relates to our role and responsibilities, as researcher in human sciences and humanities, as partners in the MIAUCE project. Considering that ethics is not a theoretical knowledge that can be learned and appropriated by hearing experts, but is rather an attitude or a posture in life and work, the role we have held in the project, with reasonable success, consisted in enabling our partners to acquire a reflexive and ethically enlightened posture, which allows them to both understand and reflect on the ethical, legal and societal impacts – both actual and potential – of industrial and technological choices. Our methodology therefore always promoted a participative and deliberative determination of the ethical, legal and social constraints and values to be implemented through technological design and industrial orientations. This was a mutual learning process through which we, as human scientists, have learned to better define our position (or posture) and interventions and through which our scientific and industrial partners have had the opportunity to better understand their ethical, legal and social responsibilities in an increasingly technologized world.

The second result of this WP5 second year consists in the actual introduction of value sensitivity as a guiding criteria for the design of the scenarios as they are now described, following the changes that have been considered necessary not for industrial nor scientific reasons, but for ethical, legal and societal reasons justifying changes in the initial specifications of the technologies or in the organizational arrangements supporting their deployments (blurring faces, clear specification of the finalities of the technology, sensible data to be protected, responsibility and liability constraints …) These changes and recommendations are developed in the chapter 3 of the present deliverable.

Still critical issues remain with regard to the general epistemological, cultural and political paradigm supporting the design and deployment of such multimodal observation technologies. In the next section, we explore these most critical issues, which no adaptation or change in technological design or industrial organization can solve, since these questions concern the broader epistemological, cultural and political bases on which these emerging technologies are grounded.

MULTIMODAL OBSERVATION TECHNOLOGIES: SOCIETAL CHALLENGES

The body as privileged source of truth

The MIAUCE technologies are largely inspired by a sort of general postulate holding the human body as a privileged source of 'truth' about persons. Although persons are always susceptible to lie, their bodies, it is assumed, is the natural repository of personal authenticity. This assumption, a contrario, holds as systematically suspicious, narrative autobiographical accounts. These kinds of reductionism (holding that multimodal observation allows to gain particularly objective and reliable information about a person's preferences, needs, emotions, personality...) and essentialism (holding that a person's preferences, needs, emotions, personality,...are necessarily 'readable' on his or her face or body, or expressed in his or her attitudes and positions) are worrisome as such, from an epistemological point-of-view. They also challenge among the most fundamental ethical and legal assumptions about individual autonomy or self-determination, the meaning of individual consent, and the necessity of 'user empowerment.

Besides, in such a multimodal observation paradigm, the human body is not anymore necessarily understood as a unified entity, but rather as a collection of fragments that match together (or not). In the MIAUCE scenarios, particular patterns of physical attitudes are targeted (eye gaze, head positions, silhouette...), from which operational information is inferred.

The privilege acknowledged to the body as a source of meaning is paralleled by a general disregard for the part of personal subjectivity that escapes multimodal detection, and for the specifically human capability of individuals to define – in part at least – and develop as they please, their own unique personality. In caricatural words, the presumption is that "our body knows – and says - better than us". A kind of standstill about the subject appears, that we can assume as a lack of autonomy and a loss of self-determination. It participates to a sort of suspicious statement regarding the capacity of the subject to explain his/her behavior and then to be at the centre of his/her social life.

Moreover, these multimodal observation technologies seem to ignore that the body is also socially and culturally shaped. R. Hall has demonstrated that the body carries the settings and is the vehicle of social identity and communication. To a certain extent, people construct their bodies in order to feel conformed, marginal or recognizable amongst the others. So the body is an intrinsic part of the social personality and identity of the persons. This is another reason to question the current development of multimodal observation systems.

From body to mind: determinism and reductionism

Multimodal observation technologies also raise questions with regard to the instrumental use they make of human sciences that were originally developed to explore and not to control or determine what is 'real'. This is particularly the case for the technologies at work in TV1.1.presupposing a kind sort of causal and deterministic link between facial expressions and emotions.

In fact, with facial recognition technologies especially aimed at emotions reading based on the Ekman model, there is an attempt to reduce the complexity of emotions to the simple expressions of emotion; in that case these expressions are defined by a series of points of the face. This scientific model is linked to a methodological reduction of human beings and their emotions. As this model is

only able to 'detect' plain emotions, it also reduces the social and cultural meanings of emotions to a dramatic extent (it is indeed unable to translate the infinite emotional nuances existing in humans) It will therefore have troubling consequences on the interpretation made of its results by the potential users or end-users, in the sense where they can confuse the two levels.

Hence, these observation technologies, especially when oriented towards emotion recognition, must be considered for what they really are, and not for what they are not: means to gain 'truths' about emotions, feelings, sensations... they can only tell about the connections of a set of basic emotions with their pretended expressions. They tell nothing about the personal story, the preferences, the intimacy, the choices of the person whose face is captured and of whose the facial expressions are analyzed. Every connection made is pure interpretation, and represents a hermeneutic danger.

This issue claims for giving a very cautious and limited status to such technologies in the organization of our social life.

