SYnergy of integrated Sensors and Technologies for urban sEcured environMent

D10.1
Baseline Report on Legal aspects of the SYSTEM project

25 June 2019 **V3.0**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787128

Project title	SYnergy of integrated Sensors and Technologies for urban sEcured environment
Project acronym	SYSTEM
Project number	787128
Start date of the project	1st September, 2018
Duration	36 months
Topic	SEC-10-FCT-2017. Integration of detection capabilities and data fusion with utility providers' network

Deliverable number	D10.1
Deliverable title	BASELINE REPORT ON LEGAL ASPECTS OF THE SYSTEM PROJECT
Leading partner	VUB
Partners contributing	//
WP of reference	WP10
Title of the WP of reference	LEGAL AND ETHICS MANAGEMENT
Task of reference	T10.1
Title of the task of reference	BASELINE KNOWLEDGE AND COMPLIANCE WITH ETHICAL, REGULATORY AND SOCIAL ACCEPTANCE CONDITION AND AREAS OF CONCERN FOR SYSTEM
Deliverable type	Report
Dissemination level	PUBLIC
Due date	M10 – June 2019. Foreseen in the DoA at M6 – February 2019. Extended by Ms. Oczko-Dolny (DG HOME) with the email sent to Ms. Cavallini (FORMIT) on 12 February 2019. Request of extension after the Project Management Board Meeting and the Executive Board held on 11-12 June in Bratislava (Slovakia). The request was done by email on 11 June 2019 by Ms. Cavallini (FORMIT) to Ms. Longo (REA).

Keywords	Ethics; Social Acceptance; Baseline; Regulatory; Privacy; Data Protection; Surveillance.
Abstract	This deliverable, Baseline Report on Legal aspects (D10.1), describes the European and national privacy, personal data protection and criminal law legal frameworks, which are relevant to the SYSTEM project and to SYSTEM technology. The aim of this document is to provide the relevant legal references to anticipate the legal challenges that SYSTEM technology might face during both its research activities as well as once it is deployed in society. Specifically, D10.1 covers the legal aspects related to surveillance measures. D10.1 is the first (baseline) step in the impact assessment described in WP10. The legal frameworks outlined in this deliverable will be mobilised to assess the risks to the rights to privacy and data protection throughout the duration of the whole project.

Editor	Sergi Vazquez Maymir, Eugenio Mantovani and Paul de Hert (VUB)
Contributors	//
Reviewers	Galya Toteva Terzieva (ISEMi), Lorenzo Di Matteo (FORMIT)
Submission date of the draft to reviewers	20 May 2019
Submission date of the draft to the SAB (if required)	Not required

Register of document versions

Partner acronym	Version number	Date	Suggested relevant changes	Notes
VUB	V1.0	20/05/2019	First Draft	//
ISEMi	V2.0	24/05/2019	//	//
FORMIT	V2.1	24/05/2019	Template, page II, page III, font	//
VUB	V2.2	28/05/2019	2nd draft	Accepted suggested changes by reviewers; edited executive summary; edited bibliography
FORMIT	V3.0	25/06/2019	None	//

Every information is updated to the date of issue of this document

This document is composed by 43 pages

Table of Contents

List of acronyms and abbreviations

CA	Consortium Agreement
CFR	European Union's Charter of the Fundamental Rights
CoE	Council of Europe
DoA	Description of Action
DPIA	Data Protection Impact Assesment
EASA	European Union Aviation Safety Agency
ECHR	European Convention of Human Rights
ECtHR	European Court of the Human Rights
GA	Grant Agreement
GDPR	Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
LEA	Law Enforcing Authority
LED Directive	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, Brussels, 27 April 2016
PINS	Privacy Information Notices (PINS)
RPAS	Remotely piloted aircrafts
SME	Small and Medium Enterprise

EXECUTIVE SUMMARY

This deliverable presents the main legal considerations that, at the time of writing, the authors consider relevant to the SYSTEM project. The issues raised should be considered by partner organizations and researchers as basilen for the ensuing impact assessment. At the same time, these considerations should be taken into account by developers, policy makers, local authorities, and in particular law enforcement authorities (LEAs), as "end user" of SYSTEM technologies.

Processing activities within SYSTEM will fundamentally focus on non-personal data from sensors in the city 's sewage system, solid waste or urban air. Despite the project and the technology to be developed is not intended or meant to directly process personal data as information related to identified or identifiable individual/s, the surveillance measures of SYSTEM compel us to identify which could be the impacts on individuals' fundamental rights and freedoms, including but not only to privacy and the right to personal data protection.

The right to privacy is not an absolute right and authorities might in certain circumstances legitimately interfere with individual's personal privacy. This is the case of interferences grounded for the prevention, investigation or prosecution of crime, such as in SYSTEM. This does not mean, however, that the mere fact that where a "SYSTEM like" device is used in order to detect or prevent crime it will automatically be legal. Under EU law, a balance must be striken between security and the limitation of rights of individuals.

These conditions must be both described in law and be necessary and proportional in a democratic society. In addition, when assessing SYSTEM, it will also relevant to take into account how the U.S. Supreme Court have dealt with the use of sensor monitoring activities by law enforcement authorities and their qualification as searches under the Fourth Amendment (Kyllo v. United States). The authors cannot conclude at this stage whether all monitoring activities operated through SYSTEM will require a warrant to be performed, such decision will need to be addressed on a case-by-case basis taking into consideration the context how and the purposes of SYSTEM deployment.

The EU's data protection approach applies when personal data is being processed. As it will be discussed in section 5 of this document, where data cannot be linked to a specific individual it will not be classed as "personal data" and thus EU's data protection law does not apply. At the time of writing it is still not certain whether a SYSTEM prototype would involve the use of personal data. This is because while the data processed in SYSTEM does not directly relate to any particular individual; however, it cannot be excluded the possibility that as a result of its correlation with other data sets, individuals residing in certain areas might potentially be singled out from the area being profiled.

Similarly, it cannot be excluded that as a result of its processing activities, the envisaged SYSTEM prototype will be able to facilitate inferences of information on individuals pertaining to certain groups. Indeed, the implementation of sensor technologies such as SYSTEM might potentially result in a more fine-grained discrimination and classification of citizens and communities, or in other words an enhancement of social sorting practices[1]. There is a risk that SYSTEM processing activities could potentially lead to the group profiling of inhabitants living in certain areas or neighborhoods[2].

The use of drones in SYSTEM equipped with sensors will require an assessment on the risk to the rights and freedoms of individuals, taking into account the nature of surveillance that the drone poses to those

[1] Lyon, D. *Surveillance Studies: An Overview*. Cambridge: Polity Press (2007). See aslo Lyon D. *Surveillance as Social Sorting, Privacy, risk and digital discrimination*, New York 2011

[2] M.Hildebrand, S. Guthwirth, Profiling the European, Cross Disciplinary Perspectives Citizen: 2.3 Group Profiling & Personalised profiling.

individuals being monitored, as well as to the type of data that the sensors equipped in the drone are capable of collecting.

In line with the potential asymmetries between authorities and citizens resulting from the use of new sensor technologies, the right of data subjects to be informed is particularly important. Already in the research phase of SYSTEM, individuals might have a right to know that they are in an area where sensors are being placed and tested (i.e. for research purposes is occurring), and thus SYSTEM might be required to inform individuals about the collection and processing of information relating to air emissions, garbage and sewage.To that extent, the utilization of Privacy Information Notices (PINS) might be considered in order to prepare the public to a shared future of more sensing technologies in the public realms.

In those cases where SYSTEM tests involve the direct or indirect participation of workers (such as truck drivers), it might also be necessary to assess the need to fully inform workers' unions and the workers involved, as well as to obtain the approval of the latter and the consent of the former before any demonstration, according to national legislation and practices. In this event, the consent of workers will also need to ensure that workers enjoy a genuine choice to decide their say on the processing activities of personal data relating to him or her.

Finally, and taking into consideration the potential application of SYSTEM by law enforcement and public authorities it is necessary to consider how information obtained through sensors might be used as evidence in criminal proceedings and how, as a result, might interact with the rules governing due process.

1 MAIN ELEMENTS OF THIS DELIVERABLE

1.1 INPUT FROM OTHER PROJECTS

Baseline Report on Legal aspects (D10.1) receives no particular inputs from other projects.

1.2 INPUT FROM OTHER WPS AND RELATION WITH OTHER SYSTEM DELIVERABLES

D10.2 will cover the social acceptance and ethical issues pertaining to the surveillance measures in use by the SYSTEM technology, drawing contribution from the subcontractor in WP10, AND consulting Srl. This deliverable 10.1, together with the ethical analysis in D10.2, is the first (baseline) step in the impact assessment described in WP10. According to that plan, the legal frameworks outlined in this deliverable will be mobilised to assess the risks to the rights to privacy and data protection throughout the duration of the whole project. The first "impact assessment (IA)" exercise (D10.4) will address the legal and ethical conditions to carry out research activities at pilot sites.

1.3 APPLICABILITY

The deliverable provides legal referencese to partner organizations and researchers as they proceed to test and demonstration activities. At the same time, those references should be taken into account by researchers, IT developers, policy makers, local authorities, and in particular law enforcement authorities (LEAs), as "end user" of SYSTEM technologies.

1.4 REFERENCE DOCUMENTS

1. Grant Agreement (GA);
2. Consortium Agreement (CA);
3. The Project Operational and Management Plan (D12.1).

The hierarchy related to the documents above implies that the latter document needs to be consistent with the former. In case of issues, the hierarchy of the documents is mandatory.

1.5 PURPOSE OF THE DOCUMENT

The aim of this document is to provide the relevant legal references to anticipate the legal challenges that SYSTEM technology might face during both its research activities as well as once it is deployed in the society.

1.6 STRUCTURE OF THE DOCUMENT

The document is structured in the following way:

2. **Privacy And Surveillance In The System Project** introduces the concepts of privacy and surveillancet;
3. **System And The Right To Private And Family Life** focuses on the right to private and family life and describes the test of legality to assess whether surveillance measures engage the qualification permitted in article 8(2) European Convention of Human Rights. The research includes a brief analysis of the US Supreme Court on the Fourth Amendment (serach and Seizures) as affecting surveillance measures;
4. **System And The Right To Personal Data Protection** analyses the European legal framework on data protection, the definition of personal data and their processing in SYSTEM, principles in matter personal data processing, what is a data protection impact assessment (DPIA), rights of the data subject and their exercise by the GDPR;
5. **Profiling And Discrimination Of Certain Groups** deals with the right to not be discriminated against in police operations;
6. **System And The Use Of Drones** delves on the legal aspects about drones and tehri use in the context of the SYSTEM activities;

7. **General Rules Concerning Due Process In Criminal Proceedings** are analised in the light of the principle of fairness, quality of evidence, issues related to entrapment and appropriate oversight on the surveillance activities;
8. **Bibliography** with sources is also provided.

