PRIVACY PRESERVING PERIMETER PROTECTION PROJECT

SEVENTH FRAMEWORK PROGRAMME

GRANT NUMBER 312784

D2.1 Social acceptability studies

ABSTRACT

"Virtual fences" can be defined as a set of interconnected technologies composed of radars, acoustic and thermal sensors, lasers and cameras. While such a technology is being developed through the Privacy Preserving Perimeter Protection Project, it poses many questions regarding its social acceptability. Indeed, P5 system contributes to the growing field of surveillance and security technologies which more and more pervade public spaces, shape tomorrow's societies and raise many problematic issues. This report deals with the political and collective dimensions of virtual fences. It unfolds a variety of political problems posed by virtual fence based on state-of-the-art social science literature. Then it addresses different prospective publics for this technology, through "deliberative arenas", to explore collectively the problems identified in the first place.

Keywords: Social acceptability, Publics, Deliberative arenas, Politics of virtual fence

The research leading to these results has received funding from the European Community's Seventh Framework Programme Security Theme (10) under grant agreement number 312784. The research is a part of the efforts in the pan-European and FOI-coordinated project P5.

Author	François Thoreau, uNamur	Date	31/10/2014
		Deliverable	D2.1
Co-Author	Jérémy Grosman, uNamur	Version	Prel, 27/10/2014
	Olya Kudina, uNamur	B/W Print	Yes
	Alain Loute, uNamur	Page Count	68

Executive Summary

"Virtual fences" can be defined as a set of interconnected technologies composed of radars, acoustic and thermal sensors, lasers and cameras. While such a technology is being developed through the Privacy Preserving Perimeter Protection Project, it poses many questions regarding its social acceptability. Indeed, P5 system contributes to the growing field of surveillance and security technologies which more and more pervade public spaces, shape tomorrow's societies and raise many problematic issues.

While such issues are usually understood in individualistic terms (privacy, personal data), this report deals with the political and collective dimensions of virtual fences. Throughout this report, our main concern is to figure out "who is the public" for virtual fences. If virtual fences are a collective and political phenomenon, then who is the public concerned by these technologies, whose life might be affected?

First, we acknowledge that virtual fences are still at a very early stage of development, hence being still prospective in scope and tentative in their outreach. For this reason, we adopt a speculative approach taking the object and P5's project of "virtual fences" seriously, and we draw on the best social science literature on the issues of fencing and surveillance to unfold the potential problematic dimensions of virtual fences.

Second, the collective dimension lies in what we call "deliberative arenas". Because virtual fences are still prospective in scope and tentative in their developments, they don't have yet a predetermined public, which could be addressed per se*. Instead, we initiate a threefold quest for a public: 1) by looking at the consortium members as the primary concerned public; 2) by questioning a particular social context which could be of interest for the development of virtual fences, the case study of prisons, using qualitative materials and; 3) the "public at large", where we try to gather a sense of "public opinion" using an online survey.*

Contents

1 Introduction

"Virtual fences" can be defined as a set of interconnected technologies composed of radars, acoustic and thermal sensors, lasers and cameras. Merged together, those technologies allow for permanent and automated monitoring of "protected areas", through a system architecture which allow to gather and put together various fluxes of information. This architecture rests on algorithms that manage this information and allow for early detection and warning with respect to potential threats, i.e. threatening intrusions in the concerned area. For this purpose, "virtual fences" can be described as a combination of hardware, software and algorithms.

While this technology is being developed through the P5 project, it raises many issues regarding its social acceptability. Indeed, this technology contributes to the development of a larger field, namely the technologies of the security, which more and more pervades public spaces and shape our societies.

While such issues are usually understood in the narrow terms of "privacy" or "personal data", all notions tied with the individual and that can be solved by adequate technical answers, this report deals with the political and collective dimensions of virtual fences. In other words, it pays interest to the phenomenon which go beyond the individual, so as to put things into perspective and take a higher stance on these ongoing developments.

Throughout this report, our main concern is to figure out "who is the public" for virtual fences. If virtual fences are a collective and political phenomenon, then who is the public concerned by these technologies, whose life might be affected? In our view, the collective dimension must exist in what we call "deliberative arenas" (see chapter 4) but this is precisely where the difficulty begins. Because they are still prospective in scope and tentative in their developments, virtual fences don't have yet a public which could be addressed *per se*. There are not visible in the public area, they do not raise controversies, there are no local settings where there are to be found as such.

So there are two solutions methodologically to solve this issue. The first one is to carry out an intensive inquiry on other technologies of surveillance, and attempt at inferring lessons for the matter at stake, i.e. virtual fences. This is not the option we followed. Instead, we decided to take the object seriously, in its current stage (still prospective, still tentative) of development. So in an experimental manner we tried to figure which kind of issues virtual fences could give rise to, in which kind of social settings they might get inserted and, lastly, we tried to anticipate / speculate on their potential effects and consequences.

Doing so, we rely on a notion of the "public" which is borrowed from John Dewey in the *Public and its problems*. In this book, Dewey argues that a public is always assembled by an object of preoccupation which is core to its action as a public. For instance, it could be environmental activists who are preoccupied with the question of nuclear energy and reassembled by nuclear power plants as their "matter of concern" (Latour, 2004). In other words, we contend that the public is not already constituted, existing out there and waiting for us to "discover" it. All the contrary, envisioning different publics for a technology such as virtual fences should read as an active process from publics themselves and, in this case most importantly, from social scientists. In the case of a technology which is still in its very early stages of development, it belongs to social scientists to "generate" this public, as Norwegian philosopher Roger Strand would say to "spark the public into being".

In this respect, we envision the role of the social sciences as to render the picture more complex, not deliver a "go" or "no go". As what we need to assess it not even out there and ready to perform, it is a very difficult process to unfold the different problems raised by virtual fence with different publics. So, in this report, we proceed by trial and error approaches, working hypothesis, to explore as much problematic dimensions of virtual fences as we could, trying both to be faithful to the very definition of the technology and its characteristics, but also trying to infer from there on the collective and political dimensions they could lead our societies to.

Hence the "fil rouge" we will follow: how to carry out "social acceptability" issues on an object that barely exists, which is still a mere prospect? Again, we wish not to produce ready-made advice for decision-making, but to provide "food for thought" so as to nurture, enrich and complexify the decision-making process. For this reason, we really needed to focus on a prospective case study, as we learned from Science and Technology Studies (STS) scholars that technological innovations should never be detached from their actual context of application. In other words, innovations are never purely technical, they are all the like socio-technical, i.e. they succeed only if they can insert themselves in a certain context of application where actors will deploy, relay them and use them.

For this reason, we chose to focus on the case study of prisons. We tried to think about what would (likely) happen if a technology such as the one promoted in P5 would be implemented tomorrow in prisons, trying to figure out who would be the impacted publics, how they would react, what their concerns would be, and so on.

Such a process bears lots of uncertainties (Callon, Lascoumes & Barthes, 2001) and it takes a *trial* to determine whether or not the technology will effectively be in use or not. In our view, this means that the technology has to go through a series of events in a specific social context. For example, in the case of prisons, virtual fence are very much dependent on all these publics we seek to address. Public authorities have to go for it, penitentiary administration must follow, it must be possible budget-wise, it must be timely, etc. then it all goes down to the level of prison director who will determine the use of the technology, if any, then below to the level of guards who need to learn how to work with it — or not, to cite but a few of all the different steps the technology must cross in order to be successfully implemented.

In this respect, certainly the state of public opinion is an important matter, but it does not suffice to determine the local conditions of application and / or use of the technology. It might probably be a necessary step when time comes (when virtual fenc-

es are developed and steadily ready to be put on the market), but it is certainly not enough. In chapter 4, we attempted nonetheless to carry out an online survey targeting "the general public", but it failed precisely for the reasons we just reported here (and that we expand in chapter 4). However, we decided to produce some of its interesting results and features because we take it that we can gain insights from that experience, and that it considerably helped us, in contrast, to think with a sufficient level of granularity about what might be the pitfalls or shortcomings in the other case study we showcase. These are more qualitative, textured, and carry forth contextualized methodologies which help building a sound case study.

Chapter 2 provides a brief overview of how we frame "social acceptability" within P5 project. We address multidisciplinary issues with respect to the notion of "privacy", then with respect to the notion of "social acceptability" itself.

Chapter 3 is a theoretical state of the art. In this chapter, we explain how we frame the problem of virtual fence as a "script" that is a program in itself (what does it do?). Then, we draw on the classic literature on surveillance, from Foucault's panopticon to nowadays conceptions of "state of emergency". In a third part, we get more specific and start to think about the spatiality of virtual fence and the problematic dimensions of their deployment in controlled space. What does distinguish virtual fences from former tools of space delineation such as the barbwire? To which extent is it "virtual" and/or material? Finally, the last part raises practical theoretical questions and issues with virtual fence, by looking at them through the lenses of their "modes of existence" (Latour, 2012). It is a way to suggest three different ways to look at them, as techniques, as a way of organizing things, but also as a way to produce particular environments in the zone which are being protected by virtual fences.

Chapter 4 builds on these problems to open up what we call "deliberative arenas" using qualitative and quantitative methods we designed to address the problems of virtual fences mentioned above. The first "arena" is called "internal" in the sense that it encompasses P5 partners themselves and explore the question of how they frame "normality" as in "detecting abnormal behavior". What is normal and what is abnormal? The results were gathered using a structured qualitative questionnaire, the consortium meetings and informal interactions with partners. The second arena is the public of prisons. In this section we elaborate on prisons as a case study and try to unfold a variety of prospects regarding the way Belgian prisons work, with in mind the question of "what would happen if a virtual fence device was ready to implement in Belgian prisons"? In this part we question the potential effectiveness of such a technology in a social context such as this one, and try to highlight many practical challenges in situation. This part rests on qualitative material, extended literature review of the penitentiary field in Belgium and semi-structured interviews with key actors of this field in Belgium. Lastly, the third part deals with the "public opinion" at large, trying to suggest what virtual fences could do or not do in a variety of settings. To do that, we set up an online survey which gathered 288 complete answers but which has met some limitations which we make explicit. It is the reason why we suggest in the conclusion some paths to better approach the public of virtual fences and to collect its intelligence in order to shape the future of the virtual fences.

2 A multidisciplinary scope on « social acceptability »

2.1 Guidelines on « social acceptability » and the role of SHS

To start this report, we would like to address the major issues arising from the implication of Human Scientists in the design of a technology. It is mostly developed towards the learning experience we capitalized into the P5 project. It is divided in three parts. First of all, the discussions do concern the limits of our initial or original mandates within the P5 project. In the second part, we present the general principles and values that have supported and framed our intervention in this design. The third part addresses the methodological steps we have elaborated to manage our intervention in the project design.

The position of human scientists should be very clear form the beginning of the project. Two main statements can be done. The first one refuses the status and the responsibilities of the expert in charge of telling what is good, fair, and reasonable to adopt a position of facilitator who helps all the stakeholders to deliberate the technology. The second one questions the limits of the social acceptability concept traditionally used to analyze a technology in progress. Both of these statements go in the same direction: a clear refusal to reduce the human scientists' role to an instrumental one.

2.1.1 The limits of the expert's status

Usually, human sciences play an instrumental role in technological project. Engineers as industrials expect that they fix a socially acceptable frame for their design telling them what they can do and what they should do according to some normative and ex-ante principles. That confirms the position of human scientists as instrumental experts.

The adopted position is inspired to a large extent by Jean Ladrière approach of ethics (Ladrière, 1997). More than a set of standards to be complied with, ethics, as Jean Ladrière suggests, are a "savoir-faire" (a form of know-how), a capacity to exercise moral choices when faced with situations raising unprecedented ethical dilemmas or challenges. In that frame, Ladrière 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.*
>
> *Ladrière, J., L'éthique dans l'univers de la rationalité, Artel / fides, Namur, 1997.*

Following Ladrière's position forces us to consider alternative figures we could endorse, as human scientists in a technological project, and to clearly identify our responsibilities and our legitimacy into the project.

This status must be defined according to the pedagogical aims human scientists should try to achieve into a technological project. Our reference to "pedagogical aims" means a clear refutation of any expert approach in which human scientists would endorse the responsibilities of defining the "good" or the "fair". To be brief, it is not the role of the SHS researchers to legitimize any options and their technological specifications.

According to Ladrière, 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 with ethical reflection and action.

This position is very close to that developed by Dewey (Dewey, 1975 [1916]). This author underlines 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, the role of the so-called expert is not to decide instead of the concerned actors but to facilitate the deliberation and to enlighten it by clarifying the ethical questions raised by the questioned situation.

2.1.2 The limits of the 'social acceptability' concept

The usual expected mandate of human scientists in technological project consists of addressing the social, legal and ethical issues raised by the surveillance and observation technologies developed in the project, and to assess its social acceptability.

Let us consider this concept of "social acceptability".

Inspired by a kind of preference in favor of an utilitarian approach, maintaining that whatever satisfies the preferences or desires of an individual involved in an action is morally right Brunson (1996) defines social 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 favorable 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 po-

litically relevant segment of the citizens. In this perspective the norms emerge form a democratic exercise involving all the concerned actors.

Beyond the pragmatic problems (democratic representation, deliberative procedures, asymmetry of actors capabilities, etc.) raised by such an approach, we are confronted to two major fundamental objections.

- 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. By using this social acceptability realm, we are led to refuse any radical critique, opposition or contestation, and subtly we are engaged 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 et al., 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. "* (Marris et al, 2001).

- 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 criterion. 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 since it exhibits as an evidence of their social acceptability and thus of their legitimacy, the trade-off between liberty (and privacy) rights and aspirations to security wished by the majority of the citizens and thus imposed to the entire population.

2.2 A multidisciplinary approach from social science

A rapid overview of the recent research initiatives funded by the European Commission within the Seventh Framework Programme (FP7, 2008-2013) and United States agencies such as the Defense Advanced Research Project Agency (DARPA) and the National Science Foundation (NSF) shows that the majority of the EU projects and the to-

tality of the US ones are technical, i.e. “they focus on engineering issues and technological development and demonstrations” (Frieddewald, & Bellanova 2012).

However, in Europe, there is also a place devoted to the analysis of the broader ethical and legal issues related to surveillance and security technologies, e.g. there is an “ethics, security and society” theme in the Security Programme under Activity 6 (Security and Society) in the current Seventh Framework Programme where several related “Science and Society” themes cover also social and individuals implications of surveillance and security technologies.

While P5 project is concerned mostly with technological and industrial partners, the University of Namur is questioning the social and ethical issues in the project. For this project a multidisciplinary scope is needed. A multidisciplinary approach is defined as the presentation of virtual fence as they can be analyzed from a variety of different disciplinary frameworks, but within such frameworks. An interdisciplinary approach is defined as the work between disciplines from the perspective of what may be blinding in them regards to virtual fences. The hypothesis is that the difficulties and controversies existing inside a discipline can receive a better understanding with the help of the other disciplines. Henceforth we seek complementarity instead of replacement. While identifying the limits of our mainstream discipline regards to the issues at stake, the interdisciplinary work is needed in order to look outside our discipline and draw insights from other disciplines.

The two main concerns are “privacy” (1) and “social acceptability” (2). To address them both, we undertook a multidisciplinary approach, although each of these broad concerns have been addressed separately. All in all, different disciplinary perspectives are mobilized to deal with each of those two concerns, while the prospects for social acceptability have been undertook from the varied perspectives of political science, philosophy of science and techniques, as well as from the field of research known as “science and technology studies” (STS).

2.2.1 Privacy

In P5 project, it has been decided that “privacy” would be dealt with using a third-party protocol designed together by lawyers and computer specialists.

As many scholars have already stated, privacy is “a flexible and fluid concept” (Dourish. & Bell, 2011, p. 143), for which there is no single definition or meaning, a concept which is very difficult and challenging to define (DeCew, 2012). “Attempts to define it have been notoriously controversial and have been accused of vagueness and internal inconsistency – of being overly inclusive, excessively narrow, or insufficiently distinct from other value concepts” (Nissenbaum, 2010).

Is privacy, asks Nissenbaum, “a claim, a right, an interest, a value, a preference or merely a state of existence” ? The enterprise of defining privacy conceptually has often resulted in adding confusion to the point of, eventually, thwarting progress in helping to clarify privacy issues. The one of describing empirically the way people do experience their privacy, either individually or collectively, has not filed better results. Indeed, a lot of empirical surveys about the perception citizens have of privacy in general and of their own privacy in particular are of poor methodological quality, as a very recent study shows (Watson & Wright, 2013).

The difficulties are very important while attempting to grasp the parameters which make sense of privacy and privacy harms for people or groups of people and while attempting to give an account of them in order to reinforce privacy protection against possible privacy harms, risks and concerns. Taking in isolation those parameters have no utility while most of them overlap and interact with each other, are possibly in contradiction or in mutual reinforcement, are highly dependent of a political regime, a personal and/or a political history, and while their relevance concerning privacy issues is possibly changing regards to the type of surveillance technology at hand and the specific context in which they operate. Among those classical parameters, there are: class, race, sex, age, culture, country, profession, social statute, health, political regimes, legal system, economic wealth and/or (in)stability in their country, surrounded or not by trustworthy people (friends, family), etc.

Although the admission of inability to grasp the concept of privacy has become an obligatory exercise opening any study devoted to this matter, a wise first step is to start "by identifying a series of different ways that the topic of privacy is approached in the research literature" (Dourish & Anderson, 2006).

As one may gather, "privacy" is a very problematic concern as it were, but in P5 we decided to implement it technically instead of entertaining much discourses on its very definition, making sure the right to privacy as defined by current legislations and courts is enforced into a filter build within the P5 architecture.

The argument in favor of the elusiveness of the concept of privacy is, in this case, expressed from the perspective of a judging practice (WHAT), which involves for the judge (WHO) the responsibility to "qualify" in law (HOW) what is privacy and what is a privacy harm. Regards to this practice, the judge has to articulate different dimensions of privacy and has to leave some of those dimensions out of the scope of his/her practice of judging. The borders between the articulated zones and the zones of undecidability are not framed once for all, rather their possible redefinition, regards to novelty (the case, the issues, the technology involved and so on) is part of the practice of judging.

For any practice which is engaged in its protection, privacy has become a "key lens through which many new technologies, and most especially new surveillance technologies, are critiqued." (Finn *et al.*, 2013, p. 4). "The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as 'our' privacy, it still finds a way to remain elusive", says Serge Gutwirth who explains why privacy is substratum of democracy and "of contemporary Western Society because it affects self-determination; the autonomy of relationships, behavioral independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioral manipulations. " (Gutwirth, 2002).

Many scholars have argued in favor of the elusiveness of the privacy's concept for the main reason that its inherently heterogeneous, fluid and multiple dimensions "may be necessary to provide a platform from which the effect of new technologies can be evaluated" and, therefore, the relevant protection be identified and created. "This potential necessity is supported by the fact that different technologies impact upon different types of privacy, and further technological changes may introduce or foreground previously unconsidered privacy dimensions" (Finn *et al*., 2013).

In this respect, the multidisciplinary approach has been chosen in order to give to all the partners engaged the full opportunity to make visible from the perspective of its own discipline and background, the different ways that the topic of privacy has been approached. The current section on privacy is deemed to be complementary with the work provided by the lawyers and the computer specialists who actually build the TTP and to enrich further their reflection on the topic, although we will not get further into it and its problematic dimensions here.

2.2.2 Social acceptability

To deal with social acceptability the narrow scope of privacy needs to be broadened up. As we suggested, social acceptability problems require different disciplinary perspectives. We undertook this thematic from a variety of perspectives: political science, philosophy of science and techniques, as well as from the field of research known as "science and technology studies" (STS).

In particular social acceptability is a tricky challenge in the case of prospective technology which has not yet come to reality such as virtual fence. Such technologies are at an early stage of their development. It makes it very difficult to see how they will insert in a social setting, how they will integrate societies, which publics they will target, i.e. who will benefit from them and who will see their existence affected, in one way or another, by the development of such technologies.

In particular in this report we provide extended prospective analysis based on the specificity we see playing out in the case of protected perimeters and virtual fence.

We do this from a variety of disciplines, because we gather that the plurality of disciplinary viewpoints will provide a sounder perspective on the specificity of this technology, how it operates and what it entails. To do that, we cross perspectives from political science and political theory, philosophy of science and STS. But it should be underlined that the research itself has been led on a collective basis, so that each of these disciplinary perspectives is reflected in this report but at once integrated with its contents.

Political science is a discipline interested in the forms of government in their variety. For this reason in this study we pay attention to the political effects of such technologies as virtual fence, and try to unfold what kind of power relationship they give rise to. So, in that sense, one must not read here "political science" as a mere study of political systems which is obviously out of scope here, but rather a "science of politics" in that respect.

