ABSTRACT

Two projects funded under the Horizon 2020 programme, IMPETUS and S4AllCities, have dealt with some common topics in order to develop technologies for a safe physical and digital environment in smart cities in the fight against crime and terrorism.

The partners of the consortia discussed their findings during the final dissemination event of the S4AllCities Project that was held in October 2022 in the city of Bilbao.

The result was a White Paper which is intended as a practical guide to help smart cities in the adoption of new disruptive technologies and tools in compliance with the applicable European legislation.

Smart cities have frontline responsibility to ensure a secure and safe physical and digital ecosystem promoting cohesive and sustainable urban development for the well-being of EU citizens. At the same time, the safety of citizens shall not limit other fundamental rights and freedoms. The balance between contrasting needs may sometimes be hard, but there are for sure precautions and security measures that may help. In particular, the White paper identifies the main challenges with reference to the protection of personal data and the requirements for the marketing of AI-enabled technologies and underlines the importance of a societal impact assessment. Moreover, the White paper provides some concrete examples of possible solutions to tackle the identified challenges.

Guidelines for Soft Target Protection:
Best practices to tackle
ethical, privacy and societal issues

White Paper released jointly by IMPETUS and S4AllCities projects

Authors:

IMPETUS: M. Soccol, I. Negri

S4AllCities: G. Melenikou, A. Cuesta Jimenez, G. Ortiz Romero

Release date: May 2023

ACKNOWLEDGEMENT: The work reported here received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286 (IMPETUS) and grant agreement No 883522 (S4AllCities).

Executive summary

The European Projects IMPETUS (Grant Agreement 883286) and S4AllCities (Grant Agreement 883522), which were funded under the European Union's Horizon 2020 research and innovation programme, have dealt with some common topics in order to develop technologies for a safe physical and digital environment in smart cities in the fight against crime and terrorism. The partners of the consortia had the opportunity to meet and share ideas during the lifetime of the Projects and discussed their results during the final dissemination event of the S4AllCities Project that was held in October 2022 in the city of Bilbao. One of the outcomes is this joint White Paper, which reflects the common thematic lines of the two Projects from an ethical and legal viewpoint. It is intended to define practical guidelines to help smart cities in the adoption of new disruptive technologies and tools in compliance with the applicable European legislation.

The concrete recommendations presented in this Whitepaper represent the outcomes of the pilot cases of the Projects, which involved a total of 5 cities in 5 European countries and enabled the Projects to validate the use of novel technologies and the practices adopted for the protection of public spaces. In this White Paper we will focus on legal issues related to surveillance technologies and artificial intelligence, considering especially their impact (i) on data protection, (ii) on ethics and (iii) on society. We will also consider further issues that may arise when considering a stable adoption of the technological tools, not only for testing. Therefore, the following guidelines are addressed mostly to smart cities and law enforcement agencies, which we consider as "end users". On the other hand, technology developers and citizens are also stakeholders that could benefit from the guidelines provided by this White Paper, to get informed and to understand fundamental requirements for the use of advanced technologies.

List of abbreviations

AI	Artificial Intelligence
AIA Proposal	Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
EU	European Union
GD	Gender Dimension
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
ICT	Information Communication Technologies
IoT	Internet of Things
LEA	Law Enforcement Agency
LED	Law Enforcement Directive (EU Directive 2016/680)
ML	Machine Learning
OSINT	Open-Source Intelligence
SIA	Societal Impact Assessment

Definitions

Artificial Intelligence system (AI system)	A system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.
Data controller	The natural or legal person that decides why and how personal data will be processed, also establishing the legal basis and the purposes for processing.
Data processing	Any action performed on data, whether automated or manual; this term includes, but is not limited to, collecting, recording, organizing, structuring, storing, using, erasing.
Data processor	The natural or legal person that processes personal data on behalf of a data controller; the GDPR has special rules for these individuals and organisations.
Data protection officer (DPO)	A figure at the heart of the legal framework established by GDPR, facilitating many organisations in complying with its provisions. Under the GDPR, it is mandatory for certain data controllers and processors to designate a DPO. Nevertheless, even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis. Data Protection Officers must be appointed in case of: - public authority other than a court acting in a judicial capacity performing data processing, - core activities requiring an entity to monitor people systematically and regularly on a large scale, - core activities are large-scale processing of special categories of data or data relating to criminal convictions and offenses.
Data subject	The identifiable natural person whose data is processed.
Machine learning	A subset of AI which allows a machine to automatically learn from past data and makes software applications more accurate in predicting outcomes without having to be specially programmed.
Personal data	Any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, IP addresses, religious beliefs, web cookies, and political opinions are also considered to be personal data. Pseudonymised data also fall under the definition. Anonymised data can also fall under the definition if there is a possibility of reidentification, hence, the most prudent course of action is to apply the GDPR.
Smart city	This term has several definitions depending on the country, legal contexts, type of technologies considered, and so forth. The International Telecommunication Union (ITU) provides the following definition: “a smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to

	improve quality of life, the efficiency of urban operation and services, and competitiveness while ensuring that it meets the needs of present and future generations concerning economic, social, and environmental aspects". A smart city is therefore an urban area in which different technological-based solutions and sensors are networked to collect data and to promote sustainable development. Insights gained from the data are used to enhance the quality of life for citizens by managing assets, resources, and services more efficiently. We will consider a "smart city" as the totality of public bodies, such as municipality, law enforcement agencies, security forces, firefighters, and other emergency services. Having regard to data protection, one or more of these subjects will be considered as "Data controllers".

Overview of the Projects

IMPETUS

IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety) is a Horizon 2020 Research and Innovation project that provides city authorities with new means to improve the security of public spaces in smart cities, and so help protect citizens.

IMPETUS provides a solution that brings together:

• Technology: leverage the power of Internet of Things, Artificial Intelligence and Big Data to provide powerful tools that help operational personnel manage physical and cyber security in smart cities.

• Ethics: Balance potentially conflicting needs to collect, transform and share large amounts of data with the imperative of ensuring protection of data privacy and respect for other ethical concerns - all in the context of ensuring benefits to society.

• Processes: Define the steps that operational personnel must take, and the assessments they need to make, for effective decision making and coordination - fully aligned with their individual context and the powerful support offered by the technology.

Technological results are complemented by a set of practitioner's guides providing guidelines, documentation and training materials in the areas of operations, ethical/legal issues and cybersecurity.

