SEVENTH FRAMEWORK PROGRAMME

Collaborative project
Small or medium-scale focused research project
FP7-SEC-2011-1
Grant Agreement no. 285533

TACTICS

TACTICAL APPROACH TO
COUNTER TERRORISTS IN CITIES

TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	6.2
Title	Ethical overview
Author(s)	TCD, ITTI, PRIO, TNO
Due date	30/11/2014
Delivered date	27/2/2015
Dissemination level	PU
Contact person EC	Mr. Ngandu Mupangilai

Cooperative Partners	
1.	LERO
2.	TNO
3.	ITTI
4.	PRIO

Table of Contents

Executive Summary

The use of TACTICS raises many challenges in regards to privacy, ethics, human rights and legal aspects. This report provides an insight of the privacy considerations investigated and the resulting measures to make the system less privacy invasive and make its use even more ethical. To this end, we illustrate the legal background, mainly focusing on European privacy and data protection regulations. Where appropriate, we explain the technological challenges that these regulations introduce and discuss how they could be resolved. Due to the interaction of the TACTICS components, even if the deliverable is targeted to the TMT, the discussion in several parts is more spherical, as there is a need to discuss other aspects as well. Note that the main focus of the deliverable is on the TACTICS system and not validation prototype.

After the introduction, chapters 2 and 3 discuss the ethical and legal implications of surveillance, deviant behaviour and biometrics, respectively. The main principles are the ones of proportionality, fairness, legality and expediency. In chapter 4 we discuss some applicable legal requirements for the TACTICS system, and in chapter 5 we provide an overview of some of the related Private Enchancing Technologies that can facilitate making the TACTICS system even more privacy aware. The report concludes in chapter 6. In the appendix, we provide some implementations that can guide the technical reader in implementing some of the methods referred to in the report.

The most relevant challenges related to the TACTICS system, and the TMT in particular, concerning legal conditions, ethics, human rights and privacy as well as some extensions on them, are described. Moreover, we have provided an overview of how some of these problems could be resolved from the technological and implementation aspect.

The nature of the TACTICS system makes it balance on the legal and ethical limits of current legal and ethical framework. It should be understood that the TACTICS system is the last resort in order to prevent an extreme event, a terrorist attack, for which the information is very sparse. One could go back to Hippocrates and his quote “For extreme diseases, extreme methods of cure, as to restriction, are most suitable.” and claim that “desperate times (a terrorist threat) call for desperate measures (use of TACTICS)”, nevertheless, after several centuries we have the technological means to contain these desperate measures and make them less invasive.

Regardless of the methods, the scope of the TACTICS system is ethical as it can prevent a terrorist attack and save many human lives. However, its use must be strictly contained in this sole environment and event, any further use makes it unethical. Its capabilities and resources set very strict constraints on when it is used, who is using it, where it is used and for how long. As discussed in this report, most of these aspects can be resolved with technological means, e.g. strong authentication, authorization protocols, blurring of faces on camera images (many of which have already been implemented in the prototype). Nevertheless, it is important to note that while there is a solid European framework on Data Privacy, the fragmentation of the legal system in each member country implies further and different constraints. Moreover, practically each member country has its own system to deal with such extreme events, setting even more practical constraints in terms of a unified approach as each member has different authorization models, different procedures and different structures. Therefore, even if TACTICS provides a baseline approach, compliant with EU regulations, configuring it for each member possible member state is still an open challenge, specially, when this legal framework is not stable and is subject to changes, but this is out of the scope of this project.

1 Introduction

TACTICS is a cyber-physical system[1] designed to deal with threats to national security involving a potential for mass deaths or catastrophic damage to national critical infrastructures. To avoid such catastrophic damages, TACTICS gets input from the intelligence and operates in a very well defined timeframe to collect information and help anti-terrorist units prevent the strike. For this purpose, and only under specific guarantees and based on specific law, it should be considered justified for a national force to intrude the privacy of individuals for the sake of their security and well-being. One could regard this in accordance with the definition of privacy of Westin Margulis, fitted for the public and not the individual citizen:

"*Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability*"[2]

Nevertheless, the capabilities of TACTICS may point to "big-brother" scenarios or oppressive panopticon designs[3], which can certainly be augmented in the eyes of the public after the recent Snowden disclosures on the dataveillance[4] of citizens. The main reason for this is that:

"*Both collecting and collating personal information are ways of acquiring power, usually at the expense of the data subject*"[5]

As noted by Gutwirth and De Hert, the rationale of both privacy and data protection are those of typical "constitutional tools":

"*the history and the practice of democratic constitutional states […] always reveal the use and articulation of two distinct constitutional or legal tools. On the one hand there are tools that tend to guarantee non-interference in individual matters and the opacity of the individuals. On the other hand […] tools that tend to organise and guarantee the transparency and accountability of the powerful. These two instruments have the same ultimate objective, namely the limiting and controlling of power but they realise this ambition in a different way, from a different perspective*"[6].

In this regard, citizens have many reasons to be worried about the use of TACTICS, since not only does the system automate the data collection procedures, but it also performs data aggregation and fusion which can further expose innocent citizens[7]. However, it is important to understand that privacy cannot be understood isolated from the other human rights; it has to be understood in the wider context. For instance, Etzioni states that:
"*privacy is not an absolute value and does not trump all other rights or concerns for the common good*"[8]
which leads Solove to argue that:
"*The value of privacy should be understood in terms of its contributions to society.*"[9]

---

[1] Lee, Edward A. "Cyber physical systems: Design challenges." Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on. IEEE, 2008.

[2] Margulis, S. T. 2003a. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," Journal of Social Issues (59:2), pp. 411-429.

[3] Foucault, Michel. *Discipline and punish: The birth of the prison*. Random House LLC, 1977.

[4] Clarke, Roger. "Introduction to dataveillance and information privacy, and definitions of terms." Roger Clarke's Dataveillance and Information Privacy Pages (1999).

[5] Froomkin Michael A. (2000) The Death of Privacy; Stanford Law Review, Vol. 52, No:5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May 2000), pp. 1461-1543.

[6] Gutwirth, Serge, and Paul De Hert (2008) "Regulating profiling in a democratic constitutional state." In *Profiling the European citizen. Cross disciplinary perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 271-291. Dordrecht: Springer, p. 275 (italics in original).

[7] Paul Ohm (2009) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation; 57 UCLA Law Rev. 1701.

[8] Amitai Etzioni (1999) The Limits of Privacy, Basic Books; NY.

[9] Solove, Daniel J., "Understanding Privacy"; Harvard University Press; Cambridge, MA, 2008.

The positive outcome to the society means that privacy violation can be justified if it is for the sake of the common good. In this regard, the use of TACTICS, despite the temporary privacy violations, can be justified, as its scope is to protect citizens from imminent terrorist attacks. This justification is also depicted in the European Charter on Human Rights, and in particular Article 8 which sets limitations and exemptions to privacy. More precisely:

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

Both the right to privacy and the right to the protection of personal data have been also enshrined in the Charter of Fundamental Rights of the European Union (EU): respectively as Article 7 and Article 8. As noted above, there is a distinction between data protection and privacy. Nevertheless, the two notions are correlated in many aspects. A fundamental differentiation in regard to where a problem resides is based on whether the collected data concern the private life of the individual. If that is the case, the EU Directive 95/46/EC should always be applied (the so-called Data Protection Directive)[10].

While countering terrorism is generally considered a legitimate purpose to set limitations of other rights to preserve the security of the people, there must be some restrictions on how far these limitations can be applied. For example, in the recent judgement concerning the so-called EU Data Retention Directive (cf. section 1.3 below), the EU Court of Justice states that:

"As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary"[11].

A previous United Nations Special Rapporteur on respecting human rights while countering terrorism, based on the International Covenant on Civil and Political Rights has proposed the following guidelines[12]:

(a) Any restrictions must be provided by the law (paras. 11–12);

---

[10] It should be noted that the Data Protection Directive, adopted in 1995, has been transposed by all EU member states (and other non-EU countries). Currently, a major reform of this and other legislative instruments in the field of data protection is undergoing (but has not yet been finalized). Finally, it should be noted that the Data Protection Directive does not cover the processing of personal data for state security and law enforcement purposes (cf. Article 3(2)). This kind of processing is generally regulated at the level of national legislation, and specific forms of data exchange and processing are regulated by other European instruments (e.g. the so-called Council Framework Decision 2008, regulating the transfer of data between member states, or the specific provisions of the Visa Information System, etc.). Nevertheless, it should be also considered that all these forms of processing, including for state (or national) security and law enforcement, have to respect the European Convention of Human Rights, the Charter of Fundamental Rights and the relevant case-law of the European Court of Human Rights and of the EU Court of Justice (and obviously, the national laws, constitutions and the related national case-law).

[11] Judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria)) – Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12), paras 51 and 52 [available online at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=81736]. Hereinafter: Joined Cases C-293/12 and C-594/12

[12] Scheinin, Martin 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism'

(b) The essence of a human right is not subject to restrictions (para. 13);

(c) Restrictions must be necessary in a democratic society (para. 11);

(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);

(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);

(g) Any restrictions must be consistent with the other rights guaranteed in the ICCPR (para. 18).”

The scope of this deliverable is to highlight some ethical and privacy concerns that arise by the use of the TACTICS system, report some related legal background and propose some technical details on how these could be tackled to make it more privacy-aware. However, this report has no ambition to provide an exhaustive analysis of all ethical, legal and socio-political aspects potentially linked to TACTICS. Two other reports – Deliverables D4.3 and D5.4 – contribute to complete an overview of the main issues, and potential solutions, linked to the development of a TACTICS-like system. Furthermore, it should be noted that these reports should not be considered as an ethical and/or legal validation of the TACTICS system, but a sort of “companion” to the work carried on within the TACTICS project. The main reason is that the very purpose and scope of TACTICS-like systems necessitates an adoption at national level, and therefore a preliminary adjustment, and verification, of its design to specific national legal requirements and administrative constraints. While the European Union (EU) and the international legal frameworks provide essential references and guidance, the conditions of possibility and legitimacy of counter-terrorist systems are highly dependent on national legislations and regulations. Therefore, the decisions taken in each specific implementation of TACTICS would be crucial for the ethical and legal validation of the system, and each time a tailored, and thorough, assessment will be needed.

Finally, it is important to note that the validation system that was built to evaluate the efficacy of the whole project, and that it was deliberately designed to be modular in several aspects to allow extensibility for future technologies and features. While some initial measures to secure the system have already been implemented, many features regarding privacy were tested separately, but were not included in the complete validation system. The main reasons for not including them in the validation system were the performance overhead, and that many of these methods cannot be found in commercial projects, but only experimental academia projects, therefore, not stable enough for validation on the TACTICS maturity level. However, the architecture of the project can easily be adapted to embed them.

2 Legal and ethical aspects of surveillance

Generally, the term surveillance is associated with the video surveillance systems; however, nowadays this notion has been extended to also include other means. The scope of surveillance is to monitor groups and individuals in order to prevent an unlawful action or timely detect it. However, it must be proportionate to the problem it is trying to solve[13]. EU laws permit the use surveillance or interception of communications[14] as long as this is provided for by law and it constitutes a necessary measure in the interest of: protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others. In this regard, the use of these methods within TACTICS is legitimate, nevertheless, the amount of information that is collected from individuals, must be justified and subject to the level of threat of each stage, to avoid excessive privacy invasion of individuals who are not involved. It should be highlighted that the nature of current surveillance systems extends their scope, as most of them fuse information with other sources. For instance, a camera provides number plate detection or face detection and it is connected with a database to identify the car or individuals, or automated cross-checking the passenger list with the payments and the database of suspected terrorists. Therefore, modern surveillance is extended to what is now called *dataveillance*, which has been proven far more effective.

Despite its effectiveness, dataveillance is prone to profiling as a means to aggregate the results that are presented to the controller. The initial definition of profiling was given by Clarke according to whom: “It is a means of generating suspects or prospects from within a large population, and involves inferring a set of characteristics of a particular class of person from past experience, then searching data-holdings for individuals with a close fit to that set of characteristics”[15]. While this definition matches very well with the common practice of everyone to interpret things in our daily lives, the results of profiling in surveillance can introduce many ethical issues as it can easily introduce biases based on sex, religion, look or race of the data objects and be used to limit their freedom and invade their privacy without any actual evidence.

Mass dataveillance, also defined by Clarke, “is concerned with groups of people and involves a generalized suspicion that some (as yet unidentified) members of the group may be of interest.” The key difference in this case, compared to individual dataveillance is that it involves many individuals and all their transactions “Whether or not they appear to be exceptional.”. The concerns about mass dataveillance, the applied methods and its extent have been drastically augmented after the latest revelations from Snowden. Nevertheless, the Commission acknowledges that: “(…) the ever growing importance, in terms of legislative activity, of the area of Justice, Freedom and Security (…) increasingly (…) raise fundamental rights issues”[16], which more or less accepts that the balance between human rights and security that was held for many years has been disrupted by the recent terrorist events, forcing a trade-off between security and rights. Therefore, it can be considered legitimate, up to a certain degree[17], to limit some rights to provide security[18].

It should be understood that some resources, e.g. traffic cameras, are governed by specific legal bases, therefore the data processing is allowed for a specific purpose only. Even if the data are used for another legitimate purpose for the sake of public safety, their legitimate processing is limited to its initially specified purpose. Therefore, further processing, especially the use from a third party such as the TACTICS system,

---

[13] On 24/7/2013, the Information Commissioner of UK issued a decision asking the Hertfordshire police to stop using their vehicle plate tracking system. The reason was that collected data were stored in the databases for far longer than needed, exposing further information about individuals.

[14] Note that this involves electronic communications pertains not only to the content of a communication but also to traffic data, such as information about who communicated with whom, when and for how long, and location data, such as from where data were communicated.

[15] Clarke, Roger. "Information technology and dataveillance." Communications of the ACM 31.5 (1988): 498-512.

[16] 1 European Commission, 'Report on the Practical Operation of the Methodology for a Systematic and Rigorous Monitoring of Compliance with the Charter of Fundamental Rights. Com(2009) 205 Final', at 3.

[17] Martin Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', (Geneva: General Assembly 2009b).

[18] Articles 3.2 and 3.5, 21.2 (a) and (c) of the Treaty on the European Union

requires legal justification, which in most of these cases are governed by national security laws that vary in each EU member. Note that Convention 108, Article 8(a) introduces the transparency principle allowing each data subject to access their data whenever they are processed, the use of TACTICS falls within the exemptions of Articles 10 and 11, nevertheless, this implies that it should justify all actions to the according authorities. For instance, in Köpke v. Germany[19] the use of covert surveillance video within a workplace to determine whether an individual was stealing was considered a legitimate means to achieve the goal. On the contrary, in Allan v. the United Kingdom[20] the court decided that secretly recording (through audio and video) all the conversations of a prisoner with one of his visitors and with a co-accused was invading the right to private life. It should be highlighted that while one could justify these actions by the fact that they could provide additional information regarding the legal case, at that period the UK had no legal regulations regarding the use of covert recording devices by the police. Finally, due to the proper use of safeguards to regulate information flow, the court concluded that there had not been a violation of Article 8 of the ECHR in case of Klass and Others v. Germany[21] as the interception of communication was in accordance with German legislature and justified to preserve the interests of national security and prevent disorder or crime.

Due to the huge amount of data, it is practically impossible to have operators monitor all the data that a system such as TACTICS can collect and process. The system, as a human artefact, can have bugs, but the bigger danger is that such systems try to link information from different sources in order to connect them to a specific goal. During this process and the constraint that facts are definitely connected, a system can derive very loose links and overlook obvious logical constraints wrongly identifying an individual into certain categories.

Within the context of surveillance, TACTICS focusses on a limited set of specific technologies: biometrics and the detection of deviant behaviour. The legal and ethical aspects of both are discussed in the next subsections and chapter. The legal and ethical framework around biometrics is more mature, so this warrants a more extensive deliberation in a separate chapter.

2.1 Ethical implications of detecting deviant behaviour

One of the important issues that are raised from the use of TACTICS is the detection of deviant behaviour, i.e. predictive behavioural profiling. TACTICS end users can apply this in different use cases or combinations thereof.

First, they can choose to have trained professionals look for deviant behaviour. Based on interaction with the public, these professionals can decide to select individuals for further security questioning. Second, they can use ICT systems, such as behavioural camera's, to look for specific predefined patterns of behaviour.

The main challenge in this regard is how to define deviant behaviour, as in principle there is no average human behaviour. TACTICS describes nine different kinds of deviant behaviour[22], and does not enforce or prevent specific kinds.