2 PRIVACY AND SURVEILLANCE IN THE SYSTEM PROJECT

The term privacy, which derives from the Latin verb *privare,* evokes the action of taking something out of the public and make it *privatus*.[3] Besides this general intuitive notion, privacy is a term without a single definition, associated with concepts such as "private life", "private sphere", "intimacy", "secrecy", "confidentiality", sharing indeed features with these notions, without coinciding with them.[4][5] It is expedient to briefly rehearse some attempts in literature to define what privacy protects, while asking to ourselves whether any of these notions are mobilized by the actions put in place by SYSTEM researchers and technology.[6]

Daniel Solove, an American legal scholar, [7] suggests six ideas of privacy: (1) as the right to be let alone – Samuel Warren and Louis Brandeis's famous formulation for the right to privacy[8]; (2) as limited access to the self – the ability to shield oneself from unwanted access by others; (3) as secrecy – the concealment of certain matters from others; (4) as control over personal information – the ability to exercise control over information about oneself; (5) as personhood – the protection of one's personality, individuality, and dignity; and (6) as intimacy – as control over, or limited access to, one's intimate relationships or aspects of life." Beate Rössler, another privacy scholar, has identified three dimensions:[9] a. Decisional privacy, which establishes a space for maneuver in social action that is necessary for individual autonomy, b. Informational privacy, i.e. who knows what, about a person and how they know it (control over information relating to that person) [10] and c. Local privacy, i.e. privacy of the household, of one's flat or room and thus privacy of personal objects.[11]

The foregoing definitions convey the idea that privacy may be interpreted in a narrow sense, notably informational privacy, or the right to be left alone, or as control over one's domestic space; next to it, there is also a broader understanding of privacy that emerges from the references to "personal autonomy", "personhood" and "decisional privacy". This broader understanding is apt to describe the potential of surveillance measures to have steering effects on individual's freedom and autonomy. [12] The awareness of being watched, for example, the presence CCTV is capable of imposing upon individuals in a psychological sense.[13] Individuals may alter their behavior, even when such behavior is legal. Others may feel disturbed at

[3] By contrast, the etymology of publicare conveys the reverse notion of placing something private into the public domain. Bart van der Sloot Aviva de Groot(2019), The Handbook of Privacy Studies: An Interdisciplinary Introduction. Amsterdam University Press, p.70

[4] R. Post, Three Concepts of Privacy', *Faculty Scholarship Series*, Faculty Scholarship Series,(Paper 185) (2001) pp.

[5] S. Gutwirth, *Privacy and the Information Age* (New York: 2002).

[6] Some of the material of this report is taken from the Deliverable "Report of relevant legal and normative standards and their evolution" from the FORENSOR project (Advanced Video Surveillance archives search Engine for security applications). Grant agreement no. 285024

[7] Quote originally taken from D. Solove, *Understanding Privacy.* (Cambridge: 2008).

[8] Brandeis, Louis, and Samuel Warren, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220.

[9] B. Rossler, *The Value of Privacy* (Cambridge: 2005).P111

[10] Ibid.,

[11] Ibid.,pp14

[12] P. Quinn and P. De Hert, Self respect—A "Rawlsian Primary Good" unprotected by the European Convention on Human Rights and its lack of a coherent approach to stigmatization?', *The International Law of Discrimination and the Law*, 14,((2014) pp. 19-53 Under the ECHR's privacy approach for example it is recognized that there is a need to protect individuals from harmfull forms of hate speech.

[13] C. Held, J. Krumm and R. Schenke, Intelligent Video Surviellance', *Computer*, 45,(3) (2012) pp. 83-84

the prospect that the police could be alerted to their presence, even if they are not taking part in any illegal activity. [14] Some people may not only behave differently in monitored areas, they may as well avoid going to those areas at all. This broader understanifng of privacy explains the fallacy of the "nothing to hide argument." The basic problem with this argument is its underlying assumption that "privacy is about hiding bad things."[15] As explained in these lines and below, the value of privacy is not about hiding but about setting, and respecting, limits, a space of freedom where something can be hidden.[16] Famously, Orwell's hallucinating novel *1984* portrays an unfree society where cameras installed everywhere, including in public spaces, leave no room for a single bit of privacy. In that society, where free thinking is suffocated in the cradle, there is no possibility for democratic government. In recent years, various scandals, such as those revealed by the PRISM case[17] and the Snowden revelations, have raised the concern that surveillance technologies may proliferate out of control, i.e., with no limitation to what data security or law enforcement agencies can collect and process. The concern has only heightened in recent years: the pace of collection is accelerating as the cost of collection decreases. In addition, the development of data processing technology, algorithms, allows these data to be cross-indexed effectively and cheaply with available historical data or self-reported data, to which the sensor data can be linked. Under these circumstances, citizens may find themselves living in the digital equivalent of a "goldfish bowl."[18] Thus, looking at surveillance in terms of narrow, informational privacy, would probably not be sufficient.[19] In the broader sense, instead, privacy emerges as a fundamental value, a cornerstone of pluralistic democratic states.[20].

Surveillance technologies like SYSTEM may pose a risk to privacy, creating the conditions to monitor and thus unduly pressure citizens. At the same time, In order to ensure security, the state may take measures that may infringe upon the privacy of individuals.[21] Citizens accept to restrain certain behaviors in public, for instance; or willingly comply with demands to provide personal details, e.g., when booking airline tickets. While these measures impinge upon privacy, these privacy infringements are not deemed unacceptable. Surveillance measures may thus be acceptable when they are necessary, e.g., they relate to crime and security, and when the level of infringement on privacy is proportional. Furthrmore, the social acceptability of privacy infringements needs to be considered in context. There is a difference between sensors monitoring private property or public areas; there is a difference between a permanent system of montioring sewage and air emissions, and a surveillance system that is only deployed when there are suspects suggesting that a specific are is more likely to correlate to criminal activity.The surveillance measures may be socially accepted by a valid aim, to tackle serious crime, such as drugs pr explosives manufacturing; they may not be as accepted justified if they intended to tackle petty criminality, such as self-consumption of the manufactured drugs. In deciding upon whether a potential use would be acceptable it would be necessary to take all such factors into account.

This introductory chapter has pointed at some areas of tension between privacy nd surveillance. In the next chapter, the authors discuss how a court of law, the European Court of Human Rights, has broached these tensions between privacy and surveillance. Where SYSTEM encroaches upon privacy in a wider sense

[14] S. Gutwirth, (2002) Gutwirth for example refers to a need to reduce steering forces upon individuals which unduly pressure them to make decisions in certain ways.
[15] Daniel, J., Solove, D.J.: I've Got Nothing to Hide and Other Misunderstandings of Privacy. San Diego Law Review 44, 745–757 (2007)
[16] Mordini, Emilio. "Nothing to hide biometrics, privacy and private sphere." European Workshop on Biometrics and Identity Management. Springer, Berlin, Heidelberg, 2008, pp.252.
[17] A. Galetta and P. De Hert, Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approachto a Human Rights Framework for Surveillance | Volume 10, Issue 1 (January) 2014 | URN:NBN:NL:UI:10-1-115810
18 Froomkin, A. M. (2017). Privacy Impact Notices to address the privacy pollution of mass surveillance. In Privacy in Public Space. Edward Elgar Publishing, pp. 195.
[19] S. Gutwirth, (2002)
[20] C. Bennet, (2011). H. Nissenbaum, Protecting Privacy in the Information Age: The problem of Privacy in Public', *Law and Philosophy*, 17,((1998) pp. 559-596
[21] For a critical view on such an idea see: M. Neocleous, Security, Liberty and the Myth of balance: towards a critique of security politics', *Contemporary Political Theory*, 6,(2) (2007) pp. 131-149

(i.e., the awareness that surveillance systems exist influence privacy), the project will have to take into consideration the limits and constraints imposed by fundamental rights law, in particular the right to private and family life.

3 SYSTEM AND THE RIGHT TO PRIVATE AND FAMILY LIFE

This chapter outlines how human rights law in the Council of Europe area recognises and protects privacy in the second, broad, sense mentioned in the previous chapter, i.e., as protection against steering or influence.[22] This will involve highlighting the prominent sources of international and European law, pausing in particular on the European Convention of Human Rights, which is binding on all states involved in the project.[23] As anticpated, the chapter also includes a review of the relevant jurisprudence of the USA Supreme Court, as affected by surveillance measures. At the end of this chapter, a preliminary assessment offers partners a list of principles and areas of concern to be borne in mind throughout the project's impact assessment.

3.1 THE RIGHT TO PRIVATE AND FAMILY LIFE

The decision to accord privacy the status of a fundamental right is arguably tributary to political choices taken by states in the 20th century and after the end of WWII. In the authoritarian or totalitarian regimes of 20th Century Europe, public security justified any intrusion into citizens' private and family life. Under these circumstances, citizens are soon made aware that police controls or could control their communications, movements, meetings; this sort of total control does not only silence dissent, but stifles any voice, view, opinion, idea, innovation, creativity, which may be seen as departing from the norm or the mainstream, with effects that can be catastrophic. The insertion of a fundamental right to private and to family life in the constitutions and declaration of rights of the last century responded precisely to this societal and political need to shield the private sphere from state power. A similar rationale holds true today in decisions involving conflicts over surveillance practices.

In this sense, as a limit to power, privacy has been recognized as a fundamental or human right at the international and European levels. At the international level, article 12 of the authoritative Universal Declaration of Human Rights (1948) states that:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Article 17 of the binding International Covenant on Civil and Political Rights (1966) provides that:

> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks.*

In Europe, the European Union's Charter of the Fundamental Rights (CFR, 2009) recognizes a fundamental right to privacy in article 7, stating: "Everyone has the right to respect for his or her private and family life, home and communications."[24] Article 7 (and article 8 CFR on the protection of personal data, discussed in

[22] The term 'steering' was used by Gutwirth in describing the power of societal forces (including the state) to shape not only the behavior of individuals but also their thoughts. See: S. Gutwirth, (2002)

[23] A. Caligiuri and N. Napoletano, *The Application of the ECHR in the Domestic Systems* 2010). H. Keller and A. Stone Sweet, *A Europe of Rights: The Impact of the ECHR on National Legal Systems* (Oxford: 2008).

24 The application of the rights enshrined in the EU Charter is restricted to the activities of European Institutions and to Member states that are implementing EU law or are "acting within the scope of Community law.". This is described by Article 51(1) of the EU Charter which states: "The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers. For more see: F. Fontanelli, The European Union's Charter of Fundamental Rights two years later ', *Perspectives on Federalism*, 3,(3) (2011) pp. 22-47

the next section 5), can be derived squarely from a well-known provision contained in the European Convention on Human Rights (the ECHR), article 8, the right to private and family life, and in the case law of the European Court of Human Rights (the EctHR), based in Strasbourg, France. See next paragraphs.[25]

It has been mentioned that a right to privacy is inscribed also in states' constituions. Of the national experience, the choice of the authors has been to look at the experience of a non-EU jurisdiction, the United States. The reason for this choice is that the the Supreme Court of Justice of that country has discussed the limits to monitoring activities of law enforcement authorities when these latter constitute "a search", protected under the Fourth Amendment of the American Constitution.

3.2 THE LIMITS ON SURVEILLANCE SYSTEMS UNDER ARTICLE 8 ECHR CASE LAW

This and the next paragraphs describe a series of decisions of the court of human rights about cases involving surveillance systems allegedly interfering with article 8, the right to private and family life.
Before delving on the case law and the limits on secret surveillance systems identified by the court of Strasbourg, it is necessary to take a closer look at the provision contained in article 8 ECHR. Article 8 of the ECHR states:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence;*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.* [our underlining]

While article 8(1) establishes a principled position, "everyone has the right", article 8(2) provides for a series of exceptions to that principled position ("there shall be no interference by a public authority with the exercise of this right except such as"). This means that not all actions or measures taken by a public authority are a violation of Article 8 ECHR. Specifically, three types of actions may come under the purview of the law:

- actions (or measures) that do not interfere with Article 8 ECHR;
- actions (or measures) that do interfere with Article 8 ECHR but are compatible with the requirements laid down in Article 8(2) ECHR;
- actions (or measures) that do interfere with Article 8 but are not compatible with the requirements laid down in Article 8(2) ECHR.[26]

3.2.1 SURVEILLANCE MEASURES THAT DO NOT INTERFERE WITH ARTICLE 8.1 ECHR

Actions or measures that do not interfere with Article 8 ECHR are measures that, while individuals may think or see as privacy invasive, they are not in fact legally protected by article 8. For example, portable sensors that measure air pollution, or sensor that measure traffic flows. A challenge to such measures may not activate article 8; it may be related to other rights, or do not engage human rights, but other interests, such as envornment protection, health, or mobility.