This is why it is very important to complement it with a view from philosophy of technique. This discipline allows for taking the technologies themselves very seriously, what components they are made of, which models are fed into their conception, how they do run. All these technical aspects can be matter for philosophy, and it communicates particularly well with an analysis of power dimensions, because power phenomenon can be inferred from technical specificities in apparatuses like virtual fence.

Lastly, we generally draw on a field of study known as "Science and technology studies" (STS). This approach emphasizes the *processes* of elaboration, of construction of technology, instead of analysing it as an object already stabilized and bounded. The consequence is that we look at "hot" matters, in the process of being developed, and

we cannot insert these too quickly in well-recognized categories of classical sociology such as class struggles, domination relationships. We do argue that some of these phenomenon are certainly at play while the technology is being developed, but that it takes careful analysis and due attention to the technique itself to understand which new "lines" are being drawn by an emerging technologies, what it does operate. Then and only then it becomes possible to discuss its politics. For this reason, an STS approach seems particularly relevant to an object still emerging such as virtual fences.

3 Theoretical state of the art

The conception of a control mechanism, giving the position of any element within an open environment at any given instant (whether animal in a reserve or human in a corporation, as with an electronic collar), is not necessarily one of science fiction (…); what counts is not the barrier but the computer that tracks each person's position—licit or illicit —and effects a universal modulation.

The socio-technological study of the mechanisms of control, grasped at their inception, would hâve to be categorical and to describe what is already in the process of substitution for the disciplinary sites of enclosure, whose crisis is everywhere proclaimed.

Deleuze, 1992, p. 7.

3.1 From de-scription of virtual fence to the construction of normality with virtual fences

Social scientists asserted that technologies carry certain values and stir human actions in a certain direction (Bijker & Law, 1992; Latour, 1992; Thaler & Sunstein, 2008). Winner (2006) demonstrated how technology is also political, with its peculiar design features influencing human behavior. Aiming to explore the prescriptive and knowledge distributive nature of technology, Akrich (1992) introduced the concept of "script." Script can be explained as a manual or instruction, inscribed in technology, informing the users of its intended use and properties. A crucial role here belongs to industrials and engineers who promote or discourage from specific courses of action. Following Akrich, "designers thus define actors with specific tastes, competences, motives, ..., and they assume that morality, technology, science and economy will evolve in particular ways" (1992, p. 208). Script or scenario is thus a result of inscribing designers' motives into technology. However, the process of interpretation of technology also has to be considered. According to Latour (1987), "the fate of what we say and make is in later users' hands" (p. 29). This means that no matter how precise engineers and technology producers make its script, the users can attribute new meanings to the artefact and even reconfigure its usage (Gjoen & Hard, 2002). Pfaffenberger (1992) explained this process, referring to it as "interpretive responses to technological text" and "a discourse of technological "statements" and "counterstatements" (p. 285). Therefore, a later user can alter technological script or submit to it.

Since virtual fences as a technology has not yet been stabilized, - its scripts not yet put in action, - it is possible only to predict the possible use of technology. However, precisely because it has not been stabilized yet it is also possible to look into technical choices and motivation behind them. The algorithm that recognizes normal behavior beyond virtual fences is essentially a script. Following Akrich, one must "follow the negotiations between the innovator and potential users and to study the way in which the results of such negotiations are translated into technological form" (1992, p. 208). This act is defined by Akrich as "de-scription" and this is primarily what script analysis performs. The ultimate goal of script analysis is "to trace the transformations through the object as it moves between different actors and arenas" (Fallan, 2008, p. 67) and to provide a key to interpret the constructed meaning and prescription issued by technology. Therefore script analysis appears a useful tool in studying the algorithm of normal behavior.

However, it is impossible to proceed to any analysis before exploring the concept of normal behavior and studying the ways of its definition.

3.1.1 Description of virtual fence system and architecture, centrality of the algorithm

In this report, we argue that virtual fence dramatically redefine the politics of defense, protection and surveillance. The situation evolves from the one of a line, a drawn, physical line, such as a wall or a fence, to a zone, a perimeter. The consequence of shifting from a line to a perimeter are numerous and we will outline them in the current section.

Highly protected areas are usually understood as fortresses where the main stake consists in securing a border or strengthening a limit (Netz, 2010). However, such an approach fails to apprehend the increasing use of technologies in the shaping of what those "limits" are made of, and how they are being redefined through the use of technological devices.

But first of all it matters to redefine the system of virtual fences. "Virtual fences" can be defined as a set of interconnected technologies composed of radars, acoustic and thermal sensors, lasers and cameras. Merged together, those technologies allow for permanent and automated monitoring of "protected areas" which they redefine, both in terms of what falls under "protection" (and from whom?), and of how these areas are being delineated. Those new fences should allow for a constant and automatized monitoring of protected zones up to 30 meters thick.

But merging these pre-existing technologies in a satisfying way is a very demanding process. It requires the design of an architecture which brings together various shapes of materiality; hardware such as the above-mentioned, but also pieces of software and algorithms. The latter turn out to play a crucial role in connecting and synchronizing the fluxes of raw information together.

For that, instructions must be fed into the system so as to detect the figure of the "undesirable intruder", i.e. the physical body — a human body, a vehicle or so — which penetrates into the area and whose behavior can be categorized as a threat.

Virtual fences are still in an early stage of development, they are nonetheless being used already in border management and raise important prospects regarding their

implementation in prisons, nuclear or solar power plants, or cattle management. 'Virtual fences' hence make the case for redefining the very notion of "border", hence unfolding a particular politics of space that Razac calls "the management of permeability" (2009, 2013).

3.2 Management of permeability and qualification of spaces

Dealing with virtual fences require to pay close attention to their materiality (Aradau, 2010). As stated above, virtual fences are made of pieces of hardware and software which organize flows of information and modes of filtering such information. They do so through the use of algorithms and data-mining techniques (Rouvroy & Berns 2010). All in all, those technologies pave the way for new combinations with material fences, i.e. they are not meant to replace concrete, steel or barbwires, let alone vegetal fences, but instead to intertwine with such material fences. It would be the case for instance in prisons or around a nuclear power plant, where strong physical barriers are already put into place.

However, one could argue that virtual fence play around with the very materiality of surveillance apparatuses. This is not a new phenomenon. French philosopher Olivier Razac, in a short history of the barbwire (Razac, 2009; 2013), demonstrated that the barbwire belongs to a long history of de-materializing the fence, going from medieval fortresses with thick stone walls to fancy, thin steel devices such as the barbwire. What he shows is that there is an increasing sophistication in the way different spaces are being delineated one from the other. He contends that the less impressive are the means used to do so (materially speaking), the more they perform what they seek to perform: delineating one space from another with efficiency. *Less makes more*.

It would be a mistake, however, to assume that virtual fences are in essence dematerialized; we contend they just carry forth a different materiality. Protected perimeters are just as material as stone or concrete, but the materiality is to be found in other places and devices: cameras, sensors, radars, wires, hard drives, screens, computer scripts — softwares, algorithms. In a way, this materiality is even stronger than mere concrete, because it is much more distributed and can be found in many other and different locations, but this is not the point at stake. The point is that these plural "materialities" (Coole & Frost, 2010), tied together, form a new, distributed environment. These environments arise from various material components, technological components and pieces of software, but also the running algorithms which allow to browse from one to the other, back and forth, and concur to harmonize, regulate and synchronize the maximum of all the other components.

To this extent, the main current stake with the design of fences is tied with reconfigurations, *processes of space delineations* and subsequent *qualifications of spaces*.

3.2.1 Processes of space delineations

Typically, virtual fence raise prospects for furthering fences dematerialization processes, hence "opening up" the latter. This leads to a whole new situation. One could argue that the classical stake with fences was to reach a form of closeness, a strict fences which couldn't easily be trespassed. Yet such fences would be equipped with doors

and passage points, even in the strongest fortresses, because a minimal circulation must be reached in order to let people and supplies flow by.

Virtual fence potentially challenge this prospect by broadening circulations. Whereas classical fences could be considered as walls with a few holes, virtual fences could be considered as holes with targeted intervention. In there, as we shall argue later on, lies a new politics of the fence which belongs to the same developments as the politics of the drones, which qualify differently a space (i.e. respectively the zone of surveillance or the aerial space) and a mode of intervention (targeted instead of massive), and which operate through massive amounts of software interface (algorithms).

This broadening of circulation we call, after Razac, a "management of permeability". Virtual fences perform permeability, e.g. turning usual jail walls into more porous membranes. They allow for fluxes of circulations in and out of a perimeter in a more fluid way than concrete does, for instance. The default position is that circulations are allowed until proven otherwise, whereas physical barriers prevent circulations by default, unless specific decisions have been made to allow limited and controlled entrances or exits (doors, gates, etc.). So in this respect virtual fences allow for modalities of surveillance and control in open air, or open spaces, and this leads to changing the very qualification of those spaces *themselves*.

3.2.2 Qualification of spaces

As we mentioned above, virtual fence perform *ad hoc* ecosystems made of technological components, pieces of software and running algorithms. Put together, these elements shape proper ecosystems, i.e. an ecology on its own which lies between the many components of the system and their complex sets of interactions. This is where we see the script operating, the very *agencement* of the virtual fences, even though this agency never performs perfectly as it is meant to and is itself subjected to various perturbations such as the weather, the moment of the day or the night, the various kind of objects and their various shapes, the potentially threatening character of a detected intrusion within the perimeter, the speed of movement, and the like. In other words, the system is designed to perform a task (early warning, early detection of undesired intrusions), but at the same time it cannot guarantee it will succeed in doing so (there are too many variables at stake) and, which is of greater interest here, it is constantly overflowed by *something more* which it does, no matter how it functions on a technical basis.

This "something more" is a re-qualification of space. Let us consider a blank area, a zone where no device has been implemented, where people can circulate as they wish; the space will change irremediably if a concrete wall is built in the middle of it, and that those people can only belong to one of the side it thus delineates. If we now consider that this blank space is equipped with a "virtual fence" *dispositif*, what then does it do? Before we attempt to answer this question, we need to go a bit more in deep into the functioning of protected perimeters.

Virtual fences have multiple ways, each time specific, to collect, filter, classify, distribute and synchronize fluxes of raw information emitted by its technological components. To do so, they heavily rely on algorithms and datamining techniques. Only through such techniques can one hope to detect threatening behaviors and provide early warnings. Indeed, the system has to shape an understanding of what is threatening

and distinguish it from what it is not, and for that it needs to browse through massive amounts of data so as to detect abnormalities and to learn how to qualify them.

This kind of function — selection, qualification — has been coined “algorithmic governementality” by Rouvroy and Berns, who borrow the famous notion of “governmentality” to Foucault (Rouvroy & Berns, 2010). Governmentality is a term coined by Foucault to design “the conduct of conduct”, that is an art of governing which is essentially technical, which Foucault defines it as “The ensemble formed by the institutions, procedures, analyses and reflections, the calculations and tactics that allow the exercise of this very specific albeit complex form of power, which has as its target population, as its principal form of knowledge political economy, and as its essential technical means apparatuses of security” (Foucault, 2004).

In here we emphasized that virtual fence exert a certain kind of governemntality by filtering and discriminating “potential threats” or “abnormal behaviours” within the realm of the reality it apprehends. This selection can proceed inductively (from the various fluxes of information it organizes, by establishing regularities in commonly observed behaviours) or deductively (by matching behaviours it witnesses to predetermined behavioural patterns or models). For instance, one may walk alongside the nuclear power plant, on a bicycle lane, but what if one stops long enough to lace his/her shoes? How to discriminate the facts that this one crouches down for a while as “threatening”? That is the question raised by virtual fence and their own mode of governementality. Because in this sense it does influence the very behaviour one can adopt on a public bicycle lane, for instance. In this respect, by discriminating behaviours and learning how to proceed to early warnings of threatening intrusion, a apparatus as virtual fence requalifies the whole space that they cover with surveillance and, as a consequence, lead to a “conduct of conduct” insofar as people, knowingly or not, adjust their behaviour to the mechanism of surveillance.

In that configuration, what varies most is the sense of the “barrier” itself. The meaning of virtual fence would be far greater in “open spaces” such as public spaces, because this apparatus has the ability to constrain a certain requalification of a given space. They not only draw lines, they also — and that’s a distinctive feature — cover a space in its thickness (ca. 30 meters wide).

A good example of what virtual fences could lead to is to be found in the literature and concerns cattle management. In an article (Butler et al. 2006), the question raised is “how to incite a cattle to follow “spontaneously” the trajectory you want them to follow (most likely the shortest or most optimized one), without physical constraints?” Interestingly, in this paper, we noticed that cows tend to stick together when they are put in conditions of stress, and also to rush more effectively to a safe area — in this case their cowshed. So combined with hi-tech systems of surveillance which could be qualified as a virtual fence (as described above) the authors installed loud speakers so as to diffuse snake or tiger roarings. The lesson here is to take in the terms of “governementality” in that sense that, in here, virtual fence as a particular agencement are directed towards “the conduct of the cattle’s conduct” (even though the authors admit that if GPS tracking did work well, results are not yet satisfying when it comes to guide the cattle itself). It is oriented towards having the cows doing something you want / expect them to do. Of course, there lies the capacity but also the political danger of apparatuses like virtual fence.

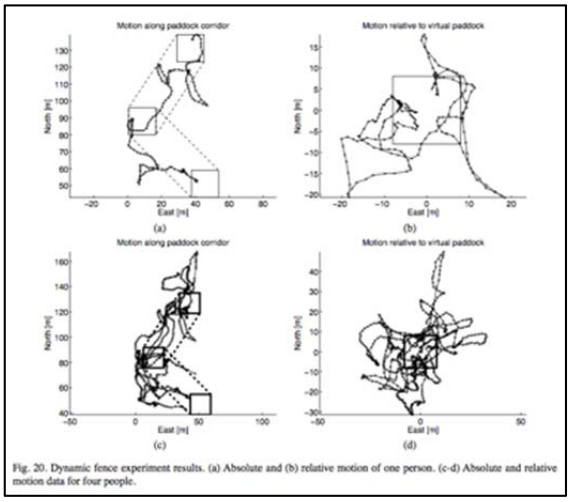

Figure 1: Butler et. al (2006), « From Robots to Animals: Virtual Fences for Controlling Cows », in International Journal of Robotics Research, vol. 25, n° 5-6, pp. 485-508.

If applied in Foucault's terms, one can now easily understand how virtual fence, by requalifying the spaces it covers up in terms of surveillance, may very well contribute to the control and management of civilian populations. Let us imagine that malls could be equipped with such systems, let alone public spaces. One could very well figure that those complex technologies might prove useful to orient consumer's paths towards specific locations (where most likely there is more business to be made) or, far better, that the whole architecture of malls could be redesigned according to new possibilities provided by "soft guidance" of targeted populations. Of course, this is only a scenario and a prospective idea, it has not been tested on various publics, but still it can have us think about what virtual fences entail politically.

It also reverts the very means of surveillance; the whole considered space is under passive surveillance (unlike surveillance carried out by guards which demands attention). Here, attention of the system is only triggered by the early warning. This implies targeted interventions instead based on an analysis of each and every detected behaviors, instead of allowing for a potential randomness in the application of control (even though the control can be "total" ex post, by watching surveillance videotapes, provided there are enough to cover the whole zone, with virtual fence it could be total "in real time" — that is at least the ambition of the project to lead to that technological capacity). This is where the shift occurs: the question is less to enclose a targeted, limited population (e.g. intelligence services to detect potential terrorist) but rather *to ensure the possibility of manhunt* for the one person who manifests an "abnormal behavior". The stake becomes how to detect and discriminate, in a crowd, or at least in a great amount of apprehended behaviors, the ones which are being critically threatening? In so doing, virtual fence systems would elaborate a model of "point and click", detect and act upon (Chamayou 2006).

This is where our working hypothesis comes near to completion: when virtual fence no longer narrow the lines which delineate an "inside" from an "outside", but rather mark out a space in squares of surveillance and produce it according to a specific function: the ability, in such a space, to apprehend each behavior as potentially threatening and to effectively intervene upon the ones which most characteristically fit the system's definition of the threat (be it inductive or deductive). It could be, for example,

the production of the security-space. A space within which a whole population is, knowingly or not, subjected to the possibility of intervention, and in return adjusts its own conducts and behaviors to the system (hence being subjected to the particular governmentality of this *dispositif*).

3.3 The modes of existence of a virtual fence

Gaining insight from Latour's work on Modes of existence (Latour, 2012), in this section we further the analysis laid out in section 3.3. We do so by addressing what Latour calls the different modes of existence, in this case of a technology such as virtual fence. Objects and people, Latour argues, can be apprehended and analyzed in different manners according to how they echo in experience, and each of these manners translate in a different view point on the stakes raised by the considered situation. Applied to virtual fence, three modes at least seem relevant: the mode of existence of technique (what if we understand virtual fences as a technique?), the mode of existence of organisation (how would virtual fences fit into a particular organization?) and, lastly, the mode of existence of "the habit" (what are the specific habits, if any, that virtual fence as a technology can develop by itself, how does it interact with its environment?).

3.3.1 Dealing with the technique *and* uncertainty

First of all, generally speaking, algorithms consists of rather particular technical objects. It is shaped like an organization. At least, one could argue it resembles very much some specific kind of organization. For instance, an algorithm can be called a « program » or a « script », i.e. an organized set of instructions, orders calling for the execution of a specific course of action[1]. The very roots of this similarity are probably to be found in the particular relation between algorithms and material components or, say, forms of materialities (broadly speaking). It does not really matter whether the algorithm runs on a 32 bits computer or a 64 one, that it is written in this or that language, Python or C++ ; that some divergence can be found in the binary serial which translate and operate it and which represents differences in tension. As a matter of fact, during second World War, first *computers* from Los Alamos would turn out to be… women in the flesh ! These women were mandated to solve impressive systems of differential equations — literally *to compute* — in order to model the shockwaves emitted by atomic fission bombing. In this respect, the genealogy of an algorithm can be understood as a succession of *metamorphosis*, each of these consisting in a proper invention on its own. What happens throughout this chain of successive metamorphosis is a reordering of the series of instruction delivered by the algorithm, e.g. the optimizing of a sequence which allow for reducing its inner complexity.

In the case of P5 we deal with algorithms which potentially detect threatening behaviors in a security perimeter. More precisely so, it is a specific tool designed in order to think *the very conditions of possibility of intervention in a certain environment*. For example, in the case of prisons, the kind of questions asked could be « what consequences this still inexistent system would give rise to, from a variety of standpoints : prisoners', guards', para-penitentiary workers, prisoners' allies outside of the prison,

1 A same "body" (computer) can execute numerous and varied scripts (algorithms). A computer is regularly provided with conflicting instructions (Latour, 2012, pp. 399-400).

but also other technical objects ? ». As simple as the technical tool might be, it is impossible to predict the whole set of uses and abuses it will be subjected to.

This point is convincingly made by Razac and Nietz regarding the barbwire. In their view, the barbwire cannot ever be considered as a mere means to reach some ends. As an object on its own, it *does produce* a considerable amount of effects, some of which human beings might very well use to serve their own purposes. This does not imply that other potential effects, other potential ends tied with the object itself, will never be actualized. Barbwire has first been invented to protect crops in the fields from cattle (who would gaze in the wild) ; then soon enough this use was reverted so as to shut up cattle in delimited areas ; later on, it was used to build low-tech and cheap barracks ; yet later, combined with automated riffles it will be used in the World war's trenches i.e. opening an era of "position battlefields"; eventually, it was used in order to delineate concentration camp from the outer world, in the English ones as well as the German Nazis ones and the Russian gulags. One understands very easily that these last uses, dramatic as they were, could not have been planned by barbwire's inventor and first users. The possibilities raised by technical objects are potentially endless, and the uses it raises cannot be predicted[2].

As soon as engineers work on a sophisticated enough kind of algorithms, they are overwhelmed by it, in the sense that they cannot analytically predict the "behavior" of their own invention. Even though they created and coded the algorithm from scratch, and know exactly how it has been done, they cannot predict exactly how it will works and what kind of functioning it will have. In other words, they face something which we could call a "grey box"; they need to experiment, modify, and re-experiment with their algorithm before they can assert something about it.

In other words, this inner unpredictability of algorithms requires to be qualified with other terms, in order for the de-scription to be more accurate. So when it comes to an algorithms such as the one we are busy with here, which must discriminate whatever shape penetrates within a certain security perimeter and determine whether this intrusion poses a threat or not, we must say this is *a sorting algorithm*. This description qualifies its function. It is fed with large sequences of images, and through the combination with many other running algorithms, this one appears to be able — or not — to detect where are the objects in motion to "look at", which kind of objects that is alongside predetermined categories (e.g., human / animal / vehicle) and each of those moving objects requires a matching qualification with one of these three categories. That is for one thing.