It is quite common to create many misunderstandings by removing the context from some actions and reactions. The human factor has simultaneously several benefits and shortcomings, especially when it comes to the evaluation of a given event. While one could infer many important details from the context of the event, the body language and human interaction, it is very difficult to remove personal biases, which in the case of TACTICS can lead to discrimination based on ethnicity, age or gender, or even unnecessary casualties. The automated approach that the TACTICS system introduces has the potential to increase this impact. For instance, the fact that a camera shows a citizen sweating while standing in the queue could have different interpretations, the citizen was running to get to the queue on time, or that the temperature is high. Therefore, if the system is programmed to highlight sweating as a deviant behaviour, e.g. caused from anxiety, lying etc., then the amount of false positives is potentially very high. Nevertheless, a "human sensor" could easily realize this context and not signal any alert. Note that signalling an alert by the TACTICS system could lead to further actions with possible privacy invasion to the citizen, which in the aforementioned case could be unnecessary and unjustified. On the other hand, while a "human sensor" could understand the

[19] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-101536#{"itemid":["001-101536"]}

[20] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-60713#{"itemid":["001-60713"]}

[21] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510#{"itemid":["001-57510"]}

[22] TACTICS conceptual solution description D3.1

context, as every human being he would be subject to personal biases, which can greatly vary, ranging from political to religious or from racial to economical to name a few.

To balance the above shortcomings, the TACTICS system must rely on undoubtful and objective deviant behaviour, derived from objective measurements which cannot have different interpetations. Some clear examples of the above include, but are not limited to, sensing that an individual has entered a sensitive/unauthorized or undesignated area, left baggage have been traced, or the detection of ammunition or poisonous materials. The above measurements can be considered objective as not only are they deprived of the personal perspective and bias, but they are repeatable facts which are self-evident and can justify further actions.

It should be understood that automated processes, even if they are unbiased, can lead to discriminative decisions, as the bulk of mining algorithms are based on ideal presumptions where the sample population has specific attributes. By changing the sample population and using a real-world scenario where the population has different attributes or has different analogies, then the methods can easily lead to biased results, as the methodology is not applied to the model it was supposed to[23]. A clear example of such case is the very well-known of Huber v Bundesrepublik Deutschland[24].

Note that while domestic laws may apply to the use of sensitive personal data, the EU law, in Article 8 of the Data Protection Directive, has specific rules on how to process categories of data that reveal: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on health or sex life. It is understood that while the processing of sensitive data is prohibited, the use of the TACTICS system resides within Article 8 (2) and (3) of the directive providing specific exemptions as it is for the vital interests and legitimate interests of others and public interest. Nevertheless, this exemption is subject to constraints regarding its legitimacy. Generally, the purpose of processing these data must have been specified by the controller prior to the data processing through declaration to the appropriate supervisory authority or, at the least, by internal documentation which must be made available by the controller for inspection by the supervisory authorities, as the processing of personal data for undefined and/or unlimited purposes is unlawful.

---

[23] Custers, Bart, et al. Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. Vol. 3. Springer Science & Business Media, 2012.

[24] http://curia.europa.eu/juris/liste.jsf?language=en&num=C-524/06

3 Legal and ethical aspects of biometrics

This section discusses the legal and ethical aspects of the usage of biometrics, presenting first the relevant general aspects and then their application to TACTICS.

TACTICS end users can encounter biometric personal data in different use cases. The first use case is identification of terrorists (black list) amidst urban citizens. This would require previously recorded biometric data of known terrorists, and the recording of biometric data of all passers-by. This is therefore also known as “perpetrator focused”.

The second use case is the authorization of certain citizens (whitelist), and raising an alarm on everyone else. This could be used in a closed environment where only known inhabitants are allowed. This requires previously recorded biometric data of known citizens, and the recording of biometric data of all passers-by.

The third use case is to recognise that the same person is visiting one location too many times, or a combination of locations in a wrong order. For example, if the modus operandi includes scouting the area around high risk objects, then an alarm could be raised if the same person walks around multiple objects within a short time frame. This use case can also be generalised further, to detect if the same people where involved in multiple suspicious situations.

Each of these use cases could use data capture subsystems that are dedicated to TACTICS, or subsystems from friendly systems. For example, a bank could use biometrics for access control. If the modus operandi includes a visit to that bank, than biometric data could be requested from that bank. This means that a broad ethical and legal analysis of the use of biometrics is required.

3.1 General legal aspects of biometric data protection relevant to the TACTICS system

The ever increasing use of the ICT systems (e.g. for security and safety purposes) such as TACTICS, and of the biometrics systems in particular, may raise concerns regarding the privacy issues – that the users’ right to privacy and to the protection of their personal data may be infringed upon. In the case of biometric systems, there is a real risk that the collection, storage and processing of personal data, including the sensitive data, will be carried out without the user being aware of it. This implies a lack of control over the data and that the user will not have the opportunity to express freely their consent to the biometric data being processed. On the other hand, it has to be remembered that personal data protection and the right to privacy can be limited in duly justified cases, when broadly understood security for the entire society needs to be ensured (e.g. counterterrorism). Therefore, in this section the general regulations for biometric data protection, the soft-law, the prospective law and the impact of S. and Marper vs. the United Kingdom case will be discussed.

3.1.1 Introduction to the problem

In the era of a wide use of ICT systems, especially applied to security purposes (such as TACTICS) there is an ever increasing risk that the users’ right to privacy and to the protection of their personal data may be infringed upon, particularly in the case of biometric systems.

The collection, storage and processing of biometric data (and personal data, more generally) should be carried out only upon an informed consent of the data subject, who should have control over their data.

In the European Union law, in the international public law and in the national laws, there are many legal guarantees for the protection of personal data and of the right to privacy, the main ones being:

- Charter of Fundamental Rights of the European Union[25] (article 7 and 8),
- European Convention for the Protection of Human Rights and Fundamental Freedoms,
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108)[26],

[25] Official Journal C 364, 18.12.2000, p.1.

- International Covenant on Civil and Political Rights[27],
- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[28],
- Council Framework Decision 2008/977/JHA of 27th November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The human right to privacy and to personal data protection is therefore broadly protected but the question arises as to whether the same protection exists for the processing of both biometric and of sensitive data. The main legal acts and important documents governing the matter of biometric data protection are the following:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108),
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,
- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,
- Council Framework Decision 2008/977/JHA of 27th November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,
- Proposal for a Directive of the European Parliament and of the Council On 25th of January 2014 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data[29],
- Charter of Fundamental Rights of The European Union.

Directive 95/46/EC and Council of Europe Convention No. 108 apply to the processing that requires biometric data, although they do not contain specific provisions relating to biometric data or biometrics. They provide that the processing of biometric data requires acquiring, transmitting, processing, recording and storage of the sound or image data related to individuals. Biometric data are a special category of personal data.

The terms related to biometrics and to biometric data can be found in documents being the so-called soft law, e.g. in the opinions of the Working Party on the Article 29 on the Protection of Personal Data. The notion of biometric data was also defined in the Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), drafted in 2012, as "*any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data*". This definition is general and may lead to abuse of privacy rights, particularly if data from DNA samples are processed. The provisions of the Proposal only address the issue of "identification" of an individual and do not cover the issue of authentication. The case that introduced new legal standards for biometric data collecting and processing by the UK police was the case of S. and Marper v. the United Kingdom (judgment in 2008) and confirmed that biometric data are considered as private data.

Therefore, in this section the general regulations for biometric data protection, the soft-law, the prospective law and the impact of S. and Marper vs. the United Kingdom case will be discussed.

---

[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, Opening for signature in Strasbourg, date : 28.1.1981.

[27] International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49.

[28] Official Journal L 281, 23.11.1995, p. 31 – 50.

[29] Doc. COM/2012/010 final - 2012/0010 (COD), Brussels 25.01.2012.

3.1.2 Regulations for personal data protection

In the European Union law, in the international public law and in the national laws, there are many legal guarantees for the protection of personal data and of the right to privacy. The main legal acts governing this matter are, among others, the European Convention for the Protection of Human Rights and Fundamental Freedoms[30], Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[31], Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[32], International Covenant on Civil and Political Rights[33]. The human right to the privacy and to the protection of personal data is therefore broadly protected, both within the international and the EU law. However, the question may be asked here whether the same protection exists for the processing of both biometric and of sensitive data. The issues concerning the interrelationships between biometrics and both personal data protection and the right to privacy, have been discussed in many papers, reviews and reports[34]. Those documents show that the existing regulations may be applied in the case of the use of the biometric technology.

3.1.3 Regulations for biometric data protection

The legal bases for the protection of biometric data are contained in several legal acts, depending on the legal regime. On 28th of January 1981 the Council of Europe adopted an international treaty, i.e. the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as the Convention No. 108. The standards contained in the Convention No. 108, supplemented in subsequent years by the collections of recommended standards[35], created the foundations of the European system of personal data protection. The provisions of the Convention No. 108 are in force only in the sphere of public law and they do not cause any legal effect directly on the citizens of the countries that have ratified it[36]. A little earlier, on 23rd of September 1980, the OECD has adopted a recommendation concerning the guidelines on the protection of privacy and the flow of personal data across borders[37]. On 24th of October 1995, the European Parliament and the Council of the European Union issued the Directive 95/46/EC of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[38]. The provisions contained in the directive are more specific than those in the Convention No. 108. But they are not contradictory to them. The basic idea behind the introduction of the directive was to realize two basic objectives: to protect the fundamental right to data protection and to ensure the free flow of data between the member states.

---

[30] B. Gronowska, T. Jasudowicz, C. Mik*, Prawa człowieka. Wybór dokumentów międzynarodowych*, Toruń 1999, p. 83.

[31] Official Journal L 281, 23.11.1995, p. 31 – 50.

[32] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, Opening for signature in Strasbourg, date : 28.1.1981.

[33] International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49.

[34] Article29 - Data Protection Working Party, *Working document on biometrics*, 12168/02/ENWP 80 Adopted on 1 August 2003; Article29 - Data Protection Working Party, Opinion 3/2005 *on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 1710/05/EN-rev WP 112,04.09.12 (Official Journal L 385 , 29.12.2004 p. 1 - 6), Adopted on 30 September 2005; Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data, *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data,* 2005 r.

[35] E.g. recommendation No. R (83) 10 of 23.09.1983 on the protection of personal data used for scientific research and statistics, recommendation No. R (86) 1 of 23.01.1986 on the protection of personal data used for social security purposes or Recommendation No. R (89) 2 of 18.01.1989 on the protection of personal data used for employment purposes

[36] M. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 71.

[37] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, OECD 1980, available at: http://www.oecd.org/dataoecd/16/49/15590241.pdf, of 04.05.2010

[38] Official Journal L 281, 23.11.1995, p. 31 – 50.

This act was supplemented by the Council Framework Decision 2008/977/JHA of 27th November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which is a general instrument at the European Union level in the fields of personal data protection in the area of police cooperation and judicial cooperation in criminal matters[39]. The Framework Decision 2008/977/JHA is, however, limited in scope, as it relates to cross-border data processing but does not include the processing of this data by the police and judicial authorities at a purely national level. In addition, the Framework Decision leaves the member states a wide margin of freedom when it comes to national provisions implementing the Decision.

New standards for the protection of personal data in the fields of law enforcement and crime prevention, as well as in the field of international relations will be ensured through the laws that are not yet in force now. On 25th of January 2014 a Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data has been adopted[40].

The article 1 defines the scope of the directive, i.e. the rules regarding the processing of personal data for the purposes of prevention of crimes, of investigation on crimes, their detection and prosecution or for the execution of criminal penalties. The provision contained in art. 1 also shows the dual purpose of the directive, namely the protection of fundamental rights and freedoms of individuals (and in particular of their right to the protection of personal data, while keeping the public safety at a high level) and ensuring the exchange of personal data between competent authorities in the European Union.

The art. 3 of the directive contains the definitions of terms used in it. Some of the definitions are taken from the Directive 95/46/EC and from the Framework Decision 2008/977/JHA, but some new terms have also been introduced, such as "genetic data" and "biometric data". “Biometric data” has been defined as any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data (art. 3.11 of the draft directive). “Genetic data” are defined in the art. 3.10 as all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development.

The legal basis related to the protection of personal data (biometric data) are also included in the Charter of Fundamental Rights of The European Union which provides in the art. 8 that everyone has the right to the protection of their personal data[41]. Such data must be processed fairly, for the purposes clearly specified and with the consent of the person concerned or based on some other legitimate basis laid down by law. According to this provision, everyone has the right of access to the data concerning him or her and the right to have it rectified. As is stressed in the jurisdiction of the EU Court of Justice, the right to the protection of

---

[39] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, L 350/60 EN Official Journal of the European Union 30.12.2008, p. 60–71, OJ C 125 E, 22.5.2008, p. 154. The resolution on the Stockholm Programme is a particularly important step in creating a comprehensive system of personal data protection in the EU (see European Parliament resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme (P7_TA(2009)0090), in which the European Parliament calls among other things for the revision of the Framework Decision. The Commission stressed in its action plan for the implementation of the Stockholm Programme the need to ensure consistent application of the fundamental right to personal data protection in the context of all EU policies (see document COM(2010) 171, final version). On 25 January 2012 the European Commission adopted a package of changes to EU regulations on data protection, including the proposal concerning a directive with specific data protection regulations for the sector responsible for the enforcement of the law.

[40] Doc. COM/2012/010 final - 2012/0010 (COD), Brussels 25.01.2012.

[41] The Chart of Fundamental Rights also lays down other rights, in which may be seen the potential interference and connection with the idea of personal data protection and the right to privacy. The most important ones are the freedom of expression (Article 11 of the Chart); freedom of economic activities (Article 16); property law, in particular the protection of industrial property (Article 17. 2); prohibition of discrimination against other persons based on factors such as race, ethnic origin, genetic features, religion or belief, political or any other opinion, disability or sexual orientation (Article 21); rights of the child (Article 24); right to a high level of protection of human health (Article 35), right of access to documents (Article 42); right to an effective remedy and to a fair trial (Article 47).

personal data is not an absolute right and should be analysed in the context of the function it plays in society[42].

3.1.4 Limitations of the current regulations

It should be emphasized that the Directive 95/46/EC and Council of Europe Convention No. 108 do not contain specific provisions relating to biometric data or biometrics[43]. Although the term "biometrics" does not appear in the directive and in the convention, it may be concluded from the content of the provisions contained in the above acts that the processing of biometric data requires "acquiring, transmitting, processing, recording and storage of the sound or image data related to individuals". Therefore, both the directive and the convention apply to the processing that requires such data.

The analysis of the provisions contained in the Directive 95/46/EC allows to conclude that biometric data are a special category of personal data. The representatives of the doctrine also show similar findings[44]. It should be remembered that the personal data is the data allowing to identify the individuals to whom it applies (art. 2.a of the Directive 95/46/EC, art. 2.a of the Convention No. 108). This assessment should be carried out separately by each of the entities processing the data[45].

Some guidance on this can be found in paragraph 26 of the preamble to the Directive 95/45/EC. It is stated there that the principles of the data protection must apply to any information concerning an identified or identifiable person. In order to determine whether a person is identifiable, account should be taken of all the ways the administrator of the data or any other person can use to identify the given person. In case the data is anonymous, the principles of the data protection do not apply to them. The provisions of the directive do not therefore apply to personal data (biometric data) which are anonymous.

3.1.5 Biometric data protection in soft law

The terms related to biometrics and to biometric data can be found in documents being the so-called soft law, e.g. in the opinions of the Working Party on the Article 29 on the Protection of Personal Data[46]. In one such opinion of 2003 on biometrics it has been noted that biometric data is the data of a special nature, since it relates to the behavioural and physiological characteristics of a person and can lead to the direct identification of the person[47]. This data can be defined as biological, physiological or life characteristics or repetitive behaviours, when these characteristics and/or behaviours concern uniquely a given person and, at the same time, are measurable, even if the patterns used in practice to measure them are characterized by a certain degree of probability.

---

[42] Judgment of the Court (Grand Chamber) of 9 November 2010, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen.

[43] The issues related to biometric data have been regulated among others in the (Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ L 385, 29/12/2004, p. 1–6); the changes to the regulation have been introduced in the Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member State (OJ L 142, 06/06/2009, p. 1–4).

[44] See e.g..P. De Hert, *Biometrics: legal issues and implications*, Background paper for the Institute of Perspective Technological Studies, DG JRC – Sevilla, European Commission, January 2005, dostępne na stronie http://www.ethical-fp7.eu/index.php?option=com_docman&task=doc_details&gid=34&Itemid=78, of 26.05.2011; L. A. Bygrave *The body as data? Reflections on the relationship of data privacy la with the human body*. Available at http://www.privacy.vic.gov.au/privacy/web2.nsf/files/body-as-data-conference-2003-lee-bygrave-presentation/$file/conference_03_no2.pdf, of 17.04.2011.

[45] For details see X. Konarski, *Internet i prawo w praktyce*, Warszawa 2002, s. 113-116.

[46] The Data Protection Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC.

[47]Article29 - Data Protection Working Party, *Working document on biometrics*, 12168/02/ENWP 80, adopted on 1 August 2003, p. 2.

The typical examples of biometric data are fingerprints, retinal patterns, facial structure, voice, as well as hand geometry, veins structure or even skills or other characteristics and behaviours that can be combined (such as e.g. the signature, keystrokes, a particular way of walking or speaking) [48].

One of the basic characteristics of biometric data is that it can be considered as the content of the information and the link between a particular person and a certain information. It may be concluded that biometric data are a kind of "identifiers". The biometric data is used to detect a person's identity.