[25] In accordance with Article 52(3) of the EU Charter, the meaning and scope of this right are the same as those in the corresponding article of the ECHR. Consequently, the meaning is the same and the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR
[26] Antonella Galetta Paul de Hert, pp.57.

3.2.2 SURVEILLANCE MEASURES THAT DO INTERFERE WITH ARTICLE 8 ECHR AND ARE COMPATIBLE / ARE NOT COMPATIBLE WITH THE REQUIREMENTS LAID DOWN IN ARTICLE 8(2) ECHR

Most surveillance measures that come under the purview of the court engages article 8, paragraph 2 ECHR. Article 8, paragraph 2 ECHR, states that interreferences and restrictions may be compatible with the law if they are taken in accordance with the law, if they are necessary in a democratic society, and proportional, what we call the test of legality.

3.3 THE TEST OF LEGALITY TO ASSESS WHETHER SURVEILLANCE MEASURES ENGAGE THE QUALIFICATION PERMITTED IN ARTICLE 8(2)

In short, the test of legality to assess whether surveillance measures engage the qualification permitted in article 8(2) include asking the following questions:

(i) Whether a measure has a valid aim or acceptable goal (i.e, 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);

(ii) Whether the measure is described in law ("in accordance with the law");

(iii) Whether it can be considered "necessary [and proportional] in a democratic society." [27]

3.3.1 SURVEILLANCE MUST PURSUE A VALID AIM AND ACCEPTABLE GOAL

In terms of "valid aim or acceptable goal", the Human Rights court acknowledges that public authorities have a leading and crucial role in defining their necessities in a democratic society. In the case *Klass v Germany* the EctHR held that "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[28]

However, the court is also well aware of the lethal threats that can result from secret surveillance, which could be "undermining or even destroying democracy on the ground of defending it."[29] As a consequence, public authorities cannot enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. Instead, the Court is particularly keen in requiring Member States to set up adequate and effective guarantees against abuse.

3.3.2 SURVEILLANCE MUST BE IN ACCORDANCE WITH THE LAW

As part of its legal assessment, the court verifies whether there are laws or powers granting to LEAs or other authorities the authority, and dictating the conditions, to carry out surveillance measures. In ***Malone v the United Kingdom***, the court explained that "in accordance with the law" means that "any interference must have some basis in the law of the country concerned."[30]There is of course no European piece of legislation

[27] Relevant cases from the perspective of surveillance in issues include Case of S. and Marper v the United Kingdom (Applications nos. 30562/04 and 30566/04), Case of Malone v. UK (Application no. 8691/79), Case of Peck v the United Kingdom (Application No. 44857/98) For more discussion on the rulings of the ECtHR in the context of surveillance issues see:V. Kosta, Fundamental Rights in EU Internal Market Legislation 2015).pp.92

[28] ECtHR, *Klass v. Germany*

[29] ibid, para. 49.

[30] ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, Judgment of 2 August 1984, pp. 27-28, para. 67.

dealing with the granting of power to law enforcement authorities to engage in surveillance, this type of laws and powers existing only at the national or local level. It is therefore important to be aware of local situation that exists in terms of the law in force in the particular jurisdiction concerned.

As the case *Malone* v. *UK* shows, the court will not be satisfied by the mere existence of a law. What matters is o the "quality" of the legal provision, which has to be particularly clear, precise and detailed, in order to prevent possible abuses. In another case *Huvig and Kruslin v France*, the EctHR explicitly stated that national laws must indicate "with reasonable clarity the scope and manner of exercise of the relevant discretion" of public authorities in exercising an intrusive power.[31] In *Liberty and Others v. the United Kingdom* of 1 July 2008, two British citizens complained their telephone, facsimile, e-mail and data communications had been intercepted by the British Ministry of Defence, form 1990-1997.[32] The Court held that there had been a violation of Article 8 of the Convention because domestic law did not provide ,in a form accessible to the public, any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. Therefore, the interference with the applicants' rights could not be considered "in accordance with the law", as Article 8(2) provides. The surveillance measure was therefore found to be illegal.

3.3.3 SURVEILLANCE MUST BE NECESSARY AND PROPORTIONAL IN A DEMOCRATIC SOCIETY

The existence of "valid aim or acceptable goal" and of good laws does not suffice to conclude that surveillance measures will not be a violation of human rights law.[33] This is because these measures must also be "necessary" and "proportional" in a "democratic society". In fact, courts of law rarely engage the question of necessity, contenting themselves to verify the existence of a valid aim and an enough detailed law. Furthermore, contesting the necessity fo a security measure would put the court is a collision trajectory with signatories' states. Thus, the legal question – where the law sets limits and constraints – arises in deciding whether a surveillance measure is "proportional."[34]

Determining what is "proportionate" will depend on a variety of factors. The remainder of this section describes some cases that exemply the how the court assessed the proportionality of surveillance measures, in the decision about its compatibility with Article 8(2) ECHR. Understanding the proportionality requirement is key because it enables the consortium, by analogy, to balance the conflict between privacy and surveillance measures or practices in SYSTEM.

In the case **S. and Marper v. the UK,** the court found that the "blanket and indiscriminate" retention of fingerprints, cellular samples and DNA profiles of persons suspected, but not convicted of offences "failed to strike a fair balance between competing public and private interests." The case concerned two British citizens who were arrested and later cleaned of all charges[35]. Once they had been cleared, both applicants requested that fingerprints, and DNA samples and profiles be destroyed. Their request was denied on the ground of a law stating that police could permanently keep the details of anybody after their arrest. The European Court of Human Rights held that the protection of Article 8 ECHR would be "unacceptably weakened" if the use of modern surveillance techniques in the criminal justice system were allowed "at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against

[31] *Huvig v France*, application no. 11105/84, Judgment of 24 April 1990, para. 28 ("*Huvig v. France*"); ECtHR, *Kruslin v France*, application no. 11801/85, Judgment of 24 April 1990, pp. 16-21, paras. 27 & 30-36 ("*Kruslin v. France*");
[32] ECtHR, Liberty And Others v United Kingdom (2008)
[33] R. Weber and D. Staiger, Bridging the Gap between Individual Privacy and Public Security', Groningen Journal of International Law, 2,(2) (2014) pp. 14-32 Staiger, (2014).
[34] See in that respect the ruling from the EU Court of Justice case C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] EU, para 28 and 37 or Joined cases CC-203/15 and C-698/15 *Tele2 Sverige and Watson and Others*, EU:C:2016:970 [para105, 106 and 107]
[35] ECtHR *S & Marper v United Kingdom* Appl. Nos. 30562/04 and 30566/04 (2008)

important private life interests." In that decision, the court underlined the principle that any surveillance measures that consists in storing information about inidividuals must be balanced against the privacy right.

In the **Uzun v. Germany** judgement of 2 September 2010, the applicant, suspect in bomb attacks by a left-wing extremist movement, complained that surveillance via GPS has breached his right to privacy.[36] The Court accepted that GPS surveillance had a interfered with the applicant's right to respect for his private life. However, the Court noted that the surveillance had pursued a valid aim, the investigation of a serious crime; secondly, the court found that the GPS surveillance had been ordered only after less intrusive methods of investigation had proved insufficient. The Court concluded that there had been no violation of Article 8 of the Convention. In this case, the Court underlined that the scope of the state's margin of appreciation is related not only to the nature of the legitimate aim pursued, but also to the particular nature of the interference involved. The Court also suggests that the proportionality is proven when least intrusive means are used or condiered. In this case, the core of the proportionality requirement consisteds in balancing the interest of the state in protecting its national security, against the interference with the applicant's right to respect for his private life.

The case of **Peck v. the UK** recognises for the first time that there is a right to privacy in public. The case concerned the disclosure of footage filmed in a street by a closed-circuit television (CCTV) camera installed by the local council, showing the applicant trying to take his life. The images, caught in a public place, were later used for a media campaign to provide help to people attempting suicide. The Court found that the legitimate objective for which images were released, the prevention of suicide, could have been achieved through more proportionate means; in particular, identifying the applicant and obtaining his consent prior to the disclosure of the film footage. For our purpose, it is important to underline the position of the defendnant government and the assessment of the court. The government contended that Peck's actions were already in the public domain as he chose to comit suicide in a public street. It was thus not cleacut that his private life had been interefered with at all.37 The court disagreed explaining that "Private life is a broad term not susceptible to exhaustive definition" and that "There is a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."[38] It is important to keep in mind this point, beacsue it means that collecting data from public facilities, managed by the munucipalty, does not exclude privacy interests from coming into existence. Even in a public context, privacy may be engaged.

However, the court further clarified that a distinction must be made between the "monitoring" of personal information (in this case, through video images) and its collection. As the court argued, "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life."In contrast, " […] on the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations."[39] This could be a crucial difference for technologies of surveillance like SYSTEM. The monitoring of data per se is not engaging privacy, while its collection, regardless of whether the data is taken in public or not, gives raise, per se, to a privacy intereference.

Referring to the American context, US scholar Helene Nissembaum argues that there is a loophole in privacy protection: she claims that privacy in public does not benefit from a level of protection similar to the protection against violation of the personal sphere, abuse of intimate information, protection of the private individual against government intrusion, etc. "Practices of public surveillance", she writes, " […] seem to fall outside the scope of predominant theoretical approaches to privacy […]. "[40] Peck is important because it

[36] ECtHR, *Uzun v. Germany*, application no. 35623/05, judgment of 2 September 2010 ("*Uzun v.Germany*").
[37] ECtHR, *Peck v United Kingdom,* (2003) 36 EHRR 41, paragraph 53
[38] ECtHR, *Peck v United Kingdom,* (2003) 36 EHRR 41, paragraph 57
[39] ECtHR, *Peck v United Kingdom,* (2003) 36 EHRR 41
[40] Nissenbaum, Helen. "Privacy as contextual integrity." Wash. L. Rev. 79 (2004): 119.

shows that, unlike in the United States, everyone has a right to privacy, even in public. Peck's recognition of privacy in public is apparently relevant for SYSTEM. The SYSTEM project's aim is to create a surveillance network located in sewage systems, in the air, in garbage bins or tracks. Sewage systems, the air, the garbage bins or the waste company tracks are usually public; so are squares, parks, and the public roads walked by a confused citizen, Peck.

One of the cases referred to in Peck was ***P.G. and J.H. v. the United Kingdom.***[41] The case concerned, inter alia, the recording of the voices of P.G. and J.H. in the ocurse of an investigation. In that case the court reasoned as follows: "*There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.*"

The court , first, recognizes that a person's private life can be concerned by measures effected outside hir or her private premises; second, the court undelines that "private-life considerations may arise once any systematic or permanent record comes into existence of such material from the public domain." As explained earlier in Peck, the files gathered on inidividuals fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.

In conclusion, the jurisprudence of the Court of Strasbourg e shows that article 8 has been interpreted to protect different aspects of private and family life.[42] Importantly for SYSTEM, the court has heard litigations instigated by citizens against the use of surveillance measures by law enforcement agencies (*Klass v. Germany*[43], *Leander v. Sweden*[44] and *Rotaru v. Romania*[45]). In addition, through its legally binding rulings that states have to respect, the jurisprudence of the court of Strasbourg has recognized a right to access to personal files (*Gaskin v. the United Kingdom*[46],); a right to delete personal data from files held by the police (*Leander v. Sweden*[47], *Segerstedt-Wiberg v. Sweden*[48] *or Marper v. United Kingdom*); a right to access information about the environment in the choice of residence (*Guerra v. Italy*[49]). The court has heard cases discussing g with individual's expectation of privacy In *Niemietz v. Germany* and in *Halford v. UK* [50]. With *Peck* v. *UK*, the court recognized that we have a right to privacy also in public.[51] The court accepts that in general, any surveillance systems that record data, (not just monitor) in public places, are capable of engaging individual rights under Article 8 ECHR, i.e. a right to private and family life. This does not however mean that such engagements" can automatically be equated to violations of Article 8.