But this algorithm we focus on in here is also a "*machine learning"* algorithm, which means that it ought to be able to "learn". In a sense, it learns inasmuch as it is "*trained*". It needs to *practice and experiment* — constantly repeat a process of trial and errors. For instance, it is provided with a set of image sequences, and for each sequence it is instructed whether or not it should identify a threatening moving object. This sequence can be considered "regular", "normal", but this other one is "abnormal" hence potentially threatening. These sequences need to be carefully crafted by algorithms designers, which is a very demanding process. In order to proceed to these tests, for example, engineers often have to play roles and to stage situations in order to "capture"

2 In that sense, it can be said that they always bound out of scripts.

them (e.g. in the form of video footage) and feed their algorithms with this data (staging prison guards, people passing by, evading inmates cutting a wired fence, a vehicle penetrating the protected area very fast, etc.). All this data is very demanding to generate dans deal with. It takes an accurate synchronization of the sensors; their geographic position must be established with great care and precision; different meteorological conditions must be tested, etc.

The inner structure of the algorithms allows it to run on various subsets of images or, say, data fluxes. It is able to apprehend different variables in order to find identical "patterns" in the data it is provided with so as to classify this data, when relevant, as "threatening". The more it learns, the more it is able to match these "models" it has been fed with to actual situations captured by the interconnected technological devices. The more it gets the more it becomes able to deal with new images. Thus, departing from the very same algorithm, it is now perfectly conceivable that even the slightest variations in the training will result in different ways to react, i.e. different ways of discriminating within the realm of reality what is threatening from what is not. Trained differently, the algorithm reacts differently.

For these reasons, we wish to emphasize that virtual fence as a set of technologies interconnected through algorithms have to deal with a great degree of uncertainty. For a great deal of variables needs to be handled by the whole setting and the possibilities for variations are countless, let alone potential conflicts which could arise between different settings, one being incompatible with another. In this last case, yet a choice still would have to be done in such a way that pros and cons might by any means result in a purely efficient solution. So in this section we underline that understood as a set of techniques, virtual fence probably cannot achieve the goal of carrying out ascertained results, but this does not only speak to the rate of "false alarms" — which could probably still be reduced in the future — but also to the very definition of the intrusion, of the threat and of the behavior.

3.3.2 Inserting in a social context

So far, we understood virtual fences as mere techniques, or technologies, but the literature in social science contends that studying a technology in itself is pointless insofar as it is detached from the social context it is meant to integrate (Pinch Bijker). True enough, it might be that nuclear power plants, for example, are "out of the world", in that sense that such facilities are highly secured through spatial and material borders. Yet, there is a whole circulation of workers, maintenance staff, cleaning staff, management staff, catering and other services and one understands easily that it might lead to some difficulties when it comes to implement a technology like virtual fence: lots of movements to handle back and forth, to apprehend, analyze and translate in the terms of a potential threat to security. Even with a sole entry point, a secured portal, what of someone who penetrates through it with an unidentified package under his arm, which might turn out to be a homemade bomb, or for what matters a mere vacuum? So, obviously, even in a case as "closed" and controllable as a nuclear power plant, the situation actually rise many difficulties. And still, one may assume that all the people involved on the secured site are, in a way or in another, professionally committed to work for that site or, on some occasions, benevolent visitors.

One understands easily that it might not go that easy in a more conflicting situation such as the prison, where prisoners and guards, guards unions and management might entertain very different and irreconcilable views on their respective roles, desires

and, more generally, their own relations to the prison. Usually such contentious points are eluded, or at least overlooked, when it comes to unfold the technicalities and specifications of a particular technology. What knowledge do we have and can we have of how harmoniously a technology will insert itself in a social setting? But this is very important: on answering this question depends the very conditions of the technology to be successfully implemented, its very "social acceptability" so to say.

In here, we refer to "social" not as a predefined entity which is made out of Society in its entirety, something which we think cannot and should not be addressed by the means of scientific knowledge in social science. "Cannot" because we tried it out, but we demonstrate in section 4.3. why public opinion polling is not satisfying in case such as "virtual fence", where the matter at stake is still prospective and does not allow for discerning a "public" which is impacted / concerned by this technology. If that was the case, then it is important to underline that it takes considerable means to reach out to a body of people large enough for claiming representativeness. But assuming it would be feasible, we also contend that we "should not", because as social scientists we cannot claim to represent the whole "Society" even through the finest research apparatuses. The publics we address and deal with are always fragmentary and partial, situated from a certain point of view (their professional stakes, their personal bonds, their citizen activities, and so on), and only in this condition can we learn something consistent as we demonstrate in section 4.2.

If one thinks for example about a prison guard, and as a technology such as virtual fence to complement this guard, or to assist him in his role, which consists in carrying out prisoners' surveillance. There are a lot of assumptions in this scenario, and to start with the assumption than the primary role of a prison guard is to carry out surveillance. It could be argued that his role implies far more something like "control" as in "controlling prisoners" and avoiding a riot in the facility. But this changes everything, because in this shift control can take many ways, and not all of them implies surveillance and its technologies. For instance, in a purely technological view, the function of surveillance would equally be filled by guards so that they would be competing with cameras, radars, and so on, until the day where the technology would fill this function better than humans — the guards would then be replaced. Of course, P5 does not sustain a scenario that simplistic, but symmetrically we argue that the necessity of thoroughly thinking the implementation of the technology in its social contexts is a work which remains largely to be done. And this work cannot be done by the sociologists or philosophers alone, since it implies engineers and designers just as well, but also all the impacted publics of the technology (here the guards, the prisoners, the unions, other prison workers dedicated to food and cleaning, the management, and possibly the visitors). This is *in* the prison, but before the technology actually comes to prison, there is countless developments from its commercial development and exploitation to its approval on markets, which is when relevant public administrations must be convinced that such a tool is needed in penitentiary facilities, and so on, so forth.

As it turns out, just to take again this one example, the prison guard actually does much more than watch out for prisoners: he talks with inmates, he authorizes exceptional releases, he prevents suicide, he tolerates certain formally prohibited actions such as soft drugs consumption — all of that for the sake of well-being in prisons, as much for the inmates than for the guards. There are constantly all sorts of negotiations going on between prisoners and their guards, in every prison as in every form of social life, and this cannot be reduced to one single problem at once: how to achieve good

surveillance? There are many more problems, they do intersect each other, and most likely different publics care for different problems.

It becomes problematic when the technology does not or is not able to take this reality into account. What of a technology so strictly programmed, which leaves so few space for negotiations, bargains and so on? The risk is not an hypothetical one, some technologies work simply too well from a technical point of view and that makes them undesirable partners in the social game. Several of our interviewees pointed out to examples of technologies which had to be deactivated after a short while, because they would trigger a signal totally out of purpose, or not in an appropriate timing, or yet it would signal way too much so that no one wouldn't pay attention anymore to the signal itself (it then becomes very loud and annoying). The examples are abundant.

To take but one example, we here report a notorious practice in prison which is known under the name of "yo-yo". This practice consists in throwing objects rubbed in a towel through the bars of the window, from one cell to the other. This object can be anything, ranging from cellphones to drugs, etc. The package is thrown to the next cell, and can travel from cell to cell until it reaches its destination. Obviously, the penitentiary staff is very well informed about this practice, since many attempts at throwing these objects do fail so that they fall on the floor or remain stuck in some wire nettings, usually on places where prisoners do not have access so as to get them back (but where the staff does). We heard stories of members of penitentiary staff putting strategies into place so to be in a position where they knowingly cannot see this "yo-yo" practice being continued and failing from time to time as it were. They could enforce and interdiction and be very strict about it, but they won't because it is not part of what life means in a prison — unless you want to make it an unbearable living and head straight to a riot.

So, to come back to sophisticated system of virtual fence, the odds is that such a system could detect the succession of throws in the air. How would it react? How should it react? How could it react otherwise? Which malleability, which parameters could fit the prisons' needs? The technology might very well succeed, i.e. by emitting an alarm for each object thrown in the air, to prevent this particular practice of "yo-yo". But then, unavoidably, it will have moved it to somewhere else, in another location and through other gestures or subterfuges. It could be argued that powerful technologies will slightly circumvent the area of the prison so that no location, no practice is no more allowed, so that the control over prisoners is total and inescapable. However, recent experiences in French new penitentiary facilities show that environment too clean, smooth and controlled lead to strikes and riots from the inmates, so as it appears in this situation that technological equipment and social peace are the two terms of an alternative which appears not likely to be solved by means of consensus.

The general point about virtual fence in social contexts is that the former considerably perturbs the equilibrium of the latter, may this equilibrium rest on maintaining peace or sustaining conflicts. At least, a powerfully performing algorithm tied with state-of-the-art technologies could enforce rules blindfully, whereas social contexts are made of complexity, negotiations and subtle balances which can accommodate such a strict enforcement only with a great deal of difficulty, and through an extensive process of *reconfiguring the milieu* in which such technologies will take place. Another possibility, as mentioned above, is that the technology is purely and simply disconnected because the organization cannot deal with the perturbation it carries forth. Put simply, if a technological setting functions too well, the social organization necessarily dysfunc-

tions, alongside lines which cannot be predicted and controlled but call for experimental trials in situations.

3.3.3 Constructing a perceived environment; the *umwelt* of virtual fences

It is very well known in social sciences that we remind ourselves of all the technologies in our lives only when they fail (typically when they break down). Suddenly, their presence is not obvious anymore and requires some consideration, at least to fix the breakdown. This is important because it implies that our relationship with technologies is based on forgetting they surround us and we use them all the time. So in this section we raise the hypothesis that in every situation, efforts should be made to remind where virtual fence originated, why they were implanted in this or that area, with which purposes, and having a constant attention to what it perturbs. In this case, the question is not to pay attention to what a technology is capable of, nor to how it is inserted in social context, but to learn how to deal with the disruptive presence of the technology itself, in situation.

For instance, it might very well be that in a particular situation, some people can very well afford to forget about this very presence of the technology ("it is there, it performs its tasks, and so what?") but some cannot ("if I forget about this technology, what will be the consequences onto me, what risks will I be taking, can I afford to forget it?"). Let us imagine again a setting where some people control the lives of some others, where there are guards and people in their custody. In this case, it is easy to understand that the latter will not be able to forget about the technological settings in their surroundings, because their acts and behaviors can potentially be captured, analyzed and reported to the authorities in charge. Unlike people "who don't have something to hide", some people do have some things to hide for which they cannot necessarily be blamed by advance. But our point is that these people know exactly that they must deal with the silent presence of technologies and what they perform or, better, *could potentially perform* in the very spaces where the subjects of surveillance circulate around.

This conscience of the presence, e.g. of a virtual fence system, could trigger some unattended reactions. In the case of machine learning algorithms described above, one could wonder if for instance a prisoner could be able to "adopt" an algorithm. Let us suppose that an inmate noticed that an alert is emitted each time he runs or walks fast through a corridor, but remains silent if he slows down the pace. He could legitimately infer that the technology comes with a "user notice" and that it is possible to learn how to use it and play around with own codes. To further this example, we could think of a prohibited behavior which an algorithm could have been trained to identify and report. What would happen if someone willing to adopt this reprehensible behavior decided to trick the algorithm by mistaking him, through a long and patient "unlearning" process, by installing regularity in a quasi-prohibited behavior, flirting with the limit but never crossing it? Could that person slowly lead the system to consider this game as "normal" by repeating constantly a quasi-similar pattern of behavior, day after day, until at some points this behavior appears perfectly normalized and cannot give rise to an early warning anymore?

Of course this remains a speculative hypothesis, but still one could wonder if the technology could or not be tricked under such "experimental" circumstances. Of course a particular algorithm cannot learn from everything at once, its very learning processes are bounded by its code and even by other algorithms as in the case of meta-heuristics.

Nonetheless, its function within a system such as virtual fence may very well consist of looking for local optimums depending from a certain and limited amount of predetermined parameters. And we argue that someone with a fine understanding of this functioning could eventually learn how to trick it.

If that working hypothesis proves true, then there is a very important consequence to it. The system is designed to be adaptive to its environment and attempts at discerning in a certain realm what situations can be understood as a potential threat. It does so through a *daily and customary learning*. There goes the consequence: if the sensitivity of machine-learning is fine tuned enough, in other words if a genuine learning process occur, then it is necessarily experimental, made of trial and errors; the algorithm has to run hypothesis from the data it is provided with, and match them with models. Doing so, little by little, it *elaborates a perceived environment* on its own.

Virtual fences need to stabilize an environment by reducing its variables (rain, daylight, and so on) but doing so they also actively produce this environment. The learning needs to understand what environment it deals with before it could detect intrusions, disruptive elements within that environment. To do that, it needs *criterias* as for what counts as environment and what does not (from the designers and coders of the system), but our hypothesis goes a bit further. Beyond the instruction it is provided with, we argue that machine-learning themselves lead to “fabricate” or “construct” their own dedicated environment, and that this process needs by any means to evolve constantly (i.e. to keep on considering a growing three as the same three in that environment). In other words, we could say they partly produce their own environment.

The implication of this statement is important in terms of social acceptability. Because then social acceptability cannot be granted once and for good, precisely because the system is doomed to evolve over time and reconfigure all at once the acts it perceives as threatening and the environment these acts take place in. Back to our social contexts, it means that the issue with virtual fence would not be to adapt to them (as if they were intangible, taken for granted), but rather to find a dynamic way to deal with them, some sort of modularity in the relationship between this set of technologies and its social contexts.

In the very powerful sense of the term, we could say that *virtual fence do compose their own landscapes,* what Von Uexküll called an *umwelt*, i.e. a perceived environment, an environment as experienced (Despret, 2009). This is the very condition in which they can operate. The background upon which an intrusion could be detected is a necessary step in the way they operate. In yet other words, virtual fence produce — at least partly — their own realm of reality. And this is precisely the reason why it matters not to forget about their presence, because on one day it is never the same technology we deal with than the day before. The construction of their own perceived environment by virtual fence and their algorithms calls for a dynamic conception of social acceptability, constantly subject to negotiation and revisions as time passes by.

3.3.4 Normal behavior definition

According to Foucault (1995), penitentiary system was instrumental in defining normality. Humanization reform of the European penal systems in the 19th century introduced a shift from reactive to proactive judgment, aiming “not to punish the offence, but to supervise the individual, to neutralize his dangerous state of mind” (p. 18). To achieve this judges relied not only on the law, but increasingly on indirect judgments, -

of a suspect appearance, general knowledge of his behavior and estimation of the future one, the circumstances of a crime, etc. By adhering to these methods, the judge delivered more than a legal judgment – he delivered "an assessment of normality and a technical prescription for a possible normalization" (p. 21). To help the judge, a network of subsidiary judges was created, such as doctors, prison staff, scholars, etc. Together, delivering "assessing, diagnostic, prognostic, normative judgments" (p. 19), they transformed the penal system and "behind the pretext of explaining an action, [developed] ways of defining an individual" (p. 18).

Foucault also attained that prisons and their sole materiality represent "an instrument and vector of power" (p. 30) over people, where human bodies are considered as objects of knowledge. By erasing material boundaries between prisons and the outer space, virtual fences extend the boundaries of prisons and the network of knowledge collection, subjecting outside public to the judgment of normality. This brings an important problem of defining normal behavior. The dominant literary scholarship reveals two major approaches to behavior recognition – statistical (Bartlett, 2011; Helzer, 2002) and species-typical (Daniels, 1985; Sabin & Daniels, 1994). Both of these methods will be critically studied below.

Evaluating behavior: statistical approach

Antonakaki *et al.* (2009) posit that behavior recognition by the means of statistics recently gained importance for a new niche of smart surveillance that aims "to automatically model and identify human behaviors, calling for human attention only when a suspicious behavior is detected" (p. 1723). In statistical approach, normal behavior is determined by the numerically dominant group, classifying minorities whose behavior differs as abnormal. Helzer (2002) explained statistical approach by using a bell-shaped curve, on which they allocate all studied behaviors. Those falling in the middle range would be classified as normal. Those deviating to either left or right would be considered as statistically rare, atypical of the group and accordingly placed in the abnormal category. This basic method lies at heart of most advanced models applying statistical calculations.

Presently Information and Communication Technologies (ICT) specialists approach evaluation of normality through building an automatic algorithm based on statistical modeling (Rabiner, 1986; Brand, 1997; Oliver, 2000; Moeslund, 2006, etc.). According to Yamato (1992), to be successful, the algorithm, - a final product embedding all the modeling, categorization and computation, - needs to learn as many human actions as possible to recognize them as a correct (normal) observed sequence based on bell-shaped distribution or similar methods. Yamamoto claims that once that is achieved, there exists a "possibility of establishing a person-independent action recognizer" (p. 379).

A study conducted by Antonakaki et all. (2009) looks into human behavior definition by the means of multiple cameras with overlapping fields of view and in this is similar to the virtual fences project. The authors use a statistical approach to abnormal behavior, defining it as infrequent. Their algorithm is built on normal behavior models and uses two classifiers. The first one, short- term behavior, analyses brief behavior within limited area, such as walking, running, sudden movement, etc. and decides whether this behavior is normal against built in normal instances. Trajectory is the second criterion and is based on projected scenarios, built in by the authors for a specific context. The classifier determines whether a studied trajectory is normal, that is following the pre-

dicted trajectory. If either of the classifiers recognizes action as abnormal, the system issues a security alarm. The system indicated abnormal behavior accurately in 84% of cases, which authors considered as highly encouraging. However, authors admit limitations to their model, mostly associated with dependence on input videos and therefore inability to adequately detect underrepresented behavior.

Zhong et al. (2004) and Boiman and Irani (2007) use the alternative method of algorithm learning, when a system stores a big database of all the observed behavior instances, already labeled as normal or abnormal patterns. When a system studies a new person, her behavior is compared with database patterns. The obvious drawback of this method is the need to constantly update the database because if a previously unknown behavior is detected, it is automatically classified as abnormal.

As briefly mentioned above, statistical definition of abnormal behavior sparks some problems. French philosopher Desrosières (2008) criticizes statistical approach based on a number of principle and most importantly on "the quality of quantity." Desrosières viewed statistics as a tool for governing populations, not just reflecting on reality but "creat[ing] new ways of thinking, representing, expressing and acting on it" (back cover) and claiming that different people cannot be judged by same categories. When applied to definition of normal behavior, Desrosières's position would translate to the following. Firstly, a large quantity of people engaged in certain behavior would serve as a criterion to judge that behavior as normal. Secondly, numerical factor is too narrow of a criterion to define normality. Instead, human behavior should be judged against multiple dimensions. Finally, statistical approach only seems objective and instead imbeds personal judgment, respect for "impartial" indicators and calculation based on disputable standards and methods. According to bioethicist Synofzik (2009), "inferring normative obligations from statistical normality would lead to ethically highly questionable consequences." For instance, phsychosociologist Ramsden (2013) acknowledges that statistical computation of normality "implies that being average is desirable or healthy" (p. 19), restricting the freedom of expression and choice in a society based on conformity to social standards. Therefore, statistical approach to behavior definition suffers from severe limitations, primarily not accounting for underrepresented groups.

Evaluating behavior: species-typical approach

Species-typical approach defines normal behavior as a common state for particular reference group depending on social and cultural environment. Bartlett (2011) posits that defining normality in a social context is also achieved by accounting for generally accepted standards of human behavior as main evaluation indicators. The problem with the standards of social behavior lies in big variations in social setting and norms typical for certain groups. Standards' limitation follows from their definition as "ubiquitous but underestimated phenomena that help regulate and calibrate social life by rendering the modern world equivalent across cultures, time and geography" (Timmermans & Epstein, 2010, p. 70). Standards, just like scripts, have prescriptive nature as regards ethics and values and frequently in fact disregard the social, cultural, individual contexts.

Implying the "lowest common denominator" (p. 79) of how people should behave, standards render as abnormal parties non-conforming to the dominant group beliefs.

According to Ramsden, human behavior should always be evaluated in the given context and abnormal behavior should always be judged "with regard to a specific time

frame, social norms and expectations of behavior for that venue/place and it must be judged against what is 'normal behavior' and normal expectations" (p. 9). Ramsden argues that the way people behave is dependent on different factors, such as gender, ethnicity, culture, etc. – "If lifestyles, culture and world views affect how we behave overall it would logically follow that it affects the expression and determination of abnormal behavior" (p. 13). However, this makes it hard to categorize human behavior because of large variability. Synofzik (2009) also points to the difficulty in identifying species- and social group-typical functions and to what extent they prevail.

Hence, species-typical approach attempts to draw on social context when defining human behavior, however fails to do so relying on social standards as evaluation criteria.

Normality definition: construction of truth

Reviewing statistical and species-typical approaches to normality revealed that no strict definition of "normal" behavior can be found. Szasz (1960) refuted the idea of abnormal behavior as such, saying that it all depends on a perspective one is coming from and that people classified with abnormal behavior are denied of a chance to fit in the society at large. Other scholars indicated that the concept of abnormal behavior was created to govern social order by controlling and straightening up individuals behaving in unusual ways (Scheff, 1966; Sarbin & Mancuso, 1980). Therefore, normal behavior definition is also a political function of what is considered to be normal under given circumstances, what is socially acceptable.