3.1.6 Impact of S. and Marper vs. UK case

In the European human rights protection system, the efficiency of safeguards protecting broadly understood privacy rights and personal data (including but not limited to biometrics) is affected by a number of factors. One of them are is the case law of the European Court of Human Rights and the European Court of Justice, although for the most part it concerns legal protection of personal data, as judgments relating to biometrics are relatively innumerous. In Strasbourg case law there has been a discernible evolution in the approach towards protecting personal data contained in public data repositories, aimed at developing specific legislation in this regard[49].

On 4 December 2008 the European Court of Human Rights passed its judgment in the case of S. and Marper v. the United Kingdom[50]. This break-through case introduced new legal standards for biometric data collecting and processing by the UK police[51]. Furthermore, the ECHR judgment confirmed that biometric data are considered as private data. In the case in question the petitioners claimed that their right to privacy provided for in Article 8 of the European Convention of Human Rights[52] had been violated. In their petition they explained that after they had been cleared of charges (or after the criminal procedure had been discontinued) their fingerprints, cell samples and DNA profiles were not deleted and therefore could be used again[53]. The Court found that the categories of personal data listed by the petitioners and stored by the state (fingerprints, cell samples and DNA profiles) constituted personal data within the meaning of the data protection convention[54], because they were related to identified or identifiable individuals[55]. The Court drew attention to the fact that the said data contained a great number of sensitive information on an individual, including his/her medical condition.

3.1.7 Prospected law and possible interpretation problems

The notion of biometric data was defined in the Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[56], drafted in 2012. In accordance with the legal definition contained in Article 4(11) of the said Proposal, “biometric data means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data”.

The definition proposed by the European legislator is rather general. As a matter of consequence it may lead to abuse of privacy rights, particularly if data from DNA samples are processed. Information stored in human DNA is classified as sensitive data and should therefore be protected by safeguards more powerful than those used to protect such biometrics as fingerprints. Rules governing DNA sample data processing should

---

[48] Article29 - Data Protection Working Party , Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, adopted on 20th June, p. 8.

[49] In one of its judgments, the ECHR found that information that is systematically stored and processed in public administration systems may lead to privacy violations. *Cf*. Judgment 04.05.2000 , Case of Rotaru v. Romania, Application no. 28341/95, § 43 and 44.

[50] Applications nos. 30562/04 and 30566/04.

[51] More information can be found in the next subchapter.

[52] *Ibidem*, § 58.

[53] *Ibidem*, § 71.

[54] Convention 108 of the Council of Europe of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[55] § 68 of the judgment in the case of *S. and Marper v. the United Kingdom*.

[56] COM (2012) 11 final 2012/0011 (COD), Brussels, 25.1.2012.

be addressed in a separate regulation. Attention is drawn to the fact that the definition put forward in the Proposal identifies two examples of biometric modalities that can be used for data processing. Facial images and dactyloscopic data are commonly used across a variety of ICT systems. Quite importantly, biometric authentication can be effected by analysing a fairly high number of features, such as palm geometry, iris and retina recognition, or signature biometrics. Given the pace at which biometric technologies have been developing recently, there are reasonable grounds to believe that the range of human features used for biometric purposes will keep growing.

Furthermore, the provisions of the Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) only address the issue of "identification" of an individual. However, biometric systems allow for both biometric identification and biometric authentication. Furthermore, it needs not to be forgotten that technical sciences define biometric authentication as a process of comparing biometric data of an individual (sampled in real time during the process) with a unique biometric model stored in the device (the so-called "one-to-one" matching process). Thus, the wording used in the definition contained in the proposed legislation is all the more surprising. As a matter of consequence, the imprecise nature of the provision presented in Article 4(11) of the Proposal may cause interpretation problems in the future.

3.1.8 Summary

Legal regulations provide a broad protection for the human right to privacy and to personal data protection. The protection is weaker in case of biometric and sensitive data. Biometric data are a special category of personal data and as such are covered by the provisions related to personal data protection.

There exist some legal acts and soft law documents that address the issue of biometry directly (fully or partly) but they are not fully coherent and do not cover all the aspects related to this question. There is a new European Union law that will regulate this question, i.e. the Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, drafted in 2012. But experts point at some questions that are not covered by this act and at the provisions that may lead to different interpretations and so it appears that some precisions would still be needed at this level, for biometric data to be well protected. Biometric technologies are developing at a fast pace, the range of human features used for biometric purposes will keep growing, and so the regulations should be updated regularly so to reflect those changes.

It needs to be emphasised that in duly justified cases the right to personal data protection and the right to privacy can be limited. None of those rights are of absolute nature. More often than not, the underlying reason for introducing such limitation is the need to ensure broadly understood security for the entire society.

Concluding, the threat is that the necessary balance between the two values seems to be missing, and 'war on terrorism' becomes a justification for limiting personal data protection rights. Therefore the legal principles and requirements shall be fulfilled in ICT systems (such as TACTICS) applied to security and counterterrorism.

3.2 Legal principles and requirements for biometric data processing in TACTICS

The use of biometric technologies for authorization and authentication involves the processing of a special category of personal data, i.e. biometric data. The processing of biometric data must be done in accordance with the fundamental legal principles related to the personal data protection. The most important of those are the principles of proportionality, fairness, legality and expediency. All of those legal principles and requirements for using biometric data should be fulfilled in ICT systems like TACTICS. Therefore, the goal of this section is to present and shortly describe those legal principles and requirements.

3.2.1 Introduction

Processing of biometric data is used for an automatic verification or identification. Verification is based on the unique identifier distinguishing a particular person (e.g. an identification number) and on biometric characteristics of that person, and so it is based on a combination of authentication methods. Identification is based on biometric measurements only. It involves comparing the measurements results with the entire

database of registered people, and not only with one record selected on the basis of the identifier[57]. Verification and identification are two basic methods of authentication.

Biometric data can be processed after they have been retrieved from the biometric pattern (e.g. a fingerprint or an iris of eye image). Biometric pattern, which is an organized reduction of the biometric image, is represented in the digital form and stored in the database. Alternatively, the data processing is done on the basis of raw biometric data. Patterns can be stored in the biometric device, in a central database or on plastic, optical or electronic cards[58].

The legal bases for the processing of biometric data, being a special category of personal data, are contained, among others, in Directive 95/46/EC and Convention No. 108. Important information that may be interpreted as related to biometric data processing may be found as early as in points 14 and 15 of the preamble to Directive 95/46/EC. According to point 14: "Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data)"[59]. According to point 15: "Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question". Biometric data (e.g. in the form of an image or audio) is captured and recorded in an appropriate manner and its processing is fully automated[60].

When considering the mutual relationship between the law and biometrics, the opinions developed by the Working Party on the Article 29 on the Protection of Personal Data are an especially valuable source of knowledge. In a document drawn up in 2003, the Working Party has established several fundamental issues, stressing that the principle of proportionality played a key role in processing of biometric data[61]. The application of this principle in the context of biometrics has also been commented by the Consultative Committee of Convention No. 108[62].

3.2.2 Requirements for biometric data processing (in TACTICS)

It is widely recognized that the requirement of acting in a fair and lawful manner is the main principle setting the standards for personal data protection[63]. But the principle of proportionality and the purpose of personal data processing are one of the most important rules that relate to personal data processing in biometric systems. The application of the principle of proportionality in biometric technologies means that the developers of applications or biometric systems should weigh their application in relation to the right to privacy. This makes that this principle is closely linked to the idea of personal data protection[64]. According to the principle of proportionality, it must be examined whether the goal can be achieved in a less invasive manner, without prejudice to the right to privacy.

Biometric data must be processed in accordance with Article 6 of Directive 95/46/EC. This means that the data should be processed in a fair and lawful manner. It should also be collected in clearly defined and legitimate purposes and it cannot be further processed in a way incompatible with those purposes. Further

---

[57] R. Bolle, J. Connell, S. Pankanti, N. Ratha and A. Senior, Guide to Biometrics, ISBN: 0387400893, Springer, October 2003. (translation Warszawa 2008), p. 5; K. Ślot, *Wybrane zagadnienia biometrii*, Warszawa 2008, p. 77-78.

[58] Article 29 - Data Protection Working Party, *Working document on biometrics*, 12168/02/ENWP 80, adopted on 1 August 2003, p. 4.

[59] See P. De Hert, *Biometrics: legal issues and implications*, Background paper for the Institute of Perspective Technological Studies, DG JRC – Sevilla, European Commission, January 2005, p. 13; available at: http://www.ethical-fp7.eu/index.php?option=com_docman&task=doc_details&gid=34&Itemid=78, as of 26.05.2011

[60] D. Chorąś, *Biometrics and Data Protection* [in:]. A. Mitas (red.), *Biometrics – 2010. Monograph*, Gliwice 2011, p. 37.

[61] See Article 29 - Data Protection Working Party, Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 1710/05/EN-rev WP 112 04/09/12 Adopted on 30 September 2005, p. 9.

[62] *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), p.18,* available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf, as of 28.08.2011.

[63] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, p.78-87.

[64] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, p.78-87.

processing of data for historical, statistical or scientific purposes shall not be considered as incompatible with the regulations, provided that EU member states ensure appropriate safeguards[65]. Similar provisions relating to biometric data processing can be found in Article 5 of Convention No. 108[66].

According to the opinions of the Working Party on the Article 29 on the Protection of Personal Data, some other aspects should also be taken into account when processing biometrics data[67]. They relate to the principles of collecting information in a fair way and of processing information legitimately. Processing of biometric data must be based on one of the conditions of legality provided for in Article 7 of Directive 95/46/EC [68].

The first such condition of legality defined in Article 7 (a) of Directive 95/46/EC is that the data subject has unambiguously given his consent for the processing of data. The Directive specifies in Article 2 (h) the concept of the "consent of the data subject". According to the legal definition contained in that provision 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. The concept of this consent consists of several components. Among those are the right to revoke the consent given previously and the right to give the consent before the processing of biometric data takes place. Not always, however, will it be possible that the consent is given on a conscious and voluntary basis. In the case of biometric systems (e.g. using for authentication the face image derived from surveillance recordings) it is hard to speak about the voluntary and informed consent of the subject of biometric data. In such case, the base of legitimacy of data processing can be found in the further part of the provision contained in Article 7 of Directive 95/46/EC. In accordance with Article 7 (b), processing of biometric data may be necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. In such case we are dealing with a situation in which the parties entered into a contract and the need to undergo a specific procedure is its essential element. For example, a person enters into a contract with the bank, and the contract stipulates that the check of the person's identity will be carried out with the use of fingerprints (e.g. login to the ATM).

3.2.3 Case: M. Schwartz vs. Stadt Bochum

The legal basis for the processing of biometric data can also be found in Article 7 (c) of Directive 95/46/EC, in case the data processing is necessary for compliance with a legal obligation to which the controller is subject. For example, in the countries within the Schengen area, there is an obligation to issue passports with biometric data. The authority issuing such a document obliges citizens to submit fingerprints and to deliver a digital photo. The legislation adopted by the EU legislator introducing the obligation to provide fingerprints for the purpose of issuing passports are not always accepted by the society. In 2013, a German citizen M. Schwarz applied to the relevant departments of the Stadt Bochum (city of Bochum) for a passport, while opposing the obligation of providing the fingerprints. On 8 November 2007, the authorities concerned with the case stated that the passport cannot be issued without the mandatory provision of fingerprints. The legal basis for the adverse decision regarding M. Schwarz was Article 4 (3) of the German law on passports of 19 April 1986, as amended by the law of 30 July 2009[69].

---

[65] According to point 28 of Directive 95/46/WE „Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified".

[66] According to Article 5 of Convention: "Personal data undergoing automatic processing shall be: a) obtained and processed fairly and lawfully; b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are stored; d) accurate and, where necessary, kept up to date; e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored".

[67] Article 29 - Data Protection Working Party, *Working document on biometrics*, 12168/02/ENWP 80, adopted on 1 August 2003, p. 8.

[68] For more on data processing principle please see: M. Jagielski, *op. cit*., p. 81-87; M. Polok, *Bezpieczeństwo danych osobowych*, Warszawa 2008, p. 90-94.; Article 29 - Data Protection Working Party Opinion 3/2012 *on developments in biometric technologies*, adopted on 27th April 2012, p. 10-13.

[69] Paßgesetz vom 19. April 1986 (BGBl. I S. 537), das durch Artikel 8 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749) geändert worden ist.

As a result, M. Schwarz filed a court complaint, in which he demanded that the referring court ordered Stadt Bochum to issue the passport without fingerprinting. He was proving that the provisions of Article 1 (2) of Regulation No 2252/2004, as amended[70], which are the source of the obligation of the member states to retrieve two fingerprints from each person applying for a passport, were void. In the present case, the court shared the view of the plaintiff and on 12 June 2012 referred a question for a preliminary ruling to the Court of Justice.

The Court of Justice in case C-291/12[71] examined among others whether the Article 1 (2) of Regulation No 2252/2004 may violate the right to the personal data protection and the right to privacy. The Court relied on Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and on Article 8 of the Charter of Fundamental Rights of the European Union. In Case C-291/12 it was stated that the obligation contained in Article 1 (2) of Regulation No 2252/2004 as amended relating to the collection and storage of fingerprints by the national authorities, is a violation of the fundamental right to the personal data protection[72]. The judgment emphasized that the procedure of taking fingerprints by the competent authorities in the circumstances set out in Article 1 (2) of Regulation No 2252/2004 as amended is mandatory. It further indicated that biometric data are recorded and stored in passports and that there is the possibility of transferring such data to the police authorities without the consent of the person concerned, which obviously constitutes a violation of the right recognized in Article 8 of the Charter of Fundamental Rights of the European Union. The Court also emphasized that a person applying for a passport may not object to taking and storing their fingerprints. The only exception to this obligation will be when a person does not want to have a passport. In its judgment, the Court of Justice also stated that EU citizens cannot freely object to the processing of their fingerprints. Therefore, it may not be considered in this situation that the consent to the processing of personal data in the form of fingerprints is given on a voluntary basis[73].

On the other hand, the arguments contained in the judgment of the Court of Justice indicate that the infringement resulting from the mandatory fingerprinting should be seen as "provided by law", in the meaning of Article 52 (1) of the Charter of Fundamental Rights of the European Union, as it is expressly provided for in Article 1 (2) of Regulation No 2252/2204 as amended[74]. Furthermore, it corresponds to the requirements of accessibility, clarity and predictability in accordance with the case law of the European Court of Human Rights. In its judgment, the Court of Justice also indicated that "the rights recognised by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union are not absolute rights, but must be considered in relation to their function in society"[75].

3.2.4 Requirements for TACTICS data controller

It should be noted that the processing of biometric data is possible if it is “necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject (…)” (Article 7 (f)).

The Working Party on the Article 29 on the Protection of Personal Data also drew attention to the obligation of the data controller to take technical and organizational measures to protect personal data, and in particular to use such measures since the beginning of the process. Particular caution should be exercised in order to avoid erroneous rejection of the person authorized and erroneous acceptance of the persons unauthorized. The task of the controller is to provide such technical and organizational measures, necessary for the protection of personal data that prevent the accidental or illegal destruction of biometric data or the unauthorized disclosure of such data. This is of special significance in the case where the data processing

---

[70] *Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member State, OJ L 142, 06/06/2009,* p. 1–4.

[71] Judgment of the Court (Fourth Chamber) 17 October 2013, C-291/12 - Michael Schwarz v Stadt Bochum.

[72] Judgment of the Court, C- 291/12, point 30.

[73] Judgment of the Court, C- 291/12, point 32.

[74] *Ibidem*, point 34.

[75] *Ibidem*, point 33.

involves the transmission of data over a network (Article 17 of the directive). Ensuring a high level of security for the processing of biometric data is therefore of particular importance[76].

In the case of biometric data processing the central data storage of data for authentication should be avoided. But the fact is that the centralized storage of biometric data is inevitable in the identification, but in this case the principle of proportionality should be applied[77]. But the question is whether such a method of biometric data storing and processing is not a too deep state interference in the right to privacy? Is it really the case that the purposes of biometric data processing are always "justified"? As pointed out by Els Kindt: "the principle of proportionality has its origins in public law[78] and its purpose is to protect individuals against undue state interference in the rights of individuals". In the context of respect for human rights the state interference is not allowed if it is not "permitted by law" for "legitimate purposes"[79] and to the extent to which the interference is "substantial"[80]. Processing of biometric data in large centralized databases carries the risk of infringement of the right to privacy and personal data protection because of the potentially harmful effects in relation to the persons whose data are processed[81]. The purpose and the principle of proportionality should be applied to biometrics. According to the provisions of Directive 95/46/EC, member states shall ensure that personal data is processed fairly and lawfully[82]. The concept of "fairness" may mean that data processing should not unreasonably violate the privacy, independence and integrity of a person[83], and that it should be open. And "lawfulness" is a concept that specifies that the processing would not be against the law.