[41] Case of PJ & H v United Kingdom (Application Number 0004478/98 2001)
[42] N.A. Moreham, 'The right to respect for private life in the European Convention on Human Rights: a re-examination', 2008 European Human Rights Law Review 1, no. 1, pp. 44-79.
[43] ECtHR, *Klass v. Germany*, (1978) 2 EHRR 214.
[44] ECtHR, *Leander v. Sweden*, (1987) 9 EHRR 433.
[45] ECtHR, *Rotaru v. Romania*, Application no. 28341/95 judgement of 4 May 2000.
[46] ECtHR, *Gaskin v. the United Kingdom,* (1989) 12 EHRR 36.
[47] ECtHR, *Leander v. Sweden*, (1987) 9 EHRR 433. In this case there was a breach of article 8.1 because the use of the secret police files, coupled with a refusal to allow L access to this information, amounted to an interference with the applicant's right to private life. However, the breach of Article 8(1) was justified by the legitimate aim under 8(2) of protecting national security. (para. 74)
[48] ECtHR, *Segerstedt-Wiberg v. Sweden*, application no. 62332/00, judgement of 6 June 2006.
[49] ECtHR, *Guerra v. Italy*, (1996) 26 EHRR 357.
[50] ECtHR, *Halford v UK,* (1997) ECHR 32, para. 44; *Niemietz v. Federal Republic of Germany ,* 251 Eur. Ct. H.R. (ser. A) (1992), para. 32. I.
[51] ECtHR, *Peck v United Kingdom,* (2003) 36 EHRR 41, *para.* 85.

More in detail, and finally, the case law review indicates a series of criteria that should be taken into account in determining what is "proportionate" surveillance under article 8(2) ECHR:

- The nature of the measure taken (its reach, whether it is general or absolute, its adverse consequences, the scope for abuse of the measure),
- whether the state concerned could have taken other measures or implemented them in a less drastic way,
- any status of the persons involved which legitimately renders their rights subject to greater limitation (e.g. prisoners)
- whether there are any safeguards which can compensate for the infringement of rights which a measure can create.[52]

3.3.4 THE FOURTH AMENDMENT OF THE AMERICAN CONSTITUTION ON SURVEILLANCE

This sub paragraph describes the limits put on surveillance measures warranted in cases decided in front of the US Supreme Court.[53] As suggested earlier, the legal protection of privacy in the United States does not harbor the broader notion of privacy discussed in the introduction as protection from steering from undue influence or control, not does it recognise a right to privacy in public.

Although not explicitly mentioned, the right to privacy emerges from the "penumbra" of the U.S. Constitution.[54] Legal scholars agree that different aspects of privacy are protected against government action through many Amendments, including the First (speech, religion, and association), Fourth (search and seizure), Fifth (self-incrimination), Ninth (general liberties amendments).[55] In particular, privacy law concerning governmental surveillance measures has developed out of the case law on the Fourth Amendment of the United States Constitution. The Fourth Amendment of the American Constitution provides:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

This Amendment places limits to monitoring activities of law enforcement authorities when these latter constitute "a search." Through the years the interpretation and interplay between the fourth amendment

[52] See I. Cameron, National Security and The European Convention on Human Rights, The Hague/London/Boston, Kluwer Law International, 2000, (479p.), 97-101 and M. Delmas-Marty, The European Convention for the Protection of Human Rights, Dordrecht, 1992, 71, As quoted in P.de Hert, op.cit., pp.80.
[53] Rachel L. Finn and David Wright, Laura Jacques and Paul De Hert, Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations (2014), pp. 130-135.
[54] Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum
[55] H. Nissenbaum, Privacy as Contextual Integrety', Washington Law Review, 79,((2004) pp. 104-139

and law enforcement activities has left several landmark cases by the U.S Supreme Court, requiring our consideration.

In ***Katz v. United States***[56], the Court examined whether warrantless wiretapping operations of private communications inside a public telephone booth, constituted an unreasonable search under the Fourth Amendment. Reminding that "the Fourth Amendment protects people, not places" , the court famously ruledout its "reasonable expectation of privacy test " (or Justice Harlan's test).[57] The reasonable expectation test repealed the traditional notion of "trespass" to determine whether "a search" is taking place, introducing two main criteria: first the "person has exhibited an actual (subjective) expectation of privacy" in the thing searched and, second, that "the expectation be one that society is prepared to recognize as reasonable".[58]

The new test, the reasonable expectation of privacy, relies on society to determine what is "reasonable" to expect in terms of privacy invasion or protection. Accordingly, in ***California v. Ciarolo***, the Court ruled that photographing openly visible areas with a normal, off the shelf camera while operating a small aircraft flying over residential and commercial areas, did not constitute a search under the Fourth Amendment: for the court, these areas are open to the public view and therefore there is no expectation of privacy.[59] Similarly, in ***Florida v. Riley***, the majority of the court held that viewing the defendant's greenhouse from a low-flying helicopter was not to be categorized as a search, thus reuiqring a warrant. The Court contened that people do not have a reasonable expectation of privacy from air, because flights have become a common technology, part of modern lives. Hence, monitoring activities carried out in public do not require a prior warrant.[60]

Conversely in ***Kyllo v. United States***, the question presented to the Court was whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a "search" within the meaning of the Fourth Amendment. The judges held that the use of a thermal camera to collect information regarding the interior of a home amounted to an invasion of an individual's reasonable expectation of privacy. Therefore,
thermal imaging to monitor the radiation of heat from a person's home constituted a "search" within the meaning of the Fourth Amendment, requiring a warrant. The judges underlined that an important element to be considered in attesting the reasonable expectation of privacy was the quality of the technology used. In this case, the Court held that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[61] In Kyllo, the Court concluded the Fourth Amendment had been breached; however, this conclusion was reached after it was ascertained that thermal imaging on a private residence, unlike helicopter visions, was not common practice; and therefore, it should be considered as a search. The reasoning has been criticized because it ties expectation of privacy to practice and convention.[62]

As a result, in the United States, whether monitoring activities constitute a search under the Fourth Amendment, and thus require a warrant, seems to depend on four main factors:

1- the privacy expectation of the society regarding the thing searched;

2- the area of the monitoring operation (public, private);

[56] US Supreme Court, Katz v. United States, 389 U.S. 347 (1967);
[57] See Peter Winn "Katz and the Origins of the "Reasonable Expectation of Privacy" Test.
[58] Ibid, by reference to Katz, 389 U.S. at 361 (Harlan, J., concurring).
[59] US Supreme Court, *California v. Ciraolo*, 476 U.S. 207 (1986) ("*California v. Ciraolo*").
[60] US Supreme Court, *Florida v. Riley*, 488 U.S. 445, 450 (1989).
[61] Kyllo v. United States, 533 U.S. 27 (2001)
[62] Nissembaum, op.cit., p.126.

3- the technology used, which affects the expectation of privacy;

4- the duration of the surveillance.

It is sensible to point out that, as mentioned earlier, the US Supreme Court has not developed a notion of privacy as freedom fro steering similar to that developed by the ECHR. In addition, the notion of privacy in public in not hosted in the case law of theis court.

3.3.4.1 PRIVACY IMPACT NOTICES (OR SURVEILLANCE AS A TYPE OF ENVIRONMENTAL POLLUTION)

The notion of using Privacy Impact Notices to inform citizens about surveillance measures is grounded in the argument, which emanates from legal doctrine in the United States, that today's mass surveillance is "nothing less than a form of pollution of the public sphere".[63] In the *Kyllo* case, writes Froomkin, "the measurement of the heat emanations from his home was a search that required a warrant. But when the measurement is by a private party, at a distance, and at a mass scale, there is no warrant requirement."[64]

According to this orientation, modern sensor-based surveillance measures create a serious asymmetry in information, whereby citizens lack knowledge about whether information collection activities are undergoing, and about the consequences of such gathering, or of the potential of data crossing and mining from other data sets.[65] To mend this asymmetry, Froomkin proposes to "require Privacy Impact Notices (PINs) before allowing the construction of the deployment of large projects (public or private) that risk having a significant impact on personal information privacy or on privacy in public."[66]

Learning from Environmental Impact Assessment (EIA), the overarching goal of the PINs would be:

a. to encourage decision makers to consider privacy and public opinion from an early stage of the decision-making process leading to adoption of surveillance measures;
b. to inform the citizens of decision considered or made that affect it and to solicit public feedback as plans are designed.

The decision as to whether or not issues a privacy notice, falls on actors, e.g., data protection authority, policy makers, police, - required to investigate whether any technology *potentially* capable of persistently infringing on some aspects of privacy poses risks; describe them; verify if designers have built mitigation strategies, and deliberate whether a privacy impact notice is necessary, whether partial notice or full disclosure notice.

Conceiving as mass surveillance as a type of pollution, in conclusion, underline the need to start a more informed debate by creating more informed citizens. [67] PINs underline the responsibility to prepare the public to a shared future of more sensing technologies in the public realms; it worth underlining that the use of PINs may be part or be one of the outcomes of privacy impact assessment or data protection impact assessment processes, discussed under Section 5.

3.4 CONCLUSION

[63] Froomkin, A. Michael. "Privacy Impact Notices to address the privacy pollution of mass surveillance." In Timan, Tjerk, Bryce Clayton Newell, and Bert-Jaap Koops, eds. *Privacy in public space: Conceptual and regulatory challenges*. Edward Elgar Publishing, 2017.p.185.
[64] Ibid. pp.192.
[65] Ibid
[66] Ibid.pp.195.
[67] Ibid. pp.209.

Although the European Court, as well as the US Supreme Court, have not yet dealt with the specific question of whether sensor technologies monitoring sewage systems, trash bins and air emissions, infringe on article 8 or on the Fourth Amendment, both courts have built some relevant principles that can be useful to assess and to mitigate the privacy risks for technology like SYSTEM's.

This conclusive paragraph offers a preliminary assessment of the SYSTEM project against the principles developed in the case law of the European Court of Human Rights and of the Supreme court of the US. This is done with the purpose of providing partners with a list of conditions, derived from human rights law, to be borne in mind throughout the project's impact assessment.

- To reflect on what threats can SYSTEM surveillance pose to the what the fundamental right to privacy in constitutional democratic states. Consider that surveillance activities carried by law enforcement authorities exert psychological pressure upon individuals and this may be capable of altering their behavior. Individuals may not feel comfortable acting in a way that they may have otherwise have done so if they feel themselves under monitoring or if they believe that their actions may draw unwanted attention from authorities. And it is worth noting that such aversion is not necessarily linked to any type illicit activity but simply on the rejection towards unwanted interference with one's private life. It is important to recognize that privacy and related rights and freedoms, such as freedom of expression, or assembly, cannot be reduced to information concerning specific individuals, but can and must be thought of in a wider sense[68].

- To ask to what type of "actions" do the activities of a LEAs using SYSTEM pertain and, to what type of "actions" do the actions of a LEA testing SYSTEM in the research venues, pertain:
  1. actions (or measures) that do not interfere with Article 8 ECHR;
  2. actions (or measures) that do interfere with Article 8 ECHR but are compatible with the requirements laid down in Article 8(2) ECHR;
  3. actions (or measures) that do interfere with Article 8 but are not compatible with the requirements laid down in Article 8(2) ECHR.[69]

- Ensure that SYSTEM technologies are used as part of surveillance measures based on legitimate basis, laws or powers, found at the local level;

- Asses the quality of the laws and powers, which must state with reasonable clarity the scope and manner for the exercise of the relevant discretion of the public authorities in exercising an intrusive power, about foreseeability of the procedures to be followed for selecting for examination, sharing, storing and destroying collected information.