The centrality of consent and the focus on "user empowerment"

The major characteristic of data processing in MIAUCE is that it involves genuinely constant recording « multimodal interactions of users », going from anonymous trivial events happening in a given environment and susceptible to cause safety issues (S.1.3.) to constant tracking of the user's eye gaze (M.1.1.) and monitoring of variations of the user's « emotions », inferred from facial expressions (TV1.1). The pace (real time) of data collection makes it unrealistic that any data subject would expressly consent to each instance of data processing. Most collection, observation and processing of personal data will happen without « active » reflection by the data subject on the merits and dangers of having « his » information processed, as the scenarios intend to be as least intrusive and obtrusive as possible.

A second concern, is that, in the perspective of MIAUCE technologies (and the multitude of applications they may give rise to) whenever users are requested to consent on the processing of one type of data - those which qualify as 'personal data' according to the classical definition – they do not thereby gain any control over the other types of data which may relate to 'contextual elements' with which their 'personal data' will be cross-matched in order to produce operational knowledge about that user's 'needs, preferences, risks, dangerousity, personality etc'. Personal data (the only type of data deserving adequate protection under current law) processing does not exhaust the information processing involved in multimodal observation, whereas this multimodal observation may result in troubling consequences for the user, and in consequences incompatible with his fundamental rights and freedoms.

Finally, consent given to the collection of say one type of data (facial expression) does not allow the person any control over the nature and depth of information about himself that will be made accessible through the processing of such data. It may even be hypothesised that certain applications of the technologies ensuing from the MIAUCE project will render 'visible' certain things about the 'users' of which they are not aware themselves (see 3.3.A. above, on invisibility, body and identity). In other words, multimodal observation may allow for technologies 'discovering' things, or 'creating knowledge' about 'users' that 'users' don't even know about themselves, but that is nevertheless interpreted as ultimately true, in part for the very reason that it escapes the filter of users' consciousness.

At a more conceptual yet crucial level and in line with the previous point regarding the "epistemic primacy of the body", data protection principles emphasizing data subjects' empowerment and 'informational self-determination', are at odd with the epistemic evolution attested by the focus of multimodal observation (for security-safety and marketing purposes), and which has precisely made the 'self' a very unreliable source of truth.

The crucial need of pre-defined finalities as to assess the legitimacy and proportionality of "privacy and data protection adverse" systems

The difficulty experienced in this assessment of the MIAUCE scenarios result, in a significant part, of the fact that the very technologies intervening in these scenarios may, without substantial change, be applied for a wide variety of purposes. The safety scenario would easily shift into a security scenario; the marketing scenario may easily allow thorough customers' profiling, as would the interactive web-TV scenario...The fact is that the availability of multimodal observation technologies decreases the cost of gaining 'operational' information about individuals so much that it will become increasingly tempting for for public and private bureaucracies to intensively seek and rely on such information, whatever their accurateness, reliability, and whatever disparate impact over vulnerable groups and individuals would ensue.

The principle of data minimization is at odd with the very logic of multimodal observation: In the 'multimodal observation paradigm', the principle is indiscriminate capture and recording of information of as many types as technically possible as to allow the autonomic establishment of correlations between data that are or are not in a causal relationship.

The ban, in principle, on the processing of sensitive data (ethnic origins, religious faith, political opinions, sexual preferences, health status,...), may be difficult to implement, as 'contextual' data may reveal such sensitive information, be it indirectly (through the analysis of contents requested by an interactive web-TV customer for example) .

They also raise a series of difficulties regarding the practical implementation of current data protection regimes, given:

The uncertain legal regime applicable to profiling...
The decreasing probability that 'users' (or data subjects) will claim respect of, or exercise their legally guaranteed rights, as the exponential dissemination of observation technologies de facto decrease users' expectations of privacy and sensitivity with regard to information systems inimical to privacy and data protection.

New observation capabilities versus privacy and data protection frameworks

As a result, as mentioned earlier, the *scope* of current privacy and data protection frameworks fail, in part, to guarantee against a series of excessive intrusions or interferences with individuals' privacy. Eye gaze detection, emotion recognition, context awareness, for example, are among the innovations that indeed interfere with the users' "visual privacy", "emotional or intellectual privacy", "relational privacy"...That these dimensions or facets of privacy have not been as such explicitly protected by law does not mean that they do not qualify for legal protection under the broad concept of privacy. Absent adequate protection of these and the other newly vulnerable facets of individual and social existence, phenomena (already described in detail in our first deliverable) of anticipative conformity and/or of degradation of trust (when legitimate expectations of privacy

are deceived in practice) will arise, with dramatic consequences on the vitality of our deliberative democracy (see first deliverable).

Law enforcement activities have for long relied on technology for assisting law enforcement officers in crime detection**. Time has come for the law to also seek the help of technology to ensure that the same instruments aimed at observing persons and events (for purposes ranging from safety or security to marketing and entertainment; through technologies involving observation and/or interaction and/or profiling) do not disproportionately and illegitimately deny individuals' adequate protection of their fundamental rights and liberties.** Given the decreasing awareness and sensitivity of users with regard to ever invasive multimodal observation systems, and given the above mentioned gaps and difficulties of legal protections, value-sensitive design is absolutely necessary.