Biometric data should not be kept longer than is necessary (Article 6 (1) (e) of Directive 95/46/EC, Article 5 (e) of Convention No. 108)[84]. It is worth adding that the data protection authorities of the EU member states in relation to the legal uses of biometrics, base their decisions on the principle of proportionality. They also check whether the use of biometrics for identification and verification is in line with the requirements of Article 6 of Directive 95/46/EC. Data protection authorities in the EU member states often issued very different opinions on matters related to the use of biometrics in different areas of life[85]. This reflects the existing

---

[76] See Article 29 - Data Protection Working Party Opinion 3/2012 *on developments in biometric technologies*, adopted on 27th April 2012, p. 14.

[77] Article 29 - Data Protection Working Party, *Working document on biometrics*, 12168/02/ENWP 80, adopted on 1 August 2003, p. 6 and the following. Similar issues have been analysed in Article 29 - Data Protection Working Party, Opinion 3/2005 *on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 1710/05/EN-rev WP 112, adopted on 30 September 2005, p. 3.

[78] See e.g. art 8 paragraph 2 of the Convention for the Protection of Human Rights and Fundamental Freedom, art. 13 of Directive 95/46/EC, art. 9 of Council of Europe Convention No. 108.

[79] For example, the Polish Act on Personal Data Protection dated 29.08.1997 (Journal of Laws of 2002 No. 101, item 926, as amended) indicates that the data processed for the purpose of a legally legitimate aim should be indispensable to achieve this aim. Only this data is used that is indispensable to achieve a given aim, see J. Barta, P. Fajgielski, R. Markiewicz, *op. cit*., p. 515.

[80] E. Kindt, *Biometric applications and data protection legislation. The legal review and the proportionality test*, Datenschutz und Danetsicherheit 31 (3), 2007, p. 169.

[81] Article 29 - Data Protection Working Party Opinion 3/2012 *on developments in biometric technologies*, adopted on 27th April 2012, p. 8.

[82] Article 6 point a of Convention No. 108 also indicates that personal data undergoing automatic processing shall be obtained and processed fairly and lawfully (art. 5a).

[83] See L. A. Bygrave, *Data protection law. Approaching its Rationale, Logic and Limits*, The Hague-London, New York 2002, p. 58.

[84] Article2 9 - Data Protection Working Party, *Working document on biometrics*, 12168/02/ENWP 80, adopted on 1 August 2003, p. 8 and *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005),* p. 8.

[85] For example, the Greek Data Protection Authority (DPA) adopted a restrictive approach to the protection of biometric data, which also is somewhat contradictory. Although the DPA found that processing of biometric data was lawful as regards the data related to access control to security installations in subway stations in Athens (Decision No 9/2003, available at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/27%20DECISION%20NO.%2009%20-%2031.03.2003.DOC, dated 26.07.2011), it found that processing of biometric data (fingerprints and iris) was not lawful in relation to data gathered at the airport of Athens within a pilot project on voluntary verification of the identity of the passengers (Decision No. 52/2003,

problems in the application of law in biometrics. This leads to the formation of differences in interpretation of the regulations. This is particularly noticeable in the use of biometric applications in the private sector (e.g. banking, health)[86]. A controversial issue is the use of fingerprints to control the working time[87].

In the case of the processing of biometric data the rights of the data subject cannot be forgotten. In accordance with Article 10 and 11 of the directive and Article 8 of the European Convention on Human Rights and Fundamental Freedoms, the data subject whose biometric data are being processed, has a right to know who is the controller of the data, what is the purpose of processing the data and how biometric data are used. Such a data subject has the right of access to their biometric data and to rectification, erasure or blocking of data when the terms of such processing have been violated.

It should be noted here that in some cases those rights may be limited. This is the case when such a restriction constitutes a necessary measure to safeguard among others: national security, defence, public security, investigation and prosecution of criminal offenses or of breaches of ethics for regulated professions or important economic or financial interest of a member state or the European Union (Article 13 of Directive 95/46/EC)[88]. Every person also has the right not to be subject to a decision which is based solely on automated processing of data, and which produces legal effects concerning him or her or has a significant impact on this person, and if the purpose of such data processing is to evaluate certain aspects relating to him or her of a personal nature (e.g. behaviour).

3.2.5 Summary

In this section, there are several legal principles and requirements that are related to biometric data processing - a special category of personal data. Those are specified mainly in Article 6 of Directive 95/46/EC and in Article 5 of Convention No. 108. There also are some requirements as to biometric data processing in the documents of the Working Party on the Article 29 on the Protection of Personal Data.

The main principles are the ones of proportionality, fairness, legality and expediency. Proportionality means that data should be adequate, relevant and not excessive in relation to the purposes for which they are stored. Fairness mainly means that data processing should not unreasonably violate the privacy, independence and integrity of a person. Data should also be obtained and processed lawfully (principle of legality). Expediency means that data should be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. Other requirements are data accuracy and validity (but it is not always that data should be kept up to date). Protection of data subject identity is an important principle, meaning that data should be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored, as well as ensuring basic rights of data subject. Data subject whose biometric data are being processed has a right to know who the controller of the data is, what the purpose of processing the data is and how biometric data are used. Such a data subject has the right of access to their biometric data and to rectification, erasure or blocking of data when the terms of such processing have been violated. There are some requirements on the data controller, as

---

http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/25%20DECISION%20NO.%2052%20-%2005.11.2003.DOC, dated 26.07.2011).

However, in 2010 in a similar case the Greek DPA issued a positive decision on the use of biometric data at the airport "Macedonia" in Greece. A pilot project, “Turbine”, was led there within the 7th EU Framework Programme (details available at: http://www.turbine-project.eu/). The DPA has agreed to the use of biometric data for research purposes, if some restrictive conditions are met by the controllers. For details see Decision No. 31/2010 available at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/DECISION%2031_2010%20EN_FINAL.PDF, of 30.07.2011. It is worth noting that the IRIS system has been introduced in the UK, which scans the iris of passengers who have given their consent. See the website: http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/, dated 22.10.2011.

[86] For the information on biometrics in school see e.g. *The use of biometrics in schools*, Information. Commisioner’s Office:http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view.pdf

[87] For the information on biometric data processing in the workplace in Polish regulations see M. Korga, *Przetwarzanie danych biometrycznych pracowników w świetle orzeczenia NSA z dnia 1.12.2009 r., (ISK 249/09)*, Studia Prawnicze, zeszyt 1 (187), Warszawa 2011, p. 125-140.

[88] Article 9 of the Convention No. 108 provides that the limitation of rights under article 5, 6 and 8 is justified if it is provided by an internal law, as a necessary measure in a democratic society, for: a) the protection of the country, of financial interests of the state or for the maintenance of public order and security and for the fight against crime; b) the protection of the data subject or the rights and freedoms of others.

e.g. ensuring a high level of security for processed data. Data controller must take technical and organizational measures to protect personal data, and in particular to use such measures since the beginning of the process. Particular caution should be exercised in order to avoid erroneous rejection of the person authorized and erroneous acceptance of the persons unauthorized.

The fundamental rights and freedoms of data subject are overpassing the rights of data controller. But, it has to be remembered that in general the rights related to data processing are not absolute ones and may be non-valid if it is not in line with major social interests.

4 Applicable legal (data protection and privacy) requirements for TMT

The main risks related to TACTICS as a system may be seen as (1) the use of potentially unreliable data (cf. the so-called data quality principle); (2) the absence of time limits for the deployment of the system; (3) bias towards specific groups; and (4) the disclosure of organisations' internal secrets. Mitigating violations of the data quality may be conflicting with demands for accountability concerning the management of data. One possible solution might include implementing a data verification step, but the feasibility of the latter is not unquestioned. There is also no easy solution to the time-related risk. One possible control is to better inform end-users about these dangers through a manual. Finally, in order to avoid disclosure of internal secrets, particular attention may be paid to the data minimization principle as well as to data security.[89]

This chapter analyses the solutions that may prevent the mentioned issues, and other illegal or unethical results of the TMT.

4.1 Data quality

The principle of data quality assures that data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed [Art. 6(1)], accurate and, where necessary, kept up to date [Art. 6(1)(d)]. There are four issues arising related to data quality with the CMT. One is how the data on capabilities may be preliminary assessed prior to the implementing into the tool/temporary database. Another is the *ongoing* assessment of data that the CMT has assembled, which might have been of good quality upon assemblage, but may change during the course of the operation. A third issue relates to processing into the CMT low-quality data or poorly processed formats. Finally, a double differentiation is challenging when it comes to personal data that may be applied in various ways from the CMT by the TM. Each of these issues is investigated in turn below.

4.1.1 Preliminary assessment of external data sources' accuracy

Through eased access, large amounts of data are easily aggregated and processed. Information that is viewed in isolation is not so telling about a person. Nevertheless when *collected, correlated and/or fused* it may give substantial information about him.[90] The problem may as such be greater than obtaining 'good' data from the vast amounts of data. One of the potential problems is that inaccurate data, or a data 'profile' on a person based on aggregated data, may form a wrongful picture. In the CMT situation, although the TM must draw the conclusions from the collected information, the consequences of faulty 'created' knowledge could imply serious measures being taken towards innocent citizens without their knowledge. Another challenge with aggregated data is that it becomes harder to distinguish sensitive from non-sensitive data, when all data combined with other data may turn revealing.[91] This is problematic in relation to privacy protection as the initially differentiated levels of protection depending on the sensitivity of data are hard to maintain. This may be in itself one of the core challenges with the TMT, as the (temporary) database itself aggregates different data and datasets from information sources into one database.

Therefore, apart from sending the information, the CMT must assist the TM in knowing what is 'good', i.e. reliable and inappropriate or inaccurate data. To this end, TACTICS must always have specific tags for its resources, indicating their resolution, objectivity and applicability. For instance a high-definition camera has a

---

[89] See more in another EU FP7 project, SAPIENT (Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies, project no. 261698), D4.2, p.2. SAPIENT researchers conducted surveillance impact assessments involving TACTICTS stakeholders. See TACTICS D4.3 ch.4 for details on the cooperation.

[90] Solove, D. "Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Case: Public Records, Privacy and the Constitution", *Minnesota Law Review*, no. 86, 2001.

[91] Hilst, R vd, *op cit.* 2013 p.77.

Sweeney, Latanya. "k-anonymity: A model for protecting privacy." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10.05 (2002): 557-570.

high resolution and covers the visible spectrum, so it can create images that can be used to determine the identity of an individual, whereas a night vision camera is not as useful for this purpose. Similarly, the experience of an officer reporting on the street has a significant impact on the accuracy of his findings and reports. All these factors can be weighted by the TMT, specifically by the fusion engine, so that in his response to the TM he reports his trust in the findings.

4.1.2 On-going assessment of external data collected for various purposes

Potentially, TACTICS can collect a great wealth of external data. While this data can contain vital information about the outcome of the operation, it is clear that some capabilities and resources will not provide any important information. Letting them continue to report is not only a waste of resources, but also implies that the privacy of citizens is violated for no reason. To reduce both these risks, TACTICS should provide an assessment of usefulness (based on e.g. quality) of the on-going collection of external data, while simultaneously letting the officer define the purpose of his action. The above procedure can be considered an on-the-fly privacy impact assessment[92] of the retrieved information.

Due to the fact that imminent actions must be made during the use of TACTICS, the purpose specification principle[93] can be slightly deviated to allow for postponing the specification of why the data were collected until the end of the operation. After all, as will be discussed below, all actions in TACTICS must be recorded in detailed unmalleable log files. This would enable TACTICS officers to formulate in a clear and predictable manner why their actions were made; their necessity, and their proportionality to the desired aim.

4.1.2.1 Assessment of data quality of low-quality or poorly processed formats

Since TM's and their staff have to be able to take responsibility for the entire operation, they need to make their own decision on whether the quality of information is still good enough. So, they should be informed about that. There cannot be another entity withholding data based on the single fact that it is of low quality. As already discussed in section 4.1.1, the CMT must provide specific indicators regarding the accuracy of the measurements and reports that it can receive from its resources and capabilities. But, for most combinations of data type and capability, there is no clear and strict boundary which separates low from high quality data. Ergo, there is not even a clear area where data might be considered random noise. In fact, quality of data is relative. It could be relative to a general idea of what e.g. "a good video" should be, or it could be relative to a specific function (e.g. for identification purposes). In the case of TACTICS, one single data resource (e.g. a video stream) could be used for different capabilities simultaneously. The data stream could be too low quality for one capability, but adequate for another. In addition, there are methods to get high accuracy information (including personal data such as a face) from low quality data (such as low res video). The TM and his staff must therefore be very cautious: low quality data related to a desired capability can lead to many false positives, exposing the privacy of many citizens without an actual reason. Additionally, such "random noise", depending on the experience of the TM can trigger a bias towards specific groups ethnical, religious, political etc. jeopardizing the outcome of the operation.

4.2 Data security

This section discusses data security in terms of its access, storage and conveying.

4.2.1 Access

A wide range of personnel and institutions may be involved in counter-terrorism activities on behalf of a state. The TACTICS system presupposes that it is handled by security forces consisting of public security personnel, not private actors. The latter will thus not be analysed in this report[94]. Public professionals will vary both between and within countries from secret police, to national or local police. What is necessary to keep in mind in relation to the diversity of personnel performing or applying counter-terrorism measures and capabilities, is that they may have – and should have – differentiated access to various measures. The CMT of the TACTICS system covers technical access to all available capabilities and resources. The point of

[92] Clarke, Roger. "Privacy impact assessment: Its origins and development." Computer law & security review 25.2 (2009): 123-135.

[93] http://oecdprivacy.org/#purpose

[94] See, however, on the risk of abuse D5.4 chapter 5.

departure is of course that the capabilities are legal in themselves, which includes the legal access to information. Three issues are targeted here: 1) the access to making the decision of starting or setting in motion the TACTICS system, 2) the access to the information of capabilities 'belonging' to other institutions or 'levels' of security forces, and 3) the access control to using the TACTICS system. These are discussed in turns below.

4.2.1.1 Chain of supervision and decision making

Due to its nature, TACTICS must be supervised at two levels, decision making and access control. First we discuss the decision making as the access control is going to be analysed independently. During an operation it is clear that several decisions must be made. Clearly, all the decisions must be made by authorised personnel. Therefore, TACTICS must enable the replication of the hierarchical structure of the force/LEA which is using it. Typically, this means that a Role Based Access Control (RBAC)[95] model must be applied to allow fine-grained access-control policies.

Additionally, TACTICS should provide mechanisms to monitor all the actions that are made by the system to allow external auditing at the end of the operation[96]. Each entity will then have the time to justify the decisions it took and advocate their need, the criteria and the results it led to. Further to the justification of the measures taken, this could be used as a key indicator of the efficiency of the officers and the quality of the information obtained.

4.2.1.2 Access to initially non-accessible capabilities

From its design, TACTICS automates the procedures of finding available resources and capabilities, allocating and fusing them (if possible). As a result, TACTICS can provide new capabilities, for instance mixing the input from a street camera with face recognition software. This provides a new capability which previously was not accessible. It is therefore crucial to provide the user with necessary warnings and notifications regarding the privacy impact that these new capabilities may have. Furthermore, depending on the nature of these "new" capabilities, TACTICS could enable an external mechanism for authorization (this is discussed further in the next paragraphs). The main reason for the latter is the fact that the impact of this action should be weighted by another official to grant the authorization for using the results.

It should be highlighted that while EU law guarantees the right of access to documents[97] regarding public access to European Parliament, Council and Commission documents[98].With Article 42 of the Charter and Article 15 (3) of the Treaties of the European Union (TFEU), the right of access has been extended "to documents of the institutions, bodies, offices and agencies of the Union, regardless of their form". In accordance with Article (52) 2 of the Charter, the right of access to documents is also exercised under the conditions and within the limits for which provision is made in Article 15 (3) of the TFEU. The above indicate that there might be a conflict with the right to data protection, if access to a document would reveal personal data of individuals. Therefore, when TACTICS makes requests for access to documents or information, even if it is held by public authorities, as long as the document contains personal information, the according officers must provide the proper reasoning for transparency.

4.2.1.3 Access control

Due to the nature of the TACTICS system, accessing it must be very well defined and constrained under specific rules that cannot be bypassed. The main issues that are raised can be categorised as follows:

- Who has access to the system?

---

[95] Ferraiolo, David, Janet Cugini, and D. Richard Kuhn. "Role-based access control (RBAC): Features and motivations." *Proceedings of 11th annual computer security application conference*. 1995.

[96] Due to the extreme severity of the situation under which TACTICS is operated and the immediate decisions that have to be made, on-the-fly monitoring, even if it performed, it is at least time consuming to perform the justification in real time. This part needs to be performed at the end.

[97] Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001 L 145.

[98] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents

- For how long does someone have access to the system?
- How is this access granted?
- Who is granting the access to the users?

Access to the TACTICS, as to every critical system, must be made through a set of strong credentials and only by authenticated personnel. Since the installation of the TACTICS system will be made on a high-security environment we presume that physical access to the system is tackled by the force that hosts the system and checks the identity of the people who enter the operation room.

The TACTICS system has three main entities, the Threat Manager, the Capability Manager and the Threat Decomposition Manager, each of which has his own credentials to access the system. Depending on the hierarchy and the internal procedures of each force, these credentials grant them the according rights to access the system and make the according actions.