- Assess the proportionality of surveillance measures taking into account:

  - the context of the surveillance activity and the status of the persons involved (children, prisoners, etc);
  - whether other less intrusive measures could be implemented, taking into account factors such as the duration of the surveillance;
  - the particular nature of the interference involved: does it inolve monitoring or collection of data? ;
  - whether there are any safeguards which can compensate for the infringement of rights which a measure can create.

[68] See ECtHR Catt v UK *Application no. 43514/15) (2019)*
[69] Antonella Galetta Paul de Hert, pp.57.

- Consider how to mitigate the informational asymmetry between police and citizens which make surveillance system opaque. Consider the possibility of adopting Privacy Information Notice.

- Consider that in most cases monitoring conducted by SYSTEM will amount to search. The authors cannot conclude at this stage whether all monitoring activities operated through SYSTEM will require a warrant to be performed, such decision will need to be addressed on a case-by-case basis taking into consideration the context how and the purposes of SYSTEM deployment.

- Human rights law protects the right to privacy in public if the monitoring amounts to collection of information.

- Consider the problem of dehumanization of the surveilled: by installing sensors capable of monitoring areas with little or no human intervention there is an increasing tendency to support competent authorities' decisions based on automated decisions with a priori granted objectivity. As a result, the description of threats, challenges or grounds for operational actuations tend to be less dependent on the humans from which those threats, challenges or grounds originate. To be developed on D10.2

4 SYSTEM AND THE RIGHT TO PERSONAL DATA PROTECTION

As mentioned above, informational privacy or data privacy refers to instances where SYSTEM collects information concerning individuals.[70] The relevant legal framework dealing with data privacy is the data protection legal framework, presented in section 5 of Proposal 787128 – SYSTEM – Part B *Annex 1 – Description of Action*. As described in that section and earlier in this document, the processing of personal data by police and criminal justice authorities is becoming increasingly relevant because of the proliferation of new investigative techniques supported by miniaturized sensors. SYSTEM represents an example of this new wave of surveillance techniques, as it is designed to monitor and "sense" urban, populated, areas for police and public safety purposes. In doing so, SYSTEM may also process personal data of citizens. When processing personal data of citizens, SYSTEM must abide by the relevant EU personal data legal framework.

The relevance of this framework includes both the research activities that the SYSTEM project conducts and that may involve the processing of data of individuals participating in trials and demonstrations, e.g., truck drivers. In addition, this personal data protection framework is relevant also for personal data processing activities that SYSTEM will perform when the technology is developed and deployed.

As a preliminary clarification, a distinction should be made between personal data protection and privacy. As mentioned earlier, privacy is engaged not only when a harm is inflicted on a person (e.g., harm to reputation, or disclosure of private information)[71], but also when the freedom and autonomy of individuals is influenced or steered by the presence of monitoring systems, such as CCTV camera or other surveillance technologies. Unlike privacy, which sets limits to infringements on personal life, data protection law consists of a series of organizational and control rules. As part of this transparency mechanism, data protection foresees principles, rights, obligations, sanctions, and the presence of ad hoc national data protection authorities in each Member State of the EU having the power to investigate compliance with the law.

4.1 THE EUROPEAN LEGAL FRAMEWORK ON DATA PROTECTION

At the European level, legal protection of personal data is found in article 8 of the European Convention on Human Rights (ECHR)[72] and in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108)[73]. In the European Union, the protection of personal data is enshrined in the Charter of the Fundamental Rights (CFR)[74], article 8, and in article 16 TFEU and 39 of the TEU. As mentioned above in section 3 and 4, the CFR explicitly recognizes a fundamental right to data protection (article 8) as distinct from the right to privacy (art.7). Article 8 states:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access*

70 H. Nissenbaum, (1998).

71 P. De Hert and S. Gutwirth, 2006

72 Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, Rome, 4 November 1950, ETS No. 5.

73 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 181. http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm . The Council of Europe (CoE) adopted, in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No 108) with an additional protocol regarding supervisory authorities and transborder data flows (No 181).22 The Convention applies to both private and public sectors (Article 3(1)), including police and judicial issues, unless a member state opt-outs (Article 3(2)).
Despite being supervised by the CoE these conventions are open not only to Member States of the Council of Europe but also to any other state that wishes to join them. In addition to the convention the CoE has also adopted a number of recommendations directed at Member States concerning data protection.

73 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

74 ibid

to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The EU rules concerning data protection are found both in primary law (i.e., the CFR) and in secondary law (directives and regulations). For the purpose of SYSTEM, the most important pieces of secondary law are two:

1. the General Data Protection Regulation or Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data hereinafter referred as GDPR), is in force since May 25th 2018, it repealed the 1995 Data Protection Directive;
2. the LED Directive or Directive (EU) 2016/680 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, Brussels, 27 April 2016.

While the GDPR has a general scope, applying wherever personal data is processed, the provisions of the LED Directive are exclusive to those processing of personal data carried by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Article 1 of the LED Directive). [75]

In addition to EU rules, personal data processing activities are subject to national provisions. This is particularly important for the LED Directive, whose status ("directive") entails that states adopt implementing domestic transposing legislation. The legal frameworks most relevant to the project SYSRTEM are:[76]

for Germany, Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 to the German Bundesdatenschutzgesetz (BDSG) and the Federal data protection act.

for the Slovak Republic, Act No. 18/2018 Coll. On Protection of Personal Data replacing the former lovak Act No. 122/2013 Coll. On the protection of personal data and that implements Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680.

for Poland, the Personal Data Protection Act of 24 May 2018 As of today, the transposition of the LED Directive is pending.

for Italy, Decreto Legislativo 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016. With regards to the LED Directive the Decreto del Presidente della Repubblica No. 15 of the 15th January 2018.

[75] Fundamental Rigts Agency Handbook on European data Protection law pp.32
[76] See European Judicial Network (EJN), Judicial Library for further references and links to the texts https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=435

4.2 THE DEFINITION OF PERSONAL DATA AND THEIR PROCESSING IN SYSTEM

In order to determine whether SYSTEM processes personal data it is sensible to take a closer look at the definition.

According to Article 4(1) of the GDPR personal data is defined as:

"any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

The LED Directive, in its article 3(1), uses the same definition of personal data as that provided in the GDPR.

In opinion 4/2007 the Article 29 Working Party, the group of data protection authorities tasked to clarify the obscurities of the Directive and, today, the GDPR, clarified the terminology used in the definition: (i) any information (ii) relating (iii) to an identified or identifiable (iv) natural person. [77]

i) "Any information"

the definition of personal data has to be interpreted widely. The nature of personal data covers both objective information (such as chemicals in blood) as well as subjective information (opinions or assessments). From the point of view of content, personal data embraces any sort of information about the person: "[t]he term "personal data" includes information touching the individual's private and family life "stricto sensu", but also information regarding whatever types of activity is undertaken by the individual, like that concerning working relations or the economic or social behaviour of the individual. It includes therefore information on individuals, regardless of the position or capacity of those persons (as consumer, patient, employee, customer etc)"[78]. In addition, with respect to the format of the data, the Article 29 Working Party considers that "the concept of personal data includes information available in whatever form" such as numerical, alphabetical, graphical, or acoustic, kept on a paper, on a computer memory, or videotapes etc".[79]

ii) Second criterion: "Relating to"

The data relates to an individual whenever it is "about" that person and "refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated".[80] Based on this reasoning, the Working Party 29 concludes that data can "relate" to an individual, either because there is a "content" element, a "purpose" element or a "result" element: [81]

i) Content: The "content" element is present in those cases where information is given about a particular person, regardless of any purpose, or the impact of that information on the data subject

[77] Renamed as European Data Protection Board. See Working Party, Opinion 4/2007 on the concept of personal data, Brussels, 20 June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
[78] Ibid pp. 6
[79] Ibid
[80] Ibid
[81] Working Party, Opinion 4/2007 on the concept of personal data, Brussels, 20 June 2007 pp. 10-12

ii) Purpose: That "purpose" element exists when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual.

iii) Result: Despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual when, taking into account all circumstances of the case, their use is likely to have an impact on a certain person's rights and interests. It should be noted that it is no threshold in the intensity of the impact ,it is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.

Meeting this criterion ("relating to") may seem evident in most surveillance activities, for instance in the case of CCTV and facial recognition technologies (content element); in other cases, the relationship between the person and the data collected may be less straightforward.

iii) Third criterion: "To an identified or identifiable person"

According to the Working Party 29, a person is "identified" when she or he can be distinguished among a group of people; a person is "identifiable" despite not being yet identified when " it is possible to do it by all the reasonable means likely to be used by the collector or any other person". Thus, the mere hypothetical chance of identification does not allow to directly consider that person as "identifiable". In order to define someone as identifiable, "*(..) reasonable means likely to be used" to effectively identify the person"* need to be considered.[82] The *"reasonable means likely to be used"*, are to be assessed taking into consideration:

a. the state of the art in technology at the time of the processing and
b. the possibilities for development (also the possibilities of future technologies) during the period for which the data will be processed".[83]

In other words, the identification of a person may not be possible today, but it might become possible in the future thanks to technological advances: in this case, information previously unrelated to natural persons can be considered as a personal data. This interpretation given by the Working Party is particularly relevant in SYSTEM as the analytical capabilities from sensors are subject to constant evolution and refinement.[84]

4.2.1 SPECIAL CATEGORIES OF PERSONAL DATA

According to the GDPR, special categories of personal data are personal data that reveal aspects such as (Article 9(1) GDPR):

> "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or

[82] Article 29 Data Protection Working Party, op. cit., 2007 and Fossoul, Virginie, op. cit., 2008, p.166
[83] Article 29 Data Protection Working Party, op. cit., Rachel L. Finn and David Wright, Laura Jacques and Paul De Hert, Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations (2014)
[84] The art.29 Working Part lists another criterio not relevant for our purposes in SYSTEM: i) Fourth criterion: "a natural person", which implies that the concept of personal data only applies in regard to "physical persons" identified or that are identifiable "living persons" and not to "legal persons" such as civil society, commercial society, or not-profit association. The definition includes groups of natural persons.

sexual orientation".[85]

For these types of data, the Regulation foresees stricter requirements for their processing. The stricter regime provides that processing of such data is forbidden unless in a series of exceptions (art. 9.2 of the GDPR), including the explicit consent of the person concerned.[86] On its part, the LED Directive does not establish a prohibition in principle. The LED Directive allows the processing of sensitive data only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorized by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject (Article 9 of the LED Directive).

SYSTEM does not intend to process special categories of data. However, as mentioned earlier, it cannot be excluded that as a result of its processing activities, the envisaged SYSTEM prototype will be able to facilitate inferences of information on individuals pertaining to those special categories of personal data.

An additional consideration regarding those activities where the project foresees the involvement of urban waste operators. If the consortium decides to inform them about the experiment, then it is likely that data about work status and affiliation to a trade union may be processed by the consortium. In this case, article 88 GDPR will apply and national law.

4.3 PERSONAL DATA PROCESSING PRINCIPLES

These principles must be adhered to in all instances of data processing. The following principles are described in Article 5 of the GDPR.