Another concern with regard to autonomic profiling, relates to the **claims of objectivity** raised by the proponents of multimodal observation systems aimed at assisting or, in the most extreme cases, at replacing human decision making. Unlike human observation and classifications, prone to a wide range of conscious or unconscious bias of and prejudices and impaired by the fac that humans are caught inside the limits of "bounded rationality", autonomic profiling is claimed to be more 'objective' and efficient, ignorant as it is of human biases and prejudices, and enabled as it is to deal with the complexity of reality much more efficiently than humans (always caught in their "bounded rationality"): aren't machines able to process and analyze information much more quickly and efficiently than humans? This 'objectivity' of autonomic profiling is however more a myth than a reality, for a serie of reasons. **Immunity from design flaws is indeed difficult to attain**, and autonomic decisions or recommendations are vulnerable to the potential inaccuracy of data used or incorrectedness of models or routines. These errors may be caused by a misunderstanding of underlying mechanisms that condition behaviors, for example, given that these systems are most of the time correlations-based (rather than causality-based), and prone to use categorical variables (such as ethnic, age, gender,…group variables) as elements of evaluation, with possibly mistaken results. Besides, these systems may produce rational recommendations or decisions but which are nevertheless unacceptable as they disparately impact on an already disadvantaged or vulnerable group, or lead to unacceptable discriminations. Finally, whenever multimodal observation would be used for the purpose of forward-looking evaluation (which is not the case in actual Miauce scenarios), that is, for predicting future preferences or behaviours rather than to depict actually occurring events, actions, behaviours, the 'model''s validity may be impossible to assess, as no 'ground truth' is available for that purpose.

This has already been said but it doesn't harm to repeat it: the **motivation, stage and scope of 'regulatory' monitoring of technology development and dissemination** must therefore evolve. It must obviously be motivated not merely by concerns about threats to competitive advantages, but should also, crucially, be motivated by the necessity to minimize or mitigate the social harms flowing from its use. In order to keep pace with the potential social harms accompanying technological development, regulatory control must not merely be restrospective, but must be considered and given the means to be an integral component of research and development[79].

[79] Gandy Jr., O. H., "Engaging Rational Discrimination", Conference: Ethics, Technology and Identity, TU Delft, June 18-20 of 2008

One may wonder, after careful identification of the gaps in legal protections of users, the practical difficulties of implementing existing protections, and the inadequate scope of existing legal framework, whether it would not be also fruitful to address the issues not merely from general human rights and a data protection and privacy point-of-view, but also **from a non-discrimination point-of-view**. Multimodal observation technologies are above all aimed at *proactively* discriminate (in the value neutral sense of the term), among individuals according to the level of probability that they will like a specific informational content (in the interactive web-TV), will buy a specific product at a specific prive (in a dark version of the marketing scenario), or will represent a danger for the security of goods and persons (in a dark version of the safety scenario). **Autonomic *profiling* is the horizon of what Miauce technologies are about.** The question arising in such a conceptualization relates to the disparate impact that such an autonomic profiling of persons may have on groups unequally powerful (in terms of means, wealth, political representation, health,...) in current society. The issue then becomes one of justice or fairness: **how do we guarantee that autonomic profiling will not further disadvantage those who already suffer a 'minority' status in our current society?** The third year will allow us to gather the experiences and visions of such 'minority' or 'marginal' social groups in order to assess the risks of further marginalization and provide recommendations in this regard.

Children and elder persons, who may experience, even more than the general population, difficulties in understanding and evaluating the risks and advantages of consenting to the processing of personal data in a multimodal observation context, of course constitute an obviously vulnerable group. A crucial question would be, with regard to these categories of persons, whether a new type of 'technological paternalism' would be warranted, so that their status as vulnerable person be detected by the multimodal observation system, and the reaction of this system, adapted accordingly.

FUTURE WORK

In the future work, we will address the external governance issue related to the necessity to open the democratic deliberation process about the technologies at work to the society at large. Set like that, this aim or ambition appears quite unrealistic since 'society at large' remains a very abstract and fuzzy concept.

To open this deliberation, we will explore two main orientations. . The first one consists in the "citizens' jury" methodology as an attempt to hear people's voices. This methodology is clearly an alternative to most common quantitative surveys based on large samples of people and to qualitative consultation of experts. The second orientation we would like to explore regards the composition of the jury. According to the general methodological guidelines supporting the citizens' juries approach, the panel has to be set on a 'best fit' (demographic) sample of 12 to 16 members of the public. Within the MIAUCE project, we intend to explore two types of panel: the first one, classic, based on a demographic sample of the general public and the second one, less traditional, and composed on a demographic sample of the population (or their representatives) most critically targeted by the considered technologies since they express or live situations that are at the margins of the dominant paths of the society. This confrontation between two panels should

help balancing the needs for security and safety of the ones against the risks inherent to observation technologies as perceived by the others.

We will conclude this research mandate by the elaboration of (social, ethical and legal) recommendations for both the European policymakers and technology designers to avoid that the development and deployment of multimodal observation technologies result in increased discrimination and fragility of these vulnerable groups but also in a loss of autonomy and democracy for all.

MILESTONES FROM M24 TO M36

Month	Id	Milestones	Measurable results	WP	Lead contractor
Month 30	Ms3a	Achievement of the focus groups process	Recommendations generated by the focus groups	WP5	UN
Month 36	Ms4c	Analysis and assessment of the governance approach	Governance proposals and recommendations	WP5	UN,

Table 10. Interim milestones for months 30 and 36

REFERENCES

ARTICLES

Andrejevic, M., "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance" in *Surveillance and Society*, Vol. 4, 2005.

