D11.1: LEGAL CONSIDERATION STUDY
Public

(Picture can be inserted here)
Main author(s)

<table>
<thead>
<tr>
<th>Partner</th>
<th>First name</th>
<th>Last Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center for Security Studies - KEMEA</td>
<td>Ioannis</td>
<td>Daniilidis</td>
<td><a href="mailto:i.daniilidis@kemea-research.gr">i.daniilidis@kemea-research.gr</a></td>
</tr>
</tbody>
</table>

Contributor(s)

<table>
<thead>
<tr>
<th>Partner</th>
<th>First name</th>
<th>Last Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Aegean</td>
<td>Evaggelia</td>
<td>Mitrou</td>
<td><a href="mailto:L.Mitrou@aegean.gr">L.Mitrou@aegean.gr</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version no.</th>
<th>Date</th>
<th>Released by</th>
<th>Comments</th>
<th>Document version</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>03/08/2018</td>
<td>KEMEA</td>
<td></td>
<td>Draft/final/submitted</td>
</tr>
</tbody>
</table>

Delivery Date: Measured in months from the project start date (month 1)
The information contained in this document may not be modified or used for any purpose without prior written permission of the owners and any request for such additional permissions should be addressed to the ENTRAP coordinator.
<table>
<thead>
<tr>
<th>Participant No.</th>
<th>Participant organisation full name</th>
<th>Abbreviated name</th>
<th>Country</th>
<th>Logo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Totalförsvarets forskningsinstitut</td>
<td>FOI</td>
<td>Sweden</td>
<td><img src="image" alt="FOI logo" /></td>
</tr>
<tr>
<td>2</td>
<td>Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek</td>
<td>TNO</td>
<td>Netherlands</td>
<td><img src="image" alt="TNO logo" /></td>
</tr>
<tr>
<td>3</td>
<td>Commissariat à l'énergie atomique et aux énergies alternatives</td>
<td>CEA</td>
<td>France</td>
<td><img src="image" alt="CEA logo" /></td>
</tr>
<tr>
<td>4</td>
<td>Agenzia nazionale per le nuove tecnologie, l’energia e lo sviluppo economico sostenibile</td>
<td>ENEA</td>
<td>Italy</td>
<td><img src="image" alt="ENEA logo" /></td>
</tr>
<tr>
<td>5</td>
<td>Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.</td>
<td>Fraunhofer</td>
<td>Germany</td>
<td><img src="image" alt="Fraunhofer logo" /></td>
</tr>
<tr>
<td>6</td>
<td>Nederlands Forensisch Instituut</td>
<td>NFI</td>
<td>Netherlands</td>
<td><img src="image" alt="NFI logo" /></td>
</tr>
<tr>
<td>7</td>
<td>The International Criminal Police Organization</td>
<td>Interpol</td>
<td>France</td>
<td><img src="image" alt="Interpol logo" /></td>
</tr>
<tr>
<td>8</td>
<td>Forsvarets Forskningsinstitutt</td>
<td>FFI</td>
<td>Norway</td>
<td><img src="image" alt="FFI logo" /></td>
</tr>
<tr>
<td>9</td>
<td>CBRNE Ltd</td>
<td>CBRNE</td>
<td>United Kingdom</td>
<td><img src="image" alt="CBRNE logo" /></td>
</tr>
<tr>
<td>10</td>
<td>Centre for Applied Science and Technology, Home Office</td>
<td>CAST</td>
<td>United Kingdom</td>
<td><img src="image" alt="CAST logo" /></td>
</tr>
<tr>
<td>11</td>
<td>National Institute for Aerospace Technology</td>
<td>INTA</td>
<td>Spain</td>
<td><img src="image" alt="INTA logo" /></td>
</tr>
<tr>
<td>12</td>
<td>University carlos III of Madrid</td>
<td>UC3M</td>
<td>Spain</td>
<td><img src="image" alt="UC3M logo" /></td>
</tr>
<tr>
<td>13</td>
<td>Guardia Civil</td>
<td>GUCI</td>
<td>Spain</td>
<td><img src="image" alt="GUCI logo" /></td>
</tr>
<tr>
<td>14</td>
<td>Polismyndigheten (Swedish Police Authority)</td>
<td>SPA</td>
<td>Sweden</td>
<td><img src="image" alt="SPA logo" /></td>
</tr>
<tr>
<td>15</td>
<td>KEMEA Center for Security Studies</td>
<td>KEMEA</td>
<td>Greece</td>
<td><img src="image" alt="KEMEA logo" /></td>
</tr>
<tr>
<td>16</td>
<td>Netherlands MoD</td>
<td>NLMoD</td>
<td>Netherlands</td>
<td><img src="image" alt="NLMoD logo" /></td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. ABBREVIATIONS .............................................................................................................. 6

