FP7 – SEC- 2011-284725

SURVEILLE

Surveillance: Ethical issues, legal limitations, and efficiency

Collaborative Project

SURVEILLE Deliverable 2.4
PAPER ESTABLISHING CLASSIFICATION OF TECHNOLOGIES ON THE BASIS OF THEIR INTRUSIVENESS INTO FUNDAMENTAL RIGHTS

Due date of deliverable: April 30th, 2013 (month 15)

Actual Submission date: 30 April 2013

Start date of project: 01.02.2012 Duration 39 months

SURVEILLE Work Package number and lead: WP2 led by Tom Sorrell (Warwick)

Author : Maria Grazia Porcedda (EUI)

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only members of the consortium (including the Commission Services)	

Executive summary

- This deliverable appraises the impact of surveillance technologies on fundamental rights as understood in the EU. Surveillance is defined in the SURVEILLE project as "the targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future."

- The technologies chosen are a selection of those listed in SURVEILLE Deliverable D2.1. Here, three elements are considered: the target (person/animal, object, sound, motion, data, chemical substance); their covert/overt use; and the abstract function(s) they perform, based on the description provided by the vendor and listed in D2.1.

- The following fundamental rights are analysed in detail: non-discrimination, privacy (private and family life), expression and information, data protection, thought, conscience and religion, assembly and association, and freedom of movement. Other rights have been considered: human dignity, liberty and security, health, equality, fair working conditions, effective remedy and fair trial, and prohibition of torture, inhuman and degrading treatment. The legal instrument of direct reference is the Charter of Fundamental Rights of the European Union.

- Intrusiveness has both an abstract and a contextual dimension. The contextual legal assessment of intrusiveness into fundamental rights is usually performed *ex post facto* and in context in courtrooms. However, existing court judgments provide limited guidance as to how to appraise the impact of security technologies on fundamental rights, given that the gravity of the impact is tied to the nature of the right - absolute or relative - and to the use of such rapidly evolving tools.

- Moreover, a contextual legal assessment of intrusiveness of a technology into fundamental rights can only be performed with regard to a specific use (preventive/investigative), in a specified jurisdiction, in connection with a clear legal basis. Since SURVEILLE is a European project, the analysis is primarily geared towards the developments at the European level, and the Area of Freedom, Security and Justice as the relevant framework. Consequently, issues where the technology is deployed only or mainly by national authorities in the exercise of their exclusive competences are not given priority. Instead, we apply a EU nexus and we focus on the abstract dimension of intrusiveness.

- To this end, this deliverable freely draws from the work done in the context of human rights indicators on attributes of fundamental rights. This approach allows gaining in depth and granularity of the analysis, especially with regard

to the interrelatedness of fundamental rights, thus balancing the loss of contextual reference. The impact or intrusiveness into the attributes of fundamental rights is evaluated on the basis of functions, objectives and covert/overt use of the technology.

- Furthermore, the use of attributes allows highlighting potential core areas of fundamental rights, the intrusion into which would be impermissible even for rights that are relative or qualified, i.e. as such are subject to permissible limitations. The analysis tries to capture potential 'core' areas and highlight them.

- The categorization of the intrusiveness of surveillance technologies tries to capture the different impacts deriving from covert or overt use, the chilling effect on the exercise of fundamental rights, the interrelated effects, as well as intrusion into core areas. However, the categorization does not provide indications as to the technologies to be preferred. The methodology outlined here will in future SURVEILLE work be combined with an economic and ethical cost model, and applied to realistic scenarios of the use of surveillance technologies by law enforcement officials, with a view to proposing a tool for choosing a specific technology.

Table of Contents

Table of abbreviations

AFSJ	Area of Freedom, Security and Justice
ECHR	European Convention on Human Rights
ECJ	Court of Justice of the European Union (Luxembourg)
ECtHR	European Court of Human Rights (Strasbourg)
EHRC	Equality and Human Rights Commission (United Kingdom)
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
FRA	Fundamental Rights Agency
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
LEAs	Law Enforcement Agencies
OHCHR	Office of the High Commissioner for Human Rights (United Nations)
OECD	Organization for Economic Cooperation and Development
PbD	Privacy by Design
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations

1 Introduction[1]

The objective of this SURVEILLE deliverable is to establish a 'classification' of technologies based on their intrusiveness into fundamental rights. The objective requires some specifications.

First, the deliverable reviews 'surveillance' technologies and systems that are being used in the European Union (hereafter EU) for the purposes of preventing, investigating and prosecuting terrorism and fighting against serious crime. 'Surveillance' technologies and systems are understood as "(the use of) any human-made devices in surveillance" and "the intentionally designed combination of surveillance technology and its use by human beings", respectively.[2] Surveillance, in turn, is defined as "the targeted or systematic *monitoring* of persons, places, items, means of transport or flows of information, in order to *detect* specific, usually criminal, forms of conduct, or other *hazards*, and enable, typically, a *preventive, protective or reactive* response, or the collection of data for preparing such a response in the future."[3]

Second, the deliverable reviews the intrusiveness into fundamental rights as understood in the EU, which is defined as a cost, among others (see *infra* 1.1), of the use of such technologies. Fundamental rights include "privacy, data protection, non-discrimination, human dignity, personal liberty, freedom of movement, freedom of expression and freedom of thought, conscience and religion. Due to the interdependence of all human rights, however, also other parts of their normative catalogue need to be taken into account."[4] It should be noted that the expressions 'fundamental' and 'human' rights are equivalent, and are used interchangeably in this text.

Third, the legal meaning of 'intrusiveness' has two facets, permissible (legal) and impermissible (illegal). On the one hand, an intrusive technology would be permissible (legal) if it impacted upon a qualified right within the margins of the scope of a test for permissible limitations. This type of intrusiveness would be called a limitation or restriction of a fundamental right. On the other hand, an intrusive technology would be impermissible if it impacted upon a qualified right beyond the scope of a permissible limitations test, or if it impacted on an absolute right. The latter is a small group of rights that can be limited under no

[1] The author would like to thank the many contributors who have made the successful completion of this deliverable possible: Jonathan Andrew (EUI), Michelle Cayford (TU Delft), Martyn Egan (EUI), Jonathan Herington (UoB), Juha Lavapuro (Helsinki), Tuomas Ojanen (EUI), Elisa Orrú (ALU-FR), Martin Scheinin (EUI) – who also contributed with substantive additions to chapter 3–, Tom Sorell (UoW), Coen Van Gulijk (TU Delft), and the many participants in the SURVEILLE 3rd Consortium Meeting held in Florence on 10th April 2013.

[2] Surveille Project Consortium, 'Description of Work of the Surveille Project. Surveillance: Ethical Issues, Legal Limitations and Efficiency', (Seventh Framework Programme, European Union, 2011) at 5.

[3] Ibid.

[4] Ibid., at 5-6.

circumstances. Appraising such intrusiveness of surveillance technologies on rights requires establishing an adequate methodology (see *infra*). The ethical assessment, although partly incorporated in the analysis of legality, is performed in other deliverables of the SURVEILLE project.

1.1. Purpose of the classification of intrusiveness into fundamental rights

This deliverable is part of Work Package 2 of the SURVEILLE project, whose objective is to assess the efficiency, legal limitations and ethical issues of surveillance technologies and systems.[5]

The classification of surveillance technologies with regard to their intrusiveness into fundamental rights is an objective of the project, and an intermediate step towards the creation of a refined matrix of surveillance technologies deployed and under development in the EU (work package 2). The criteria used for such mapping are manifold. They include: the security threat addressed (with input from an end-user panel); the phase of the security life cycle (prevention, protection, preparation, response and recovery); the modality of use (covert/overt); the user (state/non-state actor); the purported effectiveness, as described by vendors; and the actual effectiveness. It also considers the benefits, defined as "the delivery of improved security,"[6] and the costs. The latter are understood as "economic costs, negative public perceptions, and negative effects on behaviour, and infringement of fundamental rights," [7] and include the consideration of 'privacy by design' (hereafter PbD) features (as a mitigating effect).
Explaining why the assessment of the intrusiveness into fundamental rights, understood as a cost, is relevant is the objective of the next section.

1.1.1 A tool for policy-making[8]

Appraising the intrusiveness of surveillance technologies into fundamental rights is crucial because of the EU's approach to decision and policy-making. The Commission has decided that the legislation, draft instruments, implementing acts (pursuant to article 291 of the Treaty on the Functioning of the European Union, TFEU) and delegated acts (pursuant to article 290 TFEU) it proposed must be checked for substantive [9] compliance with fundamental rights

[5] "The analysis will build further upon work done in the DETECTER project to refine an earlier classification of surveillance technologies." Ibid., at 13.
[6] Ibid.
[7] Ibid., at 4.
[8] Parts of this section have been based on research conducted by the author within the SurPRISE project: Maria Grazia Porcedda, Mathias Vermeulen, and Martin Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming', (Florence: European University Institute, 2013).
[9] European Commission, 'Report on the Practical Operation of the Methodology for a Systematic and Rigorous Monitoring of Compliance with the Charter of Fundamental Rights. Com(2009) 205 Final', (Brussels, 2009).

throughout their life cycle. This goes from the initiation of a legislative proposal by the lead department and its preparatory consultations[10] to the *ex post* evaluation.[11] Moreover, the Commission[12] strives to foster a cross-institutional "fundamental rights culture", whereby rights are both guidance for, and limitations to, the Union's activity.[13]

This is unsurprising in the light of the changes operated by the Lisbon Treaty. In fact, the EU is "founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights"[14] and human rights constitute "general principles' of the Union's law".[15] It is also true in the Area of Freedom, Security and Justice (hereafter AFSJ), which pursues the creation of an internal, borderless area, protecting citizens' fundamental rights, guaranteeing a high level of security and fostering access to justice, in respect of the different legal systems and traditions of Member States.[16] Such an approach is reflected in the five-yearly programmatic document for the AFSJ, according to which the EU's political priority is to "ensure respect for fundamental freedoms and integrity while guaranteeing security".[17]

The underlying value of (the collective goal of) 'security' is the promotion of "human rights, democracy, peace and stability."[18] It is a means to pursue one of the objectives of general interest of the EU (the promotion of peace, the preservation of its traditions and citizens' well-being[19]). The relationship between rights and security is formulated as a question of how far the collective

[10] European Commission, 'Communication. Compliance with the Charter of Fundamental Rights in Commission Legislative Proposals. Methodology for Systematic and Rigorous Monitoring. Com(2005) 172 Final', (Brussels, 2005), 8.
[11] European Commission, 'Communication, 'Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union'. Com (2010) 573/4', (Brussels, 2010).
[12] Members of the European Commission pronounce before the Court of Justice a solemn undertaking to respect the EUCFR. Ibid.
[13] European Commission, 'Report on the Practical Operation of the Methodology for a Systematic and Rigorous Monitoring of Compliance with the Charter of Fundamental Rights. Com(2009) 205 Final'. To this end, the Commission undertook to monitor the compliance with the EUCFR of the two legislative branches, and to initiate annulment proceedings before the Court of Justice if fundamental rights are infringed. The drafting of Annual Reports on fundamental rights in the domestic and external action is also part of this culture. See Dg Justice, '2010 Report on the Application of the Eu Charter of Fundamental Rights', (Brussels: European Commission, 2011), Dg Justice, '2011 Report on the Application of the Eu Charter of Fundamental Rights', (Brussels: European Commission, 2012).
[14] Article 2 TEU. 'Consolidated Versions of the Treaty on European Union (Teu) and the Treaty on the Functioning of the European Union (Tfeu)', (Official Journal C 83/01) at 5-6.
[15] Article 6.3 TEU.
[16] Article 3.2 TEU, article 67 TFEU.
[17] Council, 'Draft Internal Security Strategy for the European Union: Towards a European Security Model', (5842/2/10; Brussels, 2010a) at 4. See also European Commission, 'Communication, 'Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union'. Com (2010) 573/4'.
[18] Council, 'Draft Internal Security Strategy for the European Union: Towards a European Security Model', at 4.
[19] Article 3 TEU.

goal of public security can constitute a legitimate aim[20] that justifies permissible limitations to each individual right.

Yet, as acknowledged by the Commission, "(…) the ever growing importance, in terms of legislative activity, of the area of Justice, Freedom and Security (…) increasingly (…) raise fundamental rights issues." [21] In other words, the imperatives of the fight against serious crime and terrorism, and the politics of fear pursued in the past decade, disrupt the constitutionally established harmonious coexistence between rights and security. In fact, the reaction to the terrorist attacks of the last decade consisted in the adoption of exceptional measures, without sunset clauses, that led to a routine use of surveillance. Literature on the subject abounds.[22] The ensuing policies framed the relationship between rights and security predominantly in terms of the need to 'strike a balance' or establish a 'trade-off' between security and rights. The restrictions imposed on several fundamental rights for the purpose of security (a vaguely defined concept, referred to in articles 3.2 and 3.5, 21.2 (a) and (c) TEU, and as a threat in policy documents) have arguably exceeded the permissible scope of limitations so that it can be questioned whether all resulting limitations are actually compatible with the values these rights seek to protect.[23]

The use of technologies is often not subject to dedicated legislation at the EU level, or even at the member states' level. Courts' judgements on the use of technologies in the AFSJ tend to come too late, when the technology in place is so widespread as to be difficult to curb, even if it fundamentally affects the enjoyment of fundamental rights. Often, technologies are not even the object of judicial decisions. In light of this, the Commission's efforts to ensure a culture of fundamental rights risk failing. Thus, an evaluation of the technologies used in the AFSJ, based on a rigorous methodology, is particularly urgent.

1.2. The legacy of the DETECTER project

[20] 'C-5/88, Wachauf V Bundesamt Für Ernährung Und Forstwirtschaft', (Judgment of the Court (Third Chamber) edn.: Court of Justice of the European Union, 1989).

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

[22] Bruce Ackerman, *Before the Next Attack. Preserving Civil Liberties in an Age of Terrorism.* (New Haven: Yale University Press, 2006), Andrew Ashworth, 'Security, Terrorism and the Value of Human Rights', in Benjamin Goold and Lazarus Liora (eds.), *Security and Human Rights* (Portland: Hart, 2007), 203-26, Laura K. Donhoue, (New York: Cambridge University Press, 2008), Amitai Etzioni, *How Patriotic Is the Patriot Act.* (New York and London: Routledge, 2004), Stefano Rodotà, *Intervista Su Privacy E Libertà. A Cura Di Paolo Conti* (2005), Martin Scheinin, 'Terrorism and the Pull of 'Balancing' in the Name of Security', in Martin Scheinin (ed.), *Law and Security, Facing the Dilemmas* (11; Florence: European University Instite, 2009a).

[23] Martin Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', (Geneva: General Assembly 2009b). For a complete analysis of the costs of surveillance, see Iriss Project Consortium, 'Surveillance, Fighting Crime and Violence, Deliverable D1.1.', (2012).

This deliverable builds on, and develops,[24] the work conducted within the parent project of SURVEILLE, DETECTER. DETECTER was a three-year collaborative project aimed at identifying "human rights and other legal and moral standards that detection technologies in *counter-terrorism* must meet. It surveyed current and foreseeable applications of detection technologies in *counterterrorism*, and conducted cutting-edge legal and philosophical research into the implications of human rights and ethics for *counterterrorism* in general, and detection technologies in particular."[25]

This deliverable continues, in particular, the research carried out for work package 9 of DETECTER, which focused on the comparative human rights risks of selected detection technologies used in counterterrorism.
Deliverable 17.1[26] laid the foundations for later work. It clarified the value of privacy and data protection, and the applicable legal instruments. It proposed a number of parameters for the legal appraisal of technology, based on case law and academic research, including legitimate aim, necessity, proportionality and adequacy, mission creep, and the availability of Privacy Enhancing Technologies. It surveyed detection technologies based on the revised categories of PRISE,[27] and the theoretical understanding developed in the latter, whereby new technologies developed from existing ones inherited the human rights risks of the latter, and possibly amplified them.
Deliverable 17.3[28] had three goals: i) identifying the technologies used by counterterrorism agents, based on the interviews and focus groups conducted in deliverable 17.2; ii) describing the functioning of those technologies; iii) surveying the potential violation of the human rights enshrined in the European Convention of Human Rights[29] (hereafter ECHR) caused by the use of such technologies.
Finally, Deliverable 17.4[30] ranked tracking technologies by their human rights risk.

1.3. The innovation of the SURVEILLE project

The objective of this deliverable is similar to that of DETECTER D17.3. While continuing the work carried out therein, this text innovates in a number of ways, due to the constraints deriving from the difference between the two projects. There are at least four reasons, which are analysed in details below.