The cities of Oslo (Norway) and Padova (Italy) have been selected as the sites of practical trials of the IMPETUS solution during the project's lifetime, but the longer-term goal is to achieve adoption much more widely.

https://www.impetus-project.eu/

S4AllCities

The S4AllCities project aims to make cities' infrastructures, services, ICT systems and Internet of Things more resilient while promoting intelligence and information sharing amongst security stakeholders. To achieve this, it integrates advanced technological and organisational solutions into a market-oriented, unified cyber–physical security management framework. The system focuses on risk-based open smart spaces security management, cybersecurity shielding, suspicious activity, behaviour tracking, the identification of unattended objects, the real-time estimation of cyber-physical risks in

multiple locations and measures activation for effective crisis management. This work plays a role in promoting good safety and security practices in European cities.

S4AllCities technology aims to revolutionize the way smart cities become more protected, prepared and resilient to both physical and cyber-attacks on city soft targets, smart spaces and critical infrastructure networks, by greatly augmenting City Spaces Situation Awareness with intelligence, context and evaluated real-time cyber and physical security threat levels.

The cities of Trikala (Greece), Bilbao (Spain) and Pilsen (Czech Republic) have been selected as the sites of practical trials of the S4AllCities system during the project's lifetime.

https://www.s4allcities.eu/

1. Introduction

Smart cities have frontline responsibility to ensure a secure and safe physical and digital ecosystem promoting cohesive and sustainable urban development for the well-being of EU citizens. The Projects integrated advanced technological and organizational solutions in a market oriented unified cyber-physical security management framework, aiming at raising the resilience of cities' infrastructures, services, ICT systems, IoT and at balancing it with the compliance with applicable laws and the respect of fundamental rights of citizens.

During the Projects, the opinions of various stakeholders were collected and compared, therefore, it was possible to consider the point of view both of private citizens and of persons who should be directly involved in the use of technological tools for security aims.

The partners of the two Projects have shared some guidelines and practices they have followed to define how smart cities should behave when adopting innovative technologies that may be used especially for surveillance and prevention of terrorist attacks or other criminal offences against soft targets.

The outcomes are reported in this White Paper and refer to these three main topics:

- Data protection,

- AI ethics guidelines and current regulatory framework,

- Societal impact of surveillance technologies.

More specifically, this White Paper will:

- present European applicable laws and regulations;

- describe ethical and legal issues to be faced when adopting AI-enabled tools;

- give recommendations on technical measures and good practices to implement and follow.

This White Paper is therefore intended to be a practical and concrete instrument to help smart cities adopt new disruptive technologies. It will enable smart cities' representatives to reflect upon, evaluate and take into account privacy, data protection and security aspects of surveillance and new AI-technologies, as well as relevant ethical and social concerns.

2. Data protection

Context

Smart cities' administrations are responsible for ensuring a secure and safe physical and digital environment for their citizens. The quick development and improvements of technologies allowing big data analytics, objects and persons recognition and, in general, new means of surveillance have a relevant impact in pursuing the safety of cities. Processing of personal data is a core part of the process that is deemed to be necessary for reasons of substantial public interest, i.e., the accomplishment of safety and security of public spaces. At the same time, a **fair balance** must be ensured between human safety, as a social good that derives from the fundamental human rights to life and human dignity, and the fundamental human right to protection of personal data.

Privacy acquires also a new role and significance when applied to AI technologies. Indeed, the Ethics Guidelines for Trustworthy AI list **among the key requirements "Privacy and data governance"**, stating that, "besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data" (see more information in the next chapter).

During the Projects, we have directly faced challenges related to data protection in the context of urban surveillance while testing the tools in real-life situations in five different European cities. We will then, first of all, present the main privacy issues that were reported.

Challenges

The first main concern related to privacy is that AI-based applications and services are generally considered **"data-hungry" tools**, whose intended functionality is often accompanied by other collateral activities which imply the use and collection of personal data. For instance, AI providers may use their customers' data to improve the AI service's model and it may sometimes be possible (for providers or external attackers) to analyse a system's inputs and outputs to extract information about the model's training data, with varying degrees of accuracy. Moreover, AI systems facilitate the combination of different data sets. In this way, it is possible to deduce also involuntary correlations, leading to the specific identification of individuals.

Public entities may not have the necessary skills to control and correctly qualify the data shared with AI systems and therefore they have to **rely on AI providers**. These providers may adapt the tools to the specific requirements of public entities or may prefer to provide a standardised version of them, which could be in contrast with applicable laws. In this context, it may be not straightforward to attribute the roles of Data controllers and Data processors and the consequent responsibilities in accordance with GDPR. Moreover, given the powerful role of AI providers, it will be risky to collaborate with subjects that develop one or more parts of their business outside the European Union, since they may not be subject to equivalent legislation and they may transfer personal data outside the European Union not always in accordance with art. 44 ff. of the GDPR.

In this context, it may often happen that public entities are **not able to transparently inform citizens** about which data they collect and how they are processed.

Another issue is of greater importance for smart cities and refers to the tracking of spatial mobility, e.g., in relation to pedestrians, consumers and vehicles. Tracking is already a legitimate part of smart city technologies, as per ensuring safety in the public space, but **with AI technologies there is a higher fear of misuse**, e.g., related to unwanted (non-targeted) surveillance or to attacks such as backdoor injections, data poisoning and model thefts.

Solutions presented

This section focuses on summarizing findings, experiences, good practices and solutions coming from the pilot exercises organised during the Projects' implementation in the cities addressed by their activities. The solutions presented highlight how a strict collaboration among public authorities, lawyers and technology developers and attention to the feelings and impressions of citizens can actually increase the users' acceptance of technological tools and their potential adoption.

Hereinafter we will report some aspects that smart cities involved in the Projects had to take into consideration for the pilot tests, but we will provide also hints on the recommended approach for a stable adoption of technologies and tools that involve processing of personal data.

I. Define the context of use of the tools

- Who will be responsible for the use of the tools within the public entity? Who will be concretely involved in their use and to what extent? Will data be shared with external parties?
- Precisely define the intended use of the tools, its aim and duration.

Good practice → Time limits on storing information: Information that is collected should be stored for limited times and then discarded responsibly.

- Which data will we collect about data subjects?

Good practice → Collect less rather than more: collect the least amount of data possible to carry out safety services in a responsible manner (principle of data minimisation).

- Identify on which data subjects the use of the tools may have an impact (typically, individuals to whom the data refer).