Lawfulness, fairness and transparency: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation**:** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

Data minimization: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation"); this principle acts to restrict the use of personal data, even where there is a valid legal basis for its collection. Data must be collected for specific, explicitly defined and legitimate purposes and not further processed in a way incompatible with those purposes.[87] In addition, data should be only retained for as long as is necessary to fulfil that purpose. Afterwards it should be deleted.[88]

Data accuracy**:** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy"); measures must be taken to ensure the personal data is of satisfactory quality. This includes ensuring that the data is adequate, relevant and not excessive in relation to the purposes for which it is collected and processed. In addition, data must be accurate and, where necessary, kept up to date. [89]

[85] Article 8(1)
[86] For more in deep analysis on the LED Directive see: J. Sajfert, T, Quintel Data Protection Directive (EU) 201/2018 for police and criminal justice authorities; to be published in in 2019 for Edward Elgar publishing.
[87] Article 5(1)(b) of the GDPR
[88] Article 5(1)(c) of the GDPR
[89] Article 5(1)(d) of the GDPR

***Storage limitation**:* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");[90]

***Integrity and confidentiality**:* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organisational measures.[91]

In addition, article 5.2 of the GDPR establishes the principle of **accountability** to the controller of the personal data, who shall be responsible for, and be able to demonstrate compliance with the mentioned principles.

While substantially sharing the core of its processing principles, the LED Directive presents certain differences with regard to the GDPR that reflect the nature of the objectives underlying the processing activities of this law.[92]

In relation to the purpose limitation principle, the LED Directive introduces the notion of "subsequent processing" instead of referring to the "further processing" of data, used in the GDPR. In that way, the LED Directive recognizes the possibility of re-processing personal data for different purposes than those originating the collection[93]. This expansion in the scope of the processing exists whenever the competent authority determining the new purpose is authorized by law to do so and if such subsequent processing is also deemed necessary and proportionate (Article 4 (2), (3) of the LED Directive).

As for the principle of data minimization, the wording used in the LED Directive appears more flexible when it comes to qualitatively and quantitatively determine which data can be processed by the controller. In that respect Article 4(1)c of the Directive uses the notion of "excessiveness" instead of the traditional concept of "necessity" of the GDPR, which might invite broader interpretations for the justification of the processing activity.[94]

In addition, the LED Directive, in articles 6 and 7, states that that where applicable and as far as possible, controllers should distinguish between different categories of data subjects based on their condition of suspects, convicts, victims, witnesses and between personal data based on facts from that information based on personal assessments. This goes in line with the jurisprudence of the EctHR and the obligation of LEAs to prevent from disproportionate interferences to the rights of data subjects due to indiscriminate retentions of personal data.[95]

[90] Article 5(1)(e) of the GDPR
[91] Article 5(1)(f) of the GDPR
[92] De Hert, Paul, and Vagelis Papakonstantinou, "The data protection framework decision of 27 November 2008, regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for", *computer law & security review,* Vol. 25, 2009, J. See also Sajfert, T, Quintel Data Protection Directive (EU) 201/2018 for police and criminal justice authorities; to be published in in 2019 for Edward Elgar publishing)
[93] Ibid
[94] Ibid
[95] See ECtHR App nos 30562/04 and 30566/04 *S and Marper* v United Kingdom (4 December 2008)2008] discussed above in section 4.

4.3.1 THE LEGITIMATE BASIS PRINCIPLE

The GDPR in Article 5(1) demands that personal data must be "lawfully" (as well as fairly and transparently) processed. Personal data may be processed on one of the grounds described in article 6 (article 9 for special categories of data, mentioned earlier):

> **(a)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes; or
>
> **(b)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> **(c)** processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> **(d)** processing is necessary in order to protect the vital interests of the data subject or another natural person;
>
> **(e)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
>
> **(f)** pro processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Within the context of research projects, usually the most relevant legal basis is the consent of the research participant/data subject. However, consent is a valid basis only when the data subject can genuinely have a say about the processing activities of personal data relating to him or her. The basis of consent is not the appropriate one when

a. no personal data are processed and/or
b. when the data subject does not have a possibility to choose, for instance in the context of criminal investigation or in certain labour relationships, or in surveillance cases.

Unsurprisingly in the LED Directive, the basis for processing is just one, "if [the processing of personal data] is necessary for the performance of a task carried out by a competent authority for the purposes of the Directive and based on Union or Member State law".[96]

4.4 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

In the light of uncertainty concerning the qualification of data processed by SYSTEM as personal data, mentioned earlier in the introductory section, it is important to point out at one of the innovations of the GDPR, the Data Protection Impact Assessment (article 35 GDPR).

[96] Article 8, LED Directive.

In general, impact assessments have been introduced as procedures to respond to new dangers to individual and collective societal concerns or goods.[97] For example, technology assessments (TAs) emerged in 1960s, in the United States, to anticipate the potentially dangerous consequences of the techno-scientific discoveries, such as atomic energy. Environmental Impact Assessments (EIAs) surfaced in response to the degradation of the natural environment. Privacy Impact Assessments (PIAs) and subsequently Data Protection Impact Assessments or DPIAs emerged later, in the 1990s, in response to risks posed by the transition towards a record holding society, now *digital* or information society. After being introduced in common law jurisdictions, such as New Zealand, Australia and Canada, in Europe, the earliest policy for PIA was developed in the United Kingdom in 2007.

The GDPR introduces an obligation to carry out a DPIA in case the processing of personal data "is likely to result in a high risk to the rights and freedoms of natural persons" (Art 35.1). Similar to the GDPR, also the LED directive foresees a duty to carry out a DPIA under article 27.

Art. 35(3) clarifies that DPIA shall in particular be required in the case of:

(a) systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; or
(b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

Points (a and (c resonate with the activities of surveillance supported by SYSTEM technologies.

Data Protection Impact Assessments, as Article 35(7) specifies, shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purpose;

(c) an assessment of the risks to the rights and freedoms of data subjects;

For instance, asking what other uses of data from sewage systems may be possible? Will technology be able to detect foodstuff and single out cultural groups? Will data from the waste disposal sensors be combined with other data sets? Will data be collected to discover the health status of the population?

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

For the purpose of the SYSTEM project, Section 5.1 of the Proposal, Annex 1 Part B, contains the consortium's commitment to conduct an impact assessment on the research activities carried out during the

[97] This section draws from Kloza, D., van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E., & Quinn, P. (2017). Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals.

duration of the project. This process has been explained in the introduction (as well in WP10 description and in Section 5 of the Proposal). For SYSTEM as a prototype hitting the market,
LEAs that will adopt SYSTEM technologies to conduct a "a systematic monitoring of a publicly accessible area on a large scale", are going to have to conduct their *own* data protection or privacy impact assessment. As it was emphasized in the previous chapter, not all impacts of technologies like SYSTEM can be foreseen. They always need to be assessed in the specific context where they are deployed. Furthermore, an increasingly ubiquitous data society means that new possibilities (function creep) can be added. One of the potential outcomes of impact assessment may be the publication of Privacy Impact Notices (PINs), discussed previously in relation to the US context.

Who should conduct such as impact assessment? Impact assessments require a supportive, pro-active environment to bear fruit. In the context of large-scale surveillance operations, representatives from national data protection authorities, police and local authorities may be the ones who will be called upon to assess the rationale, risks, mitigating strategies of surveillance measures adopted.

4.5 RIGHTS OF THE DATA SUBJECT

The GDPR provides in its Chapter III a list of rights ascribed to "data subjects". These are:

- The right to be informed of the processing of his or her personal data (Article 13 and 14 of the GDPR);
- Right to access to an individual's own data (Article 15 of the GDPR);
- The right to rectify incorrect personal data (Article 16 of the GDPR);
- The right to erasure, or the right to be forgotten (Article 17 of the GDPR);
- The right to restriction of processing (Article 18 of the GDPR);
- The right to data portability (Article 20 of the GDPR);
- The right to object on legitimate grounds (Article 21 of the GDPR);
- The right not to be subject to an automated decision making, including profiling (Article 22 of the GDPR);
- The right to lodge a complaint with a supervisory authority (Article 77 of the GDPR);
- Right to an effective judicial remedy against a supervisory authority (Article 78 of the GDPR);
- Right to compensation (Article 82 of the GDPR).

Of particular relevance to the SYSTEM project are:

- the right to be informed of data processing;
- the right to access personal data;
- the right not to be subject to an automated decision making, including profiling;
- The right to object.

As for the LED Directive, Chapter III of the Directive shares to a great extent the set of rights provided in the GDPR, such as communication (article 12), information (article 13), access (article 14 and 15), rectification, erasure and restriction of processing (Article 16). Because of the nature of its scope, the Directive excludes

rights provided in the GDPR that would not be of application, namely the right to be forgotten or the right to data portability.[98]

When addressing the practical implementation of the data subject rights, the LED Directive delineates in a stricter manner the circumstances and the procedures how data subject rights can be exercised. In particular, the Directive foresees the possibility for Member States to adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject (Article 13 (3)), and their right to access (Art. 15(3)) and to obtain a response in regard to the refusal of his or her request for rectification, erasure of restriction of processing and concerning the reasons for such refusal (Art. 16(4)).[99]

Whenever the data subject rights are limited or restricted Member States must provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy. In that respect article 17 of the LED Directive establishes that Member States will need to adopt measures allowing data subjects to address the competent supervisory authority (see above Legal framework).

Finally, and differently from the GDPR in the context of processing operations in automated processing systems, the LED Directive establishes an obligation for controllers to provide for logs to be kept in processing activities such as the collection, alteration, consultation, disclosure including transfers, combination and erasure. The existence of logs and the possibility of their consultation aims to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data (Article 25 of the LED Directive). The objective is to allow for the verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. Both the controller and the processor shall make the logs available to the supervisory authority on request. Accordingly, SYSTEM might be required to set up such log capacity in its data processing structure.

The right to be informed is particularly important in the research phase of SYSTEM, where individuals **might** have a right to know that they are in an area where sensors are being placed and tested (i.e. for research purposes is occurring). In light of this right, the deployment of SYSTEM might require informing individuals about the collection and processing of information relating to air emissions, garbage and sewage. That being said, also the right to be informed is not absolute. It must be must be balanced against:

a. the security requirements (related to the risk that sensors are stolen or damaged) and
b. the possibility that public awareness may conflict of hinder the attainment of the project's objectives.

It may be enough to inform citizens, for instance informing elected representatives, or putting public notices in areas where prototypes are being tested or simulations are being made. In other cases, for instance when surveillance involve workers, such as urban waste operators. In those cases, it might be necessary to assess whether it is necessary to a. fully inform workers' unions and the workers involved and, b. to obtain the consent of the former before any demonstration, according to national legislation and practices. In this event, the consent of workers will also need to ensure that unionised workers enjoy a genuine choice to decide their say on the processing activities of personal data relating to him or her (Article 88 of the GDPR)[100].

[98] J. Sajfert, T, Quintel Data Protection Directive (EU) 201/2018 for police and criminal justice authorities; to be published in in 2019 for Edward Elgar publishing. pp.11
[99] Ibid pp. 14
[100] Article 88 of the GDPR ,see also recital 155 of the GDPR.

In any case it should be borne in mind that any restriction in the right to information of data subjects will need to be grounded and justified under necessity and proportionality criteria in a democratic society (see article 13(3) of the LED Directive).[101] These aspects will be further addressed in D10.2.

4.6 CONCLUSIONS

- The project and the technology to be developed is not intended or meant to directly process personal data as information related to identified or identifiable individual/s. However, it cannot be excluded the possibility that as a result of its correlation with other data sets, individuals residing in certain areas might potentially be singled out.
- It cannot be excluded that as a result of its processing activities, the envisaged SYSTEM prototype will be able to facilitate inferences of information on individuals pertaining to special categories of personal data.
- Function creep: the notion of function creep occurs in those situations where an item, process, or procedure designed for a specific purpose ends up serving another".[102] In SYSTEM the risks are twofold. On a first hand to provide the modulable nature in the equipment of sensors, it could occur that despite SYSTEM technology is being developed to "sense" specific elements, this could be later expanded to others. The risk of "further processing" by authorities of the data collected needs to be highlighted.
- The right to be informed is particularly important in the research phase of SYSTEM, where individuals might have a right to know that they are in an area where sensors are being placed and tested (i.e. for research purposes is occurring). In light of this right, the deployment of SYSTEM might require informing individuals about the collection and processing of information relating to air emissions, garbage and sewage.
- LEAs that will adopt SYSTEM technologies will fall under the obligation to conduct an *own* data protection or privacy impact assessment. (a systematic monitoring of a publicly accessible area on a large scale.
- Within the context of research project, explicit consent may be required when data subjects have a genuine choice and can have a say about the processing activities of personal data relating to him or her.