[24] "The analysis will build further upon work done in the DETECTER project to refine an earlier classification of surveillance technologies." Surveille Project Consortium, 'Description of Works of the Surveille Project. Surveillance: Ethical Issues, Legal Limitations and Efficiency', at 13.
[25] See at http://www.detecter.eu/.
[26] Rozemarijn Van Der Hilst, 'Human Rights Risks of Selected Detection Technologies. Sample Uses by Governments of Selected Detection Technologies. Detecter Project, Deliverable 17.1', (2009).
[27] See at: http://prise.oeaw.ac.at/.
[28] Rozemarijn Van Der Hilst, 'Characteristics and Uses of Selected Detection Technologies, Including Their Potential Human Rights Risks. Detecter Project Deliverable 17.3', (2011a).
[29] Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols No 11 and 14', (CETS n° 005; Rome, 1950).
[30] Rozemarijn Van Der Hilst, 'Ranking, in Terms of Their Human Rights Risks, the Detection Technologies and Uses Surveyed in Wp09. Detecter Project, Deliverable 17.4.', (2011b).

First, SURVEILLE tackles serious crime and not only terrorism (section 1.1.2). Second, while DETECTER D17.3 focussed on location-tracking technologies only (automatic number plate recognition, GPS-based trackers, IMSI/IMES trackers), the list of technologies to be reviewed in this deliverable cannot be restricted to a single family (section 1.1.3). Third, while DETECTER D17.3 analysed the impact of location-tracking technologies on the right to privacy only as understood in the ECHR, this deliverable has a wider purview. It reviews more rights, and the legal instrument of reference is the Charter of Fundamental Rights of the European Union (section 1.1.4), which is a more appropriate reference after the entry into force of the Lisbon Treaty. Fourth, the parameters chosen in DETECTER D17.3 to analyse the potential impact on the right to privacy were drawn from the only case on location tracking reviewed by the European Court of Human Rights (hereafter ECtHR), namely *Uzun v. Germany*[31]. However, since existing judgments do not provide guidance to legally assess intrusiveness into the wide range of fundamental rights under scrutiny, the analysis must be *in the abstract*, based on a methodology different from the test(s) for permissible limitations performed by the courts (section 1.1.5).

1.1.2 From terrorism detection to surveillance

SURVEILLE has a broader focus than DETECTER. It surveys technologies used not only for tackling terrorism, but also serious crime and other hazards. Examples can be found in the draft EU internal security strategy,[32] where serious crime encompasses, *but is not limited to*, "drug trafficking, economic crime, human trafficking, smuggling of persons, arms trafficking, sexual exploitation of minors and child pornography, violent crimes, money-laundering and document fraud."[33]
The open catalogue approach is formalized by article 83.1 TFEU on judicial cooperation in "areas of particularly serious crimes with a cross-border dimension." The article empowers the Council, with the consent of the European Parliament, to define additional crimes that are particularly serious, and presenting cross-border dimensions that require the cooperation of member states, other than those listed. Those are "terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime."

As a result of moving beyond terrorism, SURVEILLE deals with a wider category of 'end-users', which include members of local administration, police, prosecutors and judges, as well as technology developers/manufacturers and policy-makers at large. Moreover, the range of technologies analysed is necessarily broader than that considered in DETECTER, as explained below.

---

[31] 'Uzun V. Germany', (European Court of Human Rights, 2010).
[32] It encompasses any forms of terrorism, serious and organized crime, cyber crime, cross-border crime, violence, natural and man-made disasters, and road traffic accidents. Council, 'Draft Internal Security Strategy for the European Union: Towards a European Security Model'.
[33] Ibid., at 6. For additional understandings of serious crime, see at https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf.

1.1.3 Surveillance technologies available in the market

Indeed, while in *the parent deliverable in DETECTER it was possible to choose a type of technology to appraise,* this deliverable categorises a selection of the surveillance technologies, listed in the table below, mapped in SURVEILLE Deliverable 2.1[34].
The selected technologies are those already available on the market (or at an advanced stage of development) and used by end-users, represented by the European Forum for Urban Security[35], and a panel of police members[36], and for which exist information as to their functions and characteristics. The list includes thirty-seven technologies belonging in fourteen families: bio agent detector; CCTV; chemical (drugs and explosives); data analysis; GPS; image processing; infra red; mm-wave; network; network & interface; radar; sound; UAV (drones); and x-ray (see *infra* section 2.2.).

Technology type	Technology sub-type
Airborne IMS bio product	Mass spectro for detecting ions
CCTV	IPS activity detection
	Infra red-near field
	Infra red-wide area
	Visual semi automated
	Visual spectrum dome–zoom, tilt, rotate
	Visual spectrum (dome fixed)
	Visual spectrum (fixed)
Chemical	Detection by antibody
	Explosive detection near harbour (UNCOS)
	Gas Chromatography Drugs Detector (DIRAC)
	Novel detection technique (commonsense)
	Precursor and drug detection (CUSTOM)
	Standoff optical detector of explosives (optix)
Data analysis	Detection of money laundering
	Networked data analysis SCIIMS
	Analysis OMNIFIND
	Mobile phone tap (PTS)
	Data transfer analysis – name recognition
GPS	Car tracker SN
Image processing	Crowd and riot
	People counting and density
INFRA RED	Motion detector
MM-Wave	Whole body scanner EQO

[34] Coen Van Gulijk et al., 'Survey of Surveillance Technologies, Including Their Specific Identification for Further Work. Surveille Project Deliverable 2.1', (2012).
[35] Sebastian Sperber, Maye Seck, and Elizabeth Johnston, 'Surveille Deliverable 2.3: Paper by Local Authorities End-Users', (2013).
[36] John Guelke, 'Surveille Deliverable 2.2: Paper with Input from End Users', (2013).

NETWORK	AIS ship location detection and identification
	SIRIUS 3RK3
	UGM 2040
NETWORK & INTERFACE	AMFIS data fusion for ground control
RADAR	Array-based concealed weapon detection radar
	Marine
	MIMO array
	Passive through wall human tracking
	Short range for intrusion detection
SOUND	Sound recording bug AU046
UAV	Platform helikite balloon
	Platform micro helicopter
X-ray	Luggage screening

Table 1 - Surveillance technologies reviewed

Yet, like done in DETECTER 17.3, the technical characteristics, or functions, of these technologies, are reviewed in the abstract (see infra 1.1.5) and in relation to their surveillance capabilities used to fight serious crime and terrorism. These are: the object of monitoring (bodies, objects, means of transport, sound or data); the detection function (hazards or forms of conducts); their covert or overt use. Given that the objective is the scrutiny of the impact of technologies on a wide range of fundamental rights, the analysis is not country-specific (see infra 1.1.5).

1.1.4 The European Union Charter of Fundamental Rights as the reference[37]

The potential intrusiveness of surveillance technologies into fundamental rights is evaluated on the basis of the European Union Charter of Fundamental Rights (hereafter EUCFR),[38] rather than being limited to the ECHR (see *infra* 1.1.4.3). There are several reasons for doing so.

1.1.4.1 A 'bill of rights' for the EU

First and foremost, the EUCFR can be considered as the bill of rights of the EU, analogous to constitutional Bills of Rights in nation states. On the one hand, the rights, freedoms and principles set out in the EUCFR are 'constitutionalized,' in that they "shall have the same legal values as the treaties."[39] Moreover, fundamental rights are fully acknowledged irrespective of their relation with internal market objectives.[40] On the other hand, since the text is not integrated in

[37] Parts of this section have been based on research conducted by the author within the SurPRISE project: Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming'.

[38] 'Charter of Fundamental Rights of the European Union', (Official Journal C 303/1, 2007), 1–22.

[39] Article 6.1 TEU.

[40] And are fully recognized despite the oxymoronic provisions of article 51 EUCFR. Accordingly, the EUCFR "does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the

the treaties, it is not subject to the same mechanisms of amendment and revision of the latter, and as such is independent.[41]

Article 52 can be seen as laying down a "constitutional provision" for permissible limitations. Accordingly, "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." [42] Yet, restrictions must be interpreted restrictively [43] and cannot [44] "constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights'."[45]

1.1.4.2 The EUCFR as the benchmark for the EU and member states' actions

Second, since 2001 and as reiterated by the Stockholm Programme,[46] the Commission has decided that the legislation, draft instruments, implementing acts (pursuant to article 291 TFEU) and delegated acts (pursuant to article 290 TFEU) it proposes must be checked for substantive[47] compliance with EUCFR throughout their life cycle (see *supra* 1.1.1). The EUCFR applies both to EU institutions (and bodies, offices and agencies) and to the Member States when implementing EU law.[48] Justice and home affairs matters fall within the scope of EU law. Indeed, the Lisbon Treaty 'communitarized' the AFSJ, which is now an area of shared competence between the EU and the Member States,[49] subject to

---

Treaties" while EU institutions and Member States (insofar as they are implementing EU law), shall "respect the rights, observe the principles and promote the application thereof in accordance with their respective powers" (Craig and de Bùrca, 2011). Even protocol n. 30 on the non-applicability of the Charter in the UK and Poland is interpreted as being merely declarative, in that it does not deny the ECJ's review of the compatibility with the general principles of law in the context of the implementation of EU law (id.).

[41] Rodotà, *Il Diritto Ad Avere Diritti*.

[42] Emphases added.

[43] 'Joined Cases C-92/09 and C-93/09, Volker Und Markus Schecke Gbr and Hartmut Eifert V. Land of Hesse', (Judgment of the Court (Grand Chamber): Court of Justice of the European Union, 2010), 'Case C-73/07 Tietosuojavaltuutettu V Satakunnan Markkinapörssi Oy and Satamedia Oy', (Judgment of the Court (Grand Chamber): Court of Justice of the European Union, 2011).

[44] Court of Justice of the European Union, 'C-292/97 Karlsson and Others', (Judgment of the Court (Sixth Chamber), Reference for a preliminary ruling edn., 2000) at paragraph 45.

[45] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights', (2007) at 30.

[46] Council, 'The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens', (OJ C 115; Brussels, 2010b).

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

[48] Article 51 EUCFR.

[49] This is an area subject to the 'pre-emption' clause, whereby member states can "exercise their competence to the extent that the Union has not exercised its competence" (article 2TFEU, paragraph 2), which will necessarily affect the exercise of the exclusive competence of Member States in the maintenance of law and order and the safeguarding of internal security (article 72 TFEU) (Paul Craig and Gráinne De Búrca, *European Union Law: Text, Cases and Materials* (Oxford, 2011) 1320.) analogous to constitutional Bills of Rights in nation states.

the authority of the Court of Justice of the European Union as laid down by article 19 TEU. [50]

The Commission declared it would file a procedure for action for failure to fulfil an obligation, whenever the transposition of a EU law by a Member State violates provisions on fundamental rights.[51] Yet, Member States are bound to respect fundamental rights even when acting outside of the scope of EU law, as indicated by the procedure of article 7 TEU.[52]

1.1.4.3 The EUCFR as the latest catalogue of fundamental rights

Third, the EUCFR represents the latest catalogue of fundamental rights, and takes stock of the efforts previously made by overarching conventions applicable in the EU and to which Members States are party. These include the Universal Declaration of Human Rights (hereafter the UDHR), [53] Council of Europe's ECHR,[54] the United Nation's International Covenant on Civil and Political Rights (hereafter the ICCPR)[55] and on Economic, Social and Cultural Rights (hereafter ICESCR).[56]

It can be thus argued that fundamental rights in the EU should be interpreted in light of the existing applicable international legal instruments. Indeed, the Explanations Relating to the Charter of Fundamental Rights, [57] which have interpretive value,[58] clearly indicate that article 1 on human dignity derives form the UDHR. The check of substantive conformity of proposed legislations with the EUCFR, carried out by the European Commission, includes an analysis of compliance with standards established by international instruments on the

[50] Subject to the rules of Protocol 36. The jurisprudence of the Court of Justice of the European Union has developed in line with the expansion of the scope of EU law, which resulted from the evolution of the institutional framework. Before the entry into force of the Lisbon Treaty, the ECJ had limited authority on pronouncing itself on fundamental rights, for which the EU had no general legislative competence, with the exception of interventions that could facilitate the establishment of the internal market. Advocate General Léger, 'Opinion on Cases C-317&04 and C318/04', (2005). Furthermore, the ECJ could rule on issues strictly pertaining to EU law or the 'first pillar', and thus was not generally competent in the area of police and judicial cooperation disciplined by Title VI of the Treaty on the European Union. The (first) Kadi judgement marked a change in the Court's cautious attitude towards the relationship between policies in the AFSJ and the protection of fundamental rights 'Joined Cases C-402/05 P and C-415/05, Kadi and Al Barakaat International Foundation V Council and Commission (Kadi I)', (Judgment edn.: Court of Justice of the European Union, 2008).

[51] European Commission, 'Communication, 'Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union'. Com (2010) 573/4'.

[52] Ibid.

[53] General Assembly (3rd Session), 'Universal Declaration of Human Rights. Resolution 217', in United Nations (ed.), (1948).

[54] Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols No 11 and 14'.

[55] United Nations, 'International Covenant on Civil and Political Rights', (New York, 1966a).

[56] United Nations, 'International Covenant on Economic, Social and Cultural Rights', (New Work, 1966b).

[57] Charter of Fundamental Rights of the European Union. (2007). Official Journal C 303/1, p. 1–22 (14 December 2007).

[58] Articles 52.7 EUCFR and 6.1 TEU.

protection of human rights and the institutions overseeing their application.[59] A similar argument can be derived from the combined reading of article 3.5 TEU and legal scholarship.[60]

This argument is maintained, in spite of the prudence exercised by the Court of Justice of the European Union in referring to international legal instruments that are sources of human rights in interpreting the fundamental rights in the EU,[61] with the exception of the ECHR. The ECHR is in fact incorporated in the EUCFR as a subset of the fundamental rights recognized in the EU and holds "a special significance" for the interpretation of the general principles of the EU.[62] The articles of the EUCFR that derive from the ECHR should be interpreted in the light of the case law of the European Court of Human Rights, including permissible limitations. [63]

The character of complementarity between the EUCFR and the ECHR is most likely going to be reinforced by the EU's accession to the ECHR following the entry into force of the Lisbon Treaty:[64] "The Union's accession to the European Convention on Human Rights was made obligatory by the Lisbon Treaty and will complement the system to protect fundamental rights by making the European Court of Human Rights competent to review Union acts."[65]

1.1.5 A methodology to appraise intrusiveness

Although judicial decisions are informed by uniform legal principles, the weight applied to each principle often depends on the right at stake. Moreover, not all technologies listed here have undergone a process of judicial appraisal. For this reason, the analysis of the intrusiveness of surveillance technologies into the full range of fundamental rights cannot be based on parameters deriving from specific judgments, *as done in DETECTER deliverable 17.3*.

The methodology proposed here consists of appraising the impact that abstract *functions* performed by surveillance technologies can have on fundamental rights, dissected into their attributes[66] (see infra 2.3). The analysis intends to

---

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

[60]European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union', (2006).

[61] European Court of Justice, Opinion 2/94, (1996), paragraph 33. See for instance *Kadi I*: "the Court draws inspiration from (…) the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories ("Kadi I," 2008, paragraph 283).

[62] European Court of Justice, Opinion 2/94, 1996, ECR I-1795, paragraph 33.

[63] Accession by the EU to the ECHR pursuant to article 6.2 TEU will reinforce such bounds, although, pursuant to article 52.3, EU law can provide more extensive protection.

[64] Article 6(2) TEU.

[65] European Commission, 'Communication, 'Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union'. Com (2010) 573/4', at 3.

[66] Attributes are derived, and developed further, from the work on indicators done for the United Nations' Office of the High Commissioner for Human Rights.

capture the interrelatedness characterizing fundamental rights, and is instrumental to the identification of core areas of rights that can never be lawfully infringed.

The methodology is also put in relation to a more established test for permissible limitations and compliance of legislation with fundamental rights (see *infra* 2.4). However, since the analysis is country-neutral (*similarly to the approach chosen in DETECTER D17.3*), it is for further scholarship in SURVEILLE to carry out the assessment of the legality test (legal base and compliance with the rule of law) relating to the use of surveillance technologies within specific jurisdictions and in connection with clear legal bases. Consequently, this study represents a first step towards a more refined analysis of intrusiveness into fundamental rights that includes infringement and misuse.

1.4. Sources and content

Chapter 2 contains the methodology used to appraise the intrusiveness of surveillance technologies [67] into fundamental rights. Chapter 3 contains a detailed analysis of the impact of the chosen technologies into the attributes of selected fundamental rights, namely privacy, data protection, non-discrimination, freedom of movement, freedom of expression and freedom of thought, conscience and religion. However, the full catalogue of fundamental rights is kept in mind. The classification of surveillance technologies is developed in chapter 4. Finally, chapter 5 concludes the deliverable with suggestions for further research within the SURVEILLE project.

[67] Van Gulijk et al., 'Survey of Surveillance Technologies, Including Their Specific Identification for Further Work. Surveille Project Deliverable 2.1'.