Since society grows and develops, social relations are a dynamic process. Accordingly, Foucault (1991) viewed normality as temporal and individually- and socially-embedded, arguing for a constant "rediscovering [of] the 'norm'" (p. 16). Therefore, normal behavior is also an evolving process, a consensus on what is considered to be normal for a social group in given time.

Thus, no fixed definition of "normality" can be provided since it is a social and political construction, permanently updated and re-negotiated. This makes defining normal behavior and programming it into technology in the forms of algorithms a challenging task that requires a lot of consideration and context emersion.

4 Methodology: how to constitute deliberative arenas and a concerned public?

In this section we call for constituting deliberative "public arenas" for virtual fences (Hilgarner & Bosk, 1988). According to our previous findings and working hypothesis, it is best to deploy a wide array of research investigations and participatory inquiries so as to broaden the scope of prospects for virtual fence.

In this section we unfold different problems that were raised during our studies such as the ones of algorithm construction and responsibility. We then call for drawing on different "deliberative arenas" where the technology at stake can be discussed and put into perspective by different publics. Then we undertake an analysis of different arenas we briefly explored in the limited amount of time we had. The "internal arena" draws on P5 partners insights, i.e. engineers and developers of the virtual fence technology themselves. The "contextual arena" let us imagine a situation where virtual fence could actually be implemented such as in prisons. From this case study, it infers some comments on the integration of technologies in its social contexts. The third arena is a "general public" arena. While the two firsts rely mostly on interviews, the third one relies on an online survey which turn out to be inconclusive for many reason which we explain, the principal being that virtual fences are still at a too early stage ("in their infancy") so that they don't come along with precise "publics" from whom we could gather "representativeness". Lastly, we unfold the prospects for a "participatory arena", implying well-delimited publics in deliberative settings.

4.1 Deliberative arenas

The first section, "internal arena", relies on a structured questionnaire we displayed during a meeting that was held at Sagem premises in March 2014 to the P5 consortium meeting. In addition, we carried out semi-interviews with some specific members of the consortium, but not all of them. We also provided, as customary in social sciences, extensive field notes and observations, during the consortium meetings and all the informal interactions going on at these occasions. For obvious confidentiality purposes, we made sure that none of the respondents could be identified by reading this report. While our structured questionnaire was anonymous, yet given the limited amount of respondents one could have inferred their identity, we made sure this could not happen in the present report. We acknowledge that this methodology remain lim-

ited if the purpose is to generate a genuinely deliberative arena. Originally it was planned that a collective workshop / focus group with the consortium partners and a couple of external experts would be held during the meeting in Namur planned by September 16-17th. However, the late cancellation of this meeting and its rescheduling in Amsterdam made it impossible to maintain this exercise. We intend to carry out a similar for of exercise when the Namur meeting is rescheduled or at a later stage of the project.

The second section relies on targeted qualitative semi-structured interviews. We interviewed a limited amount of key experts of the field of prisons: academics in criminology, prison architects, members of civilian commissions on prisons, administrative staff. In addition, we extensively browsed the literature on prisons, from the first *Groupe d'information sur les prisons* lead by Michel Foucault to late information report on the Belgian penitentiary sector. This, we believe, also remains limited in scope. As a matter of fact, a deliberative process should happen first and foremost with the first population impacted by the potential installation of virtual fences: prisoners themselves. However, administrative procedures and access to prisons is a very long process, which has to be initiated a long time in advance and without guarantees of success. While we initiated those requests, so far they remained unsuccessful. Yet it is out contention that the material we gathered is comprehensive enough to provide a textured overview of the context-sensitive requirements of the field of prisons for the application of virtual fences.

The third section encompasses a more traditional quantitative survey, with qualitative features. It was conducted online and displayed primarily through our professional networks, due to the lack of resources to properly constitute a targeted population (this is also due to the difficulty that virtual fence are still potential in scope and not yet actualised). It is also due to the costs of randomizing a sample at the level of "society as a whole", which exceed our limited capacity in this project. While we present all the flaws of this methodology and its very limitations, we also seek to emphasize some key learning points from this experience.

Lastly, we draw a short conclusion from this section by identifying the different problems and different publics which are core to our study and which should find prolongations in the near future.

4.2 The internal arena: perceptions of the consortium partners and the question of normality

4.2.1 A formal qualitative questionnaire-based approach

Questionnaire with the partners: one of the key findings is that virtual fence can be and are apprehended from a variety of institutional belongings and perspectives (unsurprisingly perhaps, consortium members tend to favor virtual fence applications which are of uttermost interest to their host institutions).

The questionnaire revealed that a significant majority of respondents could be identified as engineers, developing technological software components and algorithms but also "user needs and system requirements" (E4). The other respondents could be

named industrials, being responsible for overall technological development, evaluation and implementation. Consequently, respondents will be mentioned as either Industrials or Engineers (I1, E1, etc.) according to their professional belonging for the purpose of anonymization. For the same reason, no identification other than professional area was required.

When asked about the main purpose of the virtual fences, the respondents mainly concentrated around the words “preventing”, “detecting”, “informing” and “counting”. For example, E2 defined the purpose of virtual fences as “preventing unauthorized access into a certain secure facility,” emphasizing preemptive and selective nature of this system. E1 provided another definition, identifying the mission to “detect potential intruders trying to enter a secured area,” raising the issue of detection and intruder evaluation, however not mentioning any criteria according to which a person can be classified as a “potential intruder.” E5 brought up the topic of early warning, saying that virtual fences need “to alert the operator of people being in areas where they shouldn’t be, or people approaching fences,” giving a rather reactive definition. E8 in contrast highlighted a proactive goal of virtual fences to “give warnings about (possible) intruders and other (potential) threats.” E3 and E5 considered another peculiar mission of virtual fences, that of “count[ing] the number of people coming in or out,” that could be used as statistical evidence for reporting on area surveillance. Therefore, according to engineers and industrials, the main purpose or script of virtual fences consisted in early warning of surveillance operators, detection and prevention of unauthorized access to site premises and statistics on income-outcome population fluxes. These goals also identified the primary actors of virtual fences network as end-users in a broad sense or security operators in a narrow one. Already here respondents approached the subject of discrimination between threatening and non-threatening situations, leading to the question of normal behavior definition.

Approaching the topic of normal behavior, all respondents admitted that it differs in particular situations. Despite this, when asked to consider defining normal behavior for one of project’s scenarios (protection of solar, nuclear plant, border, etc.), the author traced a dominant judgment pattern. Majority of respondents exercised statistical approach to normality, indicating that “a normal behavior is something that must be comprehended by observing the place for a long period of time. Once we have observed the normality, we could detect abnormal behavior as that differs from normality” (E2). What follows from this statement is that normal behavior is frequency-dependent, with higher occurrence constituting normality/abnormality belief and thus mirroring a bell-shaped curve approach, outlined in theoretical part (Helzer, 2002). E4, along with E7 and E8, reflected latter belief: “I’d say that normal behavior is a statistical property. Normal means what is common,” accordingly judging normality as a widespread, regularly occurring phenomenon. As indicated by Ramsden (2013), it seemed easier for respondents identifying abnormal behavior rather than normal in applying certain scenarios. For instance, I1 admitted that “normal behavior is more difficult to define ... In virtual fences of a solar power plant, abnormal behavior is approaching the fence at certain periods of the day and attempting to climb it.” E5 followed a similar line of thinking, pointing that “there could be a jogging track right outside the fence and then it is normal for people to be running, while it is not at all at another location.” Other respondents also provided context-dependent examples and consequently delegated normality judgment to different actors but themselves. While some believed that “it is the security personnel who can define normality” (E1), others stated that this is a function of facility owners (E4). No respondent mentioned personal involvement in delivering normal behavior judgment. Therefore, in line with ICT approach to normality

definition, engineers and industrials demonstrated personal delineation from the process of behavior evaluation, predominantly relying on statistical strategies as objective representation of reality, although admitting complexity of the task due to varying contexts.

Since the respondents indicated that identifying abnormal behavior would be an easier task, they were later asked to provide key characteristics of abnormal behavior to qualify for an intruder and trigger security alarm. Two main features were primarily mentioned, - unauthorized access to protected area (E1,3,5,8, I1-2) or access through a non-projected path (I1) and evident malicious intentions of a subject witnessed by accompanying gear (E2,4,6,8). If the first criterion could be incorporated in the security system by appropriate sensors, feasibility of the second one remains unclear. Engineers stated features, such as being "a person"(E1), "suspicious"(E3), having "bad intentions"(E1) or "trying to disguise oneself"(E4), as those that also could activate normal behavior algorithm and trigger alarm, maintaining however, that "intent to intrude is in the mind and may not be visible to sensors"(E4). Therefore, in parallel to a stated objective statistical approach, engineers and industrials also approach behavior based on evidence (trespassing) and subjectively, introducing such categories as "suspicious" or "bad intentions" in the judgment (see Figure 2 below).

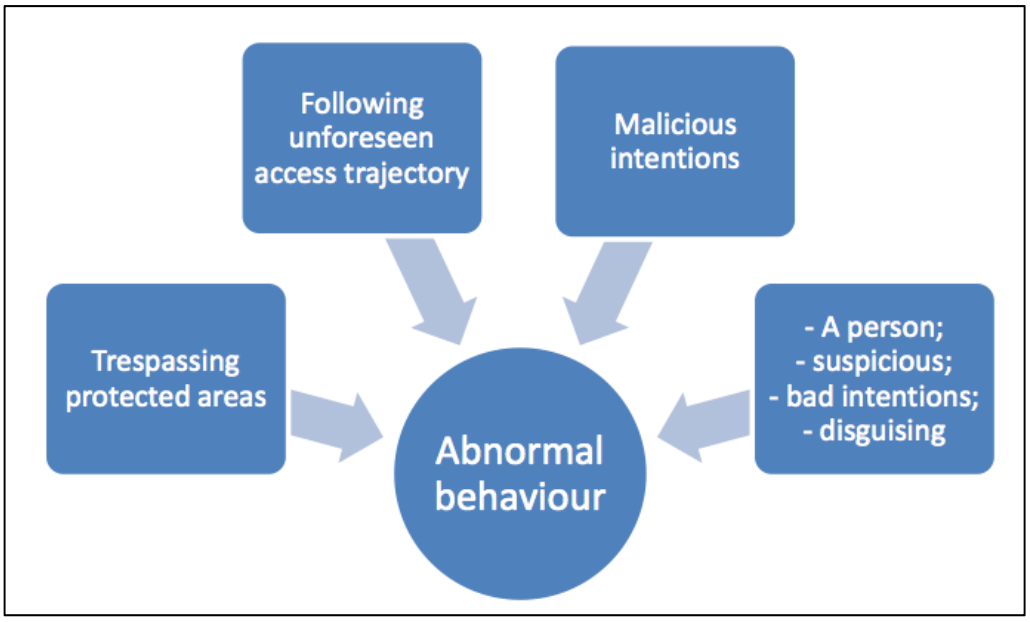

Figure 2: Abnormal behavior as viewed by engineers/industrials

Deliberating on a final questionnaire subject, - responsibility in designing virtual fences generally and particularly defining normal behavior, respondents held themselves accountable mainly for complying with legislation (I1-2, E2-3), with about one third of the interviewees denying any responsibility towards society or the public virtual fences could potentially target. E4-5 mentioned an additional responsibility "to provide best possible options of trade-off between integrity [of outside public] and security," indicating (1) that achieving facility's security requires violating public cohesion in discriminating between normal/abnormal behaviors; and (2) this tradeoff is both inevitable and necessary. Since normal behavior recognition is viewed as a milestone in achieving facility's security, algorithm of determining such behavior is revealed as a central object of the system.

To ensure data accuracy and provide additional input from engineers, the author turned to field observation methodology that included personal communication and description of working setting.

4.2.2 Informal interactions and field observations

The technical meetings on March 25-26th 2014 were held to reflect on current progress and plan further project stages by all technical partners. Technical partners consisted of seven international agencies, representing industry and engineers from those firms. Each party was responsible for developing a certain technical component of virtual fences, with some of them collaborating on designing algorithm of normal behavior. A first observation that struck the author was that during the meeting, when planning further project activities, the partners demonstrated a competitive rather than a collaborative approach. Each tried to include a new "essential" component for the system that only their company could provide and that would make them an irreplaceable point in the further development, however struggling to demonstrate added value. For instance, one of the partners pushed for adding aircraft detection element and another – for special thermal cameras. Debates around necessity of additional components were lengthy and a managing partner had to negotiate between others, judging that no additional components were necessary at that stage. The author was suspicious of underlying motifs in such negotiations. Also, if unable to cooperate at this early stage, reaching compromise when having to deliver a group product such as behavior algorithm might be challenging.

Second observation is related to meeting environment. The meeting was held in a security location with lack of windows and air-conditioning. Soon after meeting started the air in the room became warm and a couple of hours later it was hard to breath and think. That contributed to unofficial gatherings around coffee-machine in a hall next to the meeting room. During one of these improvised breaks, the author got a chance to talk to one of the engineer Partners and ask about behavior algorithms.

The partner, involved in designing the algorithm for virtual fences project (E6), told that in order to function and effectively distinguish between normal-abnormal behaviors, the algorithm needs to learn first. It is the engineers who "teach" the program and they can do it in two ways. The first way is unsupervised, when an algorithm learns in real-time from normal behavior models, identified as most typical trajectories and actions for people in a given location. If a person chooses a different path or his actions generally deviate from a standard defined by algorithm model, this person would be classified as having abnormal behavior and thus constitute a threat. Unsupervised learning model is similar to trajectory classifiers employed by Antonakaki (2009) to teach algorithms.

A second method presupposed supervised learning, with engineers inscribing real-life or modeled actions into the algorithm and supplementing them with assessment of those behaviors based on different indicators. Following E6, engineers basically would create a database of behavior for the algorithm, "statistics on how movement is done, "starting "with a database of recorded fights to design a model of abnormal behavior." Continuing with a fight example, E6 explained how behavior modeling happens: "If you want to detect a fight, you detect partially movements, partially body/facial features that capture and characterize that behavior. The same is done for other behavior types – through manual input, examples." A supervised learning approach echoes a short-

term classifier approach of Antonakaki (2009) and the alternative method of algorithm learning of Zhong (2004), where modeling human behavior was a key component.

When asked about effectiveness of these teaching methods, E6 admitted that "state of the art on behavior recognition modeling is very shaky," suggesting trial-and-error as the only way to learn. The author talked to another partner, involved in designing behavior algorithm, who echoed the expertise and opinions of E6, specifying that currently there is no defined database of algorithms of normal behavior and if created, it could be of great value "for future use." Therefore, field observation revealed that on top of technical difficulties associated with context-oriented development of algorithms, design process might also face interpersonal challenges, such as competitiveness. The key algorithm training models, elaborated by project partners, were identified with approaches outlined in theoretical part of the thesis. Therefore, the algorithm teaching methods in virtual fences project might face similar limitations, such as short durability of databases and discrimination of infrequent behaviors under statistical approach.

4.2.3 Conclusion

Questionnaire results and field notes demonstrated how engineers and industrials construct the script of virtual fences and specifically the algorithm of normal behavior based on network constitution and envisioning particular roles and responsibilities for different actors. Indeed, engineers/industrials extended a virtual fences actor-network initially with only themselves and end-users to include also policy-makers and reconstituted division of roles and responsibilities as following: end-users as goal-setting and responsible actors for defining normal behavior; policy-makers as providing legislative framework for technology development; and engineers/industrials as merely mediating between the end-users' goals, providing optimal technical solutions to achieve them within existing legal borders. However, the methods applied by engineers to program behavior algorithm have been debated by practitioners and scholars and have significant limitations. Outside public is mentioned rather implicitly, as an object of statistical study for the algorithm and as potential trespassers.

However, despite explicit mentioning of social scientist in the FP7 project and their presence at the technical meeting, neither engineers nor industrials mentioned them in projected use and design of virtual fences.

4.3 The contextual arena: a case study in Belgian prisons

4.3.1 The specific perspective of a policy-maker and an end- user in one package

Belgian Federal Public Service (BFPS) indicated interest in applying virtual fences in Belgian prisons as a part of prison modernization program. With BFPS Justice branch being responsible for correctional facilities (prisons), they are a primary Belgian end-user of virtual fences. BFPS is also a part of Belgian federal government as a policy-making institution, with BFPS Justice being responsible for the prison-related policies (BFPS, 2014). Therefore, BFPS Justice can be considered both as an end-user and a policy-maker in the virtual fences network. The author was able to reach one of the senior BFPS Justice officials (a woman), who agreed to talk about potential application of vir-

tual fences in Belgian prisons. For reasons of confidentiality, she will be referred to as PE as in Policy-maker/End-user. Instead of a scheduled 30 minutes slot, PE was so intrigued by the topic of research that the interview lasted one hour and a half.

4.3.2 Deliberating on potential application of virtual fences in Belgian prisons

Since virtual fences have not yet been implemented in Belgian prisons, PE talked about their potential application and frequently referred to an example of electronic monitoring as a basic form of virtual fences. PE distinctly took an institutional perspective here, constantly employing "we are working" or "we in the government made a decision" phrases, which could depict PE as a policy- maker. Electronic monitoring is applied to "people who are sentenced for more than three years, people in pre-trial, at the end of the sentence," who are released into society with electronic ankle bracelets to finish their term at home. According to PE, currently more than 50% of prisoners who served more than three years are released under electronic monitoring with such cases tripling in a three-year time, reaching "more than 2000 people" in 2014. With electronic monitoring imposing restrictions in space and time, constant monitoring (sometimes by GPS means) and check-ups on a detainee, PE names it "a prison at home" and refers to it as one of the forms of virtual fences, since inmates only have an illusion of being free and instead are surrounded by omnipresent invisible walls.

One of the most important reasons that led BFPS to employ electronic monitoring remains prison overcrowding. According to PE, due to this "in Belgium we had to make the laws about more and more prisons," which did not fix the situation because prison population growth is high. "We have a very bad situation in Belgium about dignity; living in prison is very difficult. You have three prisoners in one cell 24 hours a day," admits PE, referring to overpopulation in prisons as a cause of human rights violations. This factor coupled with poor prison conditions attracts attention of international monitoring organizations. PE says that "we also have Council of Europe's remarks about the situation in Belgium," admitting increasing international standards pressure on prison management and worrying about external image of Belgium. Therefore, releasing prisoners under electronic monitoring in Belgian prisons is a means of population management due to facilities overcrowding and a technological means to decrease international pressure.

However, PE does not believe technology to be a prudent tool to fix prisons' problems, indicating that "it's not wise." PE is cautious regarding technology, saying "I personally think we have a lot of questions to electronic monitoring. The place of technology – I think we have to be careful with it," hinting at adverse effects of electronic monitoring. Social consequences of at-home prisoners include changes in family life and relations since it is "all the family who lives in function to electronic monitoring." PE underlines the profile of electronic monitoring users as predominantly men and specifies that "our population – they are not men at home, they are going out." With electronic monitoring released men have to adapt their lifestyles, since now "they have schedule they have to follow." The whole family has to accustom, causing a shift in family roles and decreasing male authority because "you have a woman at home saying 'You must be here at 6 p.m.!'" Electronic monitoring largely problematizes inter-personal relations, causing "derogations in the family." Therefore, according to PE, electronic monitoring contributes to changing social foundation in Belgium.

4.3.3 Deliberating on application of classical perimeter-securing virtual fences in Belgian prisons,

PE takes on a perspective of an end-user, since she was a prison manager previously and will soon be managing a prison again, in Saint-Hubert. PE admits that virtual fences fall in trend of increasing inside and outside security and surveillance in prisons by means of new technologies. PE discusses examples of new prisons (Beveren, Marche-en-Famenne), where emphasis is put on external control and where "you would have more cameras than prisoners." Further PE acknowledges that in Saint- Hubert prison they already have something like virtual fences, called PERIDECT2[3] - "When somebody is coming from the outside, he would be arrested," revealing an interactive nature of the fence. A high-security Saint-Hubert prison "is not a classical prison; you have a little part for the young people," hence the need to prevent access into the youth facility from prisoners from other parts of the prison (see Figure 5). There is also an economic factor in play, since according to PE, "with this system they are going to decrease the number of guardians working in prison." This reveals technologically deterministic goal of prison administration – decreasing human security personnel and relying more on technology in matters of surveillance. In this regard PE also industrial lobby: "The lobby that you have from industry is very-very strong," echoing the concerns of social scientists on the virtual fences project. Following PE, if applied to prisons in Belgium, virtual fences would likely replace PERIDECT system, thus serving as a prison population management tool and an instrument to economize administering prisons.