II. Identify the applicable laws

- According to the nature of the entity and/or the activities planned, with which provisions of law do we have to be compliant?
- Does the planned use of the tools have any ethical or legal implications?
- What are the obligations towards the data subjects to minimise risk?

In this regard, it would be useful to mention the legislations that will be binding on each public entity adopting surveillance technologies within the European Union.

The **GDPR** is a globally known and respected legislation offering high levels of protection regarding collecting and processing personal data. The Regulation is directly applicable in all Member States and offers a unified approach to protecting personal data in the European Union and of European citizens in general (territorial scope extended beyond the EU Member States).

Directive (EU) 2016/680 ("**LED**") of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

- Adopted in the same package as the GDPR and effective from May 2018.
- Because the GDPR excludes its application in law enforcement bodies' criminal investigations and operations safeguarding against and preventing threats to public security, it became

necessary to separately regulate the protection of personal data being processed in such circumstances.

- LED applies to any processing for law enforcement purposes, carried out by a public or private body that fits the definition of "competent authority".

III. Choose adequate security measures to prevent violations of rights

- Designate a DPO and seek her/his advice;
- define access control policy and secure authentication methods;
- plan to train your personnel on human-rights-compliant practices and procedures for capturing, storing, accessing, managing and deleting information they obtain within the use of the new tools;
- bind your personnel with confidentiality duties;
- adopt robust information security practices and procedures that are in line with the highest industry standards and develop human-rights-compliant responses in the eventuality that the systems are breached and sensitive information is accessed by malicious actors;
- apply pseudonymisation /anonymisation when possible/needed;
- implement data minimisation by storing only the datasets that are deemed necessary and by ensuring that the personal data included in these datasets are adequate and relevant and not excessive;
- establish an adequate retention period;
- get information from the tool provider on the types and kinds of information they collect, as well as how long they have such information saved on their systems and if there are possibilities to opt out of the data collection;
- ask users of the tool to share information about detected vulnerabilities. While there are some valid reasons to delay public notification of the discovery of vulnerabilities, it is important that they are reported as soon as possible in order to notify affected customers and users of the compromise of their data and to minimize human rights risks, as well as to inform others who may be affected by the same vulnerability so that they can take measures to safeguard their systems. ENISA published a good practice guide on vulnerability disclosure on 18 January 2016;
- create documented policies to govern how the tools should be operated. These policies should include who is qualified to operate them, what training is required for operators, how to measure the performance of the tools and what should be expected from them;
- specify the circumstances in which it might be necessary for the operator to override the outcomes of the tools.

IV. Grant an effective oversight

The entity which adopts the tool should develop good practices which need to be followed in addition to law provisions.

The more the adopted tools represent technological innovations and imply the use of advanced algorithms, the more the entity should develop mechanisms for effective oversight and remedial processes in the event of rights injuries and violations. Bind the tool provider with contractual provisions in order to ensure its collaboration.

V. Clearly identify the data processing operations

Describe the personal data processing operations:

- Establish the software or database to be used;

- Describe the data flows;
- Identify the data subjects;
- Identify the types of personal data;
- Define the storage location;
- Define the retention period.

VI. Sign data processing agreements (Art.28(3) GDPR) or joint controllers' agreements (Art.26 GDPR)

The roles of the "controller", "joint controllers", "processor" must be identified based on the relevant definitions stipulated in the GDPR. Following the identification, specific agreements must be in place where the rights and obligations of the parties will be defined.

Good practice → Create a model of data processing agreement based on the Standard Contractual Clauses for controllers and processors in the EU/EEA, to fulfil the requirements of Article 28(3) and (4) GDPR, approved by the European Commission on 4th June 2021.

VII. Carry out a Data Protection Impact Assessment (DPIA) related to the specific context of use of the tools

According to Article 35 GDPR and Article 27 LED, where a type of processing using new technologies, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

For the DPIA, the Data controller (municipality/LEA) will be asked to exactly define the use case scenario and to describe the activities which involve the processing of personal data.

After that, the controller will start drafting the DPIA. The controller shall seek the advice of the DPO, where designated, when carrying out a data protection impact assessment.

In accordance with the verified level of risks, the controller will be able to identify the technological and organisational measures which are necessary and sufficient to reduce the risks to an acceptable level.

Additional security measures may be required from AI-enabled tools providers.

The DPIA is a living document that must be reviewed on an ongoing basis and updated based on any changes related to the scope, nature, context or purposes of the processing in question.

VIII. Verify if in accordance with European or national legislation a notification to national data protection authorities or other authorities is required

IX. Inform the involved data subjects

Inform the involved data subjects, in the most suitable and understandable way, about the planned activities and the related processing of their personal data.

Put physical signs in the public spaces where the AI-enabled tool is used to inform the data subjects about the processing by also referring to the official website of the Data controller.

Make the information of Article 14 GDPR publicly available on the Data controller's official website in the mother language of the data subjects and in the English language in order to enable the data subjects to exercise their rights.

Recommendations

Consider the specific context and already existing technologies and infrastructure

It is important to emphasise that there is a huge diversity of smart applications available in the market. In addition, public entities may have different networks, technological systems and other infrastructures in place. Last but not least, the importance of privacy and its relevance in comparison with other values, such as safety, may vary a lot in different sociocultural contexts.

When applying privacy-preserving technologies and procedures, it is not sufficient to consider every single process or tool. Instead, we advise that the **interactions between different tools and processes** have to be considered to design "joint privacy security measures".

It is also crucial to consider the architectural patterns that define the system's components, responsibilities, and the relationships between them.

Both joint privacy mechanisms and privacy architectures aim to integrate isolated privacy protection mechanisms into more general solutions. In smart cities, this integration could be complicated not only by a large number of subsystems but also by a large number of stakeholders. To implement joint privacy mechanisms in a coherent privacy architecture, **various stakeholders should collaborate** on an operational level. However, this collaboration can entail **privacy risks** because it may enable stakeholders to share large amounts of data and also to combine data from several sources, allowing the inference of non-requested data.

Adapt privacy-preserving measures to the level of risk

In the Projects, we have implemented a number of approaches to preserve the integrity of user data, e.g., **data encryption, data suppression, pseudonymization and anonymisation**, but we have also suggested some **complementary measures** that may be useful for a stable adoption of the tools.