The TACTICS system must authenticate each user by a set of credential, which depending on the policies of each force can be:

- Tokens
- Username/Password (TACTICS requirement SEC_TMT_REQ#002)
- Two factor authentication
- Biometrics (fingerprint, retina, iris etc.)
- A combination of the above (independently or via biohashing[99])

In any of the above cases, it is important to highlight that a user, apart from the specific role that he is assigned to, should also have specific time constraints. These constraints are necessary as arbitrary usage of the system must be prevented. The time constraints should allow the execution of an operation for a specific amount of days as TACTICS is not a preventive system to run continuously. If for some reason the system must continue its operation, then a specific request should be made to the official who is in charge of granting access to the system e.g. the minister. This official could be equipped with a mechanism to generate one-time passwords[100] (OTP) that allow access to the system. Clearly, false attempts to authenticate to the system must be immediately reported to the according officer as well, as this might imply that someone is attempting to misuse the system.

The generation of OTPs is currently very easy and widely-used, providing an alternative way to authenticate to a system. Currently, in most applications it can be considered as a means to perform two-factor authentication, but it can also work independently. Using a small device, the user can generate new passwords (usually through hash functions) that authenticate him to a system; however, they cannot be reused. Therefore, even if someone has access to some of these passwords, it is impossible to recover a new one and gain access. It is obvious that this provides a measure against arbitrary access to the system. For instance, in the typical authentication method of username and password, the user can have access to the system whenever he uses his credentials. In the case of TACTICS, this would mean that if someone is the Threat Manager, if he is not given the OTP from the minister, then he cannot access the system.

4.2.2 Storage

The sensitivity of the data that are stored by the TACTICS system implies two specific measurements, secure backup and data encryption on the system, the first is a requirement for the integrity and availability of the information, while the latter for the confidentiality.

The TACTICS system must keep authenticated backups of the information locally and remotely. For the case of local storage, the clients could use technologies such as RAID (Redundant Array of Independent Disks) so that even if a disk failure occurs, the data are not lost. Furthermore, current technologies allow on-the-fly changes of the disks that have failed. While the above insure that the data are not lost from physical/hardware problems, they do not protect from malicious internal threats.

It has been proven that physical access to storage medium can create many problems in the security and privacy of the data. An adversary could copy, delete or alter the stored information. The adversary can be an

[99] Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." Pattern recognition 37.11 (2004): 2245-2255.

[100] Haller, Neil. "The S/KEY one-time password system." Request for Comments-1760 (1995).

inside threat such as a corrupted officer who wants to sell the information to an outsider, or an insider who wants to delete some of the actions that were made during the use of the TACTICS system. It can also be an outsider that uses malware to get access to the physical storage[101]. Both actions should be countered, as the first implies many risks for the national security, while the second one can lead to arbitrary use of the system without evidence.

Therefore, it is suggested that the TACTICS system should use encryption mechanisms for storing the information. The encryption should be made in two layers: firstly a disk layer and secondly a transaction layer. By disk encryption, something that is usually made by the operating system, we can ensure that physical access to the system will prevent an adversary from altering the information of the system. In addition, by using digital signatures and cryptocounters on each transaction with the database that keeps the log files of the system, we can provide the assurance that the data are not altered by an internal adversary. If they were, then the system would locate the alteration and raise appropriate alerts.

Last, but not least, the TACTICS system must provide mechanisms to protect citizens' privacy from the recorded footages. The reason for that is that TACTICS will use many cameras, and not only public ones. To a great extent, regarding video surveillance, people might be willing to sacrifice part of their privacy for the sake of security[102], nevertheless, the amount of sensitive information that can be recovered about individuals varies, especially in regard to where the camera installation has been made. Martínez-Ballesté et al.[103] propose the notion of "*Trustworthy Video Surveillance*" (TVS), which only stores the protected version of the video. Clearly, the requirement for absence of human supervision/intervention in the case of TACTICS cannot be met, as an operator might be needed to extract more relevant information from footage. Nevertheless, TVS provides a more privacy-aware method for storing video streams, as Regions of Interest are encrypted with a separate key. Therefore, faces, licence plates and any part of the video that could identify a person can be obfuscated[104], allowing only specific officers to access this information and drastically decreasing the privacy exposure of citizens.

4.2.3 Conveying of data

Given that TACTICS is a cyber-physical system, according to the 2012 Joint Communication on a Cybersecurity[105] strategy for the EU:

"*Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field*."[106]

---

[101] TACTICS is a cyber-physical system which means that an adversary could perform a cyber attack. As already shown in previous cases (http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_OctDec2012.pdf), the adversary could have penetrated the system using honest users using highly sophisticated malware.

[102] Council of Europe. Convention for the protection of human rights and fundamental freedoms.

(http://conventions.coe.int/treaty/en/Treaties/Html/005.htm)

[103] A. Martínez-Ballesté, A. Solanas, H. A. Rashwan, "Trustworthy Video Surveillance: An Approach Based on Guaranteeing Data Privacy", Advanced Research in Data Privacy Studies in Computational Intelligence Volume 567, 2015, pp 271-284

[104] European Patent EP1410357A1 Method and system and data source for processing of image data (owned by TNO) does this. It describes a method and technology to dynamically detect (moving) personal data such as faces and number plates, to separate this from the video stream, and store separately.

[105] We are not discussing cyber security because *terrorists* might deploy a cyber attack, but because TACTICS may be a valuable cyber target itself.

[106] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; Joint Communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-planprotect-open-internet-and-online-freedom-and-opportunity-cybersecurity

While the structure of the core TACTICS system involves three interconnected subsystems (TM, CMT and TDT), it is apparent that it will communicate with other systems as well, which are going to reside outside of the premises where TACTICS is installed. For instance CMT will contact officers, retrieve data from sensors or external databases. While many sensors might be open, e.g. traffic cameras, most of this traffic is expected to contain sensitive information. The sensitivity of the information can be regarded as both personal and operational.

The personal aspect is mostly related to the exchange of citizen information. TACTICS will have to query a lot of information and exchange a lot of personal information until it has the necessary data for the terrorists. To understand this, one should think of the scenario where TACTICS processes financial transactions or telecommunications to determine suspicious connections between people.

The operational aspect is also important. It is at least irresponsible to assume that the TACTICS system will transmit messages without encryption to any entity. This would enable an adversary to intercept messages and alter them, jeopardizing the whole operation, as the terrorists could be warned of what they need to do. Depending on their skills and penetration, the existence of a compromised officer within the premises of the force can be considered a valid assumption. Therefore, any communication of the TACTICS system with any entity must be encrypted to avoid leakage of sensitive information.

4.3 Data retention

As the TACTICS measures involve obtaining, processing and (temporary) storing of data, several legal standards related to data retention must be met. TACTIS implies storing data in an *ad hoc* database, and the relevant question to assess by the user of the CMT is *which* data is being processed, whether it is all the data processed (or a limited set of data, a simplified version of data, only the results of the processing or only that relevant to make sense of specifically flagged, potential targets), *for how long* the data will be stored, and *which* is the relevant legal basis.

Electronic communication:

Several of the TACTICS capabilities concern electronic communication:

- Analysis of financial transactions
- Analysis of the billings
- Wiretapping
- (Some) analysis of localisation (GPS etc.)
- Web crawling

It should be highlighted that interception of telecommunications is a broader category than “phone interception” as it also includes the interception of emails or other messages sent via the Internet. The interception of this communication can be made in real time (e.g. phone, online messenger) or off-line (e.g. email, online messenger). An important differentiation of the level of intrusion of telecommunication interception is the access to the content. Contrary to the identification or tracking of individuals, by intercepting telecommunication one has access to the actual content, drastically increasing the intrusion to the privacy of individuals as more sensitive information can be leaked.

The **Data Retention Directive 2006/24/EC** has been adopted as an amendment of the so-called ePrivacy Directive (discussed below). It builds on Article 15 of the ePrivacy Directive to oblige communication providers operating in member states to retain telecommunication data (location and traffic, not content) so to facilitate access to these data by law enforcement authorities. In other words, it implies that all member states’ telecommunications companies and internet service providers must store certain information that may identify caller and time and means of communication, and all internet-related communication data, including broadband access, internet telephony and email event data, to be readily available to their law enforcement authorities if that is required for the purpose of investigating, detecting and prosecuting serious crime and terrorism. The data should be stored for at least six months, but for no longer than two years: it is up to member states to set up the exact length of retention within this ‘window’ at the moment of transposing the directive into national legislation.

The Data Retention Directive was found invalid by the Court of Justice in the EU (CJEU) in the joined Cases C-293/12 and C-594/12[107]. The Court found that the Directive did not meet the proportionality principle, and was lacking sufficient safeguards protecting fundamental rights such as respect for private life and to the protection of personal data. The Court of Justice notes that:

"not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law".[108]

The judgment also provides rather explicit guidelines on how such a far-reaching measure should have been conceived, so to ensure that all safeguards needed would have been in place (cf., in particular, paras 54-68). Several of these considerations may prove useful also to the further design of the TACTICS system, and definitely in the case national authorities decide to lay down legislation concerning a similar system. For example, the TM must make sure that the level of security of the data is no less than the Court suggests. The Court of Justice states that:

"as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data"[109].

The only personnel that may access the data is competent national authorities.

Only data concerning "serious crime", which is up to the Member State respectively to define, is covered by the Directive.

Note that the individual Member States' national implementing laws are not automatically invalidated by the CJEU verdict, and the procedure and further regulation may be different from country to country.[110]

---

[107] Joined Cases C-293/12 and C-594/12.

[108] Joined Cases C-293/12 and C-594/12, para 60.

[109] Joined Cases C-293/12 and C-594/12, paras 66-68.

[110] The UK government chose to replace the 2009 Regulations with new emergency legislation to fill the gap until the EU introduces alternative law on this topic. The Data Retention and Investigatory Powers Act 2014 ("DRIPA") came into force on 17 July 2014 in the UK, which is applicable only up until 31 December 2016. (http://www.purplewifi.net/update-data-retention-obligations-european-union/ [03.11.14])

The e-Privacy Directive 2002/58/EC, amended by Directive 2009/136, translates the provisions of the 1995 Data Protection Directive into rules specifically applicable for electronic communications. Electronic data includes data on traffic and location, and the related data necessary to identify subscribers or users. The Directive applies to both legal and individual persons (Art. 1(2)). Data that falls within the scope of the e-Privacy Directive must be deleted or anonymised when no longer needed for the purpose of the communication[111]. However, as it is the case of the Data Protection Directive, the ePrivacy Directive does not apply to "activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law" (Article 1(3)). Article 15, which is the basis for the Data Retention Directive, states that:

"To this end [necessary, appropriate and proportionate measure[s] within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system], Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union".

Again, data protection may be limited to allow criminal investigations or to safeguard national security, defence and public security. TACTICS has prevention and stopping of terrorist activities as a general purpose, and will thus normally fulfil one of these criteria. Withdrawal of data protection may, however, only happen when the purpose-requirement is fulfilled and the withdrawal is a "necessary, appropriate and proportionate measure within a democratic society" (cf. also section 5.1 in D5.4).

Finally, it should be noted that, even after the EU Court of Justice judgment, data still can be retained on the basis of Article 15 of the ePrivacy Directive, enabling the law enforcement agencies of the members that have implemented the Directive to request these data. However, national laws can have further restrictions on the use of this information. For instance, in the UK the interception of telecommunications can be used for investigative purposes and as an instrument for crime prevention, but not for prosecution, as they cannot be used as evidence in a public court[112].

TACTICS addresses this with requirement LOG_TMT_REQ#003 - database storing mechanism will consider at any time, ethical and legal aspects to protect citizen's privacy.

4.4 Data minimization

Data minimization implies that data should be processed only to the extent and in the form that is absolutely necessary, for legitimate purposes, and with deletion of all excess data.[113] Chesterman argues, however, that data processing by Governments will take place anyway, and the focus should instead be on *how* the data is used – instead of whether it's minimized or not.[114] A solution proposed by Mayer-Schonberger is that all electronic data is provided with an 'expiration date', which ensures that the data in question is automatically deleted within a framework for appropriate use.[115] While automatic deletion may not be the most appropriate solution, an expiration date for assessing the necessity and value of the data (set) in question, could be beneficial for the data minimization aspect of the CMT. This is important for the CMT database(s), since these are not permanent databases, and thus without all-encompassing legislative consideration

It may arguably be at least as important as the minimization of irrelevant data that the *relevant* data collected in/with the TMT is stored when needed for evidence to counter terrorism. These mechanisms must be relied on the human interface, i.e. the TM. The applicable storage and further transfer regulations must follow

---

[111] There are some exceptions which are, however, less relevant in the TACTICS context. Examples are payment issues or value-added services. See e.g. De Hert *et al.* (2008, p.154-155).

[112] s. 15(3) and 17 RIPA. See JUSTICE, Intercept evidence: Lifting the ban, Report (October 2006).

[113] Hilst, R vd, *op.cit.* 2013 p.78.

[114] Chesterman, S., *One National Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty*, 2011, Recherche, Oxford University Press, Oxford.

[115] Mayer-Schönberger, V., *Delete: The Virtue of Forgetting in the Digital Age*, 2013, Princeton University Press.

applicable national regulations, or in case of cross-border cooperation, within EU instruments such as the Schengen Convention[116] or through the Europol instruments.[117]

4.5 Control

Mining and data analysis, assembling data from various sources into a powerful tool for the Threat Manager, may imply that the original control mechanisms, for example retention periods and access limitations, are diffused. Inadequate control over who sees that information, for what reasons, how long it is retained, and to whom it is disseminated, can lead to unfairness. No matter how legitimate the reason for collection or how careful the initial use, information can take on a life of its own if not controlled, and it can be used by others for reasons unrelated to the initial collection[118]. There are two main control mechanisms that should be implemented in TACTICS for the CMT: 1) Judicial control and monitoring by external bodies, and 2) Internal audit mechanisms.

The regulation of "automated individual decisions" is to be found in Art 15 DPD, and Art 7 Council Framework Decision 2008 (more focusing on law enforcement). Article 7 states:

"Automated individual decisions

A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests. "

Furthermore, the UN High Commissioner fact sheet no. 32 states that

"Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular:

(i) Are governed by appropriate provisions of domestic law;
(ii) Are proportionate to the aim for which the collection and the processing were foreseen;
(iii) May be subject to supervision by an external independent authority."[119]

There are control mechanisms both on national, regional and global level that can carry out a number of control functions ensuring that the TACTICS system respects the legal restraints embedded in all three levels.[120]

4.5.1 Runtime checks

Because certain preemptive failsafes may not be workable or realistic in the case of an imminent terrorist attack, it may be necessary to introduce some runtime checks to prevent misuse of TACTICS.

4.5.1.1 No standby or continuous running – checks

Due to the level of privacy intrusion of the system, TACTICS must be switched off most of the time. The system must be pre-configured, however, so that when it switched on it immediately becomes available. The above means that TACTICS must not be running continuously or be in an idle mode. Measures to achieve

---

[116] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders Official Journal of the European Union. Official Journal of the European Union, L 239, pp. 19-62, 22.09.2000.

[117] Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files. Official Journal of the European Union, L 325, pp. 14-22, 11.12.2009.

[118] DeRosa, *op.cit.* 2004 p.16.

[119] UN High Commissioner fact sheet no. 32.

[120] The …. D16.3

this can be the aforementioned use of one-time passwords, well-defined time bounds for TACTICS usage and internal checks which will notify the according national and EU authorities of excessive usage.

TACTICS is expected to run only when there is an imminent terrorist threat, therefore, it is valid to assume that a minister or general according to the national laws would grant the authorization for its use, and that a minister or Prime Minister would be notified of this event. In this regard, TACTICS could have a mechanism to notify the supreme leader of each nation that it is in use as a means of national (internal) checks. Furthermore, TACTICS could integrate a mechanism to notify EU authorities that it is working, providing external monitoring on an international level. While the latter might sound that it can jeopardize the security policies of a member country, it should be highlighted that there are measures to provide the privacy guarantees, now in terms of nation. For instance, TACTICS could use the concept of n-times anonymous authentication[121]. The concept is that each installation gets an anonymous ticket that can be used n times. By using the ticket n+1 times, the user discloses his identity. In this regard, EU could have a central ticket distribution centre of anonymous tickets, giving each member a predefined number of tickets according to their needs. If a member uses all the tickets in a short period, then either the member faces many security problems, so help from other members is needed, or the member is misusing the TACTICS system. Excessive usage of a TACTICS system could also be reported to the UN Human Rights Committee, providing a global barrier to arbitrary usage.

4.5.1.2 Punishment for abuse

Auditing will not work, however, if there is not also in place a system of oversight, including regular audits and accountability for wrongdoing.

4.5.1.3 Geographical limitations

While TACTICS is a cyber-physical system, its architecture enables it to be portable. Its portability opens the door to further privacy issues. Depending on who is the user of the system and where the system is being used, specific regional and national laws may come into effect limiting its usage or granting it further access. For instance, Spain and Germany are divided in separate autonomous regions, many of which could potentially have separate laws. In other cases, the system might have to be used at the borders of two or more member countries which means that international consent might be needed. The portability of a TACTICS installation can create further problems. While the system could potentially use GPS or network data to trace its whereabouts, there is no apparent reason why the operation room should reside close to where the terrorist attack is expected to be launched. Moreover, intelligence could easily jam or spoof the data to report bogus locations. The use of Position Based Cryptography[122] has not been proven adequate mainly due to the low entropy of geographical information and network latency issues.