At the same time, PE introduces the need for public acceptability of prisons. She recalls how people usually negatively react to new prisons in their neighborhood, - "First time, it's always NIMBY effect – Not in my backyard." To convince public of their safety and prisons' security, prison administration came up with an idea of open days, so general public could "witness the reality of prison" and also its technological filling. PE talks of this method's success - "For March- en-Famenne prison they had a lot of visitors coming to see how it is organized, functions, asking hundreds of questions," promoting public interest in prisons. Thus application of virtual fences in this context would be a reassuring factor for public, soothing their safety concerns.

[3] 2 PERIDECT – Perimeter Detection System from unauthorized access that detects and locates perimeter breaches. It is a hidden system with its elements installed in traditional fences. The system is designed to recognize vibrations caused by mechanical factors, such as climbing or cutting, at the same time reducing false alarm rates from rain, wind, etc. (SIEZA Company, 2014).

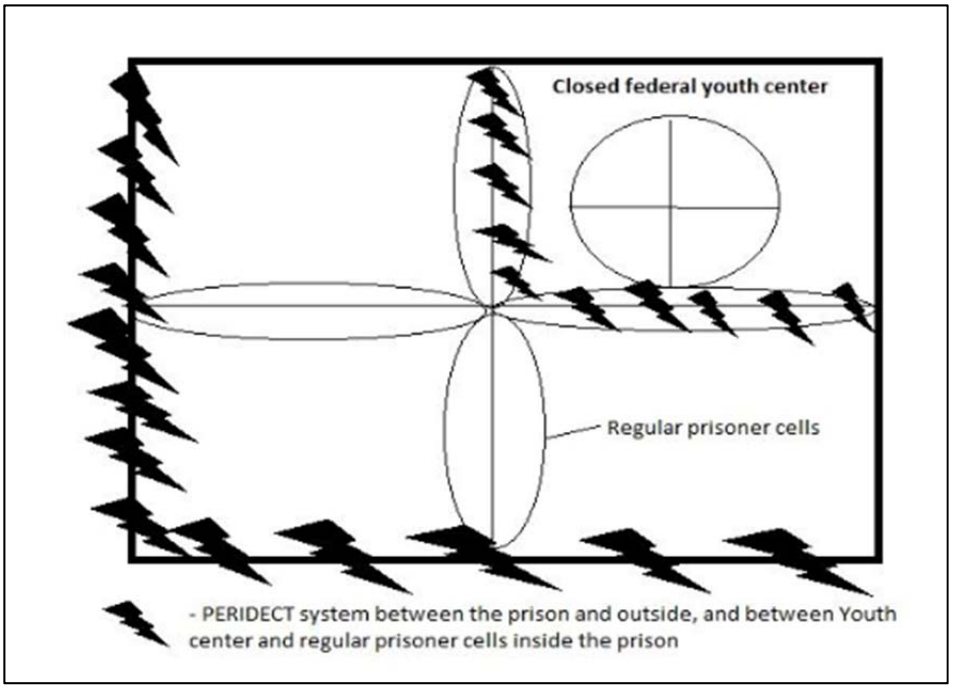

Figure 3 Saint-Hubert prison security design (after interview with PE)

Despite a high potential for virtual fences in prisons, PE is critical towards technological progress as lobbied by industry. As stated by PE, delineation of public and commercial sector is needed - "A system where you can follow movement is for me ok, but what I don't like is more the lobby and the private sector who says what is possible for the public sector." Recognizing financial ambitions of the industry, PE is sceptical towards increasing commercial influence on penitentiary sector: "The evolution of prison design and management is more and more oriented towards private sector. Sentences are the realm of public sector. You can't have this task in hands of the private sector." Therefore, virtual fences are a part of a strong industrial lobby manipulating with public aspirations for prison modernization and their application requires careful managerial consideration.

Finally, PE admits that adding new technologies to prisons forms a part of Belgian political agenda. By saying "in this period of elections in Belgium and the EU, everybody wants to build new prisons," PE asserts that prison modernization is also a politically-fuelled issue. However, she justifies politicians by lack of awareness, as in "they don't know about what they are saying. If you as a citizen are ready to pay 220 euros by day by prisoner, that's ok." Hence, BFPS interest in virtual fences project is also dictated by political agenda in Belgium, aimed at building new technologically well-equipped prisons.

PE critically approaches government's cost saving argument regarding introducing new technologies and decreasing human guardians. She stresses that aiming at decreasing prison costs, new technologies end up fostering new expenses – "It costs a lot to build and design, and also to manage new prisons with a lot of cameras and other technologies," underlining that "the cost to manage a prisoner in modern prisons is 220 euros a day. The citizens don't know it." She adds that comparing maintenance costs for new Saint-Hubert prison with decreased guards' staff is almost the same as in old-fashioned prisons of Brussels or Bruges, claiming that "this cost is because of all this

technology." Here PE also proves the hypothesis of A1 in suggesting sky-rocketing costs for servicing technology. Having refuted the savings argument financially, PE introduces the human dimension of the problem. According to PE, human involvement is crucial for prisons, since "in prisons we have to manage and educate people, make them ready to live together in society and for that we need human contact, not just the Turn On/Off button." Here PE repeats the concern of A2 regarding importance of human factor in prisons. Moreover, PE adds that "you need to have some technology, but you also need to see a limit to it. Human contact is very important," arguing against technological determinism in complex problems of penitentiary service. Finally, urging "to find a balance between human contact and technology," PE promotes a proportional approach in applying technologies to prison. Therefore, reflecting on technology use in general PE exercises a cautious balanced approach, arguing that they are not as financially beneficial as though and that people are an intrinsic part of prison management and no machine can replace them or magically solve prison- service problems.

In short, BFPS senior official presented a set of critical arguments towards technology in prisons in general and application of virtual fences in particular. Firstly, she indicated that prison manager as an end-user can challenge the script of technology according to the situation and pressing needs, using it in ways other than prescribed. Since PE is both a penitentiary policy-maker and a prison manager, it is possible to see a wide spectrum of interests that will subject virtual fences to use other than foreseen by engineers and industrials. Instead of using virtual fences as security perimeter system, prison management can use it as a tool for prison population control inside the prison; as a display of safety and security to ensure public acceptability of prisons and of government policy aimed at expanding prison network; and finally as a political display of willingness to conform with international penitentiary norms. These aims also indicate emergence of two new actors to the virtual fences network: the inside population of prisons and the general public, thus correlating with the views of social scientists on the project.

The author foresaw the involvement of outside public as a network's actor; however prisoners as an actor emerged in the course of research and were not investigated in present thesis directly. Thus to complete the picture of the virtual fences network as envisioned by the author, it is essential to approach public deliberations regarding virtual fences.

4.4 Prospects for a deliberative arena

4.4.1 The difficulty of constituting a consistent public for non-existing technologies and the limits of online polling

Most popular methods in social acceptability studies are opinion polls, such as the studies conducted by the Eurobarometers. It is an important method to determine the "state of opinion" at a certain moment and in a certain place. However, the question of whether polling is the most appropriate tool to question technologies such as virtual fences, upon which the "general public" is ill informed, remains open. While the methodology could prove useful in other situations, in our case we acknowledge that using online survey methodologies has met some severe limitations.

We carried out an online survey which gathered about 288 complete answers to an online structured form. In this form as we shall detail below, we had to take into ac-

count the prospective dimension of virtual fences and, henceforth, question the public with short scenarios upon which it was ask to position itself. In other words, the approach was quite exploratory in scope.

Furthermore, we recognize that the public we could reach given the limited amount of time and very scarce resources we could mobilize to carry this study forth it is not representative and too limited. The public is not representative first because it is very difficult to precise the scope of the technologies at stake. Hence potentially no boundary is set on "the population to survey" given that the technology potentially impacts each and every citizen. Second, the consequence is that it takes considerable amounts of resources to reach out to an audience wide enough so as to have it representing something as broad as "the public at large". But it is also limited because the sample is probably far too narrow to speak for a technology which have European ambitions in scope — as the product of a European consortium. Hence not only should the public be representative, but also reach out to an adequate audience, in this case a European one. Alongside those criterions it appears clearly that the results of the survey detailed bellow are invalid and cannot be taken into account for any sort of decision-making. However, these results do matter and might have an informative value from which partial insights can be gathered.

The main problem here is to define a targeted population: how to constitute the adequate population for such a pervasive technology as virtual fence, generic in scope, which could potentially be applied in a wide variety of settings? How to define the adequate perimeter? We also recognize that we had to answer those questions with limited means as for the sample constitution. Usually sociological work performs with what we refer to as "reference networks", i.e. already existing target populations upon which it is possible to carry on with questionnaires steadily. For instance, in prison, in could be the penitentiary staff, the administration, the prisoners themselves, and so on. On the scale of a society it could be the unions or the professional associations, for example the hotels and restaurant federation if ever virtual fence were to be installed in every restaurants for security purposes.

Another way to proceed is then to build a random sample which obeys to strict random rules. But here again, the fact that the considered population is not defined makes the random methodology impossible to perform.

More particularly, our questionnaire met some pitfalls as we shall describe more in details above. However, we can sum up the three main problems we encountered with the questionnaire:

Due to the way we had to propagate it, some nationalities are far over-represented than others (Belgian and Ukrainian particularly). We observe that the results gathered from Ukrainian respondents significantly diverge from other responses probably because at the time we launched the survey, Ukraine was entering in war with Russia and that this geopolitical setting certainly influenced answers to the questionnaire. We could stress that in war times people are more willing to turn themselves towards surveillance technologies, but we do not have the evidence to back up that claim. At best this claim can be considered as a working hypothesis to deal with counter-intuitive results, as politically active people declare themselves rather agreeing with such systems.

The respondents constitute an obviously biased public, rather well educated, informed and in general quite sensitive to the political question of surveillance. This is due to the fact that the questionnaire mostly circulated with our limited means, i.e. mostly through our personal networks and beyond. In other words, we did not reach to the broader population which is potentially less educated and informed on those topics that the respondents in the current state of the survey.

Lastly, the fact that the questionnaire addressed a technology in progress, not already visible and intelligible on the public scene makes the phrasing of the questions particularly delicate. We had to use examples, metaphors in order to make the issues at stake in the questionnaire more tangible and concrete for the audience. This brought ineluctable bias in the way people respond to the questions.

4.4.2 Methodology

In the pursuit of questioning many people of diverse cultural, educational, professional backgrounds the author chose online survey as methodological tool for questioning public opinion as regards virtual fences. Since general public is not a tangible concept, one has to create it (Coline, 2007). General public as an actor sprang as a result of designing, implementing and analyzing online survey. Following MIAUCE methodology (2007), the author wanted to distinguish and compare two populations, - experts/activists and lay people, in order to observe whether any divergences between these respondents might occur and obtain a thorough analysis of results. Those respondents who would acknowledge membership in any professional association or activist group towards fundamental liberties or politics would be classified as “Experts” since their opinions about human rights are informed and made on the basis of rationality and experience. The author mentioned them as “expert respondents” in the latter text. The second group of respondents would be classified as “Lay public” as those not possessing significant knowledge or experience in the field of human rights. This group of average people interplays with and contests social norms in pursuit of normal life (Le Blanc, 2007), forming opinions on personal perceptions. Thus, the author aimed to divide survey respondents in two populations in order to evaluate the nature and intensity of their opinions about virtual fences and see if there were any divergences between them.

Given that there were no population filters in the FP7 project, the author targeted random audience. As such, the survey did not yield responses that could be representative of general public. Instead, the survey was of explorative nature.

Since potentially anyone can be exposed to virtual fences when applied to prisons, the author did not want to limit the survey audience to the EU-28 area, as prescribed by the FP7 project. Following Bijker et al. (2009), to facilitate public participation in matters of science, the author wanted to collect data from diverse geographic locations and access people who are usually hard to reach. This justified launching the survey in four languages, - English, French, Russian and Ukrainian – as justified by lingual abilities of social scientists on the project and opportunities to disseminate the survey in native and international communities. In this regard, online survey presented a powerful tool for data collection.

Survey research method is an efficient means of data collection basing on questionnaire structure delivered to targeted audience (Fielding, Lee, & Blank, 2008). The widespread use of Internet contributed to increasingly shifting survey research to the

online environment (Andrews, Nonnecke, & Preece, 2003; Murthy, 2008; Stanton, 1998). The vast advances of online survey research include global reach, speed and timeliness, ease of data entry and analysis, question diversity and low administration costs (Evans & Mathur, 2005). However, online environment also raises methodological challenges to survey research, such as concerns as to data validity, "design, implementation, and evaluation of an online survey" (Wright, 2005, p. 1). The choice of applying web survey methodology was carefully weighed against its advantages and disadvantages.

4.4.3 Design, structure and dissemination

Following methodological guidance of Nassar-McMillan&Borders (2002), the author approached the process of survey design and implementation in several steps. Upon crafting initial survey questions in March 2014, the author constantly refined them in rigorous discussions with senior scientists from the project and established the final set in April 2014. The process of putting a survey online followed, accompanied by technical help from senior researchers. The survey was built using LimeSurvey software since the University of Namur was a licensed user and the FP7 project could benefit from it. LimeSurvey facilitated survey design, collection services and data analysis featuring multiple types of questions, such as numerical rating, multiple choice, check-lists, open questions and picture-based questions. However, some questions were left open-ended to allow respondents deliver their opinion, for instance, on how to define abnormal behavior. After putting the survey online, the author and her colleagues personally completed survey many times, revising certain issues and ensuring a friendly survey interface. The pilot survey was spread in early April between some colleagues and sample from the target audience. Extensive feedback helped revising the survey and the final version was launched on April 11, 2014 at https://survey.unamur.be/index.php/689786 and /751578.

The survey contained thirty questions structured in four sections and three subsections. The first two sections aimed to learn about the respondents and their environment. The third section introduced the subject of virtual fences and offered the respondents to learn about its three potential applications. Callon (1987) presented constructing possible scenarios as a crucial step in developing new technologies. To stimulate debate on virtual fences application, the author developed three scenarios within the survey. Scenarios were intended to approach respondents on three levels: national as in border surveillance scenario, regional as in prison security case and local/personal as in electronic detention scenario. Since the focus of this thesis is the prison case, this scenario was the primary analysis target. The results from the other two scenarios were used to contrast and compliment the prison scenario data. General storyline of the scenarios was darkened after a first set of questions so as to provoke respondents to think structurally, answering to already presented "What if ?" questions, and to raise social awareness of potential technological capabilities (SWAMI, 27 2005). The final section of the survey concerned public attitude towards virtual fences and was designed to trigger response both of individual and public relevance.

After defining the final structure of the survey and putting it online, the time arrived to spread the research. Dissemination strategies targeted social networks and personal communication channels, professional networks and individuals, colleagues and friends. The author sent personal private messages to avoid the low response rate and asked respondents to spread the survey among their networks. At the same time, there was a high drop-out rate which author relates to personal reasons, complicated

subject of the survey and at times lengthy question formulations. The survey was terminated on May 11, 2014, exactly one month after start, generating 288 fully completed responses. Compared to large-scale EU projects such as MIAUCE (2007) or SWAMI (2005), the number of results exceeded author's expectations.

4.4.4 Limitations

Despite author's attempts to address possible disadvantages of survey method, it still ran the risk of collecting superficial opinions, constrained by the nature of mostly closed questions. The issue of digital divide also has to be taken into account, since only people with access to computers and Internet were able to participate in the survey. Software weaknesses also have to be mentioned. LimeSurvey is limited to the preprogrammed languages that did not include Ukrainian. Since Ukraine is one of the biggest European countries with 44 million people (The world factbook, 2014) and since Ukrainian origin of the author would increase dissemination chances for the survey, the author created a separate survey with Russian language label enabled by the software but actually containing information in Ukrainian. To avoid confusion, the author communicated this technical issue when inviting respondents. Different cultural contexts also deserve attention. The survey was executed in the time of military intervention in Ukraine and a frequent comment from Eastern European respondents was that had the regional situation been more peaceful, responses to the survey would have been different. However, this aspect is both a weakness and strength, contributing to the heterogeneous empirical richness of the data. Overall, the author tried to overcome survey weaknesses by a thorough methodological approach to its design, implementation and analysis, as well as by seeking guidance from senior colleagues. The nature of the survey is complimentary and the results are used to contrast the data from other respondents obtained by interviews, questionnaires and observation.

Therefore, to study a multitude of attitudes and beliefs regarding virtual fences, the author relied on online survey method and created a diverse general public actor. The survey method has positive and negative sides and to mitigate the latter, the author used a thorough methodological approach when designing, implementing and analyzing the survey to generate collective and context-based responses rather than purely statistical.

4.4.5 Data analysis

Proceeding to "transformative process in which the raw data are turned into 'findings'" (Lofland, 1995, p.195), the author approached data analysis using coding and memo techniques to create structure of results by means of categorization.

Drawing from constructivist grounded theory methods (Charmaz, 2006; Strauss & Corbin, 1994), the author chose coding as a primary data analysis strategy. Lofland (1995) considered coding as a "process of sorting your data into various categories" (p. 200), with codes being "tags or labels for assigning units of meaning to ... information" (Miles, 1994, p.56). Following Charmaz (2006), coding process consists of two overlapping steps, initial and focused coding. Initial or open coding allows initially inspecting and condensing the data by open inquiry as to what the data represents, what the phenomena are, what the actors are engaged in, etc. Numerous and diverse codes are typical for this stage when researcher tries to grasp the essence of information by line-by-line analysis. In contrast, focused coding features more direct and selective analysis, drawing from initial coding. This is a more analytical step aiming to capture particular

aspects and suggestions about the general topic. Coding helps uncover patterns of related data and systemize the findings, presenting a valuable tool of qualitative analysis. In the present research the author used coding to analyze and juxtapose obtained results from all data collection techniques.

To identify the public for virtual fences and investigate their beliefs about virtual fences, an online survey was launched. As indicated in methodological part, the public was reached by social network strategies and personal communication. In the end, the survey collected 642 responses. However, 354 responses were completed only partially. The average response time needed to complete the questions was 29 minutes, which could explain the high rate of uncompleted answers along with the novelty of the subject. To ensure full and coherent representation of data, the author identified fully completed 288 responses as valid and analyzed that sample. The relatively high rate of "Neither..nor" responses was an inherent feature of the survey, with approximately 30% of respondents choosing this option for every question. This could be explained by the social desirability bias, when respondents tried to cover their ignorance or competence of the question while under the social pressure to provide a response (Blasius & Thiessen, 2001; Goldberg, 1971; Likert, 1932); by confrontation with the question, when respondents simply disliked or were annoyed by question and chose to provide a middle answer as satisfying option (Baka, Figgou, & Triga, 2012); or simply explained by ambivalence when a respondent was indecisive or neutral (Armstrong, 1987; Klopfer & Madden, 1980).

4.4.6 Biased Respondent's Profiles

Regarding the gender representation in the survey, female respondents dominated the male ones, constituting 59,4% of the audience (171 responses) in comparison to 117 male responses (40,6%). The average age of respondents was 30 years, with the youngest respondent being 18 years of age and the oldest – 86. Geographical scope of respondents (see Figure 6) was wide, covering all continents excepts Australia and Antarctica. Europe was the most frequent place of origin of respondents (64%), followed by Asia (21,6%), North America (8,3%), Africa (3%), island countries (2,4%) and South America (0,7%). The majority of respondents came from Ukraine (90), Russia (46), Belgium (40), and the USA (21), which can be explained by powerful networks in countries of origin of social scientists on the project or where they used to live/study.

Answering the "Occupation" survey field, respondents could indicate both education and work. The results indicated that 51,3% of respondents were still studying and 57% - working, meaning that 93 of the respondents were only studying (32,3%), 110 – only working (38,3%) and 55 respondents (19%) were both working and studying. 10,4% of the respondents defined their occupation differently, mostly being retired, unemployed or busy with family care.

Analyzing the level of education of respondents showed that the majority of respondents (174 or 60,4%) possessed a master degree or equivalent, considering peculiarities of national education systems; with 64 respondents holding a bachelor and 20 – a doctor degree or equivalent. The rest of the respondents finished either secondary or post-secondary training or did not finish their education.

Educational background of respondents is diverse but dominated by the fields of social sciences (23%), economics (11,5%), arts (7,6%), engineering (7,3%) and law (7%).

Those respondents (11,8%), who chose the field "Other," specified most frequently such occupation fields as business, philosophy, IT, linguistics, journalism and education.

When asked to indicate the work sector in which respondents were engaged, most frequentsectors were teaching (15,4%), social sciences (8,2%) and engineering and applied sciences (7,5%). Among work sectors, marked by respondents as "Other," education, journalism, civil activism, mass media and IT sector were most common.