For example, for tools performing big data analytics, it is important to consider which data they process. If they will be connected to datasets containing personal data and sensitive information, the access control module should be adapted in order to perform security and privacy-aware transformations, ranging from pruning and reshaping to encrypting, decrypting or anonymizing the full resource or part of it, before giving access to data.

It looks also relevant to choose adequate means to transfer the data. For instance, in the Projects we used Kafka bus, which allows the encryption of data.

Protect workers who will concretely use the tools

We have noticed that data anonymisation has an impact not only on citizens but also on people who work for municipalities and law enforcement agencies. Generic usernames and IP address anonymisation may prevent the adoption of instruments that monitor workers in breach of labour law provisions.

For a compliant use of tools which allow workers' monitoring through algorithms, critical issues may arise especially if such technologies imply and/or are connected to an **automated decision-making instrument**.

But even if there is not an automated decision-making process, constant monitoring of workers could nevertheless threaten their physical safety and well-being, thus presenting **ethical challenges and potential law violations**. It is therefore recommended to adopt internal policies to clearly inform the workers about the functioning of the tool and the intended aims for its use. It should also be clarified

which parameters are used to evaluate the "workload" of workers and which are the possible consequences of the detection of an anomaly.

Consider specific security measures and procedures for OSINT

An important category of AI-enabled tools is represented by OSINT tools and platforms. Most of them collect and process data from social networks and other similar online sources and they are based on algorithms for natural language processing (NLP).

It is really important that any public entity adopting the tool would conduct an **audit on the used datasets**, to verify the potential presence of bias and their quality. Moreover, public entities should **implement internal policies** to define the aims for which the tool can be used and the allowed criteria to set a new "project" with the tool.

Lastly, it is necessary that **the end users will be specifically trained** to grant fairness and non-discrimination in the interpretation of the analysis and insights extracted by OSINT tools.

Public entities should also **document their choice about anonymising/pseudonymising, or not,** the data collected and the reasons for that. The volume, nature and range of analysed personal data contribute to defining the level of impact on human rights. If someone may have access to deanonymised data, this has to be done in compliance with all applicable laws and would probably be legitimate only if the goal is to conduct a specific investigation or to prevent serious crimes. Indeed, there is a high risk of collecting information about plenty of people and that only a small percentage of them would actually be useful.

3. Artificial Intelligence

Public spaces constitute soft targets, i.e., they are vulnerable to terrorist attacks or other criminal offences. The protection of public spaces is primarily a responsibility of each Member State and is supported by the European Union through dedicated action plans and guidelines aiming at the anticipation, prevention, protection and effective response to terrorist attacks.

AI systems (including ML) can help substantially and significantly in the fight against crime and terrorism. The word "help" is of high importance, given that the human factor must not be ignored. Humans must be the final decision makers. The purpose of AI is to **aid** its users and **enhance their intelligence** during the execution of their tasks and **not to mandate them or replace them**.

AI systems require special attention from their creation during the design phase until their use during the deployment phase by constantly taking into consideration their impact on both end users and the general public. Ethical and legal requirements must be defined and validated following an **ethics- and privacy-by-design approach** that can be achieved through the close collaboration between technology developers, end users and ethics and legal experts. According to Article 2(7) of the AI Act proposal, the proposed Regulation shall not apply to any research and development activity regarding AI systems. Nevertheless, for trust to be built towards the citizens, AI systems have to be **trustworthy**, meaning that they have to function in conformity with fundamental human rights.

To this end, the High-Level Expert Group on AI issued the **Ethics Guidelines for Trustworthy Artificial Intelligence** with the key requirements for trustworthy AI being the following:

- **Human agency and oversight:** AI systems should not autonomously make decisions about issues that are normally decided by humans by means of free personal choices or collective

deliberations or similarly significantly affects individuals. AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches. End-users and others affected by AI systems should not be subordinated, coerced, deceived, manipulated, objectified or dehumanised, nor attached or addicted to the system and its operations. The final decision must be taken by the user of the AI system.

- **Technical robustness and safety:** AI systems need to be resilient and secure. They need to be safe, ensuring a fall-back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimised and prevented.
- **Privacy and data governance:** Full respect for privacy and data protection must be ensured, i.e., AI systems must process data in line with the requirements for lawfulness, fairness and transparency set in the national and EU data protection legal framework and the reasonable expectations of the data subjects. Furthermore, personal data must be processed for a specific purpose in accordance with the purpose limitation principle and for a specific period of time that is needed to achieve the defined purpose in accordance with the storage limitation principle. Technical and organisational measures and security measures must be implemented. In addition, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data. The EDPB has already announced that it will develop guidelines on the interplay between the proposed AI Act and the GDPR.
- **Transparency:** The data, system and AI business models should be transparent, i.e., the purpose, capabilities, limitations, benefits and risks of the system and of the decisions conveyed should be openly communicated to and understood by end-users and other stakeholders along with their possible consequences. Traceability mechanisms (from initial design to post-deployment evaluation and audit) can help achieve this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system and must be informed of the system's capabilities and limitations. They should also be able to audit, query, dispute, seek to change or object to AI or robotics activities (human intervention). Keeping records of the decisions made and on which reasons they were based is critical.
- **Diversity, non-discrimination and fairness:** Unfair bias must be avoided, as it could have multiple negative implications, from the marginalisation of vulnerable groups to the exacerbation of prejudice and discrimination. AI systems must be designed to avoid algorithmic bias, in input data, modelling and algorithm design as well as to avoid potential negative discrimination against people on the basis of any of the following grounds: sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation as well as to avoid historical and selection bias in data collection, representation and measurement bias in algorithmic training, aggregation and evaluation bias in modelling and automation bias in deployment. Processes should be in place to address and rectify potential discrimination (bias). Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life cycle.
- **Societal and environmental well-being:** AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. AI systems should be mindful of principles of environmental sustainability, both regarding the system itself and the supply chain to which it connects and not have the potential to negatively impact the quality of communication, social interaction, information, democratic processes, and social relations. Moreover, they should take into account the

environment, including other living beings, and their social and societal impact should be carefully considered.

- **Accountability:** Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. **Auditability**, which enables the assessment of algorithms, data and design processes, plays a key role therein, especially in critical applications. Moreover, adequate and accessible redress should be ensured. In this way, public entities may assess the security level **against artificial intelligence-based reconstruction attempts or similar real-time attacks**. They may also ascertain **if biases are present in the datasets** and their quality, in order to understand their impact on the outcomes.