Buttarelli, G., "Surveillance in Public Paces and Protection of Personal Data" in *European Commission for Democracy Through Law*, Study No. 404/2006, Strasbourg, 14 February 2007

Calas, M., B. and Smircich, L., "Past Postmodernism? Reflections and Tentative Directions" in *The Academy of management Review*, Vol. 24, Issue 4, 1999.

Carmi, G.E., "Dignity versus Liberty: the two western cultures of free speech", (August, 22 2008). Available at SSRN: http://ssrn.com/abstract=1246700.

Ceyhan, A., "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics" in *Surveillance and Society*, Vol. 5 (2), pp. 102-123, 2008.

Chance, S., Tootell, H. and Morris, E., "The Impact of Anti-terrorism Legislation on Dataveillance" in *Proceedings CollECTeR 2004*, http://collecter.org/archives/2004_May/12.pdf

Despret, V., Elkaïm, M. and Stengers, I., « Comment penser l'émotion ? », in *Cahiers critiques de thérapie familiale et de pratiques de réseaux*, n° 29/2, 2002.

Dubbeld, L., "Observing bodies. Camera surveillance and the significance of the body" in *Ethics and Information technology*, Vol. 5, pp. 151-162, 2003.

Flemming, J. E., "Securing Deliberative Autonomy" in *Stanford Law Review*, Vol. 48, n. 1, 1995.

Gandy Jr., O. H., "Engaging Rational Discrimination", Conference: Ethics, Technology and Identity, TU Delft, June 18-20 of 2008.

Garret, J., "Martha Nussbaum : on Capabilities and Human rights" in www.wku.edu/~jan.garrett/ethics/nussbaum.htm

Gray, M., "Urban Surveillance and Panopticism, Will we recognise the Facial recognition Society", In *Surveillance and Society*, 1/13, 2003.

Introna, L. D. and Wood, D., "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems" in *Surveillance and Society*, Vol. 2 (2/3), pp. 177-198, 2004.

Katja Franko Aas, "The body does not lie' : Identity, risk and trust in technoculture",in *Crime, Media, Culture*, 2(2):143-158,2006.

Lianos, M., "Le contrôle social après Foucault" in *Surveillance and Society*, Vol. 1 (3), pp. 431-448, 2003.

Lyon, D., "Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix" in *Surveillance and Society*, Vol. 1 (1), pp. 1-7, 2002.

Maesschalk, M., “Quelle philosophie des normes aujourd’hui? Gouvernance et apprentissage social » in *Les Carnets du Centre de Philosophie du Droit*, n°138, 2008.

Marx, G., T., “What’s New About the “New Surveillance”? Classifying for Change and Continuity” in *Surveillance and Society*, Vol. 1 (1), pp. 9-29, 2002.

McCarthy, J. and Wright, P., “Putting “felt-life” at the centre of human-computer interaction (HCI)” in *Cogn Tech Work*, Springer éd., Vol. 7, pp. 262-271, 2005.

Müller, C. and Boos, D., “Zurich Main Railway Station: A typology of public CCTV systems” in *Surveillance and Society*, Vol. 2 (2/3), pp. 161-176, 2004.

Nickel, R., “Jurgen Habermas’ Concept of Co-originilaty in Times of Globalization and the Militant Security State” in *IUE Working Paper Law*, Vol. 27, 2006.

Norris, C. and alii, “The Growth of CCTV: a Global Perspective on the International Diffusion of Video Surveillance in Publicly Accessible Space” in *Surveillance and Society*, Vol. 2 (2/3), pp. 110-135, 2004.

Rasmussen, L. B., The Narrative Aspect of Scenario Building. How Story Telling May Give People a Memory of the Future, Online publication 12-8-2005, Springer Verlag, London Limited, 2005.

Raulff, U., “Interview with Giorgio Agamben – Life, a Work of Art Without an Author: The State of Exception, the administration of disorder and private Life” in *German Law Journal*, n°5, 2004. *Special Edition, available on* http://www.germanlawjournal.com/article.php?id=437

Rouvroy, A., « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence » in *Studies in Ethics, Law and technology*, Berkeley Electronic Press, 2008.

Salter, M., B., “The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics” in *Alternatives: Global, Local, Political*, Vol. 31 (2), pp. 167-189, 2006.

Schwartz, P. M. and Treanor, W. M., “The New Privacy“ in *Michigan Law Review*, Vol. 101, 2003.

Sen, A., “Democracy as Universal Value” in *Journal Of Democracy*, 10.3, 1999.

Spiekermann, S. and Pallas, F., "Technology paternalism. Wider implications of ubiquitous computing” in *Poiesis Prax*, vol. 4, *2006*, pp. 6-18.

Townley, B., “Writing in Friendship” in *Organization*, Vol.1, Issue 1, 1994.

Wakefield, A., “The Public Surveillance Functions of Private Security” in *Surveillance and Society*, Vol. 2 (4), 2005.

Warren, S., and Brandeis, L., “The Right to Privacy”, *Harv. L. Rev.* 1890, p. 193.

BOOKS

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. and Rohs, M., *Ambient Intelligence and Ubiquitous Computing*, Institute for Pervasive Computing, ETH Zurich, Switzerland.