2 A methodology for evaluating the intrusiveness of technology: functions and attributes (and cores)

The intrusiveness into fundamental rights of surveillance technologies is a component of the definition of 'costs' of the use of technologies within the SURVEILLE Project. It is a qualitative factor, the appraisal of which requires a uniform, one-size-fits-all methodology. The objective of this section is exactly to propose a methodology for establishing the intrusiveness of surveillance technologies into fundamental rights, in the double legal meaning – permissible/impermissible – that the term holds.

2.1 An outline of the methodology

From a legal perspective, 'intrusiveness' can be either permissible or impermissible. On the one hand, if the intrusiveness is permissible and circumscribed, it qualifies as a 'limitation' of a right. On the other hand, if the intrusiveness is impermissible or unrestricted, it qualifies as a 'violation'.
The first case corresponds to qualified rights, that is those rights that can be restricted on the basis of enumerated legitimate aims clearly laid down by the law. In other words, a technology could be permissible if it interferes with a given right, provided it conforms to the provisions of a rigorous test for permissible limitations (see *infra* 2.4),
The second case corresponds to both absolute rights and the 'essence' or 'core' of qualified rights (see *infra* 2.4), which cannot be interfered with under any conditions. Legal instruments providing for the intrusion into these rights or core areas of rights would be contrary to fundamental rights, and thus illegal.

It follows that an appraisal of intrusiveness is normally composed of three steps. The first is to appraise whether a technology is susceptible of intruding into a fundamental right. The second step is to assess *in the abstract* whether it is susceptible of intruding into the essence or core of the same right. The third step consists in applying a rigorous test for permissible limitations to the technology.

The first step can be divided into two parts. First, what make a technology susceptible of intruding into a right are its *function(s)* and its *use.* The former is an abstract and objective feature, which can be identified and agreed upon by developers (see *infra* 2.2). The latter is contextual, and depends on the function of the bow-tie model developed in D2.1, or the exact purpose for which it is used.
Second, appraising the intrusion into a fundamental right entails answering the question: what does that fundamental right mean? It obliges to perform the exercise, in the abstract, of dissecting the right into its substantive characteristics or attributes (see *infra* 2.3). The idea of attributes of rights is taken from, and builds upon, the recent work on indicators carried out by the United Nations' Office of the High Commissioner for Human Rights (hereafter OHCHR), the Agency of the European Union of Fundamental Rights (hereafter FRA) and a regional institution, namely the UK Commission on Equality and Human Rights.

Such exercise, in turn, allows performing the second step, which requires identifying the essence or core of the right, based on the revisited core/periphery theory of fundamental rights of Alexy, the intrusion into which would be prohibited (see *infra* 2.4).
The third step is intrinsically contextual. It requires specifying a jurisdiction (having a specific body of law that constitutes the legal basis for the intrusion); the type of 'risk' (e.g. terrorism or serious crime); and whether it is used for preventive or reactive purposes. Only after having identified these elements can a permissible limitations test be applied.

The contextual analysis follows necessarily from the theoretical exercise 'in the abstract'. The purpose of this deliverable is to develop the methodology to identify impacts of technologies in the abstract. Further research in SURVEILLE will transpose this methodology into a contextually relevant analysis based on the test for permissible limitations.
What follows is the explanation of the main features of the methodology: the description of functions performed by the list of technologies (section 2.2), the assessment of the attributes of fundamental rights (section 2.3), and the assessment of core areas of fundamental rights (section 2.4).

1. Is a surveillance technology susceptible of intruding into a fundamental right? Assessment based on:
    a. Functions of a given surveillance technology;
    b. Attributes of the right under scrutiny.
2. Is a surveillance technology susceptible of intruding into the essence or core of the same right (or is the right in question an absolute one)?
3. Application of a rigorous test for permissible limitations to the surveillance technology to appraise permissibility or impermissibility in context.

Figure 1 - 3 steps of the test of intrusiveness into fundamental rights

2.2 Step 1a: Functions of surveillance technologies

This section reviews the features of surveillance technologies mapped in Deliverable 2.1,[68] based on the producers' descriptions, with three caveats.

First, I analyse only those technologies that are already marketed (or at an advanced stage of development) and used by end-users (the European Forum for Urban Security[69], and a panel of police members[70]), for the sake of an informed analysis.

Second, only those features of the technologies that relate to their impact on fundamental rights tied to their surveillance capabilities will be reviewed. These

[68] Ibid.
[69] Sperber, Maye Seck, and Johnston, 'Surveille Deliverable 2.3: Paper by Local Authorities End-Users'.
[70] Guelke, 'Surveille Deliverable 2.2: Paper with Input from End Users'.

features are: the object of monitoring (bodies, objects, data, chemical substance, motion and sound); the covert/overt use; the specific function(s) performed.

Third, as mentioned above, the analysis in the abstract performed here will need to be complemented by additional research on the contextual use of the technology, which depends on three factors: the type of hazardous event (threat/risk) for which it is used; the efficacy of the technology in acting as a barrier to prevent the hazardous event, or to mitigate its consequences; and the legal framework of the jurisdiction where it is deployed. Moreover, the overall acceptability of a given surveillance technology will be assessed at a later stage of the SURVEILLE project.

What follows is the list of technologies that will be reviewed here. The technologies are grouped according to the 'family' they belong in: bio agent detector; CCTV; chemical (drugs and explosives); data analysis; GPS; image processing; infra red; mm-wave; network; network & interface; radar; sound; UAV (drones); and x-ray. The following features are identified for each technology: the object of monitoring (bodies, objects, data, chemical substance, motion and sound); the covert/overt use; and the specific function(s) performed as done in D2.1. Then, technologies are regrouped according to their functions.

Technology type	Technology sub-type	Function Performed	Target	Public/private	Covert/overt
Bio agent detector	Airborne ims BIO PROTECT	Gas-chromatography ion mass spectroscopy	Environment	Public	Overt
CCTV	IPS activity detection	1. Detects (body/object/ motion) 2. Records (data retention) 3. Interprets motion 4. Alerts	Person Object	Public/private	Overt video Covert object detection
	Infra red-near field	1. Detects (body (heath)/ motion) 2. Records (data retention)	Person Object Small range	Public/private	Overt video Cover heath
	Infra red-wide-area	1. Detects (body (heath)/ motion) 2. Records (data retention	Person Object Small range	Public/private	Overt video Cover heath
	Visual semi automated	1. Detects (body/object/ motion) 2. Records (data retention)	Bodies Object	Public/private	Overt video Covert object detection

		High resolution (easier id.)			
	Visual spectrum dome–zoom, tilt, rotate	1. Detects (body (heath)/object/ motion 2. Records (data retention) 3. Sound	Bodies/ Object Large range	Public/private	Overt video The other functions are covert
	Visual spectrum (dome fixed)	1. Detects (body/object/ motion) 2. Records (data retention) 3. Sound	Bodies/ Objects Small range	Pubic transport	Overt video Covert functions
	Visual spectrum (fixed)	1. Detects (body/object/ motion) 2. Records (data retention) 3. Sound	Bodies/ Objects		Overt video Covert functions
Chemical (drugs and explosives)	Detection by antibody	1. Detects chemicals	Bodies/ Objects	Hand-held anywhere	Covert/Overt
	Explosive detection near harbour (UNCOS)	1. Detects chemicals	Objects/ Environment	Public (harbour) unmanned	Overt/covert
	Gas Chromatography Drugs Detector (DIRAC)	1. Detects chemicals (amphetamines) 2. Identifies chemicals	Bodies/ Objects	Handheld, Customs and Offices (indoors)	Covert/Overt
	Novel detection technique (commonsense)	1. Detects chemicals 2. Identifies chemicals	Waste water phase	Public (Sewer flows)	Covert
	Precursor and drug detection (CUSTOM)	1. Detects chemicals 2. Identifies chemicals [Laser photo acoustic spectroscopy and UV fluoresce]	Bodies Objects (?)	Customs, offices, trucks, cars, containers, bodies, objects	Covert
	Standoff optical detector of	1. Detects chemicals		Public/private (car-	Covert?

	explosives (optix)	2. Identifies chemicals		transportable) Range 20 m	
Data analysis	Detection of money laundering	1. Data fusion 2. Data mining (id.) 3. Data interpretation	Databases/ Person	Private (database)	Covert
	Networked data analysis SCIIMS	1. Data fusion 2. Data mining (id.) 3. Data interpretation (profiling)	Databases/ Person	Private Used for illegal migrants/ criminals	Covert
	Analysis OMNIFIND (data // to real events)	1. Data fusion 2. Data mining (id.) 3. Data interpretation	Databases/ Person	Private	Covert
	Mobile phone tap (PTS)	1. Detects data (collection)	Object/ Person	Private (smartphone-based software)	Covert
	Data transfer analysis (name recognition)	1. Data mining (id.) 2. Data interpretation	Databases	Private/public (digital networks)	Covert
GPS	Car tracker SN	1. Detects body 2. Tracks motion	Object/ Person	Private (car)	Covert
Image processing	Crowd and riot (software)	1. Detects body (crowd) 2. Detects motion (crowd)	Bodies	Public	Covert
	People counting and density	1. Detects body (crowd) 2. Interprets body (crowd n.)	Bodies	Public	Covert
INFRA RED	Motion detector	1. Detects bodies/ motion 2. Alerts	Bodies	Private/public	Covert
MM-Wave	Whole body scanner EQO	1. Detects objects	Objects/ Bodies	Person	Overt
NETWORK	AIS ship location detection and identification	1. Detects objects 2. Tracks motion	Object	Ship	Covert/over
	SIRIUS 3RK3	1. Detects hazard (fire) and body;	Bodies Hazard (fire)	Private/public	Covert/overt

	UGM 2040	1. Detects body (presence), hazard (fire); 2. Detects motion	Bodies/ Hazard (fire)	Private/public	Covert/overt
NETWORK & INTERFACE	AMFIS data fusion for ground control	1. Data fusion 2. Data interpretation (meaning)	Person/ Objects	Private/public	Covert/overt
RADAR	Array-based concealed weapon detection radar	1. Detects objects (Weapon) [electromagnetic wave]	Objects/ Bodies (short range, 1 m)	Public (airport)	Covert
	Marine	1. Detects object; 2. Tracks movement;	Objects	Public (waters)	Covert/overt)
	Array based Xaver 800	1. Detects bodies, objects, motion 2. Tracks bodies (motion) 3. Interprets object	Objects/ Bodies	Private (through wall)	Covert
	MIMO array	1. Detects bodies (presence); 2. Tracks bodies (motion) 3. Interprets data (wi-fi, gsm ect.)	People (short-range)	Private (through wall)	Covert
	Passive through wall human tracking	1. Detects bodies (presence)(through wall, through GSM or wi-fi signal)	Bodies (5-100 m)	Private/public	Covert
	Short range for intrusion detection	1. Detects body (presence), motion; 2. Tracks motion;	People/ Bodies (short range)	Perimeter?	Covert
SOUND	Sound recording bug AU046	1. Detects sound; 2. Records sound (microphone)	Bodies	Private (room)	Covert
UAV	Platform helikite balloon	1. Detect body/ motion/ object; 2. Tracks motion; 3. Interprets behaviour	People/ Objects	Public (1 Km)	Covert
	Platform micro helicopter	1. Detects body/ motion/ chemical;	Body/ Objects/ Environment	Public	Covert

X-ray	Luggage screening	1. Detects object; 2. Identification;	Objects	Public or private (airport or entrance of buildings)	Overt

Table 2 List of surveillance technologies analysed

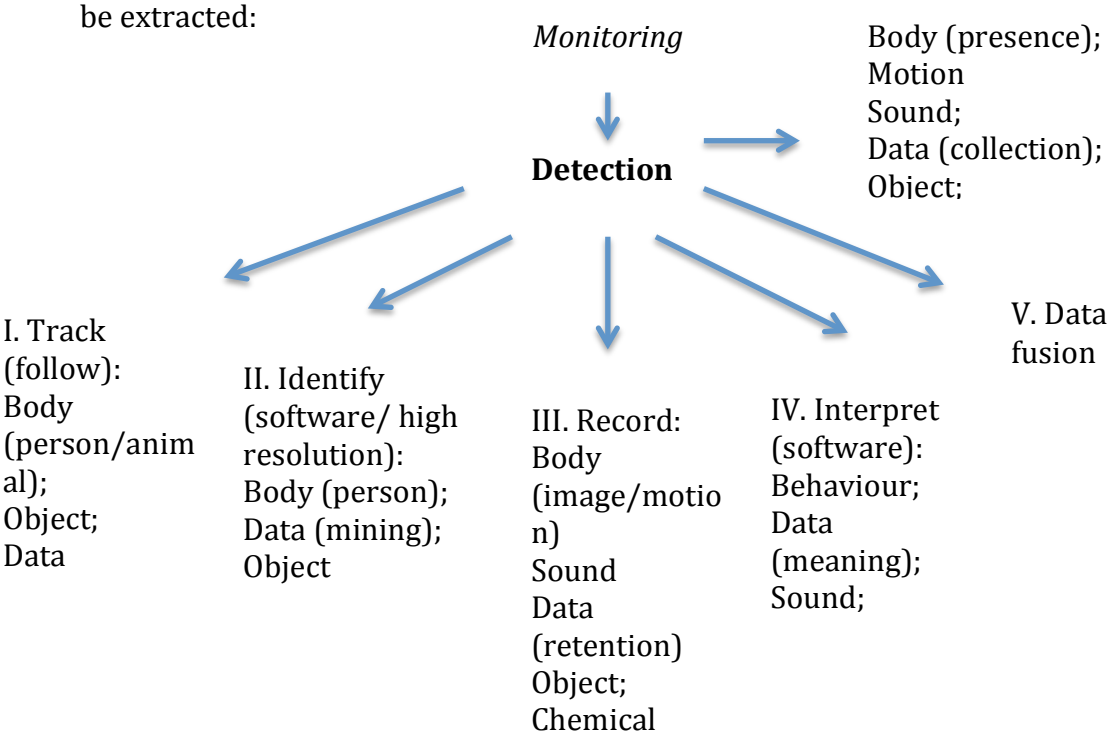
The following technologies are used to either detect the presence of dangerous chemical substances in the environment or water, to flag to ships the presence of other ships to avoid collision, or to detect the presence of fire:

- Airborne IMS bio protect (environment);
- Novel detection technique (COMMONSENSE) (waste water);
- Explosive detection near harbour (UNCOS);
- Marine radar (ship);
- AIS ship location detection and identification (ship);
- SIRIUS 3RK3;

As such, their impact on human rights is almost non-existent or positive. They will not be analysed in this deliverable for their impact on fundamental rights, but will be shown in the final classification.

2.2.1 List of Functions performed

Based on the analysis of the technologies in the table, the following functions can be extracted:



In the working definition of SURVEILLE, surveillance is the *action* of monitoring for the *purpose* of detecting forms of conduct. Detection can be 'simple', in that a device may only grasp the presence of a body (persons or animal) or its motion, objects, sound, chemical substance, or it may collect data.

Detection could be complex, in that a technology could perform the functions from I to V illustrated in the graph above:

I. Track, i.e. follow: a body (person or animal); objects; or data in motion;
II. Identify, through software or thanks to high resolution images: body (person); objects (e.g. cars); and data (mined);
III. Record what it detected: body (image/motion); object; sound; chemical substances; and retention of data;
IV. Interpret, trough software: behaviour (in accordance with pre-set definitions); sound; and data (meaning);
V. Data Fusion, that is the combination of different sources of data.

Clearly, more functions could be added – e.g. the active (intentional) or passive (unintentional) use of a technology, and obviously the lawful and unlawful use (misuse) – and the ones above need to be validated by expert judgements. In what follows a hypothesis is laid out for being tested. The more detecting functions can be performed by a single technology, the more intrusive *in the abstract* the technology can be. Technologies that simply detect (motion, body, sound, data, object and chemical substances) may often have limited intrusiveness into fundamental rights. The addition of the function 'recording' would raise additional concerns, as it could lead to cross-sources identification. Technologies able to track, identify and interpret meaning would considerably increase the level of intrusiveness. This would be higher in case the function depended on 'code', software working on the basis of pre-defined functions.

2.2.2 Grouping of technologies on the basis of their function

2.2.2.1 Detection only (data collection without retention)

Technology	Detected object	Applied to
Detection by antibody	Chemical substance	Person
Gas Chromatography drugs detector	Chemical substance	Person
Custom	Chemical substance	Person, Object
Optix	Chemical substance	Person, Object
MMwave whole body scanner	Object	Person
Infrared	Body heath	Body
UGM2040	Hazard (fire), motion	Machine
Mimo array	Body	Through wall
Array based body scanner	Objects, chemical substance	Person
X-ray	Object (gun)	Luggage

2.2.2.2 Detection and recording (data collection and retention)

Technology	Detects visual (body/ object/ movement/)	Records (data retention)	Detects Sound

Infra red-near field	Y	Y	
Infra red-wide area	Y	Y	
Sound		Y	Y
Mobile phone tap	Y	Y	

2.2.2.3 Detection and tracking

Technology	Detects visual (body/ object/ movement/)	Tracks (follows)	Records
GPS (car)	Y	Y	
Passive through wall tracking	Y	Y	
Short range for intrusion detection	Y	Y	
Platform micro helicopter (UAV)	Y	Y	?
Image processing software (crowd and riot)	Y	Y	?