Following various reports on the matter where it has been expressed the necessity for a **harmonised regulatory framework on AI in the European Union**, the **proposal** for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) was issued on 21 April 2021. The Commission's objectives for the proposed Artificial Intelligence Act are to ensure that AI systems used in the EU are safe and respect existing law on fundamental rights and EU values, ensure legal certainty to facilitate investment and innovation in AI, enhance governance and enforcement of the law on fundamental rights and applicable safety requirements and facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

Annex III of the latest version of the AIA Proposal makes an explicit reference to the **high-risk AI systems** of Article 6(3) and provides clarifications per category.

Since actions by LEAs are characterised by a significant degree of power imbalance that may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights, **AI systems used by LEAs or on their behalf** are classified as high-risk AI systems and in particular:

- AI systems intended to be used by law enforcement authorities or on their behalf to assess the risk of a natural person for offending or reoffending or the risk for a natural person to become a potential victim of criminal offences;
- AI systems intended to be used by law enforcement authorities or on their behalf as polygraphs and similar tools or to detect the emotional state of a natural person;
- AI systems intended to be used by law enforcement authorities or on their behalf to evaluate the reliability of evidence in the course of investigation or prosecution of criminal offences;
- AI systems intended to be used by law enforcement authorities or on their behalf to predict the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;
- AI systems intended to be used by law enforcement authorities or on their behalf to profile natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences.

In addition, **remote biometric identification systems** (such as facial recognition technologies) are classified as high-risk AI systems. Each public entity should therefore carefully analyse the regulatory context before deciding to combine AI-enabled tools for image analysis with facial recognition systems.

As part of IMPETUS, no biometric identification technologies/tools were developed. As part of S4AllCities, the Facial Recognition and Authentication and Gesture-Based Interaction module is designed to be used by authorised personnel to ensure secure access to a restricted area, hence, it does not fall under the notion of "remote biometric identification system". Nevertheless, it should be

pointed out that when the capabilities or the intended purpose of the system change, that AI system should be considered a new AI system which should undergo a new conformity assessment.

High-risk AI systems will be subject to **strict obligations before they can be put on the market or otherwise put into service**. Such obligations include:

- the conducting of a conformity assessment,
- the establishment of a risk management system,
- appropriate testing procedures,
- high quality of the datasets feeding the system to mitigate risks and discriminatory outcomes,
- activity logging to ensure traceability of results,
- technical documentation, record-keeping ('logs'),
- transparency and provision of clear and adequate information to the user,
- appropriate human oversight,
- high level of robustness, security and accuracy.

Certain users of high-risk AI systems that are public authorities, agencies or bodies will be obliged to **register in the EU database for high-risk AI systems** listed in Annex III of the proposal.

Users of an **emotion recognition system** will be obliged to **inform natural persons** when they are being exposed to such a system. This obligation shall not apply to AI systems used for emotion recognition which are permitted by law to detect, prevent and investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties.

New provisions have been added to the AIA Proposal about situations where AI systems can be used for many different purposes (general-purpose AI), and where general-purpose AI technology is subsequently integrated into another high-risk system. Certain requirements for high-risk AI systems would also apply to general-purpose AI systems in such cases. However, instead of direct application of these requirements, an implementing act would specify how they should be applied in relation to general-purpose AI systems.

It is highly recommended that, since the AI Act has not been issued until today, both AI system developers and end users **consult ethics and legal experts and monitor the legislative developments** in order to be informed about any further updates and, most importantly, about their obligations.

4. Societal Impact

The societal impact encompasses all the effects that interventions, projects, products, services, activities or policies have on individuals and/or communities, and covers various fields such as culture, political systems, health, environment, and personal and property rights. It is a complex concept that affects people's way of life and involves different levels, ways, and fields.

There are three main approaches that can be used to assess non-technical aspects of security innovation: Privacy Impact Assessment (PIA), Constructive Technology Assessment (CTA), and Societal Impact Assessment (SIA). PIA assesses the impact of projects/technologies on privacy and involves stakeholders in remedial actions. CTA involves a reflexive dialogue between developers and end-users/stakeholders during the development of new technologies. SIA involves participatory techniques to evaluate the social consequences of projects and any social changes caused by them. The purpose of SIA is to identify negative impacts, predict and mitigate them, and enhance benefits.

Our proposed SIA approach is not a standardized methodology, but it was successfully used in S4AllCIties. At a high level, we used the complex problem-solving approach as the basis to address the societal impact. Anticipating, focusing on essentials, dividing into parts, getting feedback from people involved or likely affected and the use of several scientific-based methods were our guiding principles (Table 1).

Guiding principle	**Description**
From the beginning	Planning from the early stages (e.g., during the proposal phase) to address concerns and requirements about the societal impacts of the funding organization while trying to find answers to key questions like: how would the project change the urban security environment and its agents? or how would citizens react to the proposed security technologies?
Effort on essentials	Focusing on the essentials to achieve a satisfactory and straightforward analysis. In the case of security innovation projects, this means paying attention to the current and possible state of stakeholders (end-users and population) regarding being protected from danger or harm without negative changes on perceptions, behaviours, rights, interactions, environments, etc.
Divide and conquer	Splitting the problem into parts (e.g., topics, subjects) and dealing with these parts (that can be broken down further into sub-parts) before connecting them to take a whole picture of the societal consequences of the project. The parts and sub-parts would be as mutually exclusive as possible ensuring that they do not interfere with each other (interference leads to complexity). In other words, the more mutually exclusive the parts and subparts the more effectively they can be addressed.
Feedback & feedforward	Getting information (opinions, perceptions, reactions) about how the future situation would be (what is likely to change and how?). This entails identifying the target groups and engaging them through cooperation in different phases of the project. In our case, this was done by collecting responses from project team members and end-users regarding the impacts of the project and responses from citizens regarding the implementation of the proposed security technologies.
Multimethod approach	Applying different scientific-based methods (qualitative and quantitative) and participatory research during the course of the project (e.g. anticipatory and scenario-based approaches).

Table 1. Guiding principles for the analysis of social aspects in security projects/interventions.

In the following we illustrate the strategy used to analyse and measure the societal impacts of the S4AllCities project. The proposed strategy focuses on three key research questions: Q1.- What are the likely societal impacts of the project? Q2.- Do the public accept the proposed technology? Q3.- Is gender relevant in the project context?