A workaround that TACTICS system could apply would be to monitor the location of the resources that is using. It is expected that the vast majority of them would reside on the area where the attack is expected, therefore, TACTICS could deduce where it is being used and apply the according policies to its usage.

4.5.2 Judicial review and other monitoring bodies

National courts

In contrast to international bodies, the strength of national courts is first of all that they can issue judicial decisions to be executed by national authorities. Furthermore, national courts are independent of the political system, and are thus to a great extent able to uphold human rights standards despite a changing political climate. A weakness of the courts' control function, especially in covert counter-terrorism cases, is that action is required by a victim. In general, many citizens may not be able to take a case to a national court, much less to an international court. Thus, other mechanisms should supplement courts in protecting human rights in combating terrorism. This is especially relevant in the cases where the victim/subject of e.g. surveillance is or has been unaware of the measure.

Global monitoring treaty bodies: UN Human Rights Committee

[121] Camenisch, Jan, et al. "How to win the clonewars: efficient periodic n-times anonymous authentication." Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.

[122] Chandran, Nishanth, et al. "Position based cryptography." Advances in Cryptology-CRYPTO 2009. Springer Berlin Heidelberg, 2009. 391-407.

As seen above, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) also establishes the right to privacy. The function of the Committee is to consider the State's implementation of this right is monitored by the Human Rights Committee. The Committee has adopted the General Comment No. 16 on 'The right to respect of privacy, family, home and correspondence, and protection of honour and reputation' (1988). So-called 'concluding observations' are adopted by the Committee on the basis of reports submitted by states parties under article 40 of the ICCPR about states' implementation of human rights obligations. A level of access for individuals' is maintained in that the Committee adopts Views on the basis of communications (complaints) from individuals under article 5, paragraph 4, of the Optional Protocol to the ICCPR.

A particular strength of the Human Rights Committee – and similar global monitoring treaty bodies – is that they represent permanent organs for standard-setting, decisions on individual cases, and development of jurisprudence through their General Comments, Concluding Observations and Views.[123] The standards of privacy protection are, however, far less developed from this body than on more regional or local levels. Another weakness is that the findings, although authoritative, are not legally binding. Further, the right to individual complaints depend on ratification of the Optional Protocol, and many states do not report to the Committee. The treaty bodies have limited possibilities to follow up their findings. Finally, the system lacks both visibility and resources.

4.5.3 Internal audit mechanisms

Although access control, as described above in Section 4.2.1, is in place for the CMT, this may not be a sufficient safeguard against personnel using their legitimate access improperly. It is necessary to have implemented audit technology that records all activity in the database(s), to be able to control who has done what, how often, using which search-words.

As De Rosa argues, the idea of rule-based processing as a privacy protection tool is that certain policy rules can be built into search queries so that data can only be retrieved consistently with those rules.[124] Rule-based processing has two elements. Firstly, the query must carry with it information about the types of permission the user has. For example, a query might indicate that it is pursuant to a search warrant, which would allow it to retrieve certain kinds of data that would be unavailable without a warrant. Secondly, data must be labelled with information about how they may be accessed. Data items might be labelled with "meta data"—data that summarize or describe the qualities of the data—that indicates how the data can be processed. De Rosa further argues that such meta-data labels could travel with the data and guide access to them wherever they reside.[125] The meta-data for a particular data item might, for example, indicate whether it identifies an American or a foreign person, and access can be controlled accordingly.

TACTICS has stated that the system should allow the usage of security policies in requirement SEC_TMT_REQ#001.

4.6 Decision making competence

The prospective TACTICS system is intended, as mentioned above, only for situations where a terrorist attack is about to happen and may be prevented, and where such an attack is happening or has happened, and there is a need to mitigate and/or stop the attack or further attacks.

The use of the TACTICS system must be exceptional, and only in the case of an imminent terrorist attack. The realization of both these constraints is not trivial. It is clear that the system does not have any method to verify how it is being used. The context of terrorism or any other activity is only mapped in the mind of its users. Therefore, one should understand that the scope of its usage is subject to the will of the officer granting usage access. The aforementioned measures to limit the usage of the system usage (e.g. access rights) do not have any relevance to the usage context. Only a posteriori could someone understand why the system was actually used. Moreover, to understand its scope he should have access to the log files of the operation.

---

[123] DETECTER (Detection Technologies, Terrorism, Ethics and Human Rights) research project: "Recommendations of improved monitoring mechanisms of secret counter-terrorism activities" (WP 8, *D16.3*), EU FP7, ch.3.

[124] De Rosa, *op.cit.*, pp.19-20.

[125] De Rosa, *ibid.*

All the above indicate that the use of the system must conform to strict rules and predefined procedures which are always followed. While some alerts could notify the respective authorities, they cannot avert the usage of the system when it is running. Failure to follow specific procedures, e.g. granting access to operational log files, could imply unauthorised/excessive use of the system.

The usage of the system from unauthorised personnel is a risk with huge impact. The intelligence that a criminal or a terrorist could gain through TACTICS could put national security at stake. Therefore, it is vital to apply both strong physical security measures and access controls in the premises where the TACTICS resides. In this regard, the use of biometrics for the authentication of the personnel can be considered a default measure. Moreover, to counter potential cyber-attacks, the TACTICS system should be installed along with properly configured and updated IDS and IPS systems.

TACTICS addresses this with requirement FU_TMT_REQ#006 - ethical and juridical restrictions must be shown to the end user, and FU_TMT_REQ#007 - a two key policy would be used for ethical related actions.

4.7 Deletion

A consequence of the inherent retentive character of digital data is that data that has been collected for one purpose may easily be used for another purpose not foreseen at the time the data was collected.[126] A challenge of the CMT and all other re-use institutions in this relation is that it becomes harder for the data subject to locate where the responsibility lies for the use of the data. Since the aim of the TACTICS system is not to establish a new *lasting* database, it is crucial that all data that is not any longer needed for security or judicial purposes is erased.

4.7.1 Mission creep and spill-over effect: the use of data concerning non-terrorist activity

The issue of police's access or use of spill-over or 'surplus' information, from for example wiretapping, is increasingly relevant as the technology to intercept, store and couple data is constantly developing. Because of the purpose limitation principle, the point of departure is that information not concerning (in the TACTICS case) the terrorist activity being mitigated, must be erased and not investigated.

This point of departure may be seen as problematic. In the case where TACTICS is 'set in motion' because the competent decision maker considers there to be (reasonable) grounds to expect that a terrorist attack is about to happen or has happened, the activities in question will in many cases span out in serious offenses. As described above, there is a requirement of *motive* for an offense to be deemed a terrorist offense. A potential situation could be that a bomb has gone off outside a parliament building, killing several people. The TACTICS system is set in motion, and the CMT provides the TM direct access to an array of private security cameras in the area around the Parliament, widespread information from several different databases and online sources of financial transactions, etc. After some investigation, it becomes clear that the perpetrator intended to kill only one person, his wife, who worked there. It is thus not an act of terrorism. Through the coupling of capabilities, additional information concerning other criminal activities has appeared. The question is then whether the evidence stemming from this information may be used, and whether it should have any impact that the TACTICS system was set off on 'false' premises.

On the one hand, it may seem unreasonable that a crime should go unpunished or un-investigated because the original purpose of the measure was another than the then unknown crime. On the other hand, powerful tools such as TACTICS and its CMT could be abused outside of their intended – and exceptional – purpose if the threshold was low, allowing the usage of information acquired there. It is also likely that other types of illegal behaviour could take on a high profile, and authorities will be under pressure to expand the use of these techniques, for example, to help investigate other violent criminals or immigration law violators.[127]

[126] Hilst, R vd, *op.cit.* 2013 p.77.

[127] DeRosa, *op.cit.* 2004, p.16.

5 Privacy Enhancing Technologies for data management

According to Hughes[128]:

"Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

While in many aspects of everyday life someone could decide what to reveal to others, modern technologies impose many challenges as the data collection and fusion can reveal a lot of additional information without his acknowledgement or his consent. A typical example is the use of someone's location where someone is willing to share his whereabouts with some e.g. traffic service. However, using data mining one could easily extract important information such as the home and work location of the user by noting where the user is at specific times, religious beliefs e.g. attendance to specific religious areas (cemeteries), temples, mosques etc., or even political beliefs e.g. attendance to a protest. To counter the privacy exposure of users, the past few years have seen a huge growth of Privacy Enhancing Technologies (PET), as introduced by Goldberg, Wagner, and Brewer[129]. PETs is the general name of a wide family of algorithms from the academia and industry that enable operations to be implemented on datasets with the least impact (if any) on users' privacy. Therefore, PET includes technologies from privacy-preserving data mining[130] and statistical methods to query databases[131], to anonymous browsing[132] and anonymous transactions.

While theoretically PETs would introduce many issues for the TACTICS system, they can be used to provide actual Privacy by Design (PbD)[133] approaches towards data management. Therefore, in the following paragraphs we outline some state of the art solutions, their efficiency and applicability in the TACTICS system to illustrate how the seven principles of PbD[134] can be practically implemented and embedded in the actual system, as the concept of PbD is quite vague and therefore there is a necessity to actually draw the lines from the concept to the actual implementation[135]. As it will become apparent, these recommendations come as separate components so the modular form of the TACTICS system as well as the validation system can easily implement them. In addition, many of the proposed algorithms have been implemented and are described in the appendix of this deliverable.

5.1 Storing Video footage

Perhaps the most widely used method used in surveillance is video surveillance. The main concept is that an operator is sitting in front of a set of monitors which display what some remote cameras are recording. This enables an operator to simultaneously monitor physical activity within large perimeters or even disjoint areas, without the need to physically be there. Modern cameras, in addition to the usual methods of zooming or night vision can provide additional operations, depending on the attached modules. For instance they can provide face detection/recognition, object detection, person/object tracking and thermal activity monitoring. It is apparent that the above may reveal sensitive information about individuals, therefore, when storing

---

[128] https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto

[129] Goldberg, Ian, David Wagner, and Eric Brewer. Privacy-enhancing technologies for the Internet. CALIFORNIA UNIV BERKELEY, 1997.

[130] Agrawal, Rakesh, and Ramakrishnan Srikant. "Privacy-preserving data mining." ACM Sigmod Record. Vol. 29. No. 2. ACM, 2000.

[131] Domingo-Ferrer, Josep, ed. Inference control in statistical databases: From theory to practice. Vol. 2316. Springer Science & Business Media, 2002.

[132] https://www.torproject.org/

[133] Cavoukian, Ann, and Jeff Jonas. Privacy by design in the age of big data. Information and Privacy Commissioner of Ontario, Canada, 2012.

[134] Cavoukian, Ann. "Privacy by design: The 7 foundational principles." Information and Privacy Commissioner of Ontario, Canada (2009).

[135] van Rest, Jeroen, et al. "Designing privacy-by-design." Privacy Technologies and Policy. Springer Berlin Heidelberg, 2014. 55-72.

information there should be mechanisms which hide sensitive information, so that only authenticated personnel can have access to it. An illustration of thisis that while a database administrator has full access to the system, user passwords are hashed so that he cannot access them and in the unlikely event of an adversary gaining access to the system, he will not be able to recover the user passwords[136]. Likewise, many video surveillance systems would first detect sensitive Regions of Interest (ROIs), encrypt/blur/distort these regions and then store them. This policy enables a user to access a video without having access to the sensitive data. Depending on the nature of ROIs there are several methods to detect them; nevertheless, the most apparent ones for the case of surveillance cameras are faces, therefore privacy-aware public surveillance through cameras is gaining more and more importance[137].

In principle, face detection techniques can be categorized into two major families. The first one is focused on the detection of Haar-like features[138]. The main concept behind them is to divide an image into small rectangles and then group adjacent rectangular regions at a specific location and sum up the pixel intensities in each region. By calculating the differences between these sums one could categorize subsections of an image very accurately. Local Binary Pattern[139] encodes both local and global facial characteristics into a feature histogram. This makes the method very lightweight but susceptible to errors as it may not detect the presence of a face. For more on face detection the interested reader may refer to [140].

Having detected the ROIs the next step is to protect them, something that can be done in the *pixel domain* or in the *compression domain*. Protecting the ROI in the pixel domain means that the obfuscation is made in the image, distorting it pixel by pixel. These methods can be categorized into:

- *Abstraction-based* techniques where the ROI is replaced/censored by a shape as in the proposal of Tansuriyavong and Hanaki[141] where they remove people's figures from a video. Of specific interest for TACTICS is the work of Cavallaro[142] which introduces a surveillance scheme that separates data into personal and behavioural on the fly, so that only authorized personnel can access the personal data. In this regard, an authorized officer could monitor citizens' behaviour, without seeing who is actually doing what, and in the event where a deviant and probable malicious behaviour is detected forward the footage to the designated personnel to recover the personal data of the individual.

---

[136] Simple password hashing is not efficient per se. For more details on how to implement secure such schemes, the interested reader may refer to:

Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[137] Moncrieff, Simon, Svetha Venkatesh, and Geoff AW West. "Dynamic privacy in public surveillance." Computer 42.9 (2009): 22-28.

Winkler, Thomas, and Bernhard Rinner. "User-centric privacy awareness in video surveillance." Multimedia systems 18.2 (2012): 99-121.

[138] Viola, Paul, and Michael Jones. "Rapid object detection using a boosted cascade of simple features." Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on. Vol. 1. IEEE, 2001.

[139] Hadid, Abdenour, Matti Pietikainen, and Timo Ahonen. "A discriminative feature space for detecting and recognizing faces." Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on. Vol. 2. IEEE, 2004.

[140] Zhao, Wenyi, et al. "Face recognition: A literature survey." ACM Computing Surveys (CSUR) 35.4 (2003): 399-458.
Viola, Paul, and Michael J. Jones. "Robust real-time face detection." International journal of computer vision 57.2 (2004): 137-154.
Rowley, Henry A., Shumeet Baluja, and Takeo Kanade. "Neural network-based face detection." Pattern Analysis and Machine Intelligence, IEEE Transactions on 20.1 (1998): 23-38.

[141] Tansuriyavong, Suriyon, and Shin-ichi Hanaki. "Privacy protection by concealing persons in circumstantial video image." Proceedings of the 2001 workshop on Perceptive user interfaces. ACM, 2001.

[142] A. Cavallaro: "Privacy in Video Surveillance.", IEEE Signal Processing Magazine,

vol. 24, no. 2, pp. 168–169, 2007

- *Pixel transformation* methods replace the pixel values introducing blurring or pixelisation or even warping on the ROIs of the image[143].
- *Cryptography-based* techniques[144] may permute the pixels of the ROI pseudo-randomly or encrypt the pixel values, rendering the protected areas useless for unauthenticated users.

In the case of compression domain methods, the obfuscation is not made in the pixels but in the encoding of the domain when it is being compressed. These techniques can be categorized as follows:

- Scrambling based techniques apply permutation on the ROIs in the compression domain[145].
- Cryptographic techniques: In this case, when the ROIs are compressed, they are first encrypted so that they can only be recovered by authorized personnel[146].
- Data hiding techniques enable layers on the image of each frame. Therefore, access to specific layers is granted depending on the user rights[147].

Finally, it should be noted that there are also other directions towards privacy-aware video surveillance such as the use of trusted computing[148], decoupling context knowledge and video[149] or even making the lens

---

[143] Korshunov, Pavel, and Touradj Ebrahimi. "Using face morphing to protect privacy." Advanced Video and Signal Based Surveillance (AVSS), 2013 10th IEEE International Conference on. IEEE, 2013.

Korshunov, Pavel, and Touradj Ebrahimi. "Using warping for privacy protection in video surveillance." Digital Signal Processing (DSP), 2013 18th International Conference on. IEEE, 2013.

A.M. Berger: “Privacy Mode for Acquisition Cameras and Camcorders",,Sony Corporation,

US patent 6, 067, 399 edition, May 2000.

E.N. Newton, L. Sweeney, and B. Main: “Preserving Privacy by De-identifying Face Images", IEEE transactions on Knowledge and Data Engineering, vol. 17, no. 2, pp. 232-243, Feb. 2005.

J. Wickramasuri, M. Datt, S. Mehrotra, and N. Venkatasubramanian: “Privacy Protecting Data Collection in Media Spaces", Proc. of the 12th annual ACM international conference on Multimedia, pp. 48{55, Oct. 2004.

[144] P. Carrillo, H. Kalva and S. Magliveras: “Compression Independent Reversible Encryption for Privacy in Video Surveillance", EURASIP Journal on Information Security -Special issue on enhancing privacy protection in multimedia systems, vol. 2009, no. 5, 2009.

[145] Dufaux, Frederic, and Touradj Ebrahimi. "Scrambling for privacy protection in video surveillance systems." Circuits and Systems for Video Technology, IEEE Transactions on 18.8 (2008): 1168-1174.