2. INTRODUCTION .............................................................................................................. 7
   2.1 Legal Framework and issues raised .............................................................................. 7
   2.2 Structure of the Deliverable ....................................................................................... 9

3. The constitutional framework on European level ......................................................... 11
   3.1 The right to privacy .................................................................................................... 11
   3.2 The right to data protection ....................................................................................... 13
   3.3 The right to Communication Secrecy ........................................................................ 18
   3.4 Balancing security and freedoms ............................................................................. 22

4. The Council of Europe’s Recommendation and Guidance ......................................... 28

5. The Police and Criminal Justice Data Protection Directive (680/2016/EU) .............. 31
   5.1 A short history and goals of the new framework ..................................................... 31
   5.2 The scope of the Directive ....................................................................................... 32
   5.3 The principles ............................................................................................................ 36
   5.4 The legal basis .......................................................................................................... 37
   5.5 The rights of the data subjects ................................................................................ 38
   5.6 Other obligations of data controllers and processors ............................................. 40
   5.7 Independent oversight ............................................................................................. 43
   5.8 Relation to GDPR .................................................................................................... 44
   5.9 Relation to other legal instruments ......................................................................... 45

6. The legal framework for the fight against terrorism .................................................... 47
   6.1 The EU Directive on combating terrorism ............................................................... 47
   6.2 Counter-tools and considerations ............................................................................. 50
   6.3 Case Studies .............................................................................................................. 53
      6.3.1 RPAs as surveillance tools and the rights to privacy and data protection .......... 53
      6.3.2 Profiling Online Social Networks (OSN) Users as a Surveillance Tool .......... 60
      6.3.3 Communications / Metadata Retention as Surveillance Tool ......................... 65
1. ABBREVIATIONS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>PCJA</td>
<td>Criminal Justice Authorities Directive</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>CFREU</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Record</td>
</tr>
<tr>
<td>DPWP</td>
<td>Data Protection Working Party</td>
</tr>
<tr>
<td>APPD</td>
<td>Automatic Processing of Personal Data</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Processing Authority</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>OSN</td>
<td>Online Social Networks</td>
</tr>
<tr>
<td>RPA</td>
<td>Remotely Piloted Aircrafts</td>
</tr>
<tr>
<td>DRF</td>
<td>Data Retention Framework</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
</tbody>
</table>
2. INTRODUCTION

2.1 Legal Framework and issues raised

The ENTRAP project aims at providing a coherent and comprehensive overview of the opportunities across the timeline of a terrorist plot to obstruct, hamper and even prevent a terrorist attack involving explosives. In the course of the project, emerging threats and the respective counter tools and measures will be identified and explored and the legal frame of operations will be investigated and adapted. Of utmost importance in this context is to provide insights for intelligence units in understanding the timeline of terrorist plots involving explosives, understanding the areas where the intelligence position should and could be improved and understanding the opportunities that exist for improving the detection and prevention of terrorist attacks involving explosives.

Surveillance research and technology for instance will support security forces in preventing criminal offenses and terrorism, but contemporaneously it has ethical and legal implications. Prevention and removal of risks have become a social and political imperative in the risk society. On the other side, the excessive use of security measures may impede social and personal development too. A common ground of systems for precautionary measures and surveillance is that they are accompanied by nuisance, incident, or annoying and irritating situations, or cases where the proportionality and adequacy determines the degree of acceptance.

Designing and deploying counter-tools to face the terrorist threat is socially desirable and constitutionally acceptable only if it is grounded on a legal basis that ensures full respect for fundamental rights, with focus on the right to privacy and communication secrecy. The freedom of the individual and the security of all, i.e., the state’s tasks of guaranteeing individual, constitutionally protected freedoms, and of attending to and providing for the community's security, are inevitably in a relationship marked by tension and even contradiction\(^1\).  