Q1.- What are the likely societal impacts of the project? Answering this question required assessing in advance the consequences likely to follow from project developments. This involved an anticipatory strategy to gain a better understanding of the effects the project may produce in short, medium, and long terms. From the proposal phase we focused on addressing this and we faced three challenges:

- Challenge 1: The abstract nature and variety of societal impacts because “societal” includes anything that affects people (e.g., security, culture, economy, education, health, working conditions, quality of life, environment, etc.). This makes difficult the categorization and the selection of societal aspects.
- Challenge 2: Relaying on self-judgments, own experience or expertise to identify potential impacts may yield subjective bias while keeping project team members away from the analysis, discussion and reflection on societal effects generated by their activities.
- Challenge 3: The inherent uncertainty when attempting to track the future effects of technologies and solutions that have not been implemented as an integrated system yet. Cause-effect relationships do not always occur in a linear and predictable way also leading to unplanned or unintended effects on society.

We addressed Challenge 1 conceptually as follows. The project is likely to influence/change the urban security ecosystem in which actors/agents behave and interact with each other and with the cyber-physical environment (Figure 1).

The urban security ecosystem refers to the community of interrelating agents and their cyber-physical environment. Agents represent individuals or communities (Attackers, Defenders, Citizens and Researchers) who behave and interact with other agents and the environment playing different roles within the urban security ecosystem. Whereas we needed to consider as many societal aspects as possible, the defined dimensions were broken down from the high level of abstraction into more operational elements (agents/domains/impact category). In total, we defined 55 candidate societal impact categories of the project. These likely impact categories were used as starting point for further analysis (i.e., items/statements for the further survey research).

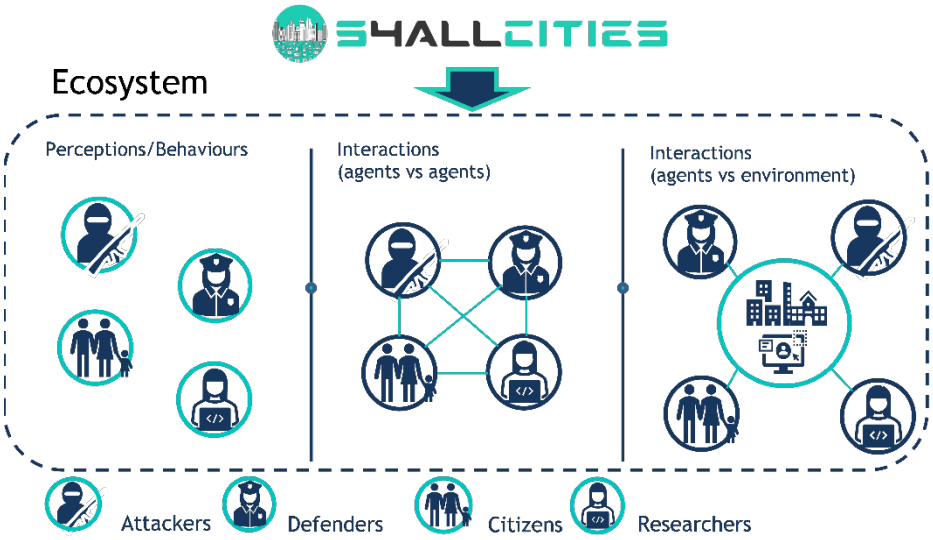

Fig. 1. Concept to define the likely impacts of a security project/intervention on the urban security ecosystem.

Challenges 2 and 3 were minimised by conducting a three-round assessment using consensus and forecasting techniques with the participation of the project team members and end-users:

- Round 1: Delphi method (pre-test questionnaire, teleconference, 1st questionnaire, workshop and 2nd questionnaire) conducted at the beginning of the project to anticipate the likely societal impacts and to encourage project partners to think about and discuss societal effects.
- Round 2: A survey with end-users after having contact with the proposed technologies to identify the possible impacts from the stakeholder's perspective.
- Round 3: A survey with project partners (once technology has been tested) to identify the unintended impacts (e.g., unforeseen, undesirable and/or adverse side-effects) of the project and to promote reflection on potential negative consequences of surveillance security technologies in general and the project in particular.

The three round assessment was proved to be a suitable participatory and transparent approach since the consensus among a group has more power than individual judgements. It is particularly useful when the goal is to improve the understanding of problems, opportunities or solutions, or to develop forecasts. This practice is recommended and can be extended to similar security projects.

Q2.- Does the public accept the proposed technology? The EU prioritizes protecting its citizens from terrorism, and technology plays a crucial role in achieving this goal. However, relying solely on technology cannot guarantee people's safety. The approach to counterterrorism has shifted from reactive measures to proactive operations that involve using surveillance-focused security technologies to neutralize potential threats before they materialize. This requires monitoring ordinary citizens which can lead to public opposition. To address this challenge, public participation in technology assessment is necessary. The EU has a well-established policy for engaging the public in science and technology innovation, which can inform policymaking and provide a better understanding of societal concerns, desires, and needs. The main concern is that citizens are the potential beneficiaries of security technology, and their acceptance is critical for successful implementation. Therefore, seeking public input in advance can help prevent rejection of innovations and provide a societal "license to operate" for security technologies and solutions.

We conducted a large-scale survey study in the form of an online questionnaire to investigate the factors associated with the public acceptance of surveillance technologies, with particular attention to the acceptability of the technologies proposed in the S4AllCities project. The aim was to understand citizens' perceptions, attitudes, and opinions towards these technologies, which could help identify constraints and opportunities for security innovation projects. The datasets produced not only have scientific value but also have the potential to inform researchers, end-users, and policymakers in the development of security policies, training programs, and communication campaigns, thereby improving terrorist security in urban public spaces.

Table 2 displays the successful factors and the constraints of the survey research conducted within the S4AllCities project.