2.2.2.4 Detection, (data collection), record (data retention) and other functions

Technology	Detects visual (body/ object/ movement/)	Records (data retention)	Detects Sound	High resolution (identifies)	Interprets	Tracks	Alerts
Visual semi automated	Y	Y		Y			
Visual spectrum (dome fixed)	Y	Y	Y				
IPS activity detection CCTV	Y	Y	Y		Y		Y
Visual spectrum dome– zoom, tilt, rotate	Y	Y	Y	Y			
Visual spectrum (fixed)	Y	Y	Y		Y		
Array-based	Y				Y (object	Y	

					s/environment)	
Platform helikite balloon (UAV)	Y				Y	Y
People counting and density (crowd)	Y				Y	

2.2.2.5 Data fusion, mining and interpretation

Technology	Data collection	Data fusion	Data mining	Data interpretation	Identification (of a person)
Hemolia (money laundering)		Y	Y	Y	Y
SCIIMS (migration)		Y	Y		Y
OMNIFIND	Y	Y	Y	Y	
Data transfer analysis	Y			Y	Y
Amfis data fusion		Y		Y	

2.3 Step 1b: the use of attributes to appraise the impact of technologies on fundamental rights

Fundamental rights attributes are the intrinsic and distinctive substantive dimensions of a right. The idea has been developed and used in the context of human rights indicators, which are "specific information on the state of an event, activity or an outcome that can be related to human rights norms and standards; that address and reflect the human rights concerns and principles; and that are used to assess and monitor promotion and protection of human rights."[71] In the OHCHR study, attributes and indicators are interlinked.[72]

Thus, it shall be highlighted that the use of attributes is inspired by the earlier work on indicators but has been further developed in the present context and remains therefore partly experimental. It does not, for instance, lead directly to the development of an indicator. It is rather used as a powerful instrument to capture the granularity of the intrusiveness of surveillance technologies into fundamental rights, taking into account their intrinsic characteristics and their

[71] United Nations International Human Rights Instruments, 'Report on Indicators for Monitoring Compliance with International Human Rights Instruments', (2006) at 3.
[72] It should be noted that the OHCHR study does not concern the use of surveillance technologies at all.

interrelatedness, interdependence and indivisibility[73]. Indeed, fundamental rights should be read as indivisible, without internal hierarchies. The enjoyment of a sub-category of rights cannot take place at the expense of another one.

In order to identify the attributes, the deliverable takes inspiration from the methodology proposed in the OHCHR study:

> "(…) It is (…) important that the narrative on the legal standard of a human right is transcribed into a limited number of characteristics or attributes of that right." (…). To the extent feasible, the attributes should be based on an exhaustive reading of the standard, starting with the provisions in the core international human rights treaties; (…) the attributes of the human right should collectively reflect the essence of its normative content (...) To the extent feasible, the attributes' scope should not overlap."[74]

Figure 2 below illustrates the proposed procedure for extracting attributes. The first step is divided into two parts. First, it is necessary to discern the applicable legal framework, which includes international as well as regional instruments, case law and authoritative interpretations. If the argument whereby the EUCFR encompasses the progress made by previous instruments is tenable, then the selection of attributes can be based on the framework relating to the EUCFR. Second, the attributes can be identified; they should be as few as possible, mutually exclusive and able to capture the full meaning of the right.

The second and third steps consist in reviewing the attributes, and validate them respectively. These actions can only tentatively be performed for this deliverable. Should the use of attributes prove advantageous in the analysis of the intrusiveness of surveillance technologies from a policy-making perspective, the steps 1 to 3 should be followed more systematically than what was possible for producing this deliverable.[75]

[73] Limitations to fundamental rights do not affect such qualities.

[74] United Nations High Commissioner for Human Rights (Ohchr), 'Human Rights Indicators. A Guide to Measurement and Implementation', (New York and Geneva: United Nations Human Rights Office of the High Commissioner, 2012) at 31.

[75] For the purposes of this deliverable the identification of attributes and their tentative validation was done under the guidance or authorship of Professor Martin Scheinin who besides being the leader of the SURVEILLE consortium was the moderator of the expert consultations that resulted in the OHCHR guide referred to above (see Acknowledgments, p. v).

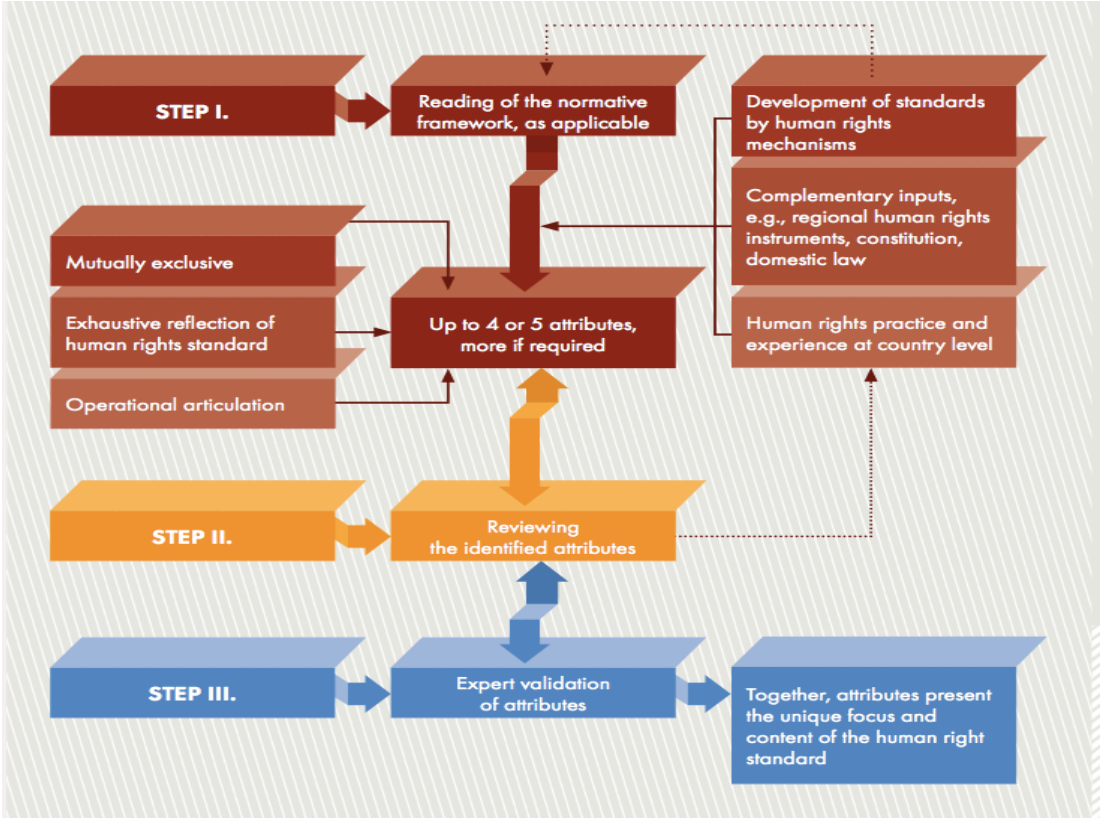


Figure 2 (United Nations High Commissioner for Human Rights (OHCHR) 2012: 72)

The instructions contained in step 1 of the procedure illustrated above have been followed to cover rights that have not yet undergone the thorough process of identification of attributes (with some sacrifice for their mutual exclusivity). This is the case of data protection, freedom of movement, freedom of thought, conscience and religion, and freedom of assembly and association.

Whenever attributes have been found, this deliverable follows them. This is the case for the attributes found by the OHCHR study for non-discrimination, liberty and security, and freedom of expression and information. The attributes for the right to private and family life (privacy) are derived from the Human Rights Measurement Framework developed by the UK Equality and Human Rights Commission.[76]

2.4 Step 2: the notions of core and periphery[77]

The identification of attributes is a preliminary step for the identification of core(s). The idea that any human right contains an essential and inviolable 'core' stems from a combined reading of article 52 of the EUCFR, the case law and

[76] Jean Candler et al., 'Human Rights Measurement Framework: Prototype Panels, Indicator Set and Evidence Base', (London: Equality and Human Rights Commission, 2011).

[77] Parts of this section have been based on research conducted by the author and others within the SurPRISE project: Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming'.

general comments by the Human Rights Committee (hereafter HRC), and a reinterpretation of Alexy's theory of rights.[78]

> "According to this constitutional law scholar and legal theorist, all legal norms are either rules (either/or) or principles (more/less). Even if Alexy sees constitutional rights mainly as broadly formulated principles, the theory can be applied to explain how any fundamental right would have an inviolable core (or more than one such core) sealed in a rule, and a periphery surrounding that core and subject to permissible limitations (i.e. article 8 ECHR, and articles 7 and 8 of the EUCFR, for privacy and data protection).[79]"[80]

Such a core/periphery approach to rights lays the basis for combining compliance with fundamental rights and the needs of LEAs when conducting an investigation and, in a more general fashion, rights and security, as opposed to simple theories of abstract balancing.

As for the EU fundamental rights doctrine, article 52 EUCFR refers to the inviolability of the essence of fundamental rights. Likewise, one of the questions of the test or 'checklist' elaborated by the Commission to assess the compliance of legislation with the EUCFR reads: "would any limitation preserve the essence of the fundamental rights concerned?" Moreover, the HRC declared in the context of several opinions that restrictions on rights must not intrude upon the 'essence' of a human right.[81]

However, the idea of a core is proposed as a metaphor, in that fundamental rights may hold multiple cores, and,

> "Speaking of an 'essence' or a 'core' should not be seen as preventing contextual assessment, as the essence or core can be defined through a multitude of factors."[82]

While not having the pretence to exhaust the discussion as to what constitutes the essence, or core, of a given fundamental right, this deliverable will try to capture the abstract intrusiveness of a surveillance technology into core areas,

---

[78] Scheinin, 'Terrorism and the Pull of 'Balancing' in the Name of Security'. See at: Robert Alexy, *Theorie Der Grundrechte* (Suhrkamp Verlag; Auflage), Robert Alexy, ' Constitutional Rights and Legal Systems', in Joakim Nergelius (ed.), *Constitutionalism - New Challenges: European Law from a Nordic Perspective* (2008).

[79] See also Postscript in Alexy (1992; 1994; 2008).

[80] As formulated by Martin Scheinin and the EUI team in Reinhard Kreissl et al., 'Surprise Deliverable 3.4. Wp3 'Exploring the Challenges': Synthesis Report', (2013) at 14.

[81] Human Rights Committee (1999). Human Rights Committee, 'General Comment No. 27. Freedom of Movement (Article 12)', Human Rights Committee, 'General Comment No. 31, the Nature of the General Legal Obligation', (2004), Human Rights Committee, 'General Comment No. 32, Right to Equality before Courts and Tribunals and to a Fair Trial', (2007), Human Rights Committee, 'General Comment No. 34, Freedoms of Opinion and Expression', (2011), Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming'.

[82] See Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming', at 43-44.

derived from attributes. Some attributes may thus be seen as peripheral, while other attributes will coincide or express a core area.

What matters here is that any use of a surveillance technology that impaired the essence, or core, of a fundamental right, even if authorized to do so by a legal basis, would be impermissible, and therefore unlawful. The parts of the legal basis authorizing the use of a technology in a way that infringed any core of the fundamental rights would also be impermissible. The contextual assessment will derive from the application of an analytically rigorous test for the permissibility of restrictions of fundamental rights, which belongs to the third step of the overall assessment.

2.5 Step 3: the test for permissible limitations to fundamental rights

An analytically rigorous test for the permissibility of restrictions of (peripheral attributes) of fundamental rights, as for instance elaborated by the former United Nations Special Rapporteur on respecting human rights while countering terrorism, based on the ICCPR, is the following:

> "(a) Any restrictions must be provided by the law (paras. 11–12);
> (b) *The essence of a human right is not subject to restrictions* (para. 13);
> (c) Restrictions must be necessary in a democratic society (para. 11);
> (d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
> (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);
> (f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);
> (g) Any restrictions must be consistent with the other rights guaranteed in the ICCPR (para. 18)."[83]

Item b), above in italics, of the test incorporates the idea of the essential and inviolable 'core'. As mentioned above, a test for permissible limitations assessing

[83]Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', at paragraph 17. (footnotes omitted, emphasis added). The bracketed references to numbered paragraphs relate to General Comment No. 27 by the Human Rights Committee, Human Rights Committee, 'General Comment No. 27. Freedom of Movement (Article 12)', (1999). The same elements for a permissible limitations test were presented in Martin Scheinin and Mathias Vermeulen, ''Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism', *Essex Human Rights Review,* 8 (2011), 20-56 at 41. See also Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming'.

the permissibility or impermissibility of a technology will be applied at a later stage of the SURVEILLE project, based on the EUCFR, which includes the ICCPR but has additional features and a wider scope.

2.6 Limits of the methodology

The theoretical steps of the methodology have some limits, as any methodology. These include the facts that: more, or different functions of surveillance performed by the technologies could be considered (e.g. passive/active use); it does not distinguish between useful and harmful uses of technologies; it does not distinguish between the use of technologies by state and non-state actors; and, as already announced, it does not distinguish between permissible and impermissible uses.
These, and other limitations, will be taken into account in the contextual assessment of surveillance technologies.

3 Impact of technology functions on the attributes of fundamental rights

This chapter contains the analysis of the impact of technologies *in the abstract* (through their functions) on fundamental rights (through their attributes). The SURVEILLE Description of Work required to analyse the following rights: "privacy, data protection, non-discrimination, human dignity, personal liberty, freedom of movement, freedom of expression and freedom of thought, conscience and religion. Due to the interdependence of all human rights, however, also other parts of their normative catalogue need to be taken into account."[84] Yet, this deliverable does not include the analysis of intrusiveness into human dignity, and liberty and security (see *infra* for the explanation).

The analysis is divided into two groups: that of rights whose attributes have been defined by the OHCHR or the EHRC, and that of rights whose attributes have not been defined yet through such an elaborate process. As mentioned above (see *supra* 2.3), the identification of attributes for the latter rights can only be somewhat experimental, and should be further validated. The rights are presented in such an order as to allow grasping their interrelatedness, as the infringements of a right may be the consequence of the infringement of another one. Whenever possible, core areas of the right are highlighted. Each list of attributes is preceded by a short description of the right.

3.1 Rights whose attributes have been defined

3.1.1 Article 21. Non-discrimination (title III- Equality)

> *1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.*
> *2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.*

Non-discrimination is a crosscutting principle of human rights, prohibited on non-exhaustive grounds. The Explanations to the Charter clarify that Article 21 of the EUCFR subsumes international legal instruments.[85] It derives from ECHR

[84] Surveille Project Consortium, 'Description of Works of the Surveille Project. Surveillance: Ethical Issues, Legal Limitations and Efficiency', at 5-6.
[85] These are the International Convention for the Elimination of all forms of Racial Discrimination (ICERD); International Convention for the Elimination of all forms of Discrimination against Women (CEDAW); Convention on the Rights of the Child (CRC), and, article 2 ICESCR, and articles 2 and 26 ICCPR.

article 14 for the corresponding parts (see *infra*),[86] but also from article 13 of the EC Treaty, thanks to which non-discrimination (alongside equality) became a transversal principle of EU law making.[87]

Even though all relevant provisions work on the basis of non-exhaustiveness of the grounds for discrimination, the members of the Convention chose to list and rank (starting with sex) all grounds that reflect the European landscape in matters of non-discrimination (thus adding genetic features, property, membership in a national minority and age).

Article 21 is different from article 14 ECHR in three important ways.
First, the scope of the right is closer to that envisaged by Protocol No. 12 to the Convention, than original article 14 ECHR, in that it is autonomous, i.e. the infringement of the right can take place independently from other protected rights. Absence of discrimination implies the application of a double requirement: equal cases have to be treated similarly but, also, different cases should be approached differently.[88]
Second, article 21.1 applies to institutions and member states when implementing EU law, but, since it does not explicitly mention public authorities, could be interpreted as being able to produce 'horizontal effects', i.e. to apply also between private persons.[89]
Third, article 21 paragraph 2 must be applied in line with Article 18 TFEU, to which it corresponds.[90] Article 18 TFEU prohibits discrimination on grounds of nationality of the member states, thus creating a preferential regime for citizens having nationality of the EU, as opposed to non-EU nationals. Such choice is justified with the needs to consolidate the creation of the EU, and as such it is not always at odds with the international rules.[91]
Yet, one may question whether article 21 is configured as absolute.