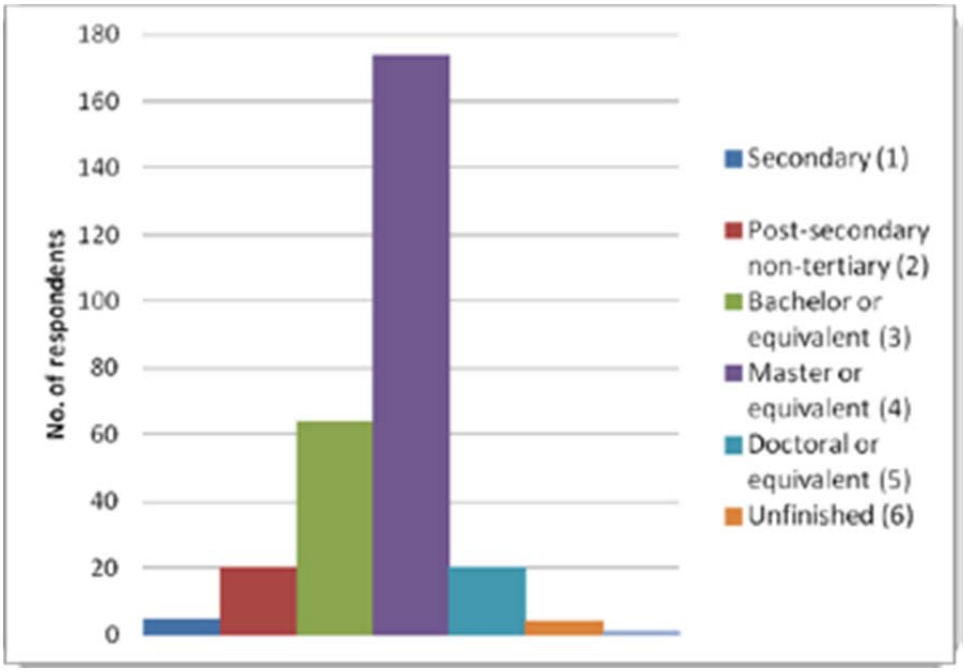

Figure 4 profiles of respondents

Out of 288 respondents, 96 (33%) indicated affiliation to certain associations or groups. The majority of the respondents belonged to an association defending fundamental human rights (46 respondents), followed by those belonging to political parties (19) and groups towards privacy rights protection (13). 18 respondents admitted affiliation to other groups, such as professional associations, ICT groups, volunteering and educational activist groups. However, only those related to the subject of human rights and consequentially politics were added to the experts' list, with the rest classified as lay public. Therefore, 73 respondents were put in the expert group and remaining 215 formed the dominant (75%) group of "lay public." Here the indicator "lay" is used in quotation marks because it does not fully correspond to the traditional sense of Le Blanc's term where lay people are viewed as a precarious group (2007). The identified survey public is generally very well- educated and thus more secure in life and grounded in their choices. The term "lay public" is rather used to contrast the views of the "experts" within the survey and distinguish two sample groups.

Thus, the general profile of a survey respondent can be outlined. The average survey respondent was a 30-year-old person most likely of European origin, well-educated, likely in the area of social sciences, working in a variety of sectors and occasionally affiliated with certain professional or activism group. This means that the survey reached active online citizens and reached previously uncovered segment of East European region, contributing to the richness of the results.

4.4.7 Investigating respondents' views regarding security and technology

Starting from this section, analysis of the data was conducted via the experts and lay public instrumental categories. In order to study respondents' ideas about public systems of safety and security, the survey asked to consider the roles of government, industry, engineers, non-government organizations (NGOs) and regular citizens.

The following group of questions was important to grasp public perception as to who is responsible, legitimizing or simply involved in the design and setting of national safety and security systems. Since virtual fences represent a security system of critical infrastructure objects and thus are a part of national security setup, this question is particularly relevant for the thesis.

When asked to regard the role of government in the design and implementation of systems of public safety and security, the expert panel deemed that this actor is almost equally responsible for (43,8%) and contributes to legalize the policy (42,5%). The lay public's answers were somewhat different in that they primarily relied on government's responsibility for public safety and security (52,6%). The experts' and lay public opinions thus held the government in its traditional role of guarantor and policy-maker for public safety and security.

The rest of the actors, namely corporate sector, engineers, NGOs and regular individuals, both the experts and lay public experts judged it to be mostly involved in the process, only occasionally admitting to their responsibility and legitimizing power. In general, the answers for this question illustrate convergence of experts' and lay public opinions regarding role allocation in national system of safety and security (see Figure 8).

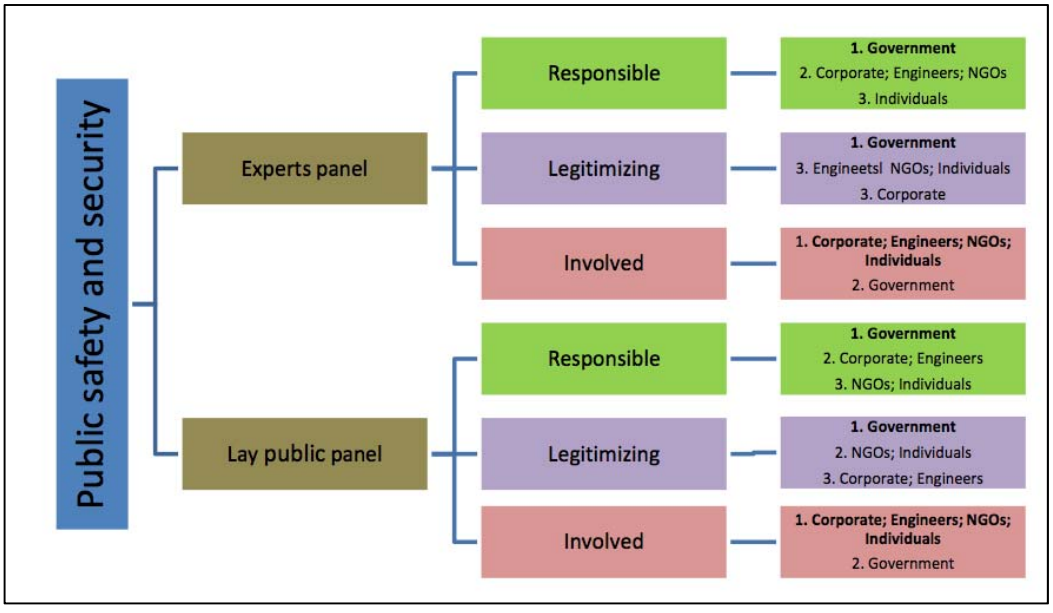

Figure 5: Allocation of roles in public safety and security systems

Approaching the problem of security generally, the experts' panel considered security as a highly important societal problem (65%) or an equally important problem to

tackle (29%). Lay public panel expressed similar opinion, considering security a major societal preoccupation (59%) or an equally important problem (37%).

As for technology, further questions studied respondents' attitudes towards technology in order to understand human-technology relationship in the survey sample groups. Respondents were first asked to assess whether they rely a lot on technology in daily life. The experts' panel in absolute majority agree with the statement (69,8% of total "Agree" answers) with 24,7% being ambivalent to the question and 5,5% disagreeing with the statement. The lay public even in bigger majority agreed with the statement (77,2%), with 17,2% choosing "Neither..nor" option and 5,6% disagreeing. Thus, opinions of experts and general public from the survey supported the perception that people greatly rely on technology.

Assessing the statement whether respondents' relationship with technology is somehow problematic, generally disagreeing responses for the experts (50,7%) largely outnumbered those agreeing with the statement (19,14%), with the similar situation for the lay public (61,9% vs. 15,36%). The "Neither..nor" response rate was relatively high – 28,8% for the experts and 21,4% for the lay public.

The experts did not support the view that technology is more fair than humans (37% of total "Disagree" vs. 17,81% of total "Agree"). Lay public displayed stronger disagreement, with 40,4% total of "Disagree" vs. 18,58% of total "Agree." The neutral "Neither..nor" category remained a frequent choice for both experts (41,1%) and lay public (34,9%), which may be explained by a controversial nature of the question.

Analysis revealed that the experts admit being largely influenced by technology in their actions and choices (58,9% of total "Agree" vs. 12,37% of total "Disagree" answers). Lay public also recognizes large technological influence, as proven by 63% of total "Agree" vs. 15,1% of total "Disagree" answers. The middle "Neither..nor" category remained a steady but a less frequent choice for both experts (28,8%) and lay public (21%).

Having admitted a large technological influence on their daily choices and actions, both experts and lay public have a soft technologically deterministic profile, as indicated by large reliance on technology and admitting its influence on daily behavior; at the same time believing in non-problematic nature of human-machine relationship and in greater human fairness as compared to technology (Smith & Marx, 1994; Wyatt, 2008). There were almost no discrepancies in the views of general public and experts throughout this section.

4.4.8 Examining virtual fences as applied to prisons: "Prison security scenario"

The following part of the survey included three potential or real examples of virtual fences application – border surveillance, prison security and electronic detention. Since the research focuses on virtual fences application in Belgian prisons, the author will concentrate on prison security scenario, contrasting it to others to adequately represent public beliefs.

In order to situate respondents regarding their relation to prisons, the scenario section commenced with probing respondents' attitudes towards penal sanctions and experience with prisons. Only a minority of both exerts (15%) and lay public (12%) ad-

mitted living near a prison. About one-thirds of both panels (36% & 27%) acknowledged direct/indirect involvement with prisons through contact with prisoners, staff, visitors, etc.

When asked whether security in prisons should be reinforced, both panels favored augmenting security. 47% of experts generally agreed with the statement and 19% disagreed. Public panel indicated stronger opinions, with 59% approving reinforced security and only 10% disagreeing. Considering reinforcement of penal sanctions in the country of respondents, both panels rather agreed with the statement. However, whereas experts indicated visible but narrow agreement (38% of total "Agree" vs. 30% of total "Disagree" answers), lay public again demonstrated more straightforward beliefs, with 41% agreeing and 21% disagreeing with the statement. Asking to assess the statement "In general, physical proximity of a prison makes me feel more unsafe," the panels rather disagreed than agreed with it. Here, however, the experts were unequivocal, with 42% disagreeing and 26% agreeing with the statement; and the public panel agreed by a narrow margin (38% vs. 29%).

Discrepancy between public and expert opinions regarding living next to a prison, as well as general agreement towards reinforcement of prison security and penal sanctions could be partly explained by public stereotypes regarding prisons, - an issue outline by PE and her consequent desire to open prisons for people to eradicate "NIMBY"-effect and apparent need to reassure public in their safety and prisons' security. PE's concerns regarding stereotypical negative attitude to prisons can be traced throughout following questions in prison scenario section.

This section investigated respondents' opinions on six statements regarding virtual fences in prisons as the focus scenario for this thesis. The first statement required respondents' assessment concerning personal safety if virtual fences are applied for prison security. Both panels indicated they would feel more safety, with experts agreeing in a slighter proportion (40% of total "Agree" vs. 29% of total "Disagree" responses) and lay public largely agreeing with the statement (50% vs. 17%).

Respondents were further asked to state whether protection in prisons was better achieve by people, indicating a narrow disagreement on the subject. Whereas experts disagreed with the statement by 3% (28% of total "Disagree" vs. 25% of total "Agree" answers), lay public disagreed by 1% (26% vs. 25%), meaning that almost as many respondents would agree that people protect prisons better than technology.

When asked to determine whether virtual fences as applied to prisons may be discriminative, both panels expressed consensus denying that possibility (38% of experts disagreed while 27% agreed; 39% of lay public disagreed while 24% agreed). Similarly, both panels discarded the statement of virtual fences potential in modifying human behavior (narrow disagreement of experts: 24% vs. 22%; and clear disagreement of lay public: 40% vs. 25%); having a negative effect on privacy (clear disagreement of experts: 38% vs. 24%; and narrow disagreement of lay public: 37% vs. 33%); or on fundamental human rights (experts disagreed with 37% over 22%; lay public – 40% over 28%).

Despite slight discrepancies, both experts and lay public generally denied any negative effect virtual fences in prisons might have on them as an outside public, arguing for their implementation in prisons for reasons of safety and more efficiency as compared to human security personnel. Notwithstanding controversial nature of the ques-

tions, the answers of both panels support identified earlier profile of respondents as slightly technologically deterministic.

In order to challenge identified hypothesis about respondents and confront them with virtual fences on a personal level, the survey presented a darkened prison scenario. Respondents were asked to imagine that they want to shop in an outlet just outside the city that neighbors a prison with virtual fences. Being close to prison automatically makes them surveillance targets. Having related the scenario to respondents personally, respondents were asked about their feelings towards several statements. Asking to assess their personal safety in given situation, responses of experts and lay public differed. While experts admitted feeling less safe when subjected to prison's surveillance system (30% of total "Agree" vs. 22% of total "Disagree" responses), lay public disagreed by narrow margin (37% vs. 34%). Despite this mismatch, when asked whether they would avoid this place in future, both panels presented corresponding views. Indeed, 37% of experts agreed rather than disagreed (27%) with the statement, with 39% of lay public agreeing and 32% disagreeing accordingly. However, assessing the statement "I wouldn't care since none of my actions could be held against me," both groups largely and almost equally agreed with the claim (48% experts and 49% lay public).

Thus, indicating fear for virtual fences (feeling less safe), willingness to modify actions when near prison (avoid shopping in preferred locations) and readiness to justify their behavior against virtual fences' potential verdict depicted respondents as subjects to technology and strengthened earlier technologically deterministic response profile. However, asking to deliberate on a darkened scenario created confusion among respondents, who previously indicated different opinions (as in virtual fences not modifying human behavior). This inconsistency can be justified by hypothetical nature of situations and thus lack of clear-cut opinions in respondents that however do not prevent from uncovering a response trend.

When asked to determine relation to the prison scenario in general, both panels posited feeling uncomfortable regarding application of virtual fences in prisons (67% experts, 64% lay public). The similar opinions were expressed for other scenarios: total of 63% "Uncomfortable" for border surveillance and electronic detention. Other scenarios pictured similar trends of responses regarding virtual fences as applied to borders or home detention, and similar inconsistent responses in darkened scenarios. This confirms a previous hypothesis of a soft technologically deterministic profile of respondents, generally welcoming introduction of virtual fences, admitting their efficiency as compared with people and denying their possible modifying powers on human life in general but reconsidering their opinions at closer look.

4.4.9 Public attitude towards virtual fences

The last section investigated public attitude towards virtual fences in general, based on the insights gained from answering previous questions. The first question was picture-based and asked to match pictures with corresponding beliefs towards safety and security (see Figure 9). When asked to determine degree of conformity of respondents' ideas regarding safety and security with the image of medieval Akkerman fortress (Ukraine), both experts and lay public indicated a high degree of correspondence (experts - 63%, lay public – 61%). Asking to do the same for the image of virtual fences border surveillance prototype (USA-Mexico border) revealed similar opinions, with correspondence degree reaching 55% for experts and 60% for lay public. This means that despite lack of "heavy-weight" medieval protection barriers, open and

"light" highly- technological modern security systems such as virtual fences imbue people with confidence. Once again, PE's suggestion of technology as a reassuring factor is echoed.

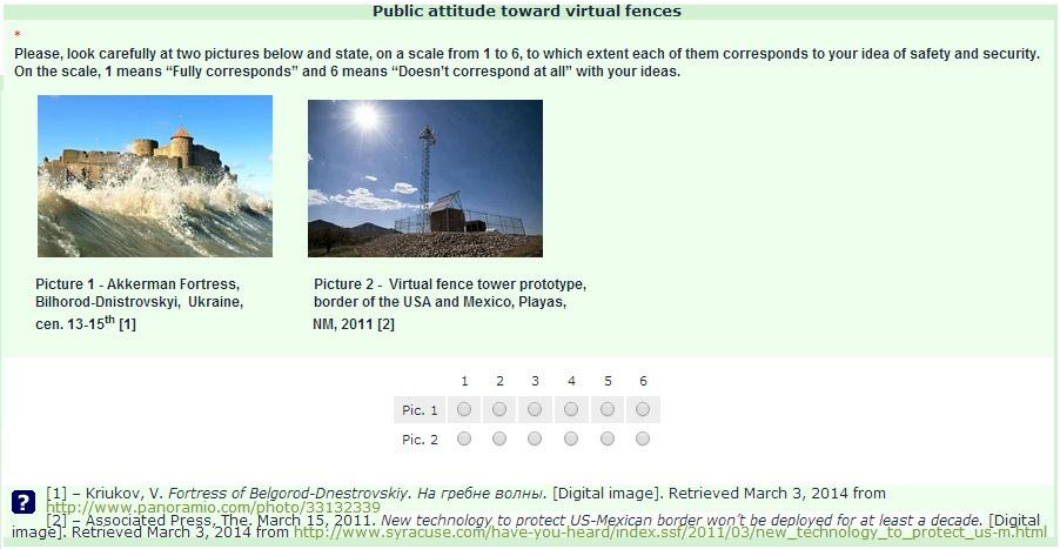

Figure 6 Picture-based question regarding safety perception

The following set of questions asked to evaluate five statements and was designed to challenge respondents' attitude towards virtual fences and see if it changed in the last section as compared to earlier ones. Respondents predominantly agreed with the first statement - "Virtual fences are necessary since they cannot be distracted and can effectively perform monotonous surveillance," with 52% of experts and 63% of lay public confirming the belief. Both groups also admitted potential risks as induced by virtual fences (40% agreement of experts and 45% - of lay public). Both panels also recognized virtual fences as a positive social phenomenon because of ensuring public safety and security (44% agreement of experts and 51% - of lay public) and almost unanimously urged for careful management of virtual fences (88% of experts and 90% of lay public). Asking opinion on whether virtual fences will replace human surveillance operators, both experts (37%) and lay public (38%) agreed on the matter. Therefore, the line of response can now be certainly identified as technologically deterministic and convergent with beliefs expressed in earlier survey questions, in admitting technological superiority over people and eventual supplanting of people with technology in workplace.

4.4.10 Approaching normal behavior by general public

Building on their beliefs and knowledge of virtual fences from the survey, respondents were asked to identify abnormal behavior that would potentially trigger security alarm. Responses of both panels (288 open responses) were diverse and difficult to group under unifying categories.

Despite the attempts to identify features of abnormal behavior, many respondents struggled to do so, conceding that "Every behavior is normal!," "There is no one right answer" or "It depends on social standards. What is normal might not be normal somewhere else." One respondent challenged the assumption that normal behavior is a statistical function, saying that this could lead to conformism expansion in society.

Some also admitted to technical fallibility, recognizing that “Technology is not perfect in calculations.” Some respondents identified engineers as primarily responsible for normal behavior algorithm and suggested that the role of engineers should be reevaluated - “It should be delegated to professional psychologists, not engineers.”

Open responses to the question supported results from the quantitative part, where respondents urged for careful management of technology. A frequently-referred theme was comparing virtual fences with “Big Brother” (Orwell & Pynchon, 2004) - “Virtual fences could mean a ‘1984’ scenario if things went wrong and could mean absolutely no freedom for anyone or they could be a real blessing. It would all depend on whose hand this technology fell into.” Some even quoted Benjamin Franklin, saying “those who sacrifice liberty for security deserve neither," identifying and discrediting the trade-off of public privacy for security that virtual fences introduce.

Respondents also posited that human intervention is necessary for behavior analyses, saying that “’abnormal behavior’ can be noticed only by the human eye” and “only human beings are able to label something as abnormal since this qualification is very time, space, place and situation- dependent!” Mentioning an example of polygraph detector convicting someone of lying only because of increased worrying, one respondent said that “humans are not robots; their behavior is always unpredictable,” indicating inability of virtual fences to adequately recognize normal/abnormal behavior. This respondent further claimed that currently there is no such thing as “normal,” therefore determining abnormal behavior by machines is complicated.

Based on the stated above opinions and their variations, present in qualitative responses, the author mapped potential identifiers of abnormal behavior under two main categories (see Figure 10):

Subjective approach:

- Social norms: deviation from ethical norms, norms approved by society; anything illegal, disrespect for society, drunk people, imprudent, suspicious actions, inappropriate gestures, social awkwardness.

Objective approach :

- Statistical definition: uncommon movements, statistically deviant, movement along not foreseen by designers trajectories;
- Physical characteristics: elevated heart-rate, rising body temperature (sign that people are getting too excited/angry/worried), nervous behavior, anxiety, inability to identify a person;
- Types of behavior: violent, aggressive, escalating behavior; yelling/silence, terrorism, robbery, murder, large accumulation of people, disguising oneself, trying to hide from, sabotage virtual fence; vandalism, leaving unknown objects, prolonged reconnaissance;
- Presence of armory: someone armed, equipped with malicious objects, destruction acts;
- Technical bugs: hacker security attack, electronic bugs, light and sound disturbance;

- Entry criteria: trespassing, crossing security line;
- Nature of movement: fast/slow movement, climbing the wall, fighting, regular back-and-forth movements, movement during night, against the main flow; standing still, lying on the ground for a long period; all moving objects, transfer of big objects.