Success factors	**Constraints**
• The pilot questionnaire allowed the possibility to detect incompatible issues and the appropriateness of questions and to know whether a designed survey fulfils the purpose of the study before the actual large-scale survey.	• The pilot questionnaire used a reduced number of people (n=41). • The aspects covered by the questionnaire were general and/or unfamiliar to the respondents. This is likely to generate ambiguity and or

• Hiring a survey company ensured the highest response rate, appropriate sampling (e.g., > 1.000 responses) and getting massive amount of information in a short period of time. • The use of the online questionnaire gave the best sense of anonymity and privacy which maximizes comfort for those answering. • Data collected could be analysed statistically. For instance, the use of statistical inference allowed going one step beyond a simple description of data and therefore drawing more consistent conclusions. • The summary of the project included in the questionnaire enabled dissemination to a high number of citizens. • Translations of the questionnaire into several languages allowed scalability (i.e., the possibility to reach responses from several countries) while enabling the involvement of several partners during the translation process, also those not directly related to the study. • The produced datasets can be extrapolated to other related analyses (e.g., compare and contrast other research studies, define new ideas and projects, etc.).	misunderstanding (differences in interpretation of the questions). • Survey taking fatigue. The survey had 40 items so it might be perceived as too long and/or including questions irrelevant to the respondents. • Translation of the questionnaire into several languages was time consuming and required the commitment of many people. • Hiring a survey company had a monetary cost. • Respondents belonged to databases of the survey company and were given a monetary incentive for their participation. In such cases dishonesty, indifference and lack of motivation can be important issues. • The survey was unsuitable for individuals with a visual or hearing impairment, or other impediments such as illiteracy.

Table 2. Lessons learnt from the survey research on EU citizens.

Q3.- Is gender relevant in the context of this project? Gender Dimension (GD) is an important aspect in security that involves integrating gender into research and innovation processes by analysing gender needs, attitudes, and behaviors to enhance knowledge and technologies. Several references formulate general rules/questions of this subject matter while providing some examples/case studies in a variety of scientific disciplines (e.g. European Institute for Gender Equality: https://eige.europa.eu/thesaurus/terms/1207, Gendered Innovations of the Stanford University: https://genderedinnovations.stanford.edu/). GD means questioning stereotypes and considering gender-sensitive aspects in projects, ranging from gender-dedicated projects to projects that may include inclusive language or visual representation. The S4AllCities project included a gender analysis to explore the role of gender in the urban security ecosystem, even though it is not a gender-dedicated project.

In summary, the presented results showed that gender is an important predictor for the public acceptance of counterterrorist technologies. Together these results provide important insights into

the importance of gender in counterterrorism and public acceptance of new security technologies and warrant further analysis. Table 3 displays the pros and cons of this analysis.

Success factors	Constraints
• The pilot questionnaire allowed the possibility to identify potential gender discrepancies among EU citizens. • The focus group enabled the project team members to rethink about research priorities, to discuss the project from a gendered perspective and reach a consensus about the actions. • Results provide new evidence to integrate gender in security projects/interventions involving technology. For instance: o whether gender may impact on constraints and opportunities for security innovation. o whether the integration of technologies need to be tailored to women/men or can be improved by gender diversity.	• The pilot questionnaire used a reduced number of people (n=41). • The hypothesis of gender differences in technology acceptance was rather intuitive and not supported by previous studies. The risk to get null findings was very high. • It was not possible to include other genders (e.g., non-binary) in the analyses.

Table 3. Lessons learnt from the survey research on gender differences.

Conclusions

Societal impacts of security projects or interventions (i.e., perceptions and attitudes of stakeholders and possible effects of technological solutions on society) need to be tackled systematically. However, the societal effects can be complex and can happen at various levels. This entails several facets likely to be analysed in different ways.

The intention of this section was to assist in determining what can be done to address the societal impacts within security innovation actions. Complex problem-solving guiding principles were proposed as the global strategy and good practice examples have been presented when analysing societal questions within the Projects. The concluding remarks are the following:

- Societal Impact Assessment needs to be integrated effectively into wider assessments and decision-making processes of security projects/interventions.
- Conducting Societal Impact Assessment requires a variety of scientific based methods being quantitative and/or qualitative based on the essential issues under consideration.
- Dealing with the social aspects of project implementation requires the active participation of the partners, end users and stakeholders (e.g., citizens). This process should start as early as possible.

5. References

AccessNow. One Year Under the EU GDPR, An Implementation Progress Report: State of play, analysis, and recommendations. AccessNow.org, 2019

Artificial Intelligence Committee, AI in the UK: ready, willing and able? Report of Session 2017-19 - published 16 April 2017 - HL Paper 100

Asilomar AI Principles (2017). Principles developed in conjunction with the 2017 Asilomar conference

Association for Computing Machinery (2018). ACM Code of Ethics and Professional Conduct: Affirming our obligation to use our skills to benefit society

Cobbe, J., Singh, J. (2021). Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges. Computer Law & Security Rev., 42

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A.C., Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rightsbased Approaches to Principles for AI. Berkman Klein Center for Internet & Society at Harvard University. Research Publication No. 2020-1

Boehm, F. (2012). Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level. Berlin: Springer-Verlag

Brundage, M. and others (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation. Future of Humanity InstituteUniversity of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI.

Bundesministerium des Innern, für Bau und Heimat, Bundesministerium der Justiz und für Verbraucherschutz (2018). The Federal Governments key questions to the Data Ethics Commission. 5 June 2018

Cate, F.H., Dempsey, J.X. (eds.) (2017). Bulk Collection: Systematic Government Access to Private-Sector Data. Oxford: Oxford University Press

Clever, S., Crago, T., Polka, A., Al-Jaroodi, J., Mohamed, N. (2018). Ethical Analyses of Smart City Applications. Urban Sci. 2018, 2, 96

Coastal Urban Development through the Lenses of Resiliency (CUTLER) (2018). This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 770469

Coeckelbergh, M. (2020). AI Ethics. Cambridge: The MIT Press.

Corea, F. (2019). An Introduction to Data: Everything You Need to Know about AI, Big Data and Data Sciences. Cham: Springer Nature.

Van Eck, G.J.R. (2018). Emergency calls with a photo attached: The effects of urging citizens to use their smartphones for surveillance. In:

Newell, B.C., Timan, T., Koops, B.-J. (eds) (2018) Surveillance, Privacy and Public Space. Routledge Publishing, 2018

Empowering privacy and security in Non-Trusted Environments (WITDOM) (2017). This project has received funding from the European Union's Horizon 2020 research and innovation programme (H2020-ICT-2014-1) under grant agreement No. 64437.

Ethics Advisory Group 2018 Report, Towards a digital ethics, available at: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf (12th January 2021)

Evas, Tatjana. European framework on ethical aspects of artificial intelligence, robotics and related technologies: European added value assessment. European Parliament: European Parliamentary Research Service, PE 654.179, 2020

Feldstein, S. (2019). The Global Expansion of AI Surveillance. Washington: Carnegie Endowment for International Peace

Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York: New York University Press.