Boltanksi, L. and Thévenot, L., *De la justification. L'économie de la grandeur*, Gallimard, Paris, 1999.

Dewey, J., *Démocratie et éducation*, Armand Collin, Paris, 1975.

Ericson, R. and Haggerty, K., *Policing the Risk Society*, Clarendon Press, oxford, 1997.

Foucault, M., *Discipline and Punish*, Pantheon, New-York, (1975) 1977.

Foucault, M., *Le gouvernement de soi et des autres, Cours au Collège de France 1982-83*, Gallimard, 2008, p. 60.

Gandy, O., *The Panoptic Sort : A Political Economy of Personal Information*, Boulder, Colo. : Westview, 1993.

Habermas, J., *Between facts and Norms*, MIT Press, 1996.

Haraway, D. J., *Modest_Witness@Second_Millenium. FemaleMan_Meets_OncoMouse: Feminism and Technoscience*, Routledge, 1997.

Ladrière, J., *L'éthique dans l'univers de la rationalité*, Artel / Fides, Namur, 1997.

Lyon, D., *Surveillance Society. Monitoring Everyday Life*, Open University press, Birmingham/Philadelphia, 2001.

Lyon, D., *The Electronic Eye: The Rise of Surveillance Society*, Polity Press/Blackwell Publishers, Minneapolis, 1994.

Norris, C. and Armstrong, G., *The Maximum Surveillance Society. The Rise of CCTV*, Berg, Oxford, 1999.

Nussbaum, M., C. and Sen, A., *Quality of Life*, Clarendon Press, Oxford, 1993.

Nussbaum, M., C., *Sex and Social Justice*, Oxford University press, Oxford, 1999.

Sen, A., *Inequality Re-examined*, Oxford University Press, Oxford, 1992.

Sunstein, C., R., *Why Societies needs Dissent*, Harvard University Press, 2005.

Westin, A. F., *Privacy and Freedom*, Athenaeum, 1967.

RESEARCH REPORTS

A Report on the Surveillance Society, For the Information Commissioner by the Surveillance Studies network, Full Report, September 2006.

Darquennes, D., Grandjean, N., Goujon, P., Lobet-Maris, C., Poullet, Y. and Rouvroy, A., MIAUCE Delivrable D.5.1., 2007.

Hempel, L. and Töpfer, E., "CCTV in Europe, Final Report", *RTD-Project*, 5th Framework programme of the European Commission, 2004.

Home Office Research, UK, about the anti-social behaviour: www.homeoffice.gov.uk/crimpol/antisocialbehaviour/

HUMAINE European Project (Human-Machine Interaction Network on Emotion), in http://www.emotion-research.net

Marris et alii, *PABE Final Report*, 2001.

McCahill, M. and Norris, C., "On the Threshold to Urban Panopticon, Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts", *Urbaneye Project*, *Working Paper n°2*, 2002.

Murakami Wood, D. and Ball, K., A Report on the Surveillance Society: Public Discussion Document, 2006.

Punie, Y., Delaitre, S., Maghiros, I. & Wright, D. (eds.) "Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities". SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507, November 2005. http://swami.jrc.es

LEGAL REFERENCES

Amann v. Switzerland [GC], no. 27798/95, §§ 65-67, ECHR 2000-II

Art. 29 WG, Opinion 25 nov. 2002, WP 67 on personal data processing by videosurveillance, available at the website of the EU Commission

Article 2 of Additional Protocol N°4 of the ECHR, Article 45 of the Charter of Fundamental Rights of the EU

Article 29 Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context, Sept. 13, 2001 (5062/01/EN/Final WP 48), at 24.

BVerfG, 1 BvR 370/07 vom 27.2.2008

ECHR, Copland v. United Kingdom, 62617/00 [2007] ECHR 253 (3 April 2007)

ECHR, P.G. and J.H. v. the United Kingdom (Application no. 44787/98), 25 September 2001

ECHR, P.G. and J.H. v. the United Kingdom (Application no. 44787/98), 25 September 2001

ECHR, Von Hannover v. Germany (2004) 40 E.H.R.R. 1 at [50].

European commission for Democracy through Law (Venice Commission), Opinion on vidéosurveillance in pubic places by public authorities and the protection of Human Rights, adopted by the Venice Commission 16-17 March 2007, CDL-AD(2007)014

Peck v. The United Kingdom, 28 January 2003

Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V

Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005, p. 8.

Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005,

WP 136,Opinion 4/2007 on the concept of personal data, adopted on 20th June, available on the website of the EU Commission

CONTRIBUTIONS TO COLLECTIVE BOOKS

Brunson, M., W., « A definition of "social acceptability" in ecosystem management" in Brunson, M., Kruger, L., Tyler, C. and Schroeder, S., (Eds.), *Defining social acceptability in ecosystem management: a workshop proceedings*, General technical Report PNW-369, Portland, 1996.

Ekman, P., "Basic Emotions", in T. Dalgleish and T. Power (Eds.) *The Handbook of Cognition and Emotion*, John Wiley & Sons, Ltd., Sussex /U.K, pp. 45-60, 1999.

Gandy, O., "Coming to terms with the Panoptic Sort", in Lyon, D. & Zureik, E. (eds) *Computers, Surveillance and Privacy*, 1996, pp. 134-156.