3.1.1.1 Potential intrusiveness of surveillance technology into attributes

In the study conducted for the OHCHR on indicators, non-discrimination was seen as a measure for accessibility, other than availability, of goods and services. It was seen as a procedural right affecting the realization of a substantive right. The OHCHR analysed non-discrimination in conjunction with equality, and tried

[86] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[87] Article 19 TFEU, which repealed article 13 ECT, has a different scope than article 21 of the Charter, in that it enables the EU to adopt any measures to combat clearly enumerated grounds of discrimination. No such power is created by article 21 of the Charter; in turn, article 21 does not affect the scope and aim of article 21. Another source of non-discrimination is article 11 of the Convention on Human Rights and Biomedicine as regards genetic heritage. European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.
[88] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[89] Ibid.
[90] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.
[91] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.

to capture economic, cultural and social dimensions that may not be immediately relevant for the context under analysis. They are: 1) equality before the law and protection of the person; 2) direct or indirect discrimination by public actors in application of a policy/measure; and 3) special measures including for participation in decision-making.

1. Equality before the law and protection of the person

In theory, if monitoring were carried out in an overt and 'uniform' (indeed non-discriminatory) manner, it would have little impact on the attribute at hand. Yet, this would not exclude the fact that a person having a particular *sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation* could feel more discriminated and excluded, and consequently decide to avoid involvement in civic and political activities. Surveillance technology can thus have an important 'chilling effect'. At the individual level, the sense of discrimination tends to overlap with the intrusion into the right to privacy.

2. Direct or indirect discrimination by public actors in application of a policy/measure

In theory, if monitoring were carried out in an overt and 'uniform', indeed non-discriminatory manner, it would have little impact on the attribute at hand. In practice, however, surveillance technologies could be used in such a way as to produce a discriminatory effect.

The (simple) detection function can be discriminatory if applied to predefined categories of people. Examples:

- Detection of chemical substances (drugs) only on young (age) people dressed in unconventional style, or of a certain nationality, or of a certain colour. Detection of chemical substances, or drones (UAV) flying, during assemblies, in particular of people expressing particular political or religious opinions;
- Body scanners only for pre-selected travellers;
- Infrared sensors/radar sensors placed in front of places of worship of a certain religion;

The addition of record functions increases the discriminatory risk of the above. This is the case of the record of motion and sound, and detection and tracking functions. Examples:

- GPS tracking of people possessing one of the grounds for discrimination;
- Drones (UAV) flying, radars placed only in neighbourhoods inhabited prevalently by minorities, or in front of places of worship of a certain religion;
- Image processing (identification) of crowds taking part in political or religious assemblies;

Complex functions (software/ human) examples:

- CCTV cameras placed, or drones (UAV) flying, only in neighbourhoods inhabited prevalently by minorities, or in front of places of worship of a certain religion;
- Software based on pre-defined notions of what constitutes anomalous behaviour, which can lead to profiling;

Data surveillance function (software) examples:

- Software that operates on the basis of a discriminatory ground (i.e. nationality, or age, or property, or religion).

3. Special measures including for participation in decision-making

This attribute refers to the adoption of special measures (including affirmative action or positive measures) by the state to address discrimination, and in particular to engage groups exposed to discrimination in policy making.

The use of *any* surveillance technology in a covert manner is likely to affect this attribute, as it will preclude persons who are potential targets of discrimination from taking part in the discussions relating to the measure, particularly in the case of the use of sense-making software and data mining functionalities.

3.1.2 Article 7. Privacy or Private and family (title II- Freedoms)

> *Everyone has the right to respect for his or her private and family life, home and communications.*

The right to private and family life, or privacy for short, derives from article 12 UDHR, which laid the basis for article 17 ICCPR, and more directly from article 8 ECHR; it should thus be read in line with the latter.[92] The term 'communications', used instead of 'correspondence', reflects the technological evolution occurred in the past 60 years. Yet, it is difficult to discern the exact content of this right, as the European Court of Human Rights acknowledged:

> "The concept of private life is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. It can sometimes embrace aspects of an individual's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8. Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world. (…) [T]he Court considers that the notion of personal autonomy is an important *principle* underlying the interpretation of its guarantees."[93]

The difficulty derives from the fact that the right to private and family life is a right to autonomy of the person (personality or self-determination) and of the person's social relations, in that the social dimension is identified as the typical life setting. As such, the right has a double valence, and contains a statement of value: people do not leave in isolation.

In metaphorical terms, it envisages the freedom for a person to lift or apply a filter to one's body, mind, and personal relations. It is difficult, if not impossible, to determine exhaustively what is relevant for one's personality and social relations across countries, times and cultures. The degree of one's privacy is

[92] 'Charter of Fundamental Rights of the European Union'.

[93] 'Pretty V. Uk, 2346/02', (Judgment of the Court (Fourth Section) edn.: European Court of Human Rights, 2002) at ground 61.

inversely proportional to the 'outsourcing' of the detailed determination of behaviours to religious or political institutions. In this respect, it is strongly linked with non-discrimination (see *supra* 3.1.1): one's private and family life could be hindered if expressing values opposing the morals of a society (e.g. women's freedom to dress as they wish, or homosexual relations). It should be noted that this right is particularly sensitive to technological innovations, insofar as those innovations affect the functioning of the 'filters' that individuals can apply.[94]

Permissible limitations (as interpreted by the Strasbourg (ECtHR) and Luxembourg (ECJ) case law) shall be the same as those envisaged by article 8.2 ECHR, namely interferences in accordance with the law by a public authority that are "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." Pursuant to article 52.3, EU law can provide more extensive protection, as limitations must be proportional to the objective pursued, meet the objectives of general interests recognized by the Union, and be interpreted restrictively.[95]

3.1.2.1 Potential intrusiveness of surveillance technology into attributes

The study realized by the Equality and Human Rights Commission (EHRC) found the following attributes for the UK legal context: physical and psychological integrity; personal social and sexual identity; personal development, autonomy and participation; personal information and surveillance; correspondence; family life; home; and Environmental rights**.** The attributes proposed here draw heavily from those found by the EHRC, but have been modified to allow for greater granularity, and to take into account that the protection of personal information, as personal data, is safeguarded by a separate right, namely the right to personal data (article 8, see *infra* 3.2.1).

1. Psychological (mental) integrity (control of feelings, emotions)

This attribute concerns what is most intimately personal: one's inner thoughts, feelings and emotions. This dimension is a strong candidate for the core of privacy. Functions that can detect personal feelings and emotions, or affect such feelings and emotions, are susceptible of infringing privacy in the sense of this attribute. Example:

- Technologies that detect or try to interpret people's psyche (e.g. brain scans, not analysed here, but also sound and data may aim at understanding features covered by this attribute).

[94] Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming'.

[95] 'Joined Cases C-92/09 and C-93/09, Volker Und Markus Schecke Gbr and Hartmut Eifert V. Land of Hesse', at 86. 'Case C-73/07 Tietosuojavaltuutettu V Satakunnan Markkinapörssi Oy and Satamedia Oy', at 56.

2. Personal development and (sexual) identity (portrayal to the outside world)

This attribute captures autonomy in the sense of one's life choices, and the way in which somebody wishes to portray oneself to the rest of the world. This is another strong candidate for the core of privacy. The attribute is affected by technologies that can decipher a person's behaviour. Example:

- Interpretation function: software classifying a person's behaviours, as well as her main features.

3. Social identity and relations (unchecked social relations)

This attribute expresses the idea that individuals should enjoy social relations free from control. Any technologies able to capture the relational network of a person can intrude upon this attribute of privacy. Examples:

- Complex functions: the use of CCTV cameras (and eventually drones) that can identify individuals;
- Detect and record functions: The use of smartphone or portable device monitoring that can reveal a person's social network, from the address and from any online activity;
- Sound: the use of a microphone recording personal conversations;
- Data analysis: the use of data fusion software using telecom and banking data that can reveal one's network (but HEMOLIA has inbuilt privacy features).

4. Autonomy and participation (movement and activity in outside world)

This attribute refers to the liberty right of being able to move without being followed, and taking part in social activities without being controlled (it has thus features in common with freedom of movement). Technologies that can intrude upon this attribute are those with tracking functionality, such as:

- GPS bars placed in one's car;
- The use of CCTV cameras that can identify and track individuals;
- Any combined use of technology able to identify somebody in the public space.

5. Physical integrity (control of the body)

This attribute relates to the control of access to one's body and its unique features (DNA, brain scans, medical conditions, etc.). The latter aspect is a strong candidate for the core. It can be intruded upon by surveillance technologies that focus on the body, and particularly a simple detection technology such as the two types of body scanners, if able to map the body (i.e. if used without privacy by design features).

6. Liberty to decide what information to share and with whom (confidential communications)

This attribute covers the confidentiality of communications, which is a strong candidate for the core. It can be intruded upon by those covert technologies that are able to capture voice, telephone, letters or electronic-based personal communications. Examples:

- The covert use of the four types of CCTV featuring sound functions, plus the microphone sound recorder;

- The use of technologies that capture (detect) data, such as the I-phone tap;
- The HEMOLIA money laundering technology, in that it re-uses data deriving from personal communications (telecom data).

7. Family life (unchecked relations)

Family life includes both the right to develop family relations free from intrusions (a potential candidate for the core). It also includes an aspect of family integrity, i.e. all members should be allowed to live together, which is not affected by the technologies at hand. Technologies susceptible of affecting family life are those that could monitor the daily routine of a family. Examples:

- Video multi-function: any CCTV or infrared system placed in such a way as to observe the entrance of a house;
- Sound: a microphone placed in a house that could capture anybody's telephone or voice conversations;
- Motion detection: the use of radar to detect the presence and movements of people in the rooms.

8. Inviolability of the private spaces where the person decides to be (home sanctity)

Any technology used covertly that intruded in a person' dwelling would affect the inviolability of the home. Examples:

- Body and motion detection: the three types of radar capable of watching through one's wall;
- Sound: a microphone installed in one's house;

9. Personal information privacy: see data protection.

3.1.3 Article 11. Freedom of expression and information (title II- Freedoms)

> *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*
> *2. The freedom and pluralism of the media shall be respected.*

Article 11.1 subsumes article 19 UDHR, articles 19 and 20 ICCPR[96] and, as clarified by the Explanations, derives from Article 10 ECHR; its meaning and scope should be read in line with it.

The case law of the European Court of Human Rights has led to a clarification and ranking of the forms of expression safeguarded (and thus limitable), in particular "'information and ideas concerning matters ... of public interest'; 'information and ideas on political issues'; and artistic expression,"[97] the latter

[96] As well as article 12 of the Convention on the Rights of the Child, Article 9 of the Framework Convention for the Protection of National Minorities provides the same freedom for minorities. European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[97] Ibid., at 117.

including creation and dissemination. Commercial information is also protected, but to a lesser extent. Both traditional and new media are covered. The right to seek information is not spelled out, but it is considered implicitly protected, as a form of autonomy, a necessary precondition for the freedom to receive information. Briefly, the full process of creation and use of an opinion is safeguarded.[98]

As for the grounds for limiting a person's freedom of expression and information, they cannot exceed those listed in article 10.2 ECHR (keeping in mind the ranking as to the form of expressions protected), which are considered as 'exceptions': "formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[99]

Member states' rights to issue licensing arrangements may be limited by requirements deriving from EU competition law.[100] However, article 11.1 innovates in that it separates freedom of expression and information from freedom of the media. Paragraph 2 addresses the consequences for freedom of the media implicated by paragraph 1, based on economic interpretations as well as the democratic value of pluralism.[101] It derives from the Court of Justice's case law (case C-288/89), the Protocol on the system of public broadcasting in the Member States annexed to the EC Treaty, and Council Directive 89/552/EC (particularly recital seventeen).[102]
Due to the limited jurisdiction of the EU in the audio-visual sector, the wording chosen was 'respect', rather than 'guarantee', which envisages positive obligations of the state. Since this paragraph is independent from article 10 ECHR, the grounds for permissible limitations that apply to it are those envisaged by article 52(1) of the Charter.

3.1.3.1 Potential intrusiveness of surveillance technology into attributes

The study commissioned by the OHCHR found the following attributes: 1) freedom of (expressing) opinion and to impart information; 2) access to/ receive information; 2) pluralism of the media.

The degree of intrusiveness of surveillance technologies into (the attributes of) this right is likely to depend on a violation of the rights to non-discrimination, and private and family life, such as in the case of the monitoring of a person based on specific political or religious views, or dissemination of particular

[98] Ibid.
[99] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.
[100] Ibid.
[101] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[102] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.

information (i.e. journalists). It is also likely to increase if such monitoring is translated into retained data, used for further purposes. The intrusiveness into this right is also strongly linked with intrusiveness into the right to association and assembly, as well as thought and religion, if indeed the surveillance is targeted.

Furthermore, lawful surveillance technology could be intrusive by triggering a chilling effect, in that the non-discriminatory monitoring (detection and recording) of the public expression of ones' opinion or the imparting of information could lead to modify one's attitudes and behaviour.

1. Freedom of opinion and to impart information (forum internum);
This attribute expresses the rights of the provider of information/ opinions. The non-discriminatory use can produce a chilling effect. A discriminatory use of technology could affect this attribute on a personal basis (expressing views as a citizen, or as part of one's jobs, i.e. in journalism, NGO activism, etc.) or in the case of assemblies organized in order to express views and opinions on any matters. Examples:

- Detection and recording functions: recording one's I-phone data with the phone tap, and one's conversations (sound) with the use of a microphone;
- Tracking function: following a person through GPS bars put in one's car;
- High-resolution/identification function: CCTV recording images with a view to track the person's movements or participation in events;
- Data fusion, interpretation and mining functions: the takedown/obfuscation of one's websites based on data analysis technologies (e.g. SCIIMS and OMNIFIND), used to monitor online activities, could affect this attribute. This can be done without discriminatory intentions.

2. Access to/ receive information
This attribute refers to the recipients of information, who should be able to enjoy it without being monitored. The *covert* use of any surveillance technologies is likely to intrude upon this attribute.

The takedown/obfuscation of websites based on data fusion, interpretation and mining functions of data analysis technologies, (e.g. SCIIMS and OMNIFIND), used to monitor online activities, could affect this attribute.

3. Pluralism of the media
The latter applies here if the websites taken down disseminate information of public relevance. Pluralism of the media could also be affected if the targets of the technologies intruding upon the first attribute are journalists.

3.2 Rights whose attributes have not been defined

3.2.1 Article 8. Protection of personal data (title II- Freedoms)[103]

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 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.

Article 8 has multiple sources of inspiration, as acknowledged by the Explanations, due in particular to its evolution in parallel with the appearance of computerized systems and their applications. First, it draws from the instruments adopted within the Council of Europe: article 8 ECHR and in particular Council of Europe Convention 108[104], which refined the safeguards to it, as decided by the European Court of Human Rights in *Rotaru v. Romania*.[105] Second, it derives from article 286 of the EC Treaty (now article 16 and 39), Directive 95/46/EC[106], as well as Regulation (EC) No 45/2001[107], which "contain conditions and limitations for the exercise of the right to the protection of personal data".[108]

The right to data protection safeguards 'the digital/electronic persona' as distinct from the physical persona, needing specific legal protection, substantiated in procedural rights allowing to control the dissemination of personal information. Article 8.2 addresses the substantive and procedural principles on processing of personal data.

---

[103] Parts of this section have been based on research conducted by the author within the SurPRISE project: Porcedda, Vermeulen, and Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project. Forthcoming'.

[104] 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data', in Council Of Europe (ed.), (CETS No. 108; Strasbourg, 1981). 'Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans-Border Data Flows', in Council of Europe (ed.), (Strasbourg, 2001) Convention 108 developed in strong relation with the Economic Cooperation and Development, 'Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', in Council of the Organization for the Economic Cooperation And Development (ed.), (1980).

[105] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.

[106] European Commission, 'Communication. Compliance with the Charter of Fundamental Rights in Commission Legislative Proposals. Methodology for Systematic and Rigorous Monitoring. Com(2005) 172 Final'.

[107] European Parliament and Council, 'Regulation 45/2001/Ec of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data', (2001), 1-21.

[108] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights', at 20.

The substantive principles correspond to the principles listed in articles 6 and 7 of Directive 95/46/EC. First, the processing must be carried out for legitimate purposes,[109] defined either by the consent of the person or by law (fairness and legitimacy) [110]. Second, transparency, i.e. the purposes must be explicit,[111] and the data subject must be adequately informed (transparency).[112] Third, all processing operations, including collection, must be carried out in accordance with the law (legality/lawfulness), which must leave no room for ambiguous interpretations, and be foreseeable, i.e. the consequences of each provision must be known *ex ante*.[113] Fourth, each processing must relate to a specified, limited purpose (necessity and proportionality, purpose limitation[114]), and the data collected must be adequate, relevant and not excessive.[115] Each new purpose should be connected to a different processing.