Floridi, L. et al., AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines (2018) 28:689–707.

Harmonized Evaluation, Certification and Testing of Security products (HECTOS). Project funded by the European Community's Seventh Framework ProgrammeFP7/2007-2013 under Grant Agreement No 606861, 2015

Institute of Electrical and Electronics Engineers (IEEE) (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. First Edition.

Leslie, D. (2019). Understanding artificial intelligence ethics safety: A guide for the responsible design and implementation systems in the public sector. The Alan Turing Institute.

Lorenz, P. (2020). AI Governance through Political Fora and Standards Developing Organizations: Mapping the actors relevant to AI governance. Berlin: Stiftung Neue Verantwortung

Menzer, S., Rubba, C., Meißner, P., Nyhuis, D. (2015). Automated Data Collection with R: A Practical Guide to Web Scraping and Text Mining. West Sussex: John Wiley & Sons, Ltd

Milaj, J., van Eck, G.J.R. (2019). Capturing license plates: police-citizen interaction apps from an EU data protection perspective. International Review of Law, Computers and Technology, 25 March 2019

OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449

OECD (2020). The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector, available at: http://www.oecd.org/finance/Impact-Big-Data-AI-in-the-Insurance-Sector.htm

Office of Homeland Security & Emergency Preparedness, City of New Orleans, available at: https://www.nola.gov/homeland-security/real-timecrime-center/ (12th January 2021)

Purtova, N. (2018). Between GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private PartnershipsInternational Data Privacy Law (2018)

Safe Data-Enabled Economic Development Horizon 2020 research and innovation programme (Safe-DEED), Grant Agreement No. 825225 Shaping the ethical dimensions of smart information systems

(SIS) – a European perspective (SHERPA) (2018). This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme Under Grant Agreement no. 786641

von Silva, B., Larsen, T. (2011). Setting the Watch: Privacy and the Ethics of CCTV Surveillance. Portland: Hart Publishing.

Timmermans, H. (ed.) (2009). Pedestrian Behavior: Models, Data Collection and Applications. Bingley: Emerald Group Publishing Limited

Vogiatzaki, M., Zerefos, S., Tania, M.H. (2020). Enhancing City Sustainability through Smart Technologies: A Framework for Automatic Pre-Emptive Action to Promote Safety and Security Using Lighting and ICT-Based Surveillance. Sustainability 2020, 12, 6142.

Voigt, Paul, von dem Bussche, Axel. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer. Cham: International Publishing, 2017

Young, M., Katell, M., Krafft, P.M. (2019). Municipal surveillance regulation and algorithmic accountability. Big Data & Society, July-December 2019: 1-14.

Zwitter, A. (2014). Big Data Ethics. Big Data & Society. July-December 2014; 1-6

On societal impact assessment:

F. Vanclay (2003), "International Principles For Social Impact Assessment", Impact Assessment and Project Appraisal, vol. 21, pp. 5-12.

F. Vanclay, A.M. Esteves, I. Aucamp and D. Franks (2015), Social Impact Assessment: Guidance for assessing and managing the social impacts of projects, Fargo ND: International Association for Impact Assessment. https://research.rug.nl/en/publications/social-impact-assessment-guidance-for-assessing-and-managing-the-, Last visited on 20-07-2021

D. Wright and C.D. Raab (2012), "Constructing a surveillance impact assessment". Computer Law and Security Review. Vols. 28, pp. 613-626.

D. Wright and K. Wadhwa (2013), "Introducing a privacy impact assessment policy in the EU member states". International Data Privacy Law. Vols. 3, pp.13-28.

J. Schot and A. Rip (1997), "The Past and Future of Constructive Technology Assessment", Technological Forecasting and Social Change 54: 251-268

A. Rip and H. Te Kulve (2008), "Constructive Technology Assessment and Socio-Technical Scenarios". Chapter 4 in E. Fisher et al. (eds.), The Yearbook of Nanotechnology in Society, Vol. 1.

A. Rip and D.K.R. Robinson (2013), "Constructive Technology Assessment and the Methodology of Insertion". In: Doorn N., Schuurbiers D., van de Poel I., Gorman M. (eds) Early engagement and new technologies: Opening up the laboratory. Philosophy of Engineering and Technology, vol 16. Springer, Dordrecht.

K.L.F. Douma et al. (2007), "Methodology of constructive technology assessment in health care". International Journal of Technology Assessment in Health Care 23(2), pp. 162-168.

R. Kreissi, F. Fritz and L. Ostermeier (2015), "Societal Impact Assessment", International Encyclopedia of the Social & Behavioral Sciences, 2nd edition, Volume 22. http://dx.doi.org/10.1016/B978-0-08-097086-8.10561-6.

L. Bornman (2013), “What Is Societal Impact of Research and How Can It Be Assessed? A Literature Survey”, Journal of the American Society for Information Science and Technology, 64(2), pp. 217–233.

R. Kreissl and M. Mueth (2014), A Case Study in applying Societal Impact Assessment in Public Transport Security. ASSERT Project Online. http://assert-project.eu/wp-content/uploads/2013/04/ASSERT_D_Test-Case-Public-Transport_HC_14-04-09.pdf Last visited on 22-04-2021.

S.A. Takyi (2014), “Review of Social Impact Assessment (SIA): Approach, Importance, Challenges and Policy Implications”, International Journal of Arts & Sciences, 07(05), pp. 217–234.

B. Schmitt. et al. (2004), “Research for a Secure Europe”, Luxembourg: Office for Official Publications of the European Communities p. 12.

V. Pavone, S. Degli-Esposti and E. Santiago (2015). D 2.4 – Key factors affecting public acceptance and acceptability of SOSTs. SurPRISE Project (European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492).

T.R. Korsvik and L. M. Rustad (2018), What is the gender dimension in research?. Case studies in interdisciplinary research. Kilden genderresearch.no. Research Council of Norway.

C. Tannenbaum, R.P. Ellis, F. Eyssel, J. Zou and L. Schiebinger (2019), “Sex and gender analysis improves science and engineering”, Nature 575, pp.137–146.

M. W. Nielsen, C. W., Bloch and L. Schiebinger (2018), “Making gender diversity work for scientific discovery and innovation”, Nature Human Behaviour 2, pp.726-734.

K. Woodward and S. Woodward (2015), “Gender studies and interdisciplinarity”, Palgrave Commun 1, 15018. 2015. doi:10.1057/palcomms.2015.18.