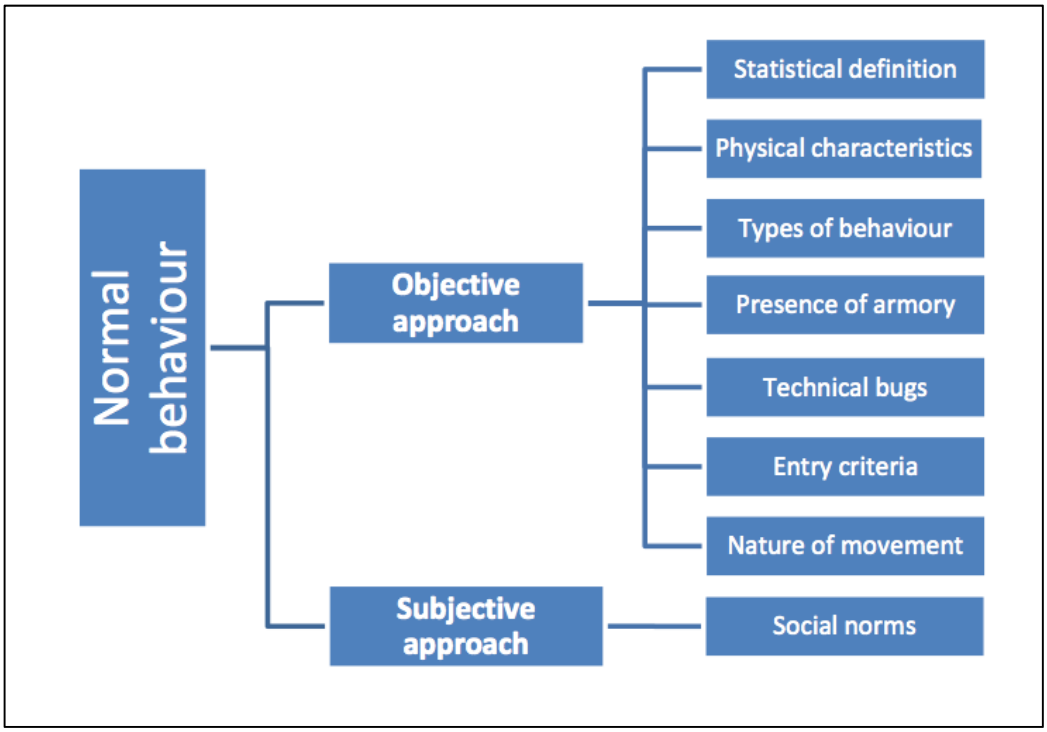

Figure 7 Criteria for abnormal behavior definition as viewed by general public

Survey respondents thus revealed reflexive opinions on behavior definition, dividing themselves into two groups: those who pursued a contextual, subjective approach and those who exercised a naturalized or objective approach legitimized by facts and figures. This division underlines a gap between two views on virtual fences of general public. The first one is utopian, where respondents consider virtual fences as a benevolent technology that will protect them and ensure their security. This view correlates with the paternalistic technological view of policy makers

Normal behavior and engineers and the objective measurement criteria to behavior definition of the latter. The second view is revealed when the author moved the direction of the survey from quantitative to qualitative and asked to define normal behavior. When confronted with such a complicated question, the respondents often did not know how to define what normal is and referred instead to social norms as defining behavior. This view is more reflexive and needs to be democratically deliberated to define what the social norm is in a given context. Thus, the qualitative question in the survey uncovered a reflexive layer, jumping from an abstract to a pragmatic response frame.

4.4.11 Conclusion

Therefore, the survey results witness the emergence of another important actor in the virtual fences framework. General public as identified by the survey is represented by generally middle- aged well-educated respondents with strong opinions on virtual fences despite novelty of the subject. For the purpose of analysis and comparison sur-

vey population was divided in experts and lay public. It should be noted that very high educational level of the "lay" public in the survey makes it a tentative category in order to juxtapose opinions of the experts in politics and human rights. Data analysis revealed convergence of two panels' opinions and ability of both experts and lay public to produce sound knowledge about virtual fences. Such results support the STS claim that experts and lay people can both provide high level of expertise and valuable contributions despite of professional background (Bijker, Bal, & Hendriks, 2009; Jasanoff & Martello, 2004).

The quantitative part of the survey uncovered deterministic tendencies of experts and lay public, describing their life choices as guided by technology and admitting to technological paternalism and higher technological efficiency that can ultimately replace people in the workplace. It is worth noticing that even the panel of experts admitted to this utopian view on virtual fences and technology in general. Since the survey also targeted respondents from Ukraine, current military unease in the country could account for both Ukrainian experts and lay public welcoming the introduction of virtual fences. As for the rest of respondents, quantitative answers go in line with the utopian technology myth as the general good. The prison scenario revealed general public as welcoming introduction of virtual fences although feeling uncomfortable about it and demanding careful management of technology. Therefore, based on quantitative data respondents can be characterized as technologically deterministic public favoring virtual fences because of their alleged ability to ensure public safety and security, maintaining however necessity for their prudent management and supervision.

The qualitative part consisted of an open question inquiring of public beliefs regarding normal/abnormal behavior. Obtained responses challenge previously identified technological determinism tendency, questioning the "normal behavior" concept as well as the role of engineers in defining it, introducing necessity of human influence and human versatility as compared to technology. Thus, qualitative responses balance earlier ones and suggest soft technological determinism as a more suitable public profile. General public appears in the survey as valuing security but feeling uneasy about virtual fences as a new technology, not being able to predict its capacities and how it plays out in real world. People live in an uncertain environment, requiring more security and technological approach to solve security issues. At the same time, survey respondents require government regulation and a more open design of technology with social and psychological consideration.

Having outlined perspectives of all virtual fences actors, the thesis proceeds to contrasting and comparing identified beliefs in order to map the politics of virtual fences as applied to Belgian prisons, particularly focusing on normal behavior construction.

Throughout the research we noticed that certain tropes and patterns were repeated by different actors as recurring arguments, while for some actors they presented distinct and even opposing attitude. The following chapter will look into these potential points of consensus and disagreement between virtual fences' actors. In order to do that, we distinguish several contentious problems: the construction of algorithms, including design approaches, values at play and responsibility; and the script of virtual fences. Based on these three problems, we then suggest a threefold "deliberative arenas" approach.

4.5 Conclusions of "deliberative arenas"

4.5.1 Algorithm construction

Our first conclusion is that how algorithms are constructed and the notion of "normality" they embed and enact do matter much.

As evident from the questionnaire with engineers, normal behavior algorithm will be built applying statistical context-dependent machine learning approach based on evidence (trespassing secure territory or entering the site through non-projected paths) and subjective judgment. Statistical approach has been earlier criticized in the literature, indicating its limiting and subjecting nature. Some of the actors voice similar concerns. For instance, one of our interviewees referred to drawbacks of statistical approach to normality definition and criticized the idea of machine-learning due to inability of representing all spectrum of dynamic human nature in a static technology. The major concern of general public regarding statistical approach to behavior definition was potential homogenization of public and making it behave to one particular standard, embedded in virtual fences algorithm. Thus, statistical approach to algorithm construction formed the first disagreement between engineers on one side and academics and general public on the other, united by their concerns regarding limitations of such method.

On a personal note, subjective judgment on what constitutes "normal" was also mentioned as a limitation to engineers' method. Despite denying being personally involved in behavior judgment, approaching the definition of threat and intruder for virtual fences engineers employed such abstract categories as "suspicious actions" or "bad intentions," that can be identified based rather on personal experience and full situation awareness than machine employing facts. This raises concerns regarding the subjective nature of algorithms despite attempts to fully automatize it. Engineers' beliefs about what "normal" are instrumental to algorithm design. On top of that, general public adds concerns regarding the sole definition of "normality," claiming that the answer is dependent on who judges it, under which social standards and circumstances, arguing that normal as such does not exist. Therefore, normal behavior definition *per se* forms another discrepancy between industrials and engineers, presenting it as an objective process, and academics and general public, presenting a series of social and subjective limitations to "normality" definition.

4.5.2 Responsibility

The second conclusion we reach is that in such a complex case as virtual fences, responsibilities are distributed but raise potentially conflicting issues. For instance, engineers and the general public might have incompatible visions of whose responsibilities is this particular development. While socio-technical developments should allow for one or several of the entities involved in their development to be held responsible for it, however the distribution of such responsibilities does not go without saying. We detected potential "patterns of contestation" which could lead to open up the conflict on responsibility attribution.

Responsibility for defining human behavior was another stumbling block for virtual fences network. Engineers chiefly denied any responsibility for the verdict the normal behavior algorithm is to deliver, stating that it would be tailored to end-users' needs. At

the same time, end-users remain a fuzzy category, not strictly defined by either the project or the engineers and not taking into account the actors, identified by this research, - general public and prisoners.

Other actors held a different opinion, pointing to engineers as key responsible figures in deciding what "normal" is and embedding their judgment in the algorithm. Some apprehends the technical process of how engineers' beliefs get inscribed in the algorithm. General public also held engineers responsible for the process, suggesting that it is a task more appropriate for trained psychologists than technically-oriented people. However, this transfer of expertise from engineers to psychologists would still obscure the question from public deliberation.

Therefore, responsibility was a crucial point of disagreement between network's actors, occasionally grouping actors in opposing camps, such as engineers on one side and academics and general public on another. Rephrasing Beck in "Risk society" (1992) in explaining redefinition of his role on the project, precisely this constant responsibility delegation and redistribution enables every actor to be preoccupied with their own goals, blaming others for unintended outcomes and making virtual fences a risky endeavor.

Thus, construction of virtual fences normal behavior algorithm presented several consensus and disputing points of virtual fences network's actors. The actors primarily disagreed with engineers on statistical approach to defining behavior, challenged the sole concept of "normal behavior," burdened by industrial values at play, as well as questioned decrease of human factor in prisons as a consequence of virtual fences implementation. Responsibility was another debatable point for the actors, creating particularly risky design environment. The actors' arguments were occasionally in line, especially when challenging the authority of engineers and their methods of algorithm development.

Identified major patterns of agreement and contestation between the actors influence their positions and decisions in the design-arena of virtual fences, encouraging certain decisions and dissuading from others. Outlined patterns also shed light on peculiarities of each actor's mindset regarding virtual fences and became guidelines in tracing the politics of this technology. The following section will be dedicated to formulating the politics of virtual fences.

4.5.3 An arena for actor-specific politics

Our third conclusion, which is yet largely to put into practice, is that conflicting responsibilities are not a problem in itself, but rather a resource we should build upon. As social scientists, we value conflict for its heuristic potential. For this purpose, we tried to bring the question of responsibility into different deliberative arenas, with the consortium partners, the contextual arena of "prisons" in Belgium and the general public. In our view, more publics could be identified and their concerns regarding a technology such as virtual fences unfolded.

As we shall argue later on in the conclusions, whereas a conflict is open up on an appropriate stage, and that all the publics concerned by a decision have been enabled to voice their concerns, the chances is that a greater social acceptability will have been gained throughout the process. This must not and cannot be an instrumental process, as we stressed already in the introduction. This process must be genuinely inclusive at

all stages of development, otherwise the technology is doomed to fail socially. We gave the illustration of all the context-sensitive modes of organisation which should be included, for example in prisons.

In his respect, it is important to remember that the original script of virtual fences as projected by the project designers and engineers is early threat detection in order to issue security alarm. Threat detection revolves around the algorithm of normal behavior, since people whose behavior is deemed abnormal are automatically identified as a threat. Therefore, normal behavior algorithm lies at the core of virtual fences and forms its essential script. However, given research unveiled that the goal embedded in the script of virtual fences initially is not necessarily the one or not the only one pursued by the actors, participating in virtual fences design and implementation in the case of Belgian prisons. This hypothesis can also be traced in the following quote from an engineer/industrial who is managing the project - "My goal as a project manager is to ensure that private goals of the partners do not prevent them from fulfilling the original goal of the project." The variety of approaches that actors exercise to virtual fences lead to believe that they form particular actor-specific politics. Actor-specific politics here builds on the politics in the sense of Feenberg (1999) and Introna (2000) and means a variety of intentions, values, needs and ambitions that guide the actors in design and implementation of virtual fences. Building on the factors, outlined in the section above and particular context of each actor, identified through empirical research, the author laid out the following politics of virtual fences' actors:

1. *Industrials/engineers politics*. During the research engineers' alleged mediating role between end-user needs, policy-makers requirements and end product was challenged by engineers' attempts to push and engage their technological solutions in virtual fences design, trying to make the firm they represent an indispensable focal actor to guide virtual fences design. Being in one group with industrials, both parties also want to innovate and gain expertise at public cost that can later be used for other purposes. Together these project partners create the demand for end-users since they have a product not necessarily having a customer, as witnesses by the Belgian Federal Public Service case. It is also worth noting that engineers/industrials treat technology as neutral, as an empty package that is upon the fuzzy group of end-users to uncover its potential and effectiveness. This artificial separation of technology and its potential use presents a way for engineers/industrials to escape from their responsibility in designing virtual fences. However, the politics of design is evident already when engineers speak of algorithm of normal behavior and make a conscious choice to account for statistical evidence as the sole design basis. Therefore, industrials/engineers politics is oriented towards knowledge and market expansion in the minimum responsibility framework.

2. *Policy-maker politics*. Even though BFPS represents a unique case of both a policy- maker and an end-user for virtual fences project, its responsibilities and goals are different, forcing the author to delineate two types of politics. As a policy-maker BFPS has to conform to international partners, pressuring it to improve prison conditions and solve human rights issues in Belgian prisons. As a partial solution to this, BFPS places building new prisons at the top of political agenda, also employing electronic detention as a version of virtual fences to decrease prison population (electronic bracelet). New prisons come well technologically-equipped, awing partly to industrial lobby and government strategy. According to this strategy and especially in view of forthcoming Belgian parliamentary elec-

tion of 2014, BFPS employs new technologies in prisons as a way to ensure public acceptability of new prisons policy and to demonstrate that new prisons are assisting in providing public safety. By bringing the symbolic technological capital of protection to the foreground, the BFPS adopts a paternalistic technological model, despite strongly criticizing technology in prisons during a private conversation. Therefore, policy-maker politics in case of Belgian prisons is oriented towards ensuring positive public and international image.

3. *End-user politics*. BFPS as an end-user managing prisons also has to worry about improving prison conditions and decreasing prison load. However, it is also preoccupied with managing prison population in balance with human influence. In this regard virtual fences can potentially be employed as an instrument either in the original script version to control access to juvenile sections in large prisons or by primarily using deactivated virtual fences as a stimulus for prisoners to behave well. This view is particularly interesting because it does not consider prisoners as a uniform group, but as a contrasted population, an independent actor in the virtual fences network who is influenced by and influences this technology. Together end-users and prisoners transform the role of virtual fences from a controller of the outside environment to an internal regulator. Therefore, end-user politics is preoccupied with control and management of prisoners. To see the more detailed analysis upon which we derive those observations and potential problems, see section 4.2. and 4.3. below.

4. *Academics politics*. Despite having different positions regarding virtual fences project, social scientists also present specific politics. Enrollment in the EU-funded project with variety of technical partners presents a means to perform research, not necessarily according to project description and an opportunity to freely define their roles and objectives in context of underfinanced independent social sciences research and promotion of industry collaboration research model. Research on virtual fences also embodies a tool to bring out voice of least represented on the project, such as prisoners and outside public, and make technology designers account for them too. The result of academics' work will be outlined in their findings report that can significantly challenge the script of virtual fences as designed by engineers and industrials, depending on the material presented and personal dedication involved. At the same time, academics are restricted by other actors by the projected role of validating social acceptability of virtual fences. Therefore, they have a marginal position in the project, being a project partner on one side and an external observer on the other. This causes difficulties to stabilize their position in the actors' network. Thus, academics politics is oriented towards self-definition on the project and challenging the attitudes of engineers by bringing ethical and social considerations into the project (cf. introduction to this report and "the limits of social acceptability").

5. *Public politics*. Despite explorative nature of the survey, it is possible to make some conclusions regarding general public attitude towards virtual fences. General public is identified as believing in high technological power to ensure prison security and their safety, potentially replacing human security operators. Anticipating increasing technological influence on their lives and fearing being subjected to technology, general public requires careful management of virtual fences from policy-makers as the main guarantor of public safety and security. General public however does not want to be judged by normal behavior algorithms installed in prisons and challenges engineers' approaches to designing,

emphasizing uniqueness of human nature, inability of technology to effectively distinguish “normal” behavior and fearing being forced to conform to behavior standards as predefined by virtual fences. They voice a requirement for an open technological design by the means of social deliberation. Therefore, public politics can be defined as admitting to the paternalistic technological view on ensuring safety and security but challenging engineers’ approaches to technological design and maintaining an importance of public consideration and involvement as well as government regulation in the design and implementation of virtual fences.

Identified actor-specific politics are implemented in parallel to each other and together actors participate in designing virtual fences, challenging its original script, adapting and supplanting it with particular needs of actors.

In conclusion, we identified here several publics, and these defined publics could probably be refined and put on trial throughout further deliberative exercises. We called for raising out loud the plurality of concerns and we set as a requirement the idea that all impacted publics should be dealt with while developing and implementing a technology such as virtual fences. This does not have to stop or lower those processes, but however costly this approach might be, we argue it is a strict democratic necessity and that technology promoters and engineers would have a lot to learn from such a process. It would open up a space for disagreement, hence making more complex the figure of a linear progress which moves on for the sake of humanity as a whole. Rather, it would allow for socially identifying who will benefit from the technology, who will suffer from it, and how due consideration to these questions could greatly improve the development of virtual fences.

5 Conclusions: next steps

In conclusion, we would like to take some time back on the work in this report, in order to better clarify the relationship between evaluation of the social acceptability of technologies and creation of deliberative arenas. This last point will allow us to better explain what we try to do through the implementation of various deliberative arenas and what will be the next steps of the project.

The refusal of an expert position and an utilitarian conception of social acceptability of technologies

As we have stated previously, we initially refused to adopt the position of experts in ethics determining, *a priori*, what is good and just. We refused to consider ethics as an expert knowledge that we mobilize to solve moral dilemmas raised by the P5 project. In addition, we have distanced ourselves with an utilitarian conception of social acceptability of technologies. The problem of an utilitarian approach is that it assumes that what is acceptable to the majority is acceptable to all.

So we refused, first, to consider ourselves as the sole source of legitimacy (stating what *should be*) and, secondly, to limit ourselves to "register" or describe the interests in presence (describing what *is*). In place of these two positions, we opted for a third way: to adopt a position of a facilitator who helps all the stakeholders to deliberate the technology. Following the philosopher Xavier Guchet , we can say that we tried to organize "la mise en réflexivité du processus d'élaboration des normes". Xavier Guchet wrote about the regulation of nanotechnologies "I assume that this is the function of philosophy and humanities in the regulation of nanotechnologies: not saying norms and impose them ready-made, from above, to all the actors of the scientific and technological research (an approach which can claim to remain pure and honest in terms of principles, but that is likely to remain totally ineffective, with no real application); nor inform policy makers on how society works, so that they can implement successful strategies of "social acceptance" (it would simply to exploit our disciplines, invited to divert issues of standards and values to target the only efficiency), but reconcile standards and values on the one hand, and social performance of the other, organizing the necessary reflexivity of the process of elaboration of norms" (Guchet 2010, p. 97).

The confirmation of the need for a third way

Polysemy and heterogeneity of values

We believe that the results of our research presented in this report demonstrate the need to adopt a third way. We have shown the inherent polysemy of the term “privacy”. This concept cannot be considered a value or principle that definitively solves the ethical dilemmas raised by the P5 project. Due to the plurality and heterogeneity of dimensions covered by this concept, we opted for a multidisciplinary approach.

Requalification of space: a collective and political issue

Our research also highlighted the collective and political dimensions of the issues raised by the virtual fences. On many occasions, we have shown that technologies such as virtual fences not only pose questions at the level of the fundamental rights of individuals. Our research also invite us to think about the effects of transformation of our “collective experience”, of the “living-together” in a common space, such as induced by technology.

Based on the work of the philosopher Olivier, we have shown that the virtual fences lead to a re-qualification of the space. The virtual fences redesign and reshape space. Rather than a delimitation of space using physical boundaries materialized by walls, the space is squared by nets which objective is to detect and analyze the profile of moving objects.

This redefinition of the space is not neutral. It is to be linked with the process of defining normal behavior that allows virtual fences technologies to identify anormal and threatening behaviors. Research on prisons highlighted the fact that by erasing material boundaries between prisons and the outer space, virtual fences extend the boundaries of prisons and the network of knowledge collection, subjecting outside public to the judgment of normality.