Sellars, W., "Philosophy and the Scientic Image of Man" in *Science, perception, and Reality*, Routledge and Kegan APul, New-York, pp. 1-40, 1963.

Shneiderman, B., "Human Values and the Future of Technology : A Declaration of Responsibility" in Shneiderman, B., (ed.), *Sparks of Innovation in Human-Computer Interaction*, Ablex Publ., 1993.

ANNEXE 1

MIAUCE SCENARIOS - QUESTIONNAIRE

We extracted the two descriptions of the three scenarios, and gathered them in order to have an overview of the situation. The aim is that the partners detail more precisely the targets, the roles of the different actors involved, the content and the limits of each scenario.

Application 1: Security - aided detection of suspect behaviours

It is one of our objectives to help the security personnel to detect suspect behaviour from video streams. The basic idea is to analyse video streams with two purposes. On the one hand, potentially dangerous behaviour can be detected and security operators can be warned to pay attention to the important events taking place in an area under surveillance. On the other hand, stored video sequences can be annotated with relevant information that can be used off-line for different purposes, such as locating events of interest (e.g. when a certain object appeared or disappear from a scene) or analysing human behaviour to characterize normal and abnormal patterns in an area under surveillance.

To this end, potential detections in which we are interested are:

People approaching a certain area or crossing a certain "virtual safety line." In many open areas, it is impossible to place physical barriers to avoid people approaching certain areas. In commercial areas, physical barriers are not well perceived by customers because they can act as a deterrent for them to approach shopping areas. The ability to watch the area with one or several cameras gives the possibility to detect automatically people approaching a restricted area and warn a security operator to verify that everything is normal.

Detection of people loitering in a certain place. The ability to characterize the motion pattern of people in a certain area can be used to detect abnormal situations. This characterization can be done statistically. This is not required that all persons in the area under surveillance must be tracked by the system.

Detection of abandoned objects. The ability to detect objects abandoned by persons in certain environments can be used to attract operator's attention and to help searching for scenes with potential suspects.

Detection of dangerous situations in certain scenarios. Applying object-tracking techniques, one can characterize situations that can be identified as "abnormal" in a certain context. Examples of interest are a person laying down in the floor in an isolated area (e.g. in a Metro station) or the presence of a person in an escalator while it is stopped (e.g. to make it possible an automatic remote start of the escalator with no potential harm to persons present in the escalator).

Detection and tracking people with odd behaviours. This is possible by profiling classes of behaviours (e.g., people behaving suspiciously in airports etc.). This can be achieved by analysing user interactions and interpreting them in a particular context.

Most of the useful detections in the security applications will be related to the application of object tracking to the video streams provided by surveillance cameras. The partner Visual-Tools will drive this application with a pool of end users, as described in the work package 6.

First application scenario: Collapsed escalator (S1.3)

This application fits in one of the most important market areas of interest of Visual Tools: *Large Public Installations*. The application will provide a customized video surveillance system with the ability to detect a typically dangerous situation in an airport, people blocking an escalator exit because of a fall or a luggage drop. This kind of event is considered a dangerous situation that must be detected in order to warn a security operator.

This scenario is concerned with the multi-modal analysis of videos recorded by surveillance systems. The main objective of surveillance systems is to have some locations continuously observed to protect them from intrusions and thefts. With this aim, cameras are installed in critical places of the premises to guard and the video signal is carried to a control room, where dedicated employees can have control of the situation and react in case something unusual happens. This control room could be close to the observed place or could be in a remote central security station connected to the site through communication lines. One such example is a camera installed at an airport to monitor the situation of escalator exits. The multi-modal interaction analysis of the recorded videos can be exploited to present informative data to the security team who needs to take prompt actions in a critical situation.

In this scenario, there is much room for investigating the role of context to increase the understanding of the current situation that is supported by the analysis of multi-modal interaction. This involves the contextualised configuration of system settings, the presentation of the current system settings for varied camera locations, as well as the visualisation of the alarms generated by the multi-modal analysis in a system user interface. Using context information to optimise the system configuration allows for using the same underlying detection algorithms in different locations and in an efficient way. The understanding of the system configuration is also important for the security team to assess the current situation.

- Could you describe more precisely the scenario following to the storyboard methodology ?
  - Sequence 1: for example, images capture
    - Context: place and actors
    - Technology and task: what technology for which task
    - Finality or utility: to do what
    - Difficulties and constraints
  - Sequence 2: for example, reading and analysis of images
    - Context: place and actors
    - .....
- Who are the main actors in the scenario? Identify them and their responsibilities and constraints.

	Constraints	Responsibilities
Actor 1=.....		
Actor 2=.....		
Actor 3=.....		

- How do you intend to categorise what is suspicious and what is not?
  - And what about categorisations of what is normal vs. abnormal; dangerous vs. not dangerous? Describe precisely your conceptions.
  - How does the system recognise those categories? How does the application works with the categories?
  - Who decides and fixes the parameters for the application? Who takes responsibility for the definition of criteria?
  - How can you guarantee the anonymity of the individuals whose behaviours are analysed?
  - How can you guarantee the transparency of the criteria used to distinguish among the categories (suspicious vs. non suspicious etc.)?
- How do you address potential privacy and discrimination issues ensuing from the scenario?
  - Who would control the system and address potential issues of privacy, discrimination etc., externally (CNIL, or other national commissions for the protection of privacy for example?) and internally?
  - Who is the owner of the installation? Who uses the collected data (retailer, a security

company)?
    - What (technical, or other) guarantees are taken to ensure that the collected data will not be used for other purposes than the original purposes for which they were collected in the first place?
    - How long will the collected data be kept?
    - What kind of communication means will be put in place to make people aware of the presence of cameras and of the remote analysis of their behaviours and actions?