The procedural principles correspond to the principles listed in articles 10 to 12 of Directive 95/46/EC: data subjects enjoy the rights to access data concerning him or her, to object to the treatment and to rectify the data whenever incorrect. Article 8.3 represents an acknowledgement of the importance of enforcement for the right to data protection, thus carving in stone the need for oversight by an independent authority.[116]"

Article 8 must be further read in conjunction with article 52. The permissible (i.e. legitimate) limitations, namely those listed in particular in articles 8.2 ECHR, 9 of Convention 108, 13 of Directive 95/46/EC, and 15 of Directive 2002/58/EC[117] must be proportional to the objective pursued, necessary in a democratic society and meet the objectives of general interest recognized by the Union. Moreover, exceptions must be interpreted restrictively, as any exception.[118]"

3.2.1.1 Potential intrusiveness of surveillance technology into attributes

No studies have been conducted yet to identify attributes to this right, which is usually recognized as an element of the right to private and family life. Yet, the acknowledgment of the autonomy to the right to personal data is one of the main

[109] Article 6.a of European Parliament and Council, 'Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data', (1995), 31-50.
[110] Ibid., article 7.
[111] Ibid. article 6.b.
[112] Ibid. articles 10-11.
[113] Ibid.article 6.a.
[114]Ibid. article 6.b.
[115] Ibid. article 6.c.
[116] 'Case C-614/10, Commission V. Austria', (Judgment of the Court (Grand Chamber) edn.: Court of Justice of the European Union, 2012).
[117] European Parliament and European Council, 'Directive 2002/58/Ec of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (E-Privacy Directive)', (2002), 37-47..
[118] 'Joined Cases C-92/09 and C-93/09, Volker Und Markus Schecke Gbr and Hartmut Eifert V. Land of Hesse', at 86. 'Case C-73/07 Tietosuojavaltuutettu V Satakunnan Markkinapörssi Oy and Satamedia Oy', at 56.

innovations of the EUCFR. What follows is a *tentative* identification of attributes based on well-known principles of data processing grounded in EU law. As a preliminary remark, many of these attributes are heavily interrelated and, for this reasons, are grouped under four headings: legitimacy; procedural rights of the data subject; procedural obligations of the data controller; and external control.

Legitimacy

1. **One authorization (by means of *consent*/law) justifies one processing only (purpose specification/ transfer)**
2. **Transparency (the processing is known by data subject and transparent)**

Procedural rights of the data subject

3. **Access to data processing (information to be given to the right of access to data) accessibility of data**
4. **Correction or objection to processing (the right to object)**

Procedural obligations of the data controller

5. **Data proportional to the purpose of processing (data minimization)**
6. **End of authorization means end of processing (purpose limitation/ data retention/ remote)**
7. **Integrity of data (accuracy, brought up to date and reliability of data)**
8. **Special regime for sensitive data (the processing of special categories of data)**
9. **Security of processing (integrity and confidentiality) of data**
10. **Man in the loop (prohibition of automated individual decisions)**

External control

11. **Oversight of independent authority.**

Any technology used *covertly* affects the group of legitimacy and procedural rights of the data subject. First, the data subject is unable to consent, thus the processing must have a clear legal basis (1) (the analysis of which is beyond the scope of this deliverable). Second, the data subject is uninformed (2), and cannot consequently enjoy his or her procedural rights: access the file (3) and correct or object to the processing (4).
However, covertness can also affect control of the fulfilment of the obligations of the data controller, which can only be ensured by an independent authority (11), whose existence, though, cannot be appraised in the abstract. Obligations include the collection of as few data as necessary for the processing (5), is severely restricted in the collection of sensitive data (8), and has to make sure that the data are secure and confidential (9) and integer (7). If data are recorded, they have to be deleted when the purposes are exhausted (6), and security becomes of paramount importance (9). This can only be ensured if there is proper oversight by an independent authority (11).
Thus, the covert use of any technology can trigger a domino effect or 'slippery slope' impacting on all possible attributes: legitimacy affects data subjects' rights, affecting control and data controller's obligations.

The intrusiveness into the attributes of legitimacy, procedural rights of the data subject and external control could be only evaluated by analysing the legal basis

for the processing, which is beyond the scope of this paper. Thus, here we focus on the procedural obligations of the controller. Whether covert or overt, the use of surveillance technologies is likely to affect the following attributes.

Data proportional to the purpose of processing (data minimization)
This attribute could be affected by all technologies able to capture more than a single type of information (among the detection technologies, body scanners), and that can record the data (data retention).

End of authorization means end of processing (purpose limitation/ data retention/ remote)
This attribute can be intruded upon by technologies able to record the information detected, unless promptly deleted.

Quality/Integrity of data (accuracy, brought up to date and reliability of data)
All technologies that detect (collect) more than one type of information can affect this attribute. Raw technologies (low-resolution CCTV), and technologies directed by software can be more intrusive.

Special regime for sensitive data (the processing of special categories of data)
Sensitive data can be detected in various ways and unintentionally. All technologies that detect more than one piece of information (body detection/ tracking/ sound/ CCTV/ data fusion and mining/ interpretation) can affect this attribute. The collection of sensitive data can pave the way to discriminatory effects.

Security of processing (integrity and confidentiality) of data
This attribute can be affected by simple detection technologies that transmit data over the Internet, technologies performing complex functions that transmit the data over a network and can record the data: CCTV with wireless mode/ Ethernet cable, and technologies able to record.

Man in the loop (prohibition of automated individual decisions)
This attribute can be affected by technologies that perform interpretation based on software, and can lead to the identification of a person.

3.2.2 Article 10. Freedom of thought, conscience and religion (title II- Freedoms)

1. Everyone has the right to freedom of thought, conscience and religion. This right includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance.
2. The right to conscientious objection is recognised, in accordance with the national laws governing the exercise of this right.

The rights guaranteed in paragraph one subsumes article 18 UDHR, as reaffirmed in article 18 ICCPR and, as clarified by the Explanations, correspond to, and shall be interpreted in line with, article 9 ECHR. The duty of the state to respect means behaving in a neutral manner with regards to the affairs of the religious community, and impartially in the regulation of the religious communities. However, the state has also positive obligations, in that it must take measures to ensure the peaceful enjoyment of the right in its three dimensions.

The internal dimension (*forum internum*) concerns the freedom to have thoughts and religious convictions, meaning "[V]iews that attain a certain level of cogency, seriousness, cohesion and importance".[119] It both implies that nobody can be forced to reveal one's convictions, and not to be coerced to adopt any. It is absolute, i.e. it can neither be derogated, nor limited, and could be an element of the core. This dimension includes the right to change religion, which is more controversial, especially in Muslim countries.

The external dimension (*forum externum*) concerns the freedom to manifest, in community or in private, one's religious belief, and to follow religious prescriptions, including through clothing. Yet, some types of manifestation of religious convictions are not safeguarded by article 9 ECHR (and thus article 11 of the Charter), such as assisted suicide (see *Pretty vs. UK*). The external dimension includes the right to proselytise, through teaching but not, for instance, the promise of social or economic advantage.[120]

The collective dimension refers to the freedom to celebrate the religion as a group, or community, without the state's intervention, insofar as none of the grounds for limitation applies. For instance, illicit sects and cults are not safeguarded by article 11. A state can require religious communities to be registered as such.[121]

Freedom of thought, conscience and religion shall only be limited on the same grounds listed in article 9(2) ECHR, namely limitations prescribed by law that are "necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others." A stricter regime for permissible limitations could be introduced pursuant to article 52 (3).[122] It should be noted that national security is not one of the grounds for restricting this right.[123]

[119] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union', at 109.
[120] Ibid.
[121] Ibid.
[122] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.
[123] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.

3.2.2.1 Potential intrusiveness of surveillance technology into attributes[124]

The following attributes have been identified based on the authoritative interpretation of this right, including the HRC General Comment n. 22. The use of intrusive surveillance technologies can trigger, or be combined with, discriminatory practices that can considerably increase the negative impact on this right for certain categories of people.

1. Choice of (= to have or to adopt) thought, conscience and religion (*forum internum*)

This attribute captures an absolute feature of this right, which can be neither derogated from, nor limited. It expresses the right of a person not to share one's religious preferences. Its intrusion can also be an intrusion of the attribute of the right to privacy named 'psychological integrity'. Any surveillance technology that can lead to unveil somebody's creed can intrude into this attribute. These are technologies that can perform tracking (GPS), data mining from data fusion (SCIIMS, data analysis) and interpretation.

The result of obtaining such information is the detection (collection and processing) of sensitive data, and can lead to discriminatory practices on grounds of faith. It also impacts on the *forum externum*.

2. Freedom to manifest religion or belief

This attribute encompasses both an individual (*forum externum*) and collective dimension, including: rituals and ceremonies, public and private symbols, days of worship and rest, dietary and clothing practices, distribution of religious texts, establishment of institutions, conscientious objection to certain otherwise lawful duties imposed by the state.

The intrusion into *the forum externum* of an individual passes through the observation of one's movements, social life and behaviour. As such, it is a consequence of the intrusion upon the following attributes of privacy: personal development and identity, social identity, and autonomy and participation. The use of body scanners, moreover, could strongly affect this right, as being subjected to it is contrary to some religions' precepts.

This attribute could be affected by the chilling effect (or feeling of intimidation), deriving from the use of any surveillance technologies against people manifesting any or specific (discrimination) religious beliefs. The chilling effect could in turn affect the *forum internum*. Thus, all of the listed technologies may cause this reaction if used in a discriminatory manner.

The intrusion into the collective dimension is analysed in the context of the explicit attribute below.

3. Collective dimension of freedom of religion and belief

This attribute covers the right to form and institutionalise religious communities, and their right to internal autonomy without interference by the state. It

[124] As identified and partly drafted by Martin Scheinin.

overlaps with the attribute immediately above (manifestation) and the attribute below (education). Examples include:

- Public CCTV cameras where used to monitor movements at places of worship or religious schools;
- Sound recording functions: a microphone installed at a place of worship/ religious school to intercept discussions among the members.
- Tracking functions: (GPS) where used to follow the members of a religious groups
- Interpretation/mining functions: takedown of website of the religious group by means of prohibited keywords (OMNIFIND); monitoring (public) activities online of members of a certain religious groups.

4. **Freedom of religious or other world-view based education**

This attribute includes the following dimensions: freedom to establish educational institutions, the prohibition against compulsory religious education against one's own conviction, and the state guarantees for neutrality.

This attribute could be affected by the chilling effect (or feeling of intimidation), derived from the use of any surveillance technologies against religious schools, or by the discrimination practiced against certain types of associations. Thus, all of the listed technologies may cause this reaction if used in a discriminatory manner.

3.2.3 Article 12. Freedom of assembly and of association (title II- Freedoms)

> *1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests.*
> *2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.*

The ECHR protects freedom of assembly and association in its article 11, which, as clarified by the explanations, informs article 12.1 of the Charter (although the scope of the latter is wider since it applies at the level of the EU, too[125]). The case law of the ECtHR has clarified that the article envisages positive obligations for the state, in that it should adopt reasonable and appropriate measures to ensure the peaceful development of lawful demonstrations.

As for freedom of assembly, it covers all types of peaceful meetings, whether private or public, static or in procession, that have not been prohibited. States

[125] Freedom of assembly and association is also enshrined in article 20 of the Universal Declaration of Human Rights and Articles 21 and 22 ICCPR, the ILO Convention 87 concerning Freedom of Association and Protection of the Right to Organize, Article 8 ICESCR, and Article 5 of the revised European Social Charter and *Article 11 of the Community Charter of the Fundamental Social Rights of Workers.* European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.

should refrain from taking measures indirectly restricting this right, including through sanctions.

As for freedom of association, the scope of the article is limited to the protection of private associations, which includes private parties,[126] trade unions, and civic associations. Associations are safeguarded from foundation to dissolution. Political parties enjoy a special protection due to their relevance in the life of the Union. The case law has widened the scope of the article, which now includes the freedom not to join an association.

Pursuant to article 52(3), limitations to the freedom of association and assembly shall be interpreted strictly, and not exceed those set in the ECHR, namely restrictions "that are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, 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. This article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State." The scope of permissible limitations for this specific category needs to be clarified. As for paragraph 2, it draws from Article 10(4) TEU.[127]

3.2.3.1 Potential intrusiveness of surveillance technology into attributes

Neither a UN indicator chart nor a HRC General Comment exists on this right. Thus, what follows is a truly experimental suggestion of attributes, based on the interpretation of the right, and the features of the neighbour right to freedom of though, conscience and religion. The use of intrusive surveillance technologies can trigger, or be combined with, discriminatory practices that can considerably increase the negative impact on this right for certain categories of people.

1. Freedom of assembly (collectively manifest opinions, creed, etc.)

This attribute encompasses both an individual (*forum externum*) and collective dimension. The *forum externum* overlaps with the freedom of expression. The collective dimension overlaps to some extent with the freedom of conscience, thought and religion.

This attribute can be intruded upon in combination with, or without, discrimination against the individual or the group.

The intrusion upon *the forum externum* of an individual passes through the observation of one's movements, social life and behaviour. As such, it is a consequence of the intrusion on the autonomy and participation attribute of privacy.

---

[126] Public associations are distinguished by the following factors: "whether an entity was founded not by individuals but by the legislature; whether it remains integrated within the structures of the State, pursues an aim which is in the general interest by exercising a form of public control; and whether it is legally invested with administrative as well as rule-making and disciplinary prerogatives." European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union', at 129.

[127] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.

Its collective element could be intruded into by the use of technologies that detect chemical substances during assemblies, or technologies that perform identification of participants in the assembly (see freedom of expression and information).

2. Freedom to form associations, including trade unions, and to collective bargaining

This attribute captures the right to create any types of association, and thus has strong connections with the attribute of 'collective dimension of freedom of religion and belief'. The following surveillance technologies could intrude upon it:

- Public CCTV cameras where used to monitor movements at the headquarters of associations;
- Sound functions: a microphone installed at the headquarter to intercept discussions among the members;
- Tracking functions: (GPS) where used to follow associations and trade unions' members;
- Data mining and interpretation: takedown of website of the association by means of prohibited keywords (OMNIFIND), monitoring of the online public activities of members of certain associations.

3. Freedom to join or not to join a private association

This attribute could be affected by the chilling effect (or feeling of intimidation), derived from the use of any surveillance technologies against associations, or by the discrimination practiced against certain types of associations. Thus, all of the listed technologies may cause this reaction if used in a discriminatory manner.

3.2.4 Article 45. Freedom of movement and of residence (title V- Citizenship)

> *1. Every citizen of the Union has the right to move and reside freely within the territory of the Member States.*
> *2. Freedom of movement and residence may be granted, in accordance with the Treaties, to nationals of third countries legally resident in the territory of a Member State.*

While the right takes stock of existing provisions, such as article 13 UDHR and article 12 ICCPR, it draws mainly from 'internal' sources.[128]

The two paragraphs of the provision refer to two different categories of right holders. Paragraph 1 concerns citizens of the EU, i.e. citizens of one of its member states. It expresses the right guaranteed by articles 20(2)(a) TFEU and 21 TFEU,[129] which are complemented by secondary law, in particular on the free movement of workers (article 45 TFEU), services (article 56 TFEU), right of

[128] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[129] See also the judgment of the Court of Justice of the European Union in Case C-413/99 (Baumbast 2002). European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.

establishment (article 50 TFEU) and the absence of internal border controls (article 77 TFEU, which applies to any person, regardless the nationality).

The legal framework is well developed in connection with certain categories, such as workers and their families (in observance of article 7 on private and family life), whereas it lags behind for students and pensioners (who must have sufficient resources). The notion of family members encompasses spouse, descendants and parents, but may not include *de facto* and same-sex couples. The right to enter and exit the territory of other EU member states is conferred by the treaties, but is not unconditional. The right to establishment is accompanied by non-discrimination, but it can be subordinated to legitimate interests of the hosting country.
Thus, article 20 TFEU recognizes that "these rights shall be exercised in accordance with the conditions and limits defined by the Treaties", as defined by article 52(2) of the Charter and the ECHR. Public order (as further defined by Directive 64/221 of 25 February 1964), national security, public health and morals can be grounds to limit the enjoyment of the right to establishment. A Member state may also adopt administrative police measures to prohibit citizens of other member states from residing in a given portion of its territory.[130]

Paragraph 2 refers to the power granted to the Union by Articles 77, 78 and 79 TFEU, and varies according to the specific institution that exercises that power.[131] The use of the modal verb 'may' suggests a possibility to be granted the right, rather than an entitlement to it; the institutions and member states are under no obligations to adopt positive measures in this sense. The category of national of third countries concerned here is 'residual', in that it includes all those that are neither family members of a citizen, nor refugees.