\(^1\) Denninger, E., Freiheit durch Sicherheit? Wie viel Schutz der inneren Sicherheit verlangt und verträcht das deutsche Grundgesetz?, Kritische Justiz, 35, 467,
Surveillance measures raise significant concerns in relation to the respect of privacy and other fundamental rights and freedoms. Governments must respond to the new security challenges in a way that effectively meets the citizens’ expectations without undermining individual human rights “or even destroying democracy on the ground of defending it” (European Court of Human Rights, Klass v. Germany, Judgment of 6 September 1978).

Decision making for deploying security and counter-tools is a complex and multi-dimensional process, but it is not a value neutral process. Counter tools have to be assessed with regard to their effects on society and individuals’ rights. Hence, it is imperative to consider the implications of the deployment not just in the short run but also in the long run. The impact of security measures and technologies that are being considered has to be assessed from the early phase of the design and development of the idea or technologies. Respect of fundamental rights and – more specifically - compliance with legal and ethical requirements is of major importance for the development and deployment of counter-tools that are not only lawful but also accepted by society and citizens.

Research activities and projects are subject to the provisions of the General Data Protection Regulation 2016/679/EU (hereafter GDPR). This means that any gathering of data and analysis, or pilots etc. have to be compliant with the rules and conditions set by GDPR with regard to consent, collection, storage, disclosure by transmission, dissemination or otherwise making available etc. The Consortium has to consider and organize the compliance with GDPR.

The tools and procedures to be designed in the context of ENTRAP have to comply with the Police and Criminal Justice Authorities Directive (hereafter PCJA) Directive, which applies on two cumulative conditions: one relative to the identity of the controller (“a competent authority2”) and one relative to the purpose of the data processing (which must be related to

---

2 Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive (..)” (Recital 11). In conclusion, the concept of competent authority is not restricted to a strict administrative law
prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties). Our initial study focuses on the provisions and requirements set by the new Data Protection Framework, which consists primarily by the General Data Protection Regulation (2016/679/ EU-GDPR) and the Police and Criminal Justice Authorities Directive (2016/680/ EU-PCJA Directive).

### 2.2 Structure of the Deliverable

The objective of this Deliverable is to identify and raise awareness of the legal considerations and the frame within which the counter tools and the respective procedures must conform or be developed.

In Section 2 the constitutional framework and the principles deriving thereof with regard to the fundamental rights of privacy, data protection and communications secrecy are presented. In this context the conflict of public interest and competing rights is presented and the balancing criteria to solve it are proposed.

In Section 3 the Recommendation and Guidance by the Council of Europe in that set the frame in regards to the processing of personal data for law enforcement purposes is reported.

In Section 4 a detailed report on the Police and Criminal Justice Data Protection Directive (680/2016/EU) is presented. This is the core of the legal consideration study as it addresses the notion of public authority. However, as pointed by recital 11, for the Directive to apply the processor should be bound with a public authority by a contract or any other legal act that gives him the authority to collect data for such purpose and to act in practice as an "agent" of the public authority for the purpose of data processing. In all the other cases, the stricter framework of GDPR applies.
the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data” including the prevention of threats to public security. It is based on the principles and guidelines that counter tools and processes must be tailored.

In Section 5 the legal framework for the fight against terrorism is addressed. It is the focus of this project to address the issue of terrorism, the counter tools and procedures and their conformance to the legal framework as set by the EU directive.
3. The constitutional framework on European level

Information-led prevention and detection policies and the respective use of security and counter-tools interfere with fundamental rights embedded in Article 8 European Convention on Human Rights (hereinafter ECHR): the right to private life (privacy), the right to data protection and the right to respect for his correspondence.

The ECHR establishes basic rules regarding fundamental rights and liberties that are applicable throughout the contracting states. According to Art. 6 (2) of the Treaty on European Union, the ECHR is binding not only for member states, but also for the European Union as well. However, it was not until 2000 that these rights were formalized in the Charter of Fundamental Rights of the European Union (hereinafter the Charter)\(^3\). The Charter became legally binding with the entry into force of the Lisbon Treaty\(^4\) on 1 December 2009 for all Member States and the right to data protection was raised to the category of fundamental right. The right to the protection of privacy is recognized also by Art. 7 of the Charter of Fundamental Rights of the European Union. Guarantees for data protection and privacy rights are to be found in a number of instruments at the EU level.