- Who takes responsibility for deciding about action when suspicious behaviour is detected? What kind of decisions can be taken in such circumstances?
    - Does the alarm put a social pressure for the security agents? Is it a professional fault to ignore the alarm?
    - Could security agents get the impression that the system has some power regarding the decision-making process?
    - What kinds of instructions are given to the security agents concerning the system?
    - How do you know that the system helps security agents? Did you survey them about their needs? Have they been consulted about it?

- One of the main problems is that there is a gap between the objectives, centred on proactive surveillance on the one hand, and the description of the scenario, which purports to be more neutral. Or we talk about the same application. How do you justify this gap?

Application 2: Personalized marketing

The application objective is to simplify every day activities of the user, in relation with acquisition of his every day or contextual needs (food, hygiene products, etc.). The application objective becomes of great practical importance and challenge when the user is an elderly person or has problems (disabled) in accessing the controlled environment (e.g., shop windows) or has auditive problem. So the technology investigated in the project, when validated, will have deep impacts on hundreds of thousands of people and hundreds of shops. We estimate therefore that this application has enough importance to justify the investment of the project.
Through the capture and analysis of user behaviours, it will be possible to analyse people behaviour in front of a shop window, and customer trajectories inside a large store. These analyses will have a great impact on meeting user needs and service personalization. And help the shop optimise its merchandizing, increase the visibility of its products to improve sales and profits.

Second application scenario: Average people looking at a shop window (M1.1)

This scenario is concerned with the multi-modal analysis of videos in a similar way to the previous scenario, but the outcome of the analysis is used for marketing purposes. This particular scenario aims to capture the multi-modal behaviour of people who look at a shop window, to determine the effect of product displays. Such analysis can be applied to a shop window of a little store or in a pedestrian street. As such, the end-user of this application can be the shop owner, store manager, or those who are responsible for display arrangements. Since there is little existing technology that can evaluate the effectiveness of product displays based on people's behaviour, the multi-modal interaction analysis is a promising technology to apply to such problems.

The environmental context of the cameras installed will be an important aspect for optimisation of the detection algorithms of multi-modal interaction analysis. The contextualised presentation of the outcome of the analysis should also improve the understanding of the relationship between the product displays and people's behaviour.

- Could you describe more precisely the scenario according to the storyboard methodology?
  - Sequence 1: for example, capture of images
    - Context: place and actors
    - Technology and task: what technology for which task
    - Finality or utility: to do what
    - Difficulty and constraint
  - Sequence 2: for example, lecture and analysis of images
    - Context: place and actors
    - .....
- Who are the main actors of the scenario? Identify them and their responsibilities and constraints.

	Constraints	Responsibilities
Actor 1=.....		
Actor 2=.....		
Actor 3=.....		

- About the objective of the scenario: “simplify everyday activities of the user”
  - What are the effective and concrete services brought to the users? Describe the services themselves, one by one.
  - Describe precisely, by sequences (as a storyboard), the system offering such services.
  - How are the data collected, treated and stored? Who treat them, in which finality?
  - What does the user know about the data collected on himself? How can he/she know what become their data, who treat them?

- About the “elderly, disabled person and those who have auditive problems”:
  - Describe precisely how the system can answer to their particularity. Which specific service can the system bring to elderly? To disabled persons? To person with an auditive problem?

- About “behaviours”:
  - What does the term “behaviour” cover exactly? Gesture? Head motion, body motion, gaze, social behaviour? The term is not elaborated enough and covers to much significances: it is ambiguous.

- About the “analysis of behaviours”:
  - Describe more precisely what are done by the “analysis of the behaviours”: contents (gesture, head motion, body motions...?) , objectives (moving time, cartography of movements, ..?) and the technical way to get it.
  - For which actors: end-users, retailers, marketing company? Precise the added-value completed for each actors.
  - What are the real needs of users encountered by the scenario? In which way does the system answer to those needs?

  - *What is the real finality of the application, encounter users needs or optimize a marketing process? This is not clearly elaborated.*
  - *Describe a typical use-case, involving **all the actors** of the scenario. “It is Christmas time. Mr X is in a shopping mall ...”*

- About “average people”: what does it mean specifically?
- About “apply to such problems”:
  - What is (are) the problem(s) the system wants to apply? Describe it (them).
  - Justify the added-value of the system in that case; actually, the application seems very weighty to solve “problem” of displays or window-shopping.
  - *There is a gap between the objectives, very large and oriented to people, and the description of the contents, which seem to be an optimization of a marketing process.*
- Does the application enable to cope with technical problems such as head orientation, movements, eyes gazes, crowds, glass reflects...?
  - What does the system grounded on? Statistics? Data mining?
  - Relevance of the sample if the problem of the crowd is not solved? (statistical analysis of the people passing, one by one?
  - General robustness of the system?