[101] Bäcker, Matthias and Gerrit Hornung, "Data processing by police and criminal justice authorities in Europe - The influence of the Commission's draft on the national police laws and laws of criminal procedure",
Computer Law & Security Review, Vol. 28, 2012, p. 632.
[102] see www.functioncreep.blogspot.be

5 PROFILING AND DISCRIMINATION OF CERTAIN GROUPS

Two legal scholars, Mireille Hildebrandt and Serge Gutwirth draw the attention to the relationship between surveillance, privacy and profiling. They claim that profiling techniques – empowered by the possibilities afforded by modern technologies – permits practices of social sorting and discrimination between the members of certain groups. Based on the collection aggregation and storage of data, profiling techniques foster the appearance of correlations, giving rise to the constitution of categories with specific attributes. For the one interpreting the information, those categories are subsequently labelled into groups and the set of attributes to them conferred become the group's profile[103]. On a similar line, Schermer stresses how profiling techniques " can be used to identify and represent a nonhuman subset (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group of a category"[104]

The GDPR (article 4) and the LED Directive (article 3) define profiling as:

"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

According to the LED Directive, the decisions based solely in automated processing, including profiling, are prohibited unless authorized by Union or Member State law (Article 11 of the LED Directive). Furthermore, and differently from the respective provision of the GDPR, Article 11(3) of the LED Directive expressly prohibits any sort of profiling based on special categories of data when this processing can lead to discriminatory impacts on natural persons.[105] In order words, profiles cannot be solely built upon data pertaining to special categories of data (see above.).

The European Data Protection Supervisor (EDPS) has highlighted the technical, legal and ethical challenges derived from profiling techniques and computerized data analysis, especially when it comes to their accuracy and transparency[106]. It warns against the risk that pervasive monitoring and profiling of certain communities could potentially result in feelings of constant surveillance.
Potentially, the implementation of sensor technologies such as SYSTEM enable competent authorities to take decisions on the basis of aggregated data capable of mapping the characteristics of certain areas and thus inferring the behaviours of citizens there residing. There is a risk that this might potentially result in a more fine-grained discrimination and classification of citizens and communities, or in other words an enhancement of social sorting practices[107]. In addition, due to the pretended objectivity of technology, it is sensible to consider whether SYSTEM could legitimize discriminatory practices both prior the deployment of the sensors and in the operational phase, as result of the generation and interpretation of community profiles. (see next paragraph).

[103]Gutwirth, Serge and Mireille Hildebrandt, "Profiling thenEuropean Citizen", Cross-disciplinary Prespectives, Springer(2009), pp.200
[104] Schermer, Bart W., "The Limits of Privacy in Automated Profiling and Data Mining", *Computer Law & Security Review*, Vol. 27, 2011. pp.45
[105]See Committee of Ministers of the Council of Europe, Recommendation Rec(2001)10 on the European Code of Police Ethics, 19 September 2001 and Explanatory Memorandum.
[106] See for instance EDPS call for consistent improvements in the EU approach on matters concerning the Area of Freedom Security and Justice; <accessible at https://edps.europa.eu/press-publications/press-news/press-releases/2017/edps-calls-consistent-improvements-approach-eu_en
[107] Lyon, D. *Surveillance Studies: An Overview*. Cambridge: Polity Press (2007). See aslo Lyon D. *Surveillance as Social Sorting, Privacy, risk and digital discrimination*, New York 2011

5.1 THE RIGHT NOT TO BE DISCRIMINATED AGAINST IN POLICE OPERATIONS

As anticipated at the end of the previous paragraph, surveillance technologies such as SYSTEM can increase the risk that police operations target certain groups or communities: placing sensors only in some areas and using evidence gathered from sensors (installed only in certain areas) may reinforce stereotyping or stigmatization of certain groups or communities (living in those areas). These possibilities must consider that human rights law has recognised that stigmatization and stereotyping can be violation of the prohibition of discrimination. According to the European Court of Human Rights, a difference in treatment is discriminatory if "it has no objective and reasonable justification", that is, if it does not pursue a "legitimate aim" or if there is not a "reasonable relationship of proportionality" between the means employed and the aim sought to be realized". Where the difference in treatment is based on race, colour or ethnic origin, the notion of objective and reasonable justification must be interpreted as strictly as possible[108].

In *Lingurar v Romania*[109], the ECtHR discussed whether the police actions targeting a Roma community had been based on extrapolations from reports supporting racial stereotypes. It was observed how authorities had automatically linked ethnicity to criminal behaviour, resulting into an ethnic profiling of discriminatory nature[110]. As a result, the Court ruled that there had been a violation of Article 14 of the ECHR on the prohibition of discrimination in conjunction with a violation of Article 3 of the ECHR concerning the prohibition of inhuman or degrading treatment.[111]

The discriminatory concerns on disadvantaged neighbourhoods attached to the use of modern surveillance technologies has been observed with the deployment and operation of CCTV systems.[112] In that respect, Rachel Finn and David Wright have documented how certain groups tend to become disproportionality targeted by CCTV operators in comparison to their presence in population.[113] Similarly, Coleman and McCahill warns that surveillance can reinforce "existing social positions, particularly positions of marginalization along lines of race, class, gender, sexuality and age."[114]

5.2 CONCLUSION

- The implementation of sensor technologies such as SYSTEM might potentially result in a more fine-grained discrimination and classification of citizens and communities, or in other words an enhancement of social sorting practices.

- There is a risk that SYSTEM processing activities could potentially lead to increased stigmatisation of certain groups.

[108]Lingurar v Romania § 68, see also D.H. and Others v. the Czech Republic [GC], no. 57325/00, § 196, ECHR 2007-IV).
[109] The case Lingurar v. Romania (application no. 48474/14) concerned a raid in 2011 by 85 police and gendarmes on the Roma community in Vâlcele (Romania). In its committee judgment in the case the European Court of Human Rights unanimously held, that there had been: a violation of Article 3 (prohibition of inhuman or degrading treatment) of the European Convention on Human Rights as concerned the ill-treatment of the applicant family during the raid, and two violations of Article 14 (prohibition of discrimination) in conjunction with Article 3 because the raid had been racially motivated and the related investigation had been ineffective. The Court found that the applicants had been targeted because the authorities had perceived the Roma community in general as criminal. That had amounted to ethnic profiling and had been discriminatory.
[110] Lingurar v Romania § 76
[111] ibid § 78
[112] Finn, Rachel, and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications", Computer Law & Security Review, Vol. 28, No. 2, 2012, pp. 184-194
[113]Ibid
[114] Rachel L. Finn and David Wright, Laura Jacques and Paul De Hert, Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations (2014)

6 SYSTEM AND THE USE OF DRONES

In order to perform air monitoring, SYSTEM foresees the equipment of sensors in remotely piloted aircrafts (hereinafter RPAS or drones). Concretely SYSTEM will use drones for the air monitoring of household's waste utility networks with the capacity to detect gases evolved from the waste disposed from drug manufacturing, with the ultimate objective of pointing out potential markers of clan labs.

In Europe, the legal framework of RPAS is established by the European Union Aviation Safety Agency (EASA) and the national Civil Aviation Authorities (CAAs). With a mandate to craft airworthiness standards and to draft implementing rules on civil aviation, EASA represents the "centrepiece of the European Union's strategy for aviation safety."[115] Both EASA and the relevant CAAs decide upon the viability of drone's applications, they enact aviation and safety rules and grant permits to governmental, commercial and individual operators. [116] The EU has recently licenced Regulation (EU) 2018/1139 which sets the common rules in the field of civil aviation.[117] It provides for common rules for a common European register of drones, which would include also a list of certified drone pilots. In addition, national laws relevant to telecommunications, CCTV and police surveillance activities might also applicable to drone's usage.

As the European RPAS Steering Group's Roadmap has stated, the use of drones by police and government operators poses a risk to the rights to respect for private life and to the protection of personal data[118]. In the case of drones used for surveillance purposes, the nature and intensity of the risks to the rights and freedoms of individuals depend on the specific capacities of the sensors installed on the drone.[119] Unlike sensors in sewage and trash, which are static, drones are by definition mobile: if they are equipped with cameras they can be considered as enhanced mobile CCTV systems. Accordingly, drones pose risks similar to those created by CCTV cameras on privacy; in addition, drones are fit to perform target monitoring, thus posing the risk of discriminating certain individuals or groups.

The Article 20 Working Party in its opinion 01/2015 on the data protection implications stemming from the use of drones has stated that the use of this technology should:

1. Be conducted for purposes that are laid down in relevant legislation.

2. Not be used for indiscriminate surveillance, bulk data processing, data pooling and,

3. Be surrounded by limits to the use of profiling techniques/capacities related to the use of drones, as to prevent them from becoming pervasive or being used for signalling targets based on data analysis.

[115] https://www.easa.europa.eu/the-agency/faqs/agency#category-about-easa

[116] For more in depth analysis on the legal framework of drones please see VUB co authored Study :Rachel L. Finn and David Wright, Laura Jacques and Paul De Hert, Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations (2014)

[117] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

[118] European RPAS Steering Group, Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, June 2013http://ec.europa.eu/enterprise/sectors/aerospace/uas/ ; See also recital 31 of the 2018/1139 Regulation.

[119] Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations:Privacy issues associated with RPAS (pp. 24).

For the purpose of SYSTEM, it must be noted that the use of drones in the project is limited geographically to controlled environments, such as police training fields, or partners' owned buildings. At the time of the writing of this deliverable, no demonstration in non-controlled environment using drones will be carried in cities or any public urban settings. In principle, SYSTEM's drones do not include a camera capable of taking images of individuals. For the purpose of SYSTEM test, drones will carry a thermal camera only (see references to Kyllo case in section 3). If there are cameras on the drones, the impact on the data protection framework needs to be revisited.

6.1 CONCLUSION

The risk stemming from the use of drones in SYSTEM depend on the specific capacities of the sensors installed on the drone, which needs to be defined clearly before an assessment is possible.

At the time of writing, the use of drones in the project is limited geographically to controlled environments, such as police training fields, or partners' owned buildings. This aspect will be considered din D10.2 and following impact assessment or risk reports.

7 General Rules Concerning Due Process in Criminal Proceedings

Taking into consideration the potential application of SYSTEM by law enforcement and public authorities it is necessary to consider how information obtained through sensors might be used as evidence in criminal proceedings and how, as a result, might interact with the rules governing due process.

There is a general disparity of resources between suspects and accused, on one hand, and the state's criminal justice machinery (prosecutor and LEAs).[120] Given this asymmetry, rules exist to restrain the state and ensure that it operates in a proper, fair, way. The idea of 'due process' is central to this. It ensures that proper procedures exist so as to ensure that evidence is collected, processed and presented in a valid way to the courts.[121]

Article 6 of the European Convention on Human Rights (which is binding in most European Legal systems) states:

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. […].

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law

3. Everyone charged with a criminal offence has the following minimum rights:
   (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
   (b) to have adequate time and the facilities for the preparation of his defence;
   (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
   (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
   (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 6 itself does not contain explicit mention of the gathering of evidence. Nor does it describe specific rules that are applicable to the gathering of evidence. The ECtHR has stated that such specific rules are a matter for Member States of the CoE to decide upon for themselves.[122] There are however a number of implicit general principles which the ECtHR has recognized apply to the collection and use of evidence in criminal proceedings and may be likely to be relevant to SYSTEM. [123]

[120] J. Jackson and S. Summers, *The Internationalisation of Criminal Evidence* 2012).