Sohn, Hosik, et al. "Privacy protection in video surveillance systems using scalable video coding." Advanced Video and Signal Based Surveillance, 2009. AVSS'09. Sixth IEEE International Conference on. IEEE, 2009.

[146] Shahid, Zafar, Marc Chaumont, and William Puech. "Fast Protection of H. 264/AVC by Selective Encryption of CAVLC and CABAC for I and P frames." Circuits and Systems for Video Technology, IEEE Transactions on 21.5 (2011): 565-576.

Peng, Fei, Xiao-wen Zhu, and Min Long. "An ROI privacy protection scheme for H. 264 video based on FMO and Chaos." Information Forensics and Security, IEEE Transactions on 8.10 (2013): 1688-1699.

K. Yabuta, H. Kitazawa and T. Tanaka: “A New Concept of Security Camera Monitoring with Privacy Protection by Masking Moving Objects", in Proc. of International Conference on Pattern Recognition, pp. 404-407, 2005.

K. Martin, and K.N. Plataniotis: “Privacy Protected Surveillance Using Secure Visual Object Coding", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 8, pp. 1152-1162, Aug. 2008.

[147] Martínez-Ponte, Isabel, et al. "Robust human face hiding ensuring privacy." Proceedings of the International Workshop on Image Analysis for Multimedia Interactive Services. Vol. 4. 2005.

[148] Winkler, Thomas, and Bernhard Rinner. "Securing embedded smart cameras with trusted computing." EURASIP Journal on Wireless Communications and Networking 2011 (2011): 8.

privacy aware[150]. In general, it becomes apparent that the on-board processing capabilities of modern embedded systems can make security and privacy protection inherent features of video surveillance cameras, allowing strict access policies, without compromising their efficiency.

5.2 Private Equality Testing

The concept of Private Equality Testing is quite straight forward. Let us assume that we have two users, Alice and Bob, each of which owns a value and they want to check whether their values are the same or not, without disclosing any further information. While the use of a Trusted Third Party could trivially solve the problem, common sense has proven that in most cases this concept cannot work. In this regard, Alice and Bob would like to perform the computation without intermediates. While the solution to the problem does not sound trivial, there are many solutions in the literature, all of which are based on cryptographic primitives.

To realize why this could be relevant to TACTICS, assume that the secret values that Alice and Bob have represent their GPS coordinates. Therefore, Alice would like to know whether Bob is close to her or not, introducing the concept of Private Proximity Testing. While most approaches would use a grid and calculate whether Alice and Bob are in the same cell, Narayanan et al.[151] introduced a method to make testing whether Alice and Bob are in adjacent cells, not necessary the same, fall into the problem of Private Equality Testing. Their method uses a set of three overlapping grids and the well-known El Gamal encryption algorithm[152] to hide the values. Typically, one could use variants of the Diffie-Hellman key agreement protocol[153], such as the protocol of Chatterjee et al.[154] or Huberman et al.[155] to perform the Privacy Equality Test. Novel approaches[156] make use of Bloom filters to encode areas of interest and allow a user to check whether he is in proximity or not, without disclosing his actual whereabouts.

The above methodologies could be adopted by the TACTICS system to allow tracking the citizens' location, without disclosing their privacy. More precisely, even if some citizens are tracked by GPS monitoring devices, TACTICS could trigger specific alarms only in the event that the individuals are in proximity of specific areas or of each other, minising the invasion to their privacy.

Winkler, Thomas, and Bernhard Rinner. "TrustCAM: Security and privacy-protection for an embedded smart camera based on trusted computing." Advanced Video and Signal Based Surveillance (AVSS), 2010 Seventh IEEE International Conference on. IEEE, 2010.

[149] Saini, Mukesh, et al. "Anonymous surveillance." Multimedia and Expo (ICME), 2011 IEEE International Conference on. IEEE, 2011.

[150] Winkler, Thomas, Adám Erdélyi, and Bernhard Rinner. "TrustEYE. M4: Protecting the sensor—Not the camera." Advanced Video and Signal Based Surveillance (AVSS), 2014 11th IEEE International Conference on. IEEE, 2014.

[151] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, D. Boneh, Location privacy via private proximity testing, in: NDSS, The Internet Society, 2011.

[152] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." Advances in Cryptology. Springer Berlin Heidelberg, 1985.

[153] W. Diffie, M. E. Hellman, New directions in cryptography, Information Theory, IEEE Transactions on 22 (6) (1976) 644–654.

[154] S. Chatterjee, K. Karabina, A. Menezes, A new protocol for the nearby friend problem, in: Proceedings of the 12th IMA International Conference on Cryptography and Coding, Springer-Verlag, 2009, pp. 236–251.

G. Yang, C. H. Tan, Q. Huang, D. S. Wong, Probabilistic public key encryption with equality test, in: Topics in Cryptology-CT-RSA 2010, Springer, 2010, pp. 119–131.

Q. Tang, Towards public key encryption scheme supporting equality test with fine-grained authorization, in: Information Security and Privacy, Springer, 2011, pp. 389–406.

[155] B. A. Huberman, M. Franklin, and T. Hogg. Enhancing privacy and trust in electronic communities.

In ACM Conference on Electronic Commerce (EC'99), pages 78–86. ACM, 1999.

[156] Palmieri, Paolo, Luca Calderoni, and Dario Maio. "Spatial Bloom Filters: Enabling Privacy in Location-aware Applications." Information Security and Cryptology-10th International Conference, Inscrypt 2014, Beijing, China, December 13-15, 2014, Revised Selected Papers}. Springer}, 2014.

5.3 Private Set Intersection

Closely related to Private Equality Testing is the problem of Private Set Intersection (PSI). In this case, Alice and Bob have some sets and they want to disclose the common ones without disclosing anything else about the rest of their elements. While the problem might sound quite far fetched, it can have many applications in the TACTICS system concept. To understand this extension, assume that the TACTICS team wants to check a sensitive database, owned by another party which is not willing to disclose its full dataset. This could include access to transactions of a financial institution, access to the list of terrorists from another country, access to telecommunication logs etc. In any of the aforementioned cases, while the information could be invaluable, it is very probable that the other party might be willing to cooperate, nevertheless, to protect its customers or for national security reasons might be reluctant to share the whole dataset. A Private Set Intersection protocol would enable them to check whether there are common elements and disclose them only, without the intelligence having to share the characteristics of the data that they are looking for either.

Freedman, Nissim and Pinkas[157] introduced the problem and several solutions have so far been proposed in the literature[158]. PSI comes in several flavours, for instance depending on who learns the outcome of the protocol, we have the unilateral and mutual flavours, where in the first case only the initiator learns the intersection of the sets, and in the latter both of them learn it. Depending on whether the according data are being transferred, we could also characterize a PSI protocol as a PSI with Data Transfer. In some protocols, the parties learn only the cardinality of the intersection, and in others, instead of two, we have multiple parties[159]. The introduction of the De Christofaro and Tsudik protocol[160] made PSI protocols far more efficient. One of the main reasons was the reduction of the complexity from quadratic to linear. If we assume that Alice has A elements and Bob has B elements, then up to that point most protocols needed to perform AxB operations when the De Christofaro and Tsudik protocol needed A+B operations. The protocol is based on the well-known RSA algorithm[161] making its implementation very easy and practical without the use of special software. Recently, Pinkas et al.[162] performed an evaluation of several PSI protocols boosting the performance of many of these protocols, making them even more efficient.

---

[157] Michael J Freedman, Kobbi Nissim, and Benny Pinkas. Efficient private matching and set intersection. In Advances in Cryptology-EUROCRYPT 2004, pages 1–19. Springer, 2004.

[158] Yan Huang, David Evans, and Jonathan Katz. Private set intersection: Are garbled circuits better than custom protocols. In Network and Distributed System Security Symposium (NDSS). The Internet Society, 2012.

Stanis law Jarecki and Xiaomin Liu. Fast secure computation of set intersection. In Security and Cryptography for Networks, pages 418–435. Springer, 2010.

Aggelos Kiayias and Antonina Mitrofanova. Testing disjointness of private datasets. In Financial Cryptography and Data Security, pages 109–124. Springer, 2005.

Lea Kissner and Dawn Song. Privacy-preserving set operations. In Advances in Cryptology–CRYPTO 2005, pages 241–257. Springer, 2005.

[159] Lea Kissner and Dawn Song. Privacy-preserving set operations. In Advances in Cryptology–CRYPTO 2005, pages 241–257. Springer, 2005.

Ronghua Li and Chuankun Wu. An unconditionally secure protocol for multiparty set intersection. In Applied Cryptography and Network Security, pages 226–236. Springer, 2007.

Yehuda Lindell and Benny Pinkas. Secure multiparty computation for privacy preserving data mining. Journal of Privacy and Confidentiality, 1(1):5, 2009.

[160] De Cristofaro, Emiliano, and Gene Tsudik. "Practical private set intersection protocols with linear complexity." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2010. 143-159.

[161] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[162] Pinkas, Benny, Thomas Schneider, and Michael Zohner. "Faster private set intersection based on OT extension." USENIX Security. Vol. 14. 2014.

We should highlight the recent scheme of Segal et al.[163] which uses Private Set Intersection to create an open, privacy-preserving, accountable surveillance processes which could be used by the FBI for targeting High Country Bandits and or NSA for its CO-TRAVELER[164] project.

5.4 Privacy-preserving sample set similarity

Privacy-preserving sample set similarity could be thought of an extension of the Private Set Intersection problem in that Alice and Bob need to evaluate the similarity of their datasets, but are reluctant to openly disclose their data to each other. To quantify the similarity of two datasets one could use the Cosine, Euclidean, Manhattan, Minkowski similarity, Hamming /Levenshtein distance or the Jaccard Similarity Index [165].

Blundo et al.[166] have recently introduced a protocol based on PSI, where they sample the two datasets with MinHash[167]. Their method is very efficient and lightweight and can have a wide range of applications.

Of specific interest to the TACTICS system are their use on biometrics. Typically, most biometric methods take a sample from a user to authenticate him to a system. While the user will present his fingerprint, his iris, retina and the like which we could assume as permanent, due to external noise, position, sensor sensitivity, movement etc., the sensor is highly unlikely to receive the exact same measurement every time a user wants to authenticate to a system. To counter these problems, instead of checking exact matching of the two measurements (the registered and the one for verification), biometric systems have a threshold T so that if the similarity of the two samples is above T, then the user is authenticated.

Similarly to the scenario of the PSI problem, the TACTICS system might have to check the biometrics of a suspect against the respective database of an external entity which is not willing to hand over their database e.g. another country's terrorist database. Clearly, the Blundo et al. protocol provides a secure, privacy-aware method to achieve this task, far more efficient that other solutions in the literature[168].

---

[163] Segal, Aaron, Bryan Ford, and Joan Feigenbaum. "Catching bandits and only bandits: Privacy-preserving intersection warrants for lawful surveillance." 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI'14). 2014.

[164] https://www.eff.org/deeplinks/2013/12/meet-co-traveler-nsas-cell-phone-location-tracking-program

[165] P. Jaccard. Etude comparative de la distribution florale dans une portion des Alpes et du Jura, 1901.

[166] Blundo, Carlo, Emiliano De Cristofaro, and Paolo Gasti. "EsPRESSo: efficient privacy-preserving evaluation of sample set similarity." Data Privacy Management and Autonomous Spontaneous Security. Springer Berlin Heidelberg, 2013. 89-103.

[167] A. Broder. On the resemblance and containment of documents. In Compression and Complexity of Sequences, 1997.

[168] Bringer, Julien, Hervé Chabanne, and Alain Patey. "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends." Signal Processing Magazine, IEEE 30.2 (2013): 42-52.

Cimato, Stelvio, et al. "Privacy-aware biometrics: Design and implementation of a multimodal verification system." Computer Security Applications Conference, 2008. ACSAC 2008. Annual. IEEE, 2008.

Bhargav-Spantzel, Abhilasha, et al. "Privacy preserving multi-factor authentication with biometrics." Journal of Computer Security 15.5 (2007): 529-560.

Bringer, Julien, et al. "GSHADE: faster privacy-preserving distance computation and biometric identification." Proceedings of the 2nd ACM workshop on Information hiding and multimedia security. ACM, 2014.

Penn, Georg, et al. "Customisation of Paillier Homomorphic Encryption for Efficient Binary Biometric Feature Vector Matching." Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'14), Darmstadt, Germany. 2014.

5.5 Accessing databases with sensitive data

The introduction of fully homomorphic encryption[169] has drastically changed the way that we think future databases will operate, since it allows us to perform any operations over encrypted data, therefore enabling calculations over encrypted data. This means that a database could be encrypted with a key that is not known to the database administrator or the system. However, the user could perform queries on the database which are executed, without decrypting the stored encrypted data, the results are encrypted and can be decrypted only by the user without leaking any information. While this ideal model can be considered something that can be implemented efficiently, unfortunately, we are far from the point where it can be considered practical for real-world applications as the encryption and decryption are very slow. Therefore, until fully homomorphic encryption becomes practical, some intermediate solutions are being used, most of which are based on partial homomorphic encryption. The difference of partial with fully homomorphic encryption is that in partial homomorphic encryption only some operations can be performed. Partial homomorphic schemes or simply, homomorphic as we usually call them are known for many years. Typical examples are RSA, El Gamal, Paillier[170] and Goldwasser-Micali[171] which allow multiplication, multiplication, addition and XOR respectively.

Closely related to homomorphic encryption is the notion of order preserving encryption (OPE), introduced by Agrawal et al.[172] The concept of OPE is that if we encrypt two messages, their order remains the same, that is if x>y then E(x)>E(y). OPE can significantly boost the performance of searching over encrypted data, nevertheless, the amount of leaked information is substantial. Since the initial scheme was not secure enough, new more secure algorithms were introduced[173], however, due its nature, several attacks are still possible.

Based on the above encryption primitives there are several approaches, such as CryptDB[174] or SADS[175] which allow encrypted queries over encrypted data, with minimal computational overhead. Due to the sensitivity of the data that the TACTICS system has, as well as the strict policies regarding information disclosure, these schemes could provide a good solution balancing privacy and security with efficiency, as for instance SADS has only around 20% computational overhead. Clearly, such schemes could provide an additional level of security in case of internal and external threats, without compromising the performance of the system.

Finally, of high interest to TACTICS is the MetaCrypt[176] concept of Seny Kamara. The scope of MetaCrypt is to provide a database where telecommunication companies store the metadata of the calls while providing the following features: (1) protect MetaDB from outsiders, (2) allow only certified queries to be performed on the database, (3) Data privacy Analysts learn at most the query response, and (4) the telecommunication companies learn nothing about NSA queries. All the above requirements can be considered valid for the TACTICS system and not only for the telecommunication metadata, but for every possible sensitive and private information as well.

---

[169] Gentry, Craig. A fully homomorphic encryption scheme. Diss. Stanford University, 2009.

[170] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." Advances in cryptology—EUROCRYPT'99. Springer Berlin Heidelberg, 1999.

[171] Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption & how to play mental poker keeping secret all partial information." Proceedings of the fourteenth annual ACM symposium on Theory of computing. ACM, 1982.

[172] Agrawal, Rakesh, et al. "Order preserving encryption for numeric data." Proceedings of the 2004 ACM SIGMOD international conference on Management of data. ACM, 2004.

[173] Boldyreva, Alexandra, Nathan Chenette, and Adam O'Neill. "Order-preserving encryption revisited: Improved security analysis and alternative solutions." Advances in Cryptology–CRYPTO 2011. Springer Berlin Heidelberg, 2011. 578-595.

[174] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing", In Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP), Cascais, Portugal, October 2011.

[175] Raykova, Mariana, et al. "Secure anonymous database search." Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009.

[176] http://research.microsoft.com/en-us/um/people/senyk/slides/metacrypt.pdf

6 Conclusions

In this report, we have described the most relevant challenges related to the TACTICS system, and the TMT in particular, concerning legal conditions, ethics, human rights and privacy as well as some extensions on them. Moreover, we have provided an overview of how some of these problems could be resolved from the technological and implementation aspect.

The nature of the TACTICS system makes it balance on the legal and ethical limits of current legal and ethical framework. It should be understood that the TACTICS system is the last resort in order to prevent an extreme event, a terrorist attack, for which the information is very sparse. One could go back to Hippocrates and his quote “For extreme diseases, extreme methods of cure, as to restriction, are most suitable.” and claim that “desperate times (a terrorist threat) call for desperate measures (use of TACTICS)”, nevertheless, after several centuries we have the technological means to contain these desperate measures and make them less invasive.

Regardless of the methods, the scope of the TACTICS system is ethical as it can prevent a terrorist attack and save many human lives. However, its use must be strictly contained in this sole environment and event, any further use makes it unethical. Its capabilities and resources set very strict constraints on when it is used, who is using it, where it is used and for how long. As discussed in this report, most of these aspects can be resolved with technological means, e.g. strong authentication, authorization protocols etc (many of which have already been implemented in the prototype). Nevertheless, it is important to note that while there is a solid European framework on Data Privacy, the fragmentation of the legal system in each member country implies further and different constraints. Moreover, practically each member country has its own system to deal with such extreme events, setting even more practical constraints in terms of a unified approach as each member has different authorization models, different procedures and different structures. Therefore, even if TACTICS provides a baseline approach, compliant with EU regulations, configuring it for each member possible member state is still an open challenge, specially, when this legal framework is not stable and is subject to changes, but this is out of the scope of this project.