Legal grey areas remain for what concerns the visa policy, which is necessary for the access to the job market, and the return of irregular migrants. Even though the issue of nationality opens a breach into the prohibition of discrimination (see *supra* 3.1.1), legal migrants enjoy the protection of article 21, which applies to employment, education, social security, health, housing and access to property and services.[132]

3.2.4.1 Potential intrusiveness of surveillance technology into attributes

The following attributes have been identified[133] based on the innovations of article 45, and the authoritative interpretation of freedom of movement, including the HRC General Comment No. 27.[134] The use of intrusive surveillance technologies can trigger, or be combined with, discriminatory practices that can considerably increase the negative impact on this right for certain categories of people.

[130] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[131] Ibid.
[132] Ibid.
[133] As identified and drafted by Martin Scheinin.
[134] Human Rights Committee, 'General Comment No. 27. Freedom of Movement (Article 12)'.

1. Liberty of movement and freedom to choose residence

This attribute bears multiple dimensions: the freedom of movement across the EU's internal borders; the prohibition against internal banishment or forced residence; and the use of control orders instead of the deprivation of liberty as permissible restrictions.

This attribute (and its dimensions) can be intruded into by technologies that perform tracking functions, applied both to the body (person, e.g. GPS-based car trackers), and to the environment. The latter includes the two types of drones if used to patrol borders (platform micro helicopter, platform helikite balloon). Image processing software (crowd and riot, people counting and density) used at the border could also affect the intra-EU liberty of movement.

2. Right to enter one's own country

In the EU, all member states qualify as 'one's own country' for EU citizens (and recognized third-country nationals). As a corollary, no one can be expelled from one's own country (however, the extradition/ arrest warrant between EU countries, and the handing over to international tribunals are not considered violations of this right).

Clearly, the right to enter one's own country may be denied on discriminatory grounds. However, the intrusion upon this attribute is extremely unlikely in the EU, and its affection would be a clear signal of the deterioration of the conditions of democracy of one of the Union's member states.

3. Freedom to leave any country, including one's own

This attribute captures, first, the opposite dimension of the right to enter one's country, namely the right to leave one's country and, second, the right to leave *any* country. Both dimensions are subject to lawful restrictions as determined by international law (e.g. imprisonment etc.).

The same remark as regards the deterioration of the conditions of democracy apply here in relation to EU citizens. Non-EU citizens are subject to a double standard, depending on the country of origin, as the EU may act in such a way as to prevent third-country nationals to leave their countries to reach the EU. The only listed surveillance technologies that could affect the second meaning of this attribute (extra-EU countries for EU citizens, and the EU for a non-EU citizen) are those that interpret data and can lead to the identification of a person, in case they produce false positives, such as Data transfer analysis and SCIIMS.

4. **Rights at border points as foreigner**

This attribute incorporates the right to request asylum, and the right to be treated fairly and lawfully at the border. This attribute could be affected if foreigners were discriminated against based on nationality. The technologies that could affect this attribute, in connection with discrimination, are those that can be used at customs/borders, i.e. 'simple' detection technologies such as the two types of body scanners and chemical substances detectors.

Surveillance technologies that perform interpretation of data and can lead to the identification of a person, such as data transfer analysis and SCIIMS, can be intrusive in case they produce false positives (which is tied to their effectiveness).

3.2.5 Article 1. Human Dignity (title I- Dignity): a special right

Human dignity is inviolable. It must be respected and protected.

The right enshrined in the EUCFR takes inspiration from the corresponding article 1.1 of the German Basic Law (constitution).[135] Article 1 enjoys a deliberately[136] unique role in the Charter. On the one hand, it is the foundation for, and gives substance to, all rights enshrined in the EUCFR, in particular articles "6, 7, 8, especially 10, 19 (2) and 21, further Articles 47, 48, also 14, 25, 41 (1) and 34 (3)", which often have priority as test standard.[137] Yet, this does not mean that it only gains substance when related to other rights. In fact, and on the other hand, it is an independent right, as the Court of Justice recognized in its judgment of 9 October 2001 in Case C-377/98 Netherlands v European Parliament and Council [2001] ECR I-7079 (grounds 70 - 77).[138] This means that value and substance are inextricably linked. The right expresses the value that dignity attaches to the human being, regardless of any additional criteria. As such, it protects self-determination. It also embodies the idea that the EU exists for the human being, for the person (and not vice versa), even after death. Accordingly, the action of the EU should be to respect and protect the dignity of the persons.[139]

As for its substantive elements, dignity is 'inviolable,' that is 'absolute': it is neither subject to permissible limitations, nor to derogation. Dignity can neither be lost, nor forfeited. Even the authors of detestable actions retain, and deserve respect for, dignity. Consequently, no one can damage another person's dignity on the basis of a right enshrined in the Charter (whereas there could be a collision between two persons' dignity[140]).
The second sentence denotes the obligation for the institutions and the member states to respect and protect. This means that they have positive obligations to take measures that ensure the widest possible enjoyment of this right.

There has not been any work on the attributes for this right; this is not surprising, given its ancillary role when it comes to test standards for infringement, and thus the difficulty of marking clear boundaries between

[135] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[136] Ibid.
[137] Ibid., at 28.
[138] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.
[139] European Union Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union'.
[140] European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights'.

dignity and the rights it informs. However, we should note an important aspect of this right, which should be highlighted in the case of those technologies that treat the person as an object of study: the obligation to treat the subject of law as a person. This should be incorporated in all policies that address the use of technologies.

3.3 Spill over to other fundamental rights and contextual approach

Clearly, the analysis conducted in the previous sections is abstract and, as a result, rough. The intrusiveness should be evaluated in context: a measure with a clear legal basis to address a threat/hazard in a given jurisdiction.
Yet, it should already be clear from now (and the classification, *infra* 4.24.2) that fundamental rights are interrelated: the intrusiveness into a right (its specific attribute) can trigger a domino effect leading to the infringements of other rights. In particular, many rights are affected as a result of an intrusion into the rights to privacy and non-discrimination. A wider selection of articles from the EUCFR could only reinforce this result.

For instance, the covert use of any technologies could trigger an infringement of the right to a good administration (article 41 EUCFR, title V - citizens' rights). Discriminatory approaches would seriously affect the right to equality before the law (article 20 EUCFR, title III - equality). Social and economic rights are also to be taken into account. The use of body scanners could seriously compromise the right to health (article 35 EUCFR, title IV - solidarity). Some practices involving the processing of DNA data could be also read under the lens of the right to the integrity of the person (article 3, title I - dignity).

If the scope of the analysis were to be enlarged beyond the use of surveillance technologies in the AFSJ, the right to fair working conditions (article 31 EUCFR, title IV - solidarity) would also be infringed, and the right of collective bargaining and action (article 28, title IV - solidarity). In fact, surveillance technologies are being extensively used to monitor employees in the workplace.

Moreover, the evidence collected through the infringement of a right could also lead LEAs to indict a person for serious crime. Is the evidence collected by means of infringement of fundamental rights admissible in courts? This is a question that can be answered in the context of the right to an effective remedy and to a fair trial (article 47 – title VI Justice). Indictment, or the collection of such evidence, could be followed by deprivation of liberty. This is when the right to liberty and security (article 6, title II – freedoms) comes into place, and why an analysis in the abstract of the intrusiveness of technologies into this right would not produce relevant results. Thus, even though the study conducted by the OHCHR identified attributes, this right has not been included in the analysis above, and should rather be assessed within a contextual analysis. This also concerns the dramatic case whereby evidence lead to repatriation of a suspect and exposure to torture or inhuman or degrading treatment (article 4, title I – dignity), or application of such aberrant practices in the territory of one of the member states of the EU.

4 Classification of technologies based on their intrusiveness into fundamental rights

What follows is a synthetic representation of the classification of technologies on the basis of their potential intrusiveness into the (attributes of the) fundamental rights reviewed. This classification does neither directly lead to ranking nor to a tool allowing to select among surveillance technologies, which is a later goal of the SURVEILLE project.
The chapter is divided into two parts: those technologies that are not intrusive into fundamental rights, and those that are potentially intrusive.

4.1 Surveillance technologies that are not intrusive into fundamental rights

The following surveillance technologies do not affect fundamental rights:

- Marine radar (ship);
- AIS ship location detection and identification (ship);
-

The following technologies may contribute to safeguarding the fundamental rights to life (article 2, paragraph 1: *Everyone has the right to life) and to health care (article 35, second clause: "*A high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities"):

- Airborne IMS bio protect (environment);
- Novel detection technique (COMMONSENSE) (waste water);
- Explosive detection near harbour (UNCOS);
- SIRIUS 3RK3.

4.2 Surveillance technologies that can intrude into fundamental rights

In the following pages, four synthetic tables summarize the potential intrusiveness of the five main functions of surveillance technologies into the attributes of fundamental rights.

The right column lists the seven rights whose attributes have been identified: non-discrimination, privacy, freedom of expression, data protection, freedom of thought, conscience and religion, freedom of assembly and association, and freedom of movement. The three horizontal strings refer, top to bottom, to the technology type, its functions, and the side effects caused by their overt or covert use. As for the latter, any surveillance technologies used covertly could intrude into the following attributes:

- Special measures/participation in policy-making (non-discrimination);

- Access to/ right to receive information (freedom of expression);
- The slippery slope of data protection, that is a domino effect involving legitimacy/ data subjects' rights/control/data controller's obligations (data protection);
- Data deletion (data protection);
- Data minimization (data protection);
- Security of processing (data protection).

If a surveillance technology were used overtly, or its existence and use were known, it could generate a chilling effect susceptible of affecting the following attributes:

- *Protection of the person* (non-discrimination/core dimension);
- Freedom to express/impart information (expression);
- Forum externum (religion);
- Freedom to join an association (association and assembly);
- Religious education.

Any surveillance technologies used in a discriminatory manner could intrude into the attribute 'Direct or indirect discrimination' (non-discrimination).
The crossing of the vertical and horizontal columns determines what attribute of a given right is intruded into in the abstract by a given technological function.

In each table, the use of bold signals a core attribute. The use of an asterisk symbol indicates that the intrusion into the attribute is a secondary effect of the intrusion into another (primary) right. In particular, one star signals secondary effect, two stars a tertiary one or more.

The tables should be read as cumulative, in that some technologies encompass several functions highlighted in tables 1-4.

4.2.1 Simple detection of bodies, objects, chemical substances, sound and data

The first table (figure 3 below) encompasses simple detection of bodies, objects, chemical substances, sound and data.

	technology type	*Antibody, gas cromatography, CUSTOM, Optix, X-ray*	*X-ray*	*Mmwave & Array-based body scanners*	*Infra-red (near field and wide area)*	*Microphone, Visual spectrum dome (mobile and fixed); visual spectrum fixed; IPS Activity detection*	*I-phone tap*			
fundamental rights	**object of detection**	**chemical substance**	**object (gun)**	**body (gun, chemical)**	**body (heath)**	**sound**	**data**	**effects from use (all)**	*covert use*	*overt use (chilling effect)*
Non-discrimination		direct/indirect discrimination		direct/indirect discrimination		direct/indirect discrimination	direct/indirect discrimination		special measures/ participation in policy making	direct/indirect discrimination (perceived); **protection of the person**
Privacy		**personal identity/development**		**physical integrity**	family life; home sanctity	**psychological integrity;** social identity and relations; family life; home sanctity; **confidential communications**	social identiy and relations; **confidential communications; psychological integrity***			**personal identity/development**
Expression and information		freedom of expressing opinion and to impart information *				freedom of expressing opinion and to impart information;freedom to express/impart information*; Pluralism of the media**	freedom of expressing opinion and to impart information		access to/receive information	freedom to express/impart information
Data protection			data minimization	data minimization; integrity of data	integrity of data	sensitive data*; integrity of data	sensitive data; security of processing		slippery slope of data protection;	
Thought, conscience, religion						**forum internum *;** forum externum*; collective dimension	**forum internum ***			forum externum; **forum internum;** religious education
Assembly and association		freedom of assembly *				freedom to form associations*				freedom to join association
Freedom of movement		foreigners' rights at border*		liberty of movement	liberty of movement					

Figure 3 - Simple detection functions

4.2.2 Tracking and recording

The second table (figure 4 below) gathers tracking in its various forms, and the recording function.

	technology type	*GPS*	*Short range for intrusion detection*	*Passive radar through wall*	*Platform micro helicopter; platform helikite balloon, people counting and density; array based*	*Image processing software*				
fundamental rights	**object of detection**	**motion (mobile or active)**	**motion (fixed or static)**		**body, object, motion (mobile)**	**bodies, object, identity(?)**	**effects from use (all)**	**covert use**	**overt use (chilling effect)**	**recording (if recording software is embedded or added)**
Non-discrimination		direct/indirect discrimination			direct/indirect discrimination (also **)	direct/indirect discrimination		special measures/ participation in policy making	direct/indirect discrimination (perceived); **protection of the person**	
Privacy		autonomy and participation; home sanctity	autonomy and participation	home sanctity; family life	autonomy and participation	autonomy and participation				
Expression and information		freedom to express/ impart information*; pluralism of the media ** (if targets journalists)				freedom to manifest & collective dimension		access to/receive information	freedom to express/ impart information	
Data protection		sensitive data*	data integrity	data integrity	data integrity; sensitive data	man in the loop		slippery slope of data protection; data minimization; security of processing;		data minimization (sensitive data); data integrity; security of processing; data retention
Thought, conscience, religion		**forum internum*;** forum externum		collective dimension					forum externum; **forum internum;** religious education	
Assembly and association		freedom to form association; freedom of assembly*		freedom to form association	freedom of assembly*	freedom of assembly*			freedom to join association	
Freedom of movement		liberty of movement/residence			liberty of movement/residence	liberty of movement		liberty of movement/residence*	liberty of movement/residence*	

Figure 4 Tracking and Recording functions

4.2.3 The interpretation and identification functions

Table three (figure 5 below) shows the impact of the interpretation and identification functions.

	technology type	*Visual semi-automated, image processing software; visual spectrum dome tilt*	*IPS activity; visual spectrum fixed; platform helikite balloon; people counting; density and array based*				
fundamental rights	**function**	**identification**	**interpretation**	**effects from use (all)**	covert use	chilling effect from overt use	detection and recording
Non-discrimination		direct/indirect discrimination (also **);	direct/indirect discrimination (also **);		special measures/ participation in policy making	direct/indirect discrimination (perceived); **protection of the person**	direct/indirect discrimination;
Privacy		social identity and relations; autonomy and participation	**personal development and identity;** social identity and relations				social identity and relations;family life; home sanctity; autonomy and participation
Expression and information		freedom to express/ impart information*; pluralism of the media** (if targets journalists)			access to/receive information	freedom to express/ impart information	freedom to express/ impart information*; pluralism of the media * (if targets journalists)
Data protection		sensitive data**	sensitive data*; man in the loop; data integrity		slippery slope of data protection; data minimization (sensitive data*)		data minimization; data integrity; security of processing; data retention
Thought, conscience, religion		collective dimension*; **forum internum***	collective dimension*; **forum internum***			forum externum; **forum internum;** religious education	forum externum*; collective dimension*
Assembly and association		freedom to form associations*; freedom of assembly*	freedom to form associations*;			freedom to join association	freedom to form association*; freedom of assembly
Freedom of movement					liberty of movement/residence*	liberty of movement/residence*	

Figure 5 Interpretation and Identification functions

4.2.4 Data fusion

Table four (figure 6) is dedicated to the 'data fusion' family and its various sub-functions: data fusion, mining, interpretation, and identification.

	technology type	*HEMOLIA, SCIIMS, OMNIFIND, AMFIS Data Fusion*	*HEMOLIA, SCIIMS, OMNIFIND*	*HEMOLIA, OMNIFIND, data transfer analysis (DTA)*	*HEMOLIA, SCIIMS, data transfer analysis (DTA)*			
fundamental rights	**function**	data fusion	data mining	data interpretation	identification throug data	**effects from use**	covert use	chilling effect from overt use
Non-discrimination				direct/indirect discrimination**	direct/indirect discrimination**		special measures/ participation in policy making	direct/indirect discrimination (perceived); **protection of the person**
Privacy		social identity and relatons*; **condifential communications** (HEMOLIA)	**psychological integrity***	**personal development and identity;** social identity and relations; **psychological integrity***	autonomy and participation; social identity and relations; **psychological integrity***			
Expression and information		freedom to express/ impart information* (SCIIMS); pluralism of the media **(SCIIMS; OMNIFIND); access to/receive information (OMNIFIND)	freedom to express/ impart information* (SCIIMS); pluralism of the media (SCIIMS, OMNIFIND); access to/receive information (OMNIFIND)	access to/receive information* & pluralism of media** (OMNIFIND)			access to/receive information	freedom to express/ impart information
Data protection		data minimization; data integrity	sensitive data*	sensitive data**; **man in the loop**; data integrity	sensitive data**		slippery slope of data protection; data minimization; sensitive data*	
Thought, conscience, religion			forum externum*; **forum internum;** collective dimension (OMNIFIND)	**forum internum*;** forum externum;colective dimension*	**forum internum*;** forum externum*;			forum externum; **forum internum;** religious education
Assembly and association				freedom to form associations	freedom of assembly**			freedom to join association
Freedom of movement				foreigners' rights at borders & freedom to leave country (DTA)	foreigners' rights at borders & freedom to leave country (SCIIMS and DTA)		liberty of movement/residence*	liberty of movement/residence*

Figure 6 Data fusion and its sub-functions

Tables 1 to 4 (figures 3-6) hopefully show that the more functions a technology performs, the more intrusive it can be on fundamental rights. The tables, however, also highlight that the functions found may be insufficient to fully grasp the intrusiveness of technologies, which calls for further research in SURVEILLE to refine them. Finally, the tables do not capture interrelatedness, which may be better portrayed through 'trees' as shown below.