In our view, this requalification of space raises political questions that can be put forward as done by the philosopher Hannah Arendt. For her, politics is inseparable from the existence of a “public space of appearance”. As Ricoeur points out, for Arendt , “avant toute détermination spécifique en termes d’Etat, (…) la cité humaine constitue le milieu de visibilité requis par les activités que nous caractérisons par des pratiques aussi élaborées que des métiers et professions, des arts, des sports, des jeux, des activités de loisir” (Ricoeur 1991, p. 162). Jonathan Crary says that for Arendt politics must be understood through a balance between this space of appearance and the withdrawal from public life : “For an individual has a policy effectiveness, there must be a balance, a movement back and forth between the light exposure of public activity and the protected, confidential sphere of domestic or private life - what she calls “the darkness of the hidden life” (...) Without this time or space for privacy (...) there would be any possibility to feed the singularity of the self, a self that can make a significant contribution to exchanges that relate to the common good” (Crary 2014, p . 31).

Thinking politics through these images of light, visibility, shadow and hidden life, permit us to question the redefinition of space that induce virtual fence technologies. Don’t they risk to transform the equilibrium between public and private spheres that support the political life ? In addition, by submitting the “common world” to the judgment of normality of the algorithms, do not the virtual fence risk to endangering the Arendtian “plurality”, this essential condition of the common world ? For Arendt, "the politics find its effectiveness in the plurality and not in the adequacy with a preconceived idea of the living together, which was defined by a few. The politics should therefore always maintain that fragile plurality and preserve the space of appearance for

everyone » (Berns, Blésin, Jeanmart, p. 249) Do not the determination of normal behavior risk to endanger the inherent unpredictability of human praxis ?

In our view, further investigate these political dimensions also requires taking distance with an utilitarian conception of the social acceptability of technologies. The latter addresses the question of the legitimacy of technology choices from the aggregation of individual preferences. But is such an approach adequate to account for the political issue that goes beyond the strict framework of individual interests?

Bounded rationality and radical uncertainty

There is one more dimension of the virtual fence that justifies the adoption of a third way between ethical expertise and utilitarian conception of social acceptability. In reference to economics, we can say that they both operate in a regime of "perfect rationality", that is to say, they postulate that it is possible to make an optimal decision, either according to moral standard or reference to a calculation of interests. However, the virtual fence plunge us further into a horizon of bounded rationality, for the simple reason that it is a new technology that has not yet been implemented. Faced with the possible effects induced by this technology, we are in a context of "radical uncertainty" (Knight, Keynes, 1921) : we can not list the possible effects, as we can not calculate the probability of occurrence of this effects.

To put it differently, in a bounded rationality regime, facing a radically uncertain future, the individual does not know what their individual preferences are. Therefore it can not be simply to decide among competing ethical values or aggregate individual preferences. A third way is to be opened that allows to organize a debate on the preferences and interests involved.

Towards public participation with virtual fences

Several results of our research therefore justify the adoption of a third way that seeks to adopt a position of facilitator who helps all the stakeholders to deliberate the technology. To this end, we created different deliberative arenas around the virtual fences. Finally, we would like to draw different points of deepening on which we want to work in the next steps of the project.

Problematize the notion of "public"

It seems useful to problematize the notion of "public". A similar remark to what we did about privacy can be made here. The term public is deeply polysemous. A diversity of concept is used to account for the actors involved in technology: users, stakeholder, citizen, etc. Polysemy and instability of the concept of the public must also be related to the fact that virtual fences plunge us in a regime of "bounded rationality" : we do not know a priori with certainty who will be affected by these new technologies. Moreover, as we noted, because of the political dimensions of several issues raised by the virtual fence, we can not limit ourselves to an utilitarian conception of the public who would equate it to the aggregation of individual preferences.

It would be helpful here to rehabilitate the pragmatist conception of public which has been problematize by John Dewey in *The Public and its Problems*. "Public" means a community of action. Rather than being based on a given collective identity or a strong consensus, a public is constituted through perception of the consequences of joint actions and of the efforts of joint control of these consequences. Ulrich Beck writes, in-

spired by Dewey: “As such, decisions leave indifferent. It is only the perception of consequences, communication on the problems they cause, annoys, worried a shock, tears individuals to their indifference and their selfish life and creates the unifying element and the community spirit of a public action space” (Beck 2002-2003, p. 893).

An experimentalist approach

The public in the pragmatist sense should not be understood as an ideal “we” or a “we” already given. It is to discover. It is to be experimented through action. In other words, the public is not the starting point of the deliberative process. Rather, it is produced through the process of deliberation. We have to think the organization of deliberative arenas so as to make possible such an experiment. To do this, the work of neopragmatists authors like Charles Sabel and Joshua Cohen may be useful. They do not consider space of deliberation as a forum for discussion, but as a form of problem-solving. Decentralizing spaces of deliberation and organizing deliberation around problem to solve may make possible a true “democratic experimentalism” (Sabel, Dorf 1998).

A contextual approach

Such a conception of deliberation must necessarily take a contextual form. We must anchor the debate in concrete problematic situations. This is what justified the choice to work on prisons. We must therefore multiply spaces of contextual deliberation. But we must not limit ourselves to contextualize and multiply deliberative arenas. We will also seek to confront these contextual deliberations, to build a social diagnosis of virtual fences.

On this point, “democratic experimentalism” is interesting because it aims to make possible a double learning : a local learning through decentralization of local experiments, and a social learning through the comparison of local experiments. In democratic experimentalism, far from being centralized in the parliamentary space, the public sphere is “organizationally dispersed” (Cohen, Sabel 1997, p. 337) through all the local spaces of resolution of problems.

Specifically, it will be for us to operate in two steps. First, organize arenas of contextual deliberation. Secondly, imagine procedures of confrontation of local experiments that allow to operate a or “mutual evaluation” which increases the capacity of social diagnosis by producing a “more complete definition and imaginative exploration of problems and solutions” (Cohen, Sabel 1997, p. 333) .

The ambivalence of the need for reflexivity

A final remark is necessary on what we can call the “ambivalence” of public deliberation about technology. In recent years, a requirement for participation of citizens is heard in our representative and technocratic societies. “Hybrid forums” and consultation spaces have emerged to compensate for the lack of legitimacy and efficiency of traditional mode of governance.

Rosanvallon showed in *La légitimité démocratique* (2008) how democratic legitimacy is linked today to a new principle of legitimacy: a legitimacy of proximity. Today, the democratic legitimacy also requires the involvement of citizens in the exercise of authority, their participation in the decision making process. Blondiaux and Sintomer suggest the existence of a genuine “deliberative imperative” (Blondiaux, Sintomer,

2002). These two authors raise a question about this new “imperative” that seems essential to keep in mind when we face the issue of social acceptability of technologies: are these process of participation new techniques of government or instruments of real democratization of the political decision? Xavier Guchet raises a similar question: “The crucial question is therefore: is it to organize public debates to make individuals actually able to influence the big choices of society - first by creating the conditions for the desire for the public life to flourish? Or is it to promote the “process of subjectivation” in the interests of industrial nanotechnology - which need, it was said, of “reflexive” subjects but captured ?” (Guchet 2011, p. 440-441).

If the opening of deliberative arenas to non-specialists represents some interest to democratize technology development, we need to ensure that this opening does not serve a single objective of legitimation of technological development. To this end, we should be able to make the *evaluation* of deliberative arenas possible. In the words of Michel Callon: do theses arenas have helped to expand the inventory of the groups involved, the inventory of connections between the problems and the exploration of options? (Callon 2001, pp. 50-54). We will also seek, in the next steps of the project, to dig this issue of evaluation of the deliberative arenas.

Tables and Figures

Bibliography

Akrich, M., 1992. The de-scription of technical objects, in Bijker, W., and Law, J. (eds), *Shaping Technology / Building Society: Studies in Sociotechnical Change*, Cambridge (MA) : MIT Press.

Aradau, C., 2010. Security that matters: critical infrastructure and objects of protection, *Security Dialogue*, 41(5), pp. 491-514.

Antonakaki, P., Kosmopoulos, D. & Perantonis, S., 2009. Detecting abnormal human behaviour using multiple cameras. *Signal Processing*, 89(9): 1723-1738.

Bartlett, S. J., 2011. Normality Does Not Equal Mental Health: The Need to Look Elsewhere for Standards of Good Psychological Health, *ABC-CLIO*.

Beck, U., 1992. *Risk Society: Towards a New Modernity*. California: Sage Publications.

Beck, U., 2002-2003. Le risque comme principe d'espace public. in *Commentaire*, n°100.

Berns, T., Blésin, L. and Jeanmart G., 2010. *Du courage, Une histoire philosophique*. Editions les Belles Lettres.

Bijker, W. E., & Law, J., 1992. *Shaping technology / building society: Studies in sociotechnical change*, Cambridge (MA): MIT press.

Bijker, W. E., Bal, R., & Hendriks, R., 2009. *The paradox of scientific authority: The role of scientific advice in democracies*, Cambridge (MA): MIT press.

Blondiaux, L. and Sintomer, Y., 2002. "l'impératif délibératif", in *Politix*, Vol. 15, n° 57.

Boiman, O. & Irani, M., 2007. Detecting irregularities in images and in video, *International Journal of Computer Vision*, 74(1), pp. 17-31.

Brand, M., *et al*., 1997. Coupled hidden Markov models for complex action recognition. Computer Vision and Pattern Recognition, 1997. *Proceedings. IEEE Computer Society Conference*, IEEE.

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.

Butler, Z., Corke, P., Peterson, R., Rus, D., 2006. Dynamic virtual fences for controlling cows. *Experimental Robotix IX: The 9th International Symposium on Experimental Robotics*: 513- 522.

Callon, M., 1987. Society in the making: the study of technology as a tool for sociological analysis. *The social construction of technological systems: New directions in the sociology and history of technology*, Cambridge (MA): MIT Press, 83-103.

Callon, M., Lascoumes, P. and Barthes, Y., 2001. *Agir dans un monde incertain*. Paris: Seuil.

Cohen, J., Sabel, C., Directly Deliberative Polyarchy, in *European Law Journal*, 3:4, 1997, pp. 313-342, p. 337.

Crary, J., *24/7,* 2014. *Le capitalisme à l'assaut du sommeil*. Paris: Éditions La Découverte.

Daniels, N., 1985. *Just health care*, Cambridge (UK): Cambridge University Press.

DeCew, J., 2012. Privacy, in Zalta, E. N. (ed), *The Standford Encyclopedia of Philosophy*, Standford: The Metaphysics Research Lab.

Deleuze, G., 1992. Postcript on the Societies of Control, *October*, 59 (Winter), pp. 3-7.

Despret, V., 2009. *Penser comme un rat*, Paris: QUAE.

Desrosières, A., 2008. *L'argument statistique: Gouverner par les nombres*, Paris : Presses des Mines.

Dewey, J., 1975 (1st ed.: 1916). *Démocratie et éducation*. Paris, Armand Collin.

Dourish, P., & Bell, G., 2011. *Divining a Digital Future - Mess and Mythology in Ubiquitous Computing*, Cambridge (MA) : MIT Press.

Dourish, P., & Anderson, K., 2006. Collective Information Practice: Exploring Privacy and Security and Culture Phenomena, *Human-Computer Interaction*, 21(3), pp. 319-42.

Fallan, K., 2008. De-scribing design: Appropriating script analysis to design history. *Design Issues*, 24(4): 61-75.

Feenberg, A., 1999. *Questioning Technology*, London: Routledge.

Finn, R., Wright, D., & Friedewald, M., 2013. Seven Types of Privacy, in Gutwirth, S., *European Data Protection: Coming of Age*, Dordrecht: Springer, p. 4.

Foucault, M., 1991. Introduction, in Canguilhem G., *The normal and the pathological*, New York, USA: Zone Books.

Foucault, M., 1995. *Discipline and punish: the birth of the prison*. New York, Vintage Books.

Foucault, M., 2004, *Sécurité, territoire et population. Cours au Collège de France 1977-1978*, Paris: Gallimard.

Frieddewald, M., & Bellanova, R., 2012. Deliverable 1.1: Smart Surveillance - State of the Art, in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies*, EC: 7th Framework Programme.

Gjoen, H. & Hard, M., 2002. Cultural politics in action: Developing user scripts in relation to the electric vehicle. *Science, Technology, & Human Values*, 27:262.

Guchet, X., 2010. La régulation des nanotechnologies, Quel rôle pour la philosophie ?, in Lacour, S. (dir.), *La régulation des nanotechnologies, Clair-obscur normatif*, Bruxelles, Larcier, 2010, pp. 89-97.

Guchet, X., 2011. Sociétés réflexives et nanotechnologies, in Maesschalck, M. et Loute, A. (éds.), *Nouvelle critique sociale, Europe-Amérique Latine, Aller-Retour.* Polimetrica: Monza, 2011.

Gutwirth, S., 2002. *Privacy and the Information Age,* Lanham/Boulder/New York/Oxford: Rowman 1 Littlefield Publishers, 30.

Hilgartner, S., & Bosk, C. L., 1988. The Rise and Fall of Social Problems: A Public Arenas Model. *American Journal of Sociology*, 94 :1, pp. 53-78.

Helzer, J. E., 2002. *Defining psychopathology in the 21st century : DSM-V and beyond*, Washington, D.C.

Introna, L.D. & Nissenbaum, H., 2000. Shaping the Web: Why the politics of search engines matters. *The Information Society*, 16(3), pp. 169-185.

Jelsma, J., 2003. Innovating for Sustainability: Involving Users, Politics and Technology. *Innovation: The European Journal of Social Science Research*, 16(2), pp. 103-116.

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

Latour, B., 1987. *Science in action: How to follow scientists and engineers through society*, Cambridge (MA): Harvard university press.

Latour, B., 2012. *Enquête sur les modes d'existence. Une anthropologie des modernes*. Paris : La Découverte.

Law, J., & Callon, M., 1992. Engineering and sociology in a military aircraft project: A network analysis of technological change, in Bijker, W. E., & Law, J. (Eds.), *Shaping technology/Building society: Studies in sociotechnical change*. Cambridge, MA: MIT Press.

Marris, C., *et al*., 2001. *PABE Final Report*.

Moeslund, T. B., *et al.*, 2006. A survey of advances in vision-based human motion capture and analysis. *Computer vision and image understanding*, 104(2), pp. 90-126.

Netz, R., 2010. *Barbed Wire*: *An Ecology of Modernity*, Wesleyan University Press.

Nissenbaum, H., 2010. *Privacy in Context. Technology, Policy and the Integrity of Socail Life* (Standford: Standford University Press, 2010), 1-4.

Oliver, N. M., *et al.,* 2000. A Bayesian computer vision system for modeling human interactions. *Pattern Analysis and Machine Intelligence, IEEE Transactions*, 22(8): 831-843.

Pfaffenberger, B., 1992. Technological dramas. *Science, Technology, & Human Values*, 17:282-312.

Pinch, T. J., & Bijker, W. E., 1984. The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other. In Pinch, T. J., & Bijker, W. E. (eds), *The social construction of technological systems: New directions in the sociology and history of technology*, Cambridge (MA): MIT Press, pp. 1917-1950.

Rabiner, L., & Juang, B.-H., 1986. An introduction to hidden Markov models. *ASSP Magazine, IEEE*, 3(1), pp. 4-16.

Ramsden, P., 2013. *Understanding Abnormal Psychology: Clinical and Biological Perspectives*. California: Sage Publications.

Razac, O., 2009. *Histoire politique du fil barbelé,* Paris: Flammarion.

Razac, O., 2013. La gestion de la permeabilité, *L'espace politique*, 20(2), 20 p.

Ricoeur, P., 1991. Langage politique et rhétorique. in *Lectures 1, Autour du politique.* Paris: Seuil, pp. 161-175.

Rouvroy, A., & Berns, T., 2010. Le nouveau pouvoir statistique, *Multitudes*, 40(1), pp. 88-103.

Sabel, C. and Dorf, M. C., 1998. *A Constitution of Democratic Experimentalism*. Cambridge MA: Harvard University Press.

Sabin, J. E., & Daniels, N., 1994. Determining "medical necessity" in mental health practice. *Hastings Center Report*, 24(6), pp. 5-13.

Sarbin, T.R., & Mancuso, J.C., 1980. *Schizophrenia: Medical Diagnosis or Moral Verdict?*, New York: Pergamon.

Scheff, T. J., 1966. *Being mentally ill: A sociology theory*. Chicago: Aldine.

Synofzik, M., 2009. Ethically justified, clinically applicable criteria for physician decision-making in psychopharmacological enhancement, *Neuroethics*, 2(2), pp. 89-102.

Thaler, R. H., & Sunstein, C. R., 2008. *Nudge: Improving decisions about health, wealth and happiness*. London: Penguin Books.

Szasz, T. S., 1960. The myth of mental illness, *American Psychologist*, 15(2): 113.

Timmermans, S., & Epstein, S., 2010. A World of Standards but not a Standard World: Toward a Sociology of Standards and Standardization. *Annual Review of Sociology*, 36(1), pp. 69-89.

Watson, H., & Wright D. (ed.), 2013. "Deliverable 7.1: Report on Existing Surveys," in *PRISMS. The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making,* EC: Seventh Framework Programme.

Winner, L., 2006. Do artifacts have politics?, in Teich A. (ed.), *Technology and the future*, 10th ed., pp. 50-92, Belmont, CA: Thomson/Wadsworth.

Wyatt, S., 2008. Technological determinism is dead; long live technological determinism, In Hackett, E., Amsterdamska, O., Lynch, M., & Wajcman, J. (eds), *Handbook of Science and Technology Studies*, Cambridge (MA): MIT Press, pp. 165-180.

Yamato, J., *et al*., 1992. Recognizing human action in time-sequential images using Hidden Markov Model. Computer Vision and Pattern Recognition, 1992. *Proceedings CVPR'92., 1992 IEEE Computer Society Conference on, IEEE*.

Zhong, H., *et al*., 2004. Detecting unusual activity in video. Computer Vision and Pattern Recognition, *Proceedings of the 2004 IEEE Computer Society Conference*.

Acronyms

P5 Privacy Preserving Perimeter Protection Project

STS Science and Technology Studies

Annexes

Annex A

First Guidelines

Author	François Thoreau, uNamur	Date	31/10/2014
		Deliverable	D2.1
Co-Author	Jérémy Grosman, uNamur	Version	Prel, 27/10/2014
	Olya Kudina, uNamur	B/W Print	Yes
	Alain Loute, uNamur	Page Count	2 plus annexes

Privacy on Critical Infrastructure

Further than Privacy

One of the main aim of the project is to develop *privacy-preserving* technologies. Is implicitly assumed the fact that the principal problem raised by the surveillance system can be grasped through the notion of privacy. However, we can not induce from the privacy-preserving technological aspects of the project that privacy will be the only relevant concern, from socio-ethical perspectives. Indeed, our current and next reports show how it raises larger political issues that can be intuitively grasped as an « excess of power ».

Further than Critical Infrastructure

Related to that, the restriction of the project scope to critical infrastructures does not appear to be pertinent. According to the sites selected, and the usual clients of the P5 partners, a large part of the installations done and considered will not fit the Critical Infrastructure as defined in the European official documents. Moreover, one of the cases initially selected by P5 partners – the prisons – does not clearly appear as a critical infrastructure. As a consequence, the ethical and social cases considered should be extended to every infrastructures supposedly interested in a such system.

Further the report

As developed in the report, the cases we studied do not provide any general or particular « go » or « do not go ». Therefore, the planned workshops will complement the reports. The main purpose of the workshops shall be to lead partners to interrogations and exigencies they are not used to deal with. Indeed, just as an appropriate scientific or technical activity cannot be processed and check through a bullet point list, so does the socio-ethical expertise.

Monitoring without Identifying

Thermal cameras, radar sensors and « automatic blurring faces algorithms » are supposed to achieve the privacy-preserving aim. If these features appears to be very promising, we should draw attention on aspects of the problem they do not solve.

Data Storage and Blurring

First, concerning the data storage. If the stored data is 'raw', untouched by the blurring feature, the goal is missed. Indeed, it would mean that the only use of this procedure would be to prevent the security agent from recognizing a passer-by. In most cases, this aspect of the surveillance system does not constitute the core of the privacy threat, it is rather incident. Therefore, if the stored data remains raw, the privacy preserving apparatus does not tackle the main problem. We would therefore recommend to store, by default, blurred data.

Non Identifying Technologies

Second, concerning the efficiency of thermal cameras and blurring faces algorithms as privacy-preserving technologies. It is not at all obvious that such technologies make impossible the recognition of individuals. In a wide variety of cases, the sole silhouette contains sufficient information for identifying a person. We could therefore imagine an extended version of the algorithm, not only blurring the faces, but the whole body of the passer-by. To a certain extent this argument can be transposed to the case of thermal cameras. Since efficient thermal cameras allow an accurate distinction of the silhouette, we could ask if it is not pertinent to blur it as well.

Workplace Surveillance

Third, concerning the recognition of known people. Since the sites targeted generally include a security perimeter, by definition rarely frequented, it inevitably raises the problem of the identification of the security team, and more generally of the workers occupying the sites. One could easily imagined that, even fully blurred silhouettes, allow the control of monitoring rounds. Thus the privacy-preserving apparatus does not avoid the traditional ethical as well legal problem of « workplace surveillance ».