7 Appendix

In this appendix we include some Python implementations that can facilitate the interested readers in adopting several technical approaches.

7.1 Implementation of the PSI protocol of De Christofaro and Tsudik

```
#!/usr/bin/python
import random
from time import time
import gmpy
import hashlib

e=2**16+1

def hash_int(x):
    return int(hashlib.sha256(str(x)).hexdigest(),16)

#generates a random prime of the requested bit length
def gen_prime(BIT_LEN):
    found=False
    while found==False:
        p=random.randrange(2**(BIT_LEN-1),2**BIT_LEN)
        found=gmpy.is_prime(p)
    return p

#generates a random safe prime of the requested bit length
def gen_safe_prime(BIT_LEN):
    found=False
    while found==False:
        q=random.randrange(2**(BIT_LEN-2),2**(BIT_LEN-1))
        p=2*q+1
        found=gmpy.is_prime(p) and gmpy.is_prime(q)
    return p


def RSA_GEN(BIT_LEN):
    # this is faster but not so secure
    # p=gen_prime(BIT_LEN)
    # q=gen_prime(BIT_LEN)

    p=gen_safe_prime(BIT_LEN)
    q=gen_safe_prime(BIT_LEN)

    n=p*q
    f=(p-1)*(q-1)
    e=2**16+1
    d=gmpy.invert(e,f)
    return d,n

def RSA_ENC(m,n):
    return pow(m,e,n)
def RSA_DEC(c,d,n):
    return pow(c,d,n)

#generate RSA key pair (public,private) for the server
d,n=RSA_GEN(256)

#now let's create some elements for the server and the client
server_elements=[random.randrange(n) for i in range(1000)]
client_elements=[random.randrange(n) for i in range(100)]

```

```
#to be sure that we have some common elements in both of them,
#we add some of the server's elements in the client's set
client_elements+=server_elements[:50]

#now let's hash the lists' elements
hs=[hash_int(i) for i in server_elements]
hc=[hash_int(i) for i in client_elements]

#now let's create Client's message
m_A=[]
rs=[]
for i in hc:
    r=random.randrange(n)
    rs.append(r)
    obf=(pow(r, e,n)*i)%n
    m_A.append(obf)

#The server will now generate the two sets to send to the client
m_B1=[RSA_DEC(x,d,n) for x in m_A]
m_B2=[hash_int(RSA_DEC(y,d,n)) for y in hs]

#The client must "remove" the r from each element
for i in range(len(m_B1)):
    m_B1[i]=hash_int((m_B1[i]*gmpy.invert(rs[i],n))%n)

#now let's count the common elements
cnt=0
for i in m_B1:
    if i in m_B2:
        cnt+=1
print "common elements:", cnt
```

7.2 Implementation of the PSI protocol using elliptic curves

For the sake of simplicity, the implementation below is made in Sage[177], an open source mathematics software based on Python.

```
import random
from time import time
import hashlib

def hash_int(x):
    return int(hashlib.sha256(str(x)).hexdigest(),16)

#generates a random prime of the requested bit length
def gen_prime(BIT_LEN):
    found=False
    while found==False:
        p=random.randrange(2**(BIT_LEN-1),2**BIT_LEN)
        found=is_prime(p)
    return p

p=gen_prime(160)
x=random.randrange(p)
y=random.randrange(p)
a=random.randrange(p)
b=y*y-x**3-a*x
F = Zmod(p)
E=EllipticCurve(F, [a, b])
G = E([x,y])

```

[177] http://www.sagemath.org

```
#server params
xs=random.randrange(p)
Hs=xs*G

#client params
xc=random.randrange(p)
Hc=xc*G

#now let's create some elements for the server and the client
server_elements=[random.randrange(p) for i in range(1000)]
client_elements=[random.randrange(p) for i in range(100)]

#to be sure that we have some common elements in both of them,
#we add some of the server's elements in the client's set
client_elements+=server_elements[:50]

#now let's hash the lists' elements
hs=[hash_int(i) for i in server_elements]
hc=[hash_int(i) for i in client_elements]

#now let's create Client's message
m_A=[]
m_A=[h*Hc for h in hc]

#The server will now generate the two sets to send to the client
m_B1=[(xs*P)[0] for P in m_A] #we only need x coordinate
m_B2=[y*Hs for y in hs]

#The client must "add" his key to the server's elements
m_B2=[(xc*Q)[0] for Q in m_B2]

cnt=0
for PP in m_B1:
    if PP in m_B2:
        cnt+=1
print "Common elements",cnt
```

7.3 Private computation of the Jaccard index

```
#!/usr/bin/python
import random
from time import time
import gmpy
import hashlib

e=2**16+1

def hash_int(x):
    return int(hashlib.sha256(str(x)).hexdigest(),16)

#generates a random prime of the requested bit length
def gen_prime(BIT_LEN):
    found=False
    while found==False:
        p=random.randrange(2**(BIT_LEN-1),2**BIT_LEN)
        found=gmpy.is_prime(p)
    return p

#generates a random safe prime of the requested bit length
def gen_safe_prime(BIT_LEN):
    found=False
    while found==False:
        q=random.randrange(2**(BIT_LEN-2),2**(BIT_LEN-1))
        p=2*q+1
        found=gmpy.is_prime(p) and gmpy.is_prime(q)
```

```
    return p


def RSA_GEN(BIT_LEN):
    # this is faster but not so secure
    # p=gen_prime(BIT_LEN)
    # q=gen_prime(BIT_LEN)

    p=gen_safe_prime(BIT_LEN)
    q=gen_safe_prime(BIT_LEN)

    n=p*q
    f=(p-1)*(q-1)
    e=2**16+1
    d=gmpy.invert(e,f)
    return d,n

def RSA_ENC(m,n):
    return pow(m,e,n)
def RSA_DEC(c,d,n):
    return pow(c,d,n)

#generate RSA key pair (public,private) for the server
d,n=RSA_GEN(256)

#now let's create some elements for the server and the client
server_elements=[random.randrange(n) for i in range(10000)]
client_elements=[random.randrange(n) for i in range(8000)]

#to be sure that we have some common elements in both of them,
#we add some of the server's elements in the client's set
client_elements+=server_elements[:2000]

#now let's hash the lists' elements
hs=[hash_int(i) for i in server_elements]
hs.sort()
hc=[hash_int(i) for i in client_elements]
hc.sort()

k=20
hs=hs[:k]
hc=hc[:k]
#now let's create Client's message
m_A=[]
rs=[]
for i in hc:
    r=random.randrange(n)
    rs.append(r)
    obf=(pow(r, e,n)*i)%n
    m_A.append(obf)

#The server will now generate the two sets to send to the client
m_B1=[RSA_DEC(x,d,n) for x in m_A]
m_B2=[hash_int(RSA_DEC(y,d,n)) for y in hs]

#The client must "remove" the r from each element
for i in range(len(m_B1)):
    m_B1[i]=hash_int((m_B1[i]*gmpy.invert(rs[i],n))%n)

#now let's count the common elements
cnt=0
for i in m_B1:
    if i in m_B2:
        cnt+=1
print "Similarity: %.2f%%" % (100*cnt/(1.0*k))
```

7.4 Hash-based one-time passwords

```
#!/usr/bin/python
import hashlib

def hash_int(x):
    return int(hashlib.sha256(str(x)).hexdigest(),16)

AUTH2ALLOW=1000
key="tactics_key"
tmp=key
for i in range(AUTH2ALLOW):
    tmp=hash_int(tmp)
server_key=tmp

tmp=key
for i in range(AUTH2ALLOW-1):
    tmp=hash_int(tmp)
user_key=tmp

#check the keys
print hash_int(user_key)==server_key
#update the server key
server_key=user_key

#now let's do it one more time
tmp=key
for i in range(AUTH2ALLOW-2):
    tmp=hash_int(tmp)
user_key=tmp
print hash_int(user_key)==server_key
```

7.5 Simple symmetric authentication

```
#! /usr/bin/python
import cv
import argparse
import random
import base64
from Crypto import Random
from Crypto.Cipher import AES
import hashlib

class AESCipher:

    def __init__(self, key):
        self.bs = 32
        self.key = hashlib.sha256(key.encode()).digest()

    def encrypt(self, raw):
        raw = self._pad(raw)
        iv = Random.new().read(AES.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return base64.b64encode(iv + cipher.encrypt(raw))

    def decrypt(self, enc):
        enc = base64.b64decode(enc)
        iv = enc[:AES.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return self._unpad(cipher.decrypt(enc[AES.block_size:])).decode('utf-8')

    def _pad(self, s):
        return s + (self.bs - len(s) % self.bs) * chr(self.bs - len(s) % self.bs)

```

```
    @staticmethod
    def _unpad(s):
        return s[:-ord(s[len(s)-1:])]

aes=AESCipher("tacticskey")

#Bob generates a fresh random number and sends it to Alice
r_B=random.randrange(2**256)

#Alice generates a fresh random number
r_A=random.randrange(2**256)
m_A=",".join([str(r_A),str(r_B),"Bob"])

m_A=aes.encrypt(m_A)


#Bob receives it and decrypts iter
c=aes.decrypt(m_A)
#extracts r_A
c=c.split(",")
#end sends it to Alice encrypted with their key
m_B=aes.encrypt(c[1]+","+c[0])
```

7.6 Hash-based authentication (SKID3)

The code below is similar to the previous, but it uses hash functions. The scope of this snippet is to provide an alternative method of authentication, as in many portable devices many cryptographic algorithms are not implemented.

```
#! /usr/bin/python
#SKID3 protocol
import random
import hashlib

def hash_int(x):
    return int(hashlib.sha256(str(x)).hexdigest(),16)

key="tacticskey"

#Bob generates a fresh random number and sends it to Alice
r_B=random.randrange(2**256)

#Alice generates a fresh random number
r_A=random.randrange(2**256)
m_A=",".join([str(r_A),str(r_B),"Bob"])

m_A=[r_A,hash_int(m_A)]

#Bob receives it and computes his part
m_B=hash_int(str(r_B)+","+str(m_A[0])+",Alice")
```

7.7 Password salting

The snippet below uses the passlib[178] to properly salt the passwords and illustrate how one could test the whether a password is valid or not.

```
from passlib.hash import pbkdf2_sha256

#create the hash to use
hash = pbkdf2_sha256.encrypt("userpassword", rounds=20000, salt_size=16)
```

[178] https://pythonhosted.org/passlib/

```
#verify if a given password matches a hash
print pbkdf2_sha256.verify("userpassword", hash)
print pbkdf2_sha256.verify("abcdef", hash)
```

7.8 The protocol of Narayanan et al.

The following code provides a non-optimal implementation of operations with elliptic curves and implements the aforementioned protocol of Narayanan et al. for location privacy.

```
import gmpy
import random
import math

def genprime(bits):
    p=1
    if bits<=1000:
        while(gmpy.is_prime(p)==0):
            p = random.randrange(math.pow(2,bits-1),math.pow(2,bits))
        return p
    else:
        while(gmpy.is_prime(p)==0):
            p1 = random.randrange(math.pow(2,bits/2-1),math.pow(2,bits/2))
            p2 = random.randrange(math.pow(2,bits/2-1),math.pow(2,bits/2))
            p=p1+2**(bits/2)*p2
        return p

def genkey(bits):
    p=genprime(bits)
    q=genprime(bits)
    n=p*q
    return n,p,q

#point addition
def padd(P,Q,a,b,n):
    if P==0:# P is the point at infinity
        return Q
    elif Q==0:# Q is the point at infinity
        return P
    elif P==Q:# Point doubling
        px,py=P
        #point doubling
        lamda=(3*px**2*px+a)%n
        if gmpy.gcd(py,n)>1:
            print "n=%d, Found div %d"%(n,gmpy.gcd(py,n))
            print "here 1"
        lamda=(lamda*gmpy.invert(2*py,n))%n
        rx=(lamda**2-2*px)%n
        ry=(lamda*(px-rx)-py)%n
    else:
        px,py=P
        qx,qy=Q
        lamda=(qy-py)%n
        if gmpy.gcd(qx-px,n)>1:
            print "n=%d, Found div %d"%(n,gmpy.gcd(qx-px,n))
            print "here 2"
        lamda=(lamda*gmpy.invert(qx-px,n))%n
        rx=(lamda**2-px-qx)%n
        ry=(lamda*(px-rx)-py)%n
    return rx,ry

def pmult(k,P,a,b,n):
    Q=0
    for i in bin(k)[2:]:
        Q=padd(Q,Q,a,b,n)
        if i=="1":
```

```
            Q=padd(Q,P,a,b,n)
    return Q

p=genprime(160)

x0=random.randrange(0,p)
y0=random.randrange(0,p)

b=(y0**2-x0**3)%p
a=0
G=[x0,y0]

x=random.randrange(p)
H=pmult(x,G,a,b,p)

#alice
r=random.randrange(p)
la=random.randrange(1000)
g1=pmult(r,G,a,b,p)
g2=pmult(r+la,H,a,b,p)

#bob
lb=random.randrange(1000)
s=random.randrange(p)
t=random.randrange(p)
tmp1=pmult(s,g1,a,b,p)
tmp2=pmult(t,G,a,b,p)
u1=padd(tmp1, tmp2, a, b, p)
tmp1=pmult(s,g2,a,b,p)
tmp2=pmult(t-s*lb,G,a,b,p)
u2=padd(tmp1, tmp2, a, b, p)

#alice
tmp1=pmult(x, u1, a, b, p)
tmp1=[tmp1[0],-tmp1[1]]
res=padd(tmp1, u2, a, b, p)
```

7.9 Face detection and obfuscation

The following code illustrates a simple face detection algorithm through the use of OpenCV library[179]. In the first case, the program takes an image, detects the face and draws a black rectangle on top of it. In the second case, it encrypts the pixels values to obfuscate the contents. Clearly, only the second result can be inverted with the proper key.

```
#! /usr/bin/python
import cv
import argparse
import random
import base64
from Crypto import Random
from Crypto.Cipher import AES
import hashlib

class AESCipher:

    def __init__(self, key):
        self.bs = 32
        self.key = hashlib.sha256(key.encode()).digest()

    def encrypt(self, raw):
        raw = self._pad(raw)
```

[179] http://opencv.org/

```
        iv = Random.new().read(AES.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return base64.b64encode(iv + cipher.encrypt(raw))

    def decrypt(self, enc):
        enc = base64.b64decode(enc)
        iv = enc[:AES.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return self._unpad(cipher.decrypt(enc[AES.block_size:])).decode('utf-8')

    def _pad(self, s):
        return s + (self.bs - len(s) % self.bs) * chr(self.bs - len(s) % self.bs)

    @staticmethod
    def _unpad(s):
        return s[:-ord(s[len(s)-1:])]


parser = argparse.ArgumentParser(description='Gets a file as input, detects the face and p
uts a black rectangle on top to hide it.')
parser.add_argument('-f', action="store", dest="infile", help='Input file.')
userargs = parser.parse_args()

infile=userargs.infile
fname=infile.split(".")[0]
outfile1=fname+"_sup.png"
outfile2=fname+"_enc.png"

image=cv.LoadImage(infile,cv.CV_LOAD_IMAGE_COLOR)

hc=cv.Load("./haarcascade_frontalface_alt.xml")

#put a black rectangle in front of the face
face=cv.HaarDetectObjects(image,hc,cv.CreateMemStorage(),1.2,2,cv.CV_HAAR_DO_CANNY_PRUNING
,(0,0))
for ((x,y,w,h),k) in face:
    cv.Rectangle(image,(int(x),int(y)),(int(x)+w,int(y)+h),(0,0,0),-1,0);
    cv.SaveImage(outfile1, image)


image=cv.LoadImage(infile,cv.CV_LOAD_IMAGE_COLOR)
hc=cv.Load("./haarcascade_frontalface_alt.xml")
aes=AESCipher("tacticskey")
#encrypt randomize the colors
for ((x,y,w,h),k) in face:
    cnt=0
    for xx in range(int(x),int(x)+w):
        for yy in range(int(y),int(y)+h):
            r,g,b= image[xx,yy]
            r=int(r)
            g=int(g)
            b=int(b)
            # print r,g,b
            rr= base64.b64decode(aes.encrypt(str(cnt)))
            rr= int(base64.b16encode(rr),16)
            rr=(rr+r)%256
            cnt+=1
            gg= base64.b64decode(aes.encrypt(str(cnt)))
            gg= int(base64.b16encode(gg),16)
            gg=(gg+g)%256
            cnt+=1
            bb= base64.b64decode(aes.encrypt(str(cnt)))
            bb= int(base64.b16encode(bb),16)
            bb=(bb+b)%256
            cnt+=1

            image[xx,yy]=[rr,gg,bb]
```

```
83.
84.     cv.SaveImage(outfile2, image)
```