4.3 Some examples of 'trees of intrusion' highlighting interrelatedness

In what follows, intrusiveness into attributes of fundamental rights is presented as either a discrete impact, or as a chain when the intrusion of a technology into a right causes an impact into other attributes.
While intrusiveness refers to the attributes, the right is marked in brackets, and possible violations into the core dimension/an absolute right are highlighted in *italics*.

4.3.1 Tree of possible intrusion of sound and data detection and recording

The table below shows the impact that the functions 'sound detection' and 'data collection' + 'recording (retention)' can have into the fundamental rights reviewed.

Sound (microphone) o	I phone tap (Data collection)

• Direct or indirect discrimination in AFSJ (non-discrimination)
  ○ Freedom of (expressing) opinion and to impart information (freedom of expression)
  ▪ Pluralism of the media (freedom of expression)
• *Psychological integrity* (privacy)
  ○ *Forum internum* (thought, conscience and religion)
• Social identity and relations (privacy)
  ○ Freedom to manifest (thought, conscience and religion)
• Family life (privacy)
• Home sanctity (privacy)
• Sensitive data (data protection)
	• Direct or indirect discrimination in AFSJ (non-discrimination)
	• Social identity and relations (privacy)
	• *Confidential communications* (privacy)
	  ○ *Forum internum* (thought, conscience and religion)
	  ○ *psychological integrity* (privacy)
	• Sensitive data (data protection)
	• Security of processing (data protection)

4.3.2 Tree of possible intrusion of simple detection (body heath)

The table below shows the impact that the detection function can have into the fundamental rights reviewed.

Body heath (infrared near-field and wide area)
• Direct or indirect discrimination in AFSJ (non-discrimination) • Family life (privacy) if directed against one's house • Home sanctity (privacy) • Integrity of data (data protection)

4.3.3 Tree of possible intrusion of tracking functions

The table below shows the impact that the tracking function can have into the fundamental rights reviewed.

Object/person/motion (Platform micro helicopter (UAV))	GPS (body in motion)

• Autonomy and participation (privacy)
  ○ Freedom of assembly (assembly and association)
• Integrity of data (data protection)
• Liberty of movement/residence (intra EU) (freedom of movement)
	• Autonomy and participation (privacy)
	  ○ Freedom of (expressing) opinion and to impart information (freedom of expression)
	  ▪ Pluralism of the media (freedom of expression).
	  ○ *Forum internum* (thought, conscience and religion)
	  ○ Freedom to manifest (thought, conscience and religion)
	  ○ Sensitive data (data protection)
	  ○ Freedom of assembly (assembly and association)
	• Liberty of movement/residence (intra EU) (freedom of movement)

4.3.4 Tree of possible intrusion of the identification and interpretation functions

The table below shows the impact that the identification and interpretation functions of different technologies can have into the fundamental rights reviewed.

Identification (High Resolution (ID.) Visual semi-automated)	**Interpretation (**IPS activity detection and Visual spectrum (fixed)

• Direct or indirect discrimination in AFSJ (non-discrimination)
  ○ Collective dimension (thought, conscience and religion)
  ○ Freedom to form
	• Direct or indirect discrimination in AFSJ (non-discrimination)
	  ○ Sensitive data (data protection)
	  ○ Collective dimension (thought, conscience and

associations (assembly and association) • Social identity and relations (privacy) o Freedom of (expressing) opinion and to impart information (freedom of expression) [as a consequence of the 3 above] ▪ Pluralism of the media (freedom of expression) o *Forum internum* (thought, conscience and religion) ▪ Sensitive data (data protection) • Direct or indirect discrimination in AFSJ (non-discrimination)] • Autonomy and participation (privacy) o Freedom of assembly (assembly and association)	religion) o Freedom to form association (assembly and association) • *Personal development and identity* (privacy) • Social identity and relations (privacy) o *Forum internum* (thought, conscience and religion) ▪ Sensitive data (data protection) • Direct or indirect discrimination in AFSJ (non-discrimination) • Man in the loop (data protection) • Integrity of data (data protection)

4.3.5 Tree of the intrusion of data fusion sub-functions

The table below shows the impact that the different functions of the HEMOLIA software can have into the fundamental rights reviewed.

Detected object	**Attributes affected**
Data fusion	• *Personal development and identity* (privacy) • *Confidential communications* • Data minimization (data protection) • Quality/Integrity of data (data protection)
Data mining	• Freedom to manifest (thought, conscience and religion) & *Forum internum* (thought, conscience and religion) o Sensitive data (data protection) o *Psychological integ*rity (privacy)
Data interpretation	• *Personal development and identity* (privacy) • Social identity and relations (privacy) o *Forum internum* (thought, conscience and religion) & freedom to manifest ▪ Sensitive data (data protection)

	▪ *Psychological integrity* (privacy) • Direct or indirect discrimination in AFSJ (non-discrimination) • Man in the loop (data protection) • Sensitive data (data protection) • Quality/Integrity of data (data protection)
Identification through data	• Autonomy and participation (privacy) • Social identity and relations (privacy) o *Forum internum* & freedom to manifest (thought, conscience and religion) o *Psychological integrity* (privacy) o Freedom of assembly (assembly and association) ▪ Sensitive data (data protection) • Direct or indirect discrimination in AFSJ (non-discrimination)

5 Conclusions: opportunities for further research

This deliverable classified the potential for intrusiveness of surveillance technologies into a selected number of fundamental rights enshrined in the EUCFR. The analysis was carried out by appraising the impact of abstract functions of technologies into attributes of the chosen fundamental rights.

The purpose of this exercise was to capture the depth, or granularity, of potential intrusiveness, as well as the interrelatedness of fundamental rights. Such analysis has value per se. In fact, it calls for reflections on how the battle for different fundamental rights could be integrated to secure their enforcement. Consider the case of the covert use of technologies, which worsens the problematic lack of public discussion on security technologies. Covert use affects the attributes 'participation in public policy-making' (non-discrimination, article 21 EUCFR); 'access to information' (freedom of expression and information, article 9 EUCFR); and triggers 'the slippery slope' of data protection (article 8 EUCFR). The latter contains 'legitimacy', which, as clarified by the formulation of article 8, is either based on law or individual's consent. Individual consent is often criticized as a rubber-stamp feature of this right due to the imbalance of power between the individual and the public/private sectors. Yet, considering the issue in conjunction with non-discrimination and freedom to expression and information may suggest that, in the use of security technologies, individual consent should be replaced by mandatory public procedures of technology assessment carried out *ex ante*, and *ex post* public scrutiny, thus guaranteeing the three rights together.

A further attempt was that of capturing potential core areas of rights: features whose intrusion would always be a violation of the right in question and hence impermissible. A limit of this exercise was the abstract reasoning behind it.

However, it is possible to draw a number of conclusions for research in SURVEILLE. First, further research and synergies among SURVEILLE partners are needed in order to select the relevant technological functions, and devise scenarios where the abstract and concrete analysis could be performed. Such scenarios should distinguish between legitimate uses and abuses of the technologies.
Second, the analysis calls for a serious assessment of the intrusiveness of technologies in relation to the admissibility of evidence in courts in the course of criminal processes, and of the test to evaluate whether the right to effective remedy and a fair trial is respected (article 37 EUCFR). In this sense, this deliverable reinforces the findings of D4.1[141]
Third, this research could provide input for a practical application of the technology assessment in further work within the SURVEILLE project. On the one hand, the study on attributes could help identifying cores of rights, the intrusion into which would always be impermissible. This could guide the

[141] Céline Cocq and Francesca Galli, 'Surveille Deliverable 4.1: The Use of Surveillance Technologies for the Prevention and Investigation of Serious Crimes', (2012).

discussion as to what types of actions and technologies our society is ready to allow.
On the other hand, the analysis in this deliverable can be used for further SURVEILLE work on "costs" of the use of surveillance as a broad notion that includes also societal factors besides economic cost. The identification of distinct attributes of a range of fundamental rights and various ways to assess the level of intrusion will help in the assessment of the "costs" related to specific surveillance technologies.

6 References

Ackerman, Bruce (2006), *Before the Next Attack. Preserving Civil Liberties in an Age of Terrorism.* (New Haven: Yale University Press).

Advocate General Léger (2005), 'Opinion on Cases C-317&04 and C318/04'.

Agency, Fundamental Rights (2001), 'Using indicators to measure fundamental rights in the EU: challenges and solutions. FRA Symposium Report', *2nd Annual FRA Symposium Vienna* (Vienna).

Alexy, Robert *Theorie der Grundrechte* (Suhrkamp Verlag; Auflage).

--- (2008), ' Constitutional Rights and Legal Systems', in Joakim Nergelius (ed.), *Constitutionalism - New Challenges: European Law from a Nordic Perspective*.

Ashworth, Andrew (2007), 'Security, Terrorism and the Value of Human Rights', in Benjamin Goold and Lazarus Liora (eds.), *Security and Human Rights* (Portland: Hart), 203-26.

'C-5/88, Wachauf V Bundesamt Für Ernährung Und Forstwirtschaft', (1989), (Judgment of the Court (Third Chamber) edn.: Court of Justice of the European Union).

Candler, Jean, et al. (2011), 'Human Rights Measurement Framework: Prototype panels, indicator set and evidence base', (London: Equality and Human Rights Commission).

'Case C-292/97 Karlsson and Others'(2000), (Judgment of the Court (Sixth Chamber), Reference for a preliminary ruling: Court of Justice of the European Union).

'Joined Cases C-402/05 P and C-415/05, Kadi and Al Barakaat International Foundation v Council and Commission (Kadi I)', (2008), (Judgment edn.: Court of Justice of the European Union).

'Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy', (2011), (Judgment of the Court (Grand Chamber): Court of Justice of the European Union).

'Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land of Hesse', (2010), (Judgment of the Court (Grand Chamber): Court of Justice of the European Union).

'Case C−614/10, Commission v. Austria', (2012), (Judgment of the Court (Grand Chamber): Court of Justice of the European Union).

'Charter of Fundamental Rights of the European Union', (2007), (Official Journal C 303/1), 1–22.

Cocq, Céline and Galli, Francesca (2012), 'SURVEILLE Deliverable 4.1: The use of surveillance technologies for the prevention and investigation of serious crimes'.

'Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)', (Official Journal C 83/01).

'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', (1981), in Council of Europe (ed.), (CETS No. 108; Strasbourg).

Council (2010a), 'Draft Internal Security Strategy for the European Union: Towards a European Security Model', (5842/2/10; Brussels).

--- (2010b), 'The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens', (OJ C 115; Brussels).

Council of Europe (1950), 'Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14', (CETS n° 005; Rome).

Court of Justice of the European Union, Opinion 2/94, 1996, ECR I-1795.

Craig, Paul and de Búrca, Gráinne (2011), *European Union Law: Text, Cases and Materials* (Oxford) 1320.

DG Justice (2011), '2010 Report on the Application of the EU Charter of Fundamental Rights', (Brussels: European Commission).

--- (2012), '2011 Report on the Application of the EU Charter of Fundamental Rights', (Brussels: European Commission).

'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', 31-50.

'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (e-Privacy Directive)', 37-47.

Donhoue, Laura K. (2008), (New York: Cambridge University Press).

Etzioni, Amitai (2004), *How Patriotic is the Patriot Act.* (New York and London: Routledge).

European Commission (2005), 'Communication. Compliance with the Charter of Fundamental Rights in Commission legislative proposals. Methodology for systematic and rigorous monitoring. COM(2005) 172 final', (Brussels), 8.

--- (2009), 'Report on the Practical Operation of the Methodology for a Systematic and Rigorous Monitoring of Compliance with the Charter of Fundamental Rights. COM(2009) 205 final', (Brussels).

--- (2010), 'Communication, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'. COM (2010) 573/4', (Brussels).

--- (2012), 'Communication on Security Industrial Policy. Action Plan for an innovative and competitive Security Industry. COM(2012) 417 final', (Brussels).

European Parliament, Council, and Commission (2007), 'Explanations Relating to the Charter of Fundamental Rights'.

European Union Network Of Independent Experts On Fundamental Rights (2006), 'Commentary of the Charter Of Fundamental Rights Of The European Union'.

General Assembly (3rd session) (1948), 'Universal Declaration of Human Rights. Resolution 217', in United Nations (ed.).

Guelke, John (2013), 'SURVEILLE Deliverable 2.2: Paper with Input from End Users'.

Human Rights Committee (1999), 'General Comment No. 27. Freedom of movement (Article 12)'.

--- (2004), 'General Comment No. 31, The Nature of the General Legal Obligation'.

--- (2007), 'General comment No. 32, Right to equality before courts and tribunals and to a fair trial'.

--- (2011), 'General comment No. 34, Freedoms of opinion and expression'.

IRISS Project Consortium (2012), 'Surveillance, fighting crime and violence, Deliverable D1.1.'.

Kreissl, Reinhard, et al. (2013), 'SurPRISE Deliverable 3.4. WP3 'Exploring the Challenges': Synthesis Report'.

Neelie Kroes (2012), 'Public-private cooperation in cybersecurity. Speech delivered at the Security and Defence Agenda dinner', (Brussels).

Porcedda, Maria Grazia, Mathias Vermeulen, and Martin Scheinin (2013), 'Report on regulatory frameworks concerning privacy and the evolution of the norm of

the right to privacy. Deliverable 3.2, SurPRISE Project. Forthcoming', (Florence: European University Institute).

'Pretty v. UK, 2346/02', (2002), (Judgment of the Court (Fourth Section) edn.: European Court of Human Rights).

'Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data', 1-21.

Rodotà, Stefano (2005), *Intervista su Privacy e Libertà. A cura di Paolo Conti*.

--- (2012), *Il diritto ad avere diritti* (Bari: Editori Laterza).

Scheinin, Martin (2009a), 'Terrorism and the Pull of 'Balancing' in the Name of Security', in Martin Scheinin (ed.), *Law and Security, Facing the Dilemmas* (11; Florence: European University Instite).

--- (2009b), 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', (Geneva: General Assembly).

Scheinin, Martin and Vermeulen, Mathias (2011), ''Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism', *Essex Human Rights Review,* 8, 20-56.

Sperber, Sebastian, Maye Seck, and Johnston, Elizabeth (2013), 'SURVEILLE Deliverable 2.3: Paper by local authorities end-users'.

SURVEILLE Project Consortium (2011), 'Description of Works of the SURVEILLE Project. Surveillance: ethical issues, legal limitations and efficiency', (Seventh Framework Programme, European Union).

United Nations (1966a), 'International Covenant on Civil and Political Rights', (New York).

--- (1966b), 'International Covenant on Economic, Social and Cultural Rights', (New Work).

United Nations High Commissioner for Human Rights (OHCHR) (2012), 'Human Rights Indicators. A guide to Measurement and Implementation', (New York and Geneva: United Nations Human Rights Office of the High Commissioner).

United Nations International Human Rights Instruments (2006), 'Report On Indicators For Monitoring Compliance With International Human Rights Instruments'.

'Uzun v. Germany', (2010), (European Court of Human Rights).

Van der Hilst, Rozemarijn (2009), 'Human Rights Risks of Selected Detection Technologies. Sample Uses by Governments of Selected Detection Technologies. DETECTER Project, deliverable 17.1'.

--- (2011a), 'Characteristics and uses of selected detection technologies, including their potential human rights risks. DETECTER Project deliverable 17.3'.

--- (2011b), 'Ranking, in terms of their human rights risks, the detection technologies and uses surveyed in WP09. DETECTER Project, Deliverable 17.4.'.

Van Gulijk, Coen, et al. (2012), 'Survey of surveillance technologies, including their specific identification for further work. SURVEILLE Project Deliverable 2.1'.