[121] J. Ingle, Overview: Criminal Law, Evidence and Proceedure', *Cambridge Journal of International and Comparative Law*, 3,((2014) pp. 265-268

122 CASE OF SCHENK v. SWITZERLAND (Application no.10862/84)

123 For a good analysis see "RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW" Council of Europe/European Court of Human Rights, 2014 Available at http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf See also: J. Ingle, (2014).

7.1 FAIRNESS

Evidence must have been collected lawfully, meaning that it must not be collected in a way that violates the legal rights of the defendant. This might include individual privacy rights as discussed in section 4. Most importantly, in "determining whether the proceedings as a whole were fair, […] it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use."[124]

7.2 QUALITY

Article 6 ECHR also has implications in terms of the quality of evidence that is used. In criminal proceedings, the quality of the evidence must be examined, in addition to the way it was obtained. Tribunals must give consideration to anything that would create doubts as towards reliability or accuracy. This is particularly important where certain evidence represents the primary or sole case being made by the state. Where the quality of the evidence in question is weak, supporting evidence of another kind should also be required.[125]

7.3 ISSUES RELATED TO ENTRAPMENT

As mentioned in chapter 5, the ECtHR has accepted that covert surveillance is a necessary part of police investigation into criminal activity of a serious nature. The use of concealed surveillance itself is not therefore itself (if conducted properly) in violation of the law.[126] However, the right to a fair trial nevertheless applies to all types of criminal offence, from the most straightforward to the most complex. [127] In this context, the Court has stated that the police whilst permitted to act undercover may not act in a way that is itself intended to incite criminal activity.[128]

7.4 APPROPRIATE OVERSIGHT

Whilst the ECtHR has accepted the possibility of covert surveillance activities, it has stated that there is a potential to infringe upon individual rights. In order to reduce this risk, such activities should be supervised by suitable individuals or organizations. This may include investigatory judges or in appropriate circumstances prosecutors.[129]

7.5 CONCLUSION

- Taking into consideration the potential application of SYSTEM it is recommended to consider how the information obtained through sensors might be potentially used as evidence in criminal proceedings and how, as a result, might interact with the rules governing due process.

- Foreseeing the utilization of SYSTEM by law enforcement and public authorities it is sensible to assess the rules governing the procedure, how the technology is going to be deployed and how the information obtained might be used in criminal proceedings and how, as a result, it might interact with the laws governing due process**.**

[124] RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW" Council of Europe/European Court of Human Rights, 2014 p 24
125 CASE OF BYKOV v. RUSSIA (Application no. 4378/02), CASE OF JALLOH v. GERMANY (Application no.5481/00)
126 CASE OF RAMANAUSKAS v. LITHUANIA (Application no.74420/01)
127 RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW" Council of Europe/European Court of Human Rights, 2014 p 25
128 CASE OF KHUDOBIN v. RUSSIA(Application no. 59696/00)
129 CASE OF BANNIKOVA v. RUSSIA (Application no.18757/06)

8 BIBLIOGRAPHY

- C. Bennet, In defence of privacy: The concept and the regime', Surveillance and Society, 8,(4) (2011) pp. 485-496
- L. Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', International Journal of Law and Information Technology, 6,((1998) pp.
- A. Caligiuri and N. Napoletano, '*The Application of the ECHR in the Domestic Systems'*, (Brill, 2010)
- J. Crocker, B. Major and C. Steel, 'Social Stigma',in: D. Gilbert, S. Fiske and G. Lindzey (eds.), Handbook of social psychology, (McGraw-Hill: Boston, 1998)
- N. Daniels, Justice, health and healthcare', American Journal of Bioethics, 1,(2) (2001) pp. 2-16
- P. De Hert and S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacety of the Individual and Transparency of the Power',in: E. Claes, A. Duff and S. Gutwirth (eds.), Privacy and the Criminal Law, (Intersentia: Antwerp - Oxford, 2006)
- P. De Hert, S. Gutwirth, A. Moscibroda, D. Wright and G. Gonzalez Fuster, Legal safeguards for privacy and data protection in ambient intelligence', Personal and Ubiqutious Computing, 13,(6) (2009) pp. 435-444
- P. De Hert and V. Papakonstantinou, The Police and Criminal Justice Data Protection Directive: Comment and Analysis', Society for Computers & Law. Computers & Law Magazine, 22,(6) (2012) pp. 21-25
- J. Dovidio, B. Major and J. Crocker, 'Stigma: Introduction and Overview',in: T. Heatherton, R. Kleck, M. Hebl and J. Hull (eds.), The Social Psychology of Stigma, (Guilford Press: New York, 2000)
- A. Etzioni, '*The Limits of Privacy'*, (Basic Books, New York, 1999)
- F. Fontanelli, The European Union's Charter of Fundamental Rights two years later ', Perspectives on Federalism, 3,(3) (2011) pp. 22-47
- S. Gutwirth, '*Privacy and the Information Age'*, (Rowman and Littlefield, New York, 2002)
- S. Gutwirth and P. De Hert, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power',in: E. Claes, A. Duff and S. Gutwirth (eds.), Privacy and Criminal Law, (Intersentia: Antwerp, 2006)

- S. Gutwirth, R. Leenes, P. De Hert and Y. Poulletn, '*European Data Protection: In Good Health?*', (Springer, 2012)
- K. Heatherton, Hebl, Hull, '*The Social Pyschology of Stigma*', (Guildford Press, New York, 2000)
- C. Held, J. Krumm and R. Schenke, Intelligent Video Surviellance', Computer, 45,(3) (2012) pp. 83-84
- J. Ingle, Overview: Criminal Law, Evidence and Proceedure', Cambridge Journal of International and Comparative Law, 3,((2014) pp. 265-268
- J. Jackson and S. Summers, '*The Internationalisation of Criminal Evidence*', (Cambridge University Press, 2012)
- H. Keller and A. Stone Sweet, '*A Europe of Rights: The Impact of the ECHR on National Legal Systems*', (Oxford University Press, Oxford, 2008)
- D. Klitou, '*Privacy Invading Technologies and Privacy by Design*', (Springer, 2014)
- E. Kosta and C. Cuijpers, 'The Draft Data Protection Regulation and the Development of Data Processing Applications',in: M. Hansen, J. Hoepman, R. Leenes and D. Whitehouse (eds.), Privacy and Identity Management for Emerging Services and Technologies (Volume 421 of the series IFIP Advances in Information and Communication Technology), (Springer: 2014)
- V. Kosta, '*Fundamental Rights in EU Internal Market Legislation*', (Bloomsbury Publishing, 2015)
- K. Lenarts, Exploring the Limits of the EU Charter of Fundamental Rights', European Constitutional Law Reivew, 8,(3) (2012) pp. 375-403
- R. Macroy, '*Regulation, Enforcement and Governance in Environmental Law*', (Bloomsbury Publishing, 2014)
- K. Moller, Proportionality: Challenging the Critics', International Journal of Consitutional Law, 10,(3) (2012) pp. 709-731
- A. Mowbray, The Creativity of the European Court of Human Rights', Human Rights Law Review, 5,(1) (2005) pp. 57-79
- M. Neocleous, Security, Liberty and the Myth of balance: towards a critique of security politics', Contemporary Political Theory, 6,(2) (2007) pp. 131-149

- H. Nissenbaum, Protecting Privacy in the Information Age: The problem of Privacy in Public', Law and Philosophy, 17,((1998) pp. 559-596
- H. Nissenbaum, Privacy as Contextual Integrety', Washington Law Review, 79,((2004) pp. 104-139
- R. Post, Three Concepts of Privacy', Faculty Scholarship Series, Faculty Scholarship Series,(Paper 185) (2001) pp.
- P. Quinn and P. De Hert, Self respect—A "Rawlsian Primary Good" unprotected by the European Convention on Human Rights and its lack of a coherent approach to stigmatization?', The International Law of Discrimination and the Law, 14,((2014) pp. 19-53
- P. Quinn, A. Habbig, E. Mantovani and P. De Hert, The Data Protection and Medical Device Frameworks ? Obstacles to the Deployment of mHealth across Europe?', European Journal of Health law, 20,(2) (2013) pp. 185-204
- J. Rawls, '*A Theory of Justice'*, (Harvard Press, MA, 1971)
- B. Rossler, '*The Value of Privacy*', (Polity Press, Cambridge, 2005)
- A. Rouvroy and Y. Poullet, 'The Right to Informational Self-Determination and the Value of Self Development: Researching the Importance of Privacy for Democarcy',in: S. Gutwirth, Y. Poullet, P. De Hert, C. Terwangne and S. Nouwt (eds.), Reinventing Data Proteciton, (Springer: 2009)
- P. Schaar, Privacy by Design', Identity in the Information Society, 3,(2) (2010) pp. 267-272
- J. Seddon and W. Currie, Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance', Health Policy and Technology, 2,(4) (2013) pp. 229-241
- D. Solove, '*Understanding Privacy.'*, (Harvard University Press, Cambridge, 2008)
- R. Taylor, Rawls's Defense of the Priority of Liberty: A Kantian Reconstruction', Philosophy & Public Affairs, 31,(3) (2003) pp. 256-271
- R. Weber, Transborder data transfers: concepts, regulatory approaches and new legislative initiatives', International Data Privacy Law, doi: 10.1093/idpl/ipt001,((2013) pp.
- R. Weber and D. Staiger, Bridging the Gap between Individual Privacy and Public Security', Groningen Journal of International Law, 2,(2) (2014) pp. 14-32

- D. Wright, S. Gutwirth, M. Friedewald, E. Vildjiounate and Y. Punie, '*Safeguards in a World of Ambient Intelligence*', (Springer, 2008)

- Bart van der Sloot Aviva de Groot, The Handbook of Privacy Studies: An Interdisciplinary Introduction. Amsterdam University Press, (2019)

- R. Post, Three Concepts of Privacy', Faculty Scholarship Series, Faculty Scholarship Series,(Paper 185) (2001) pp.

- R. Weber and D. Staiger, Bridging the Gap between Individual Privacy and Public Security', Groningen Journal of International Law, 2,(2) (2014) pp. 14-32 Staiger, (2014).

- Rachel L. Finn and David Wright, Laura Jacques and Paul De Hert, Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations (2014), p. 130-135

- Froomkin, A. Michael. "Privacy Impact Notices to address the privacy pollution of mass surveillance." In Timan, Tjerk, Bryce Clayton Newell, and Bert-Jaap Koops, eds. Privacy in public space: Conceptual and regulatory challenges. Edward Elgar Publishing, 2017.p.185

- De Hert, Paul, and Vagelis Papakonstantinou, “The data protection framework decision of 27 November 2008, regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for”, computer law & security review, Vol. 25, 2009

- J. Sajfert, T, Quintel Data Protection Directive (EU) 201/2018 for police and criminal justice authorities; to be published in in 2019 for Edward Elgar publishing).

- Bäcker, Matthias and Gerrit Hornung, “Data processing by police and criminal justice authorities in Europe - The influence of the Commission’s draft on the national police laws and laws of criminal procedure”, Computer Law & Security Review, Vol. 28, 2012, p. 632.

- Lyon, D. Surveillance Studies: An Overview. Cambridge: Polity Press (2007). See aslo Lyon D. Surveillance as Social Sorting, Privacy, risk and digital discrimination, New York 2011

- Finn, Rachel, and David Wright, “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications”, Computer Law & Security Review, Vol. 28, No. 2, 2012, pp. 184-194