- What can other domain of application be chosen? Another marketing processes? Security?
- Is it possible to recognize people by their sex, age, and ethnicity?
  - If so, describe how the system does.

- Does the system intend to categorize by sex, age and ethnicity the people?

- How does the people know that they are filmed?
  - How is the information displayed to people entering the public places?
  - Who does watch the videos and analyze them?
  - How can the people know who watch the videos?

About "the contextualised presentation of the outcome of the analysis should also improve the understanding of the relationship between the product displays and people's behaviour":

- *This relationship, between what the products displayed and the people's behaviours is not clearly elaborated.*

Application 3: Adaptive and interactive web T V

Interactive internet TV is a progressive alternative information channel, available at the time and location convenient for the viewer. Data storage, accessibility within a certain time limit and supply of customized information according to demand of the viewer are the main advantages of interactive internet TV that make it unique and enable optimum usage of the time resource for contemporary audience. The application to be developed in MIAUCE project highlights significance of adapting content type and layout to different user behaviours through a multi-modal interface associated to a browser of a content-based retrieval system.

The variety of internet TV content is virtually unlimited: it supplies broadcasts, media clips and other information for users of any age, gender, social setting and interest group. This content is usually structured by category and subcategory allowing for expansion of a certain topic in more detail to create a target-oriented set of information. E.g. there are comprehensive news channels offering the latest coverage of social and political events and their development throughout the world. There are also informative sections or databases dedicated to sports, medicine, international or local business, education, entertainment, society, technology, reference, etc.

For MIAUCE project we chose web news TV as a domain of application since news clips as well as other similar audio and video content is provided more regularly on the web and is required by increasing number of online users on a daily basis. Today more and more TV companies (TF1, BBC-World, Latvian TV etc.) provide online Web news sites.

By accomplishing its tasks as an information channel, interactive internet TV becomes a lucrative environment for e-commerce, enabling businesses and other organizations to attain their major (marketing) goals. In this case it is very important to place blogs, banners and other commercial information in appropriate place both to ensure effectiveness of commercials and keep comfortable environment for viewing selected content.

As a base for multi-directional data flow, internet is an effective means to this end. Data transmission in both directions (interactivity) is the key to an individual's interests and necessities, serving as a base for preparation and publication of information. The principle is similar when supplying non-commercial information, e.g. popular-scientific or educational data (clips). Provision of information is basically intended to add value by informing or educating the viewer in this case.

These sites are composed of articles, images and audiovisual files that complement each other for greater user enjoyment providing richer and all inclusive information set. Producers of content have rough ideas on content navigation and usage patterns of their users. Multi-modal interface will change the way users explore web sites online, as well as create avenues for further advances.

Interactive television enhances a program with content and services to create a more engaging, personalized experience for viewers, allowing them to watch and interact with television on multiple levels. Content and services can include the ability for viewers to get more in-depth information on the programs they are watching, voice opinions through online voting, chat with other show fans, play games, purchase merchandise on demand and much more.

Eye fixation, eye blink, head pose, hypermedia interactions and queries by content will open up improved ways to present and work with information. The technology will analyse user interactions through multi-modal interface associated with a content-based retrieval system. Particular importance will be paid to user needs with respect to content presentation. This is of utmost importance to news content producers in order to improve the quality of their production thus reaching higher ratings and wider audience.

The partner Tilde will drive this application in collaboration with end users of own web TV sites as we will see in the work package 6.

Third application scenario: Web TV recommendation and summarization system (TV1.1)

While the previous two scenarios aimed at analysing the recordings of surveillance cameras, this scenario mainly targets the TV programs and other video contents that can be watched through an interactive Web TV application. As such, we will investigate the analysis of user behaviour with his personal environment and will concentrate on different modalities to deliver personalized information to this user. Since the size and diversity of video contents available is increasing on the Web, it has become more difficult for the end-users to find relevant materials effectively. For example, in the Web TV applications, there are news contents, entertainment contents, as well as educational contents. In each type of contents, there are several program genres such as business news, music, films, and/or documentary. Therefore, there is a growing need to develop an effective system to support the end-users in accessing the video contents. We will concentrate on two specific aspects: recommendation of possible interesting material and summarization of material of interest for a particular user.

- Could you describe more precisely the scenario according to the storyboard methodology?
  - Sequence 1: for example, capture of images
    - Context: place and actors
    - Technology and task: what technology for which task
    - Finality or utility: to do what
    - Difficulty and constraint
  - Sequence 2: for example, lecture and analysis of images
    - Context: place and actors
    - .....
- Who are the main actors of the scenario? Identify them and their responsibilities and constraints.

	Constraints	Responsibilities
Actor 1=.....		
Actor 2=.....		
Actor 3=.....		

- Describe the application system more precisely: we do not know much about it.
  - Describe all the sequences of the process, as a storyboard.
  - Describe the parameters of the system.

- Links between information and behaviours:
  - What is captured and analysed? Eyes gazes, gestures, head poses...?
  - For which objectives?
  - How do you ensure the relations between the behaviours and the connected intentions / emotions?

- Technically, it seems to require strict constraints, regarding the head and eyes positions. How can you manage those constraints? Is the application feasible in everyday life?
- Do you intend to use facial recognition of emotions in this application?
- Who is the end-user of the application? A common web user? Is it an application dedicated to experimental tests?