3.1 The right to privacy

The right to privacy is a fundamental right that is recognised in international, European and national laws. For example, the right to privacy is protected in Art. 12 UDHR, Art. 8 of the European Convention on Human Rights (ECHR) and Art. 7 of the Charter of Fundamental Rights

\(^3\) The Charter is based on the ECHR and entails 54 articles divided into 6 chapters (dignity, freedoms, equality, solidarity, citizens' rights and justice), plus an additional chapter for interpretation and application purposes.

of the European Union (CFREU). The origins of the right to privacy in Europe consists of two main principles: the right to secrecy of telecommunications and the prohibition of unlawful home searches. According to the explanatory notes, the rights guaranteed in Article 7 of the Charter correspond to those guaranteed by Article 8 ECHR. Both are typical examples of classical fundamental rights, where interference is subject to strict conditions. The only difference between them is that Article 52 of the Charter contains a more general exception clause than Article 8 par. 2 of the ECHR.

The notion of privacy could be defined as freedom of unwarranted and arbitrary interference from public authorities or private actors/bodies into activities that society recognizes as belonging to the realm of individual autonomy (private sphere)\(^5\) (Data Retention - Impact 23). The European approach to privacy is largely grounded to the dignity of the person, who operates in self-determination as a member of a free society (German Federal Constitutional Court, Census case, 1983). Dignity as related to privacy is a concept summarizing principles such as protection of individual’s personality, non commodification of the individual, noninterference with other's life choices, and the possibility to act autonomously and freely in society\(^6\) (Data Retention - Impact 36, 16).

Measures of surveillance can constitute an interference with fundamental rights, such as the right to privacy, especially if such measures are of a secret or preventive nature\(^7\). The right to privacy protects private life even “in public” and – according to the jurisprudence of the Strasburger Court it covers also the processing of data relating to the private life of individuals,


with a broad interpretation of private life. Before 2000, it was relatively common to declare that the right to privacy (understood here as synonymous to the right to respect for private life) had evolved through the years, and had gradually come to include the protection of personal data, regarded as a sort of informational dimension of privacy, reflecting the approach of control on the (use of) personal information.8

The formulation used by the Court in case Rotaru v. Romania that “public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities”9 suggests that unsystematic processing of publicly available information does not necessarily fall within the scope of the protection of private life. As Koops notes the leading ECHR data-processing cases concern storage (with or without subsequent use) of data, leaving open the question whether the mere searching for and consultation of data, without storing or using them, constitutes an interference10. In both Peck and Friedl, as well as in Marper v UK, the ECtHR made it clear that much depends on the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained11

3.2 The right to data protection

Whenever information processing for security purposes is involved, it is necessary to take into account the right to data protection. This is a fundamental right enshrined in Article 8 of the EU

9 ECtHR, Rotaru v. Romania, App.no. 28341/954 May 2000
Charter of Fundamental Rights, and differentiated from the right to respect for private and family life, home and correspondence enshrined in Article 7 of the same instrument, which guarantees the protection of an individual’s private sphere against intrusion from others, mainly from the state.

Whereas Article 7 of the Charter echoed Article 8 of the ECHR by likewise establishing a right to respect for private life, the Charter’s Article 8 enshrined a new right to personal data protection. Article 8 on ‘Protection of personal data’ provides, in its first paragraph, that ‘everyone has the right to the protection of personal data concerning him or her’. Art. 8(2) CFR elevates a fair number of core data protection concepts into the EU fundamental rights acquis (requirements for lawful data processing such as fairness, purpose specification, consent, etc.), as well as certain rights for the individuals concerned and independent supervision of “these rules”. Art. 8(2) CFR provides that any processing of personal data must be legitimate on the basis of either the concerned individual’s consent or law. Hence, the new right to data protection also protects against the processing of personal data where there is no legitimate basis. In the second paragraph, it provides also that “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified”. In the third paragraph, it states that “compliance with these rules shall be subject to control by an independent authority”.

Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) establishes the principle that “everyone has the right to the protection of personal data”.

The Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data that also apply to judicial cooperation in criminal matters and police cooperation, requiring regulators to lay down rules relating to the protection of individuals with in these contexts.

---

12 Article 16 states “everyone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities“.
Data protection often refers to one specific form of privacy, the informational privacy. Data protection is related to the rise and growth of computer-based information technology that enables collection, processing and storage of (large amounts of) personal data, i.e. any information that refers to an identified or identifiable natural person. Data protection is a process that implicates legislation, technologies, organizations and individuals.

There is a strong relation between the concepts of privacy and data protection. The concept of data protection was developed almost four decades ago in order to provide legal protection to individuals against the inappropriate use of information technology for processing information relating to them. It was designed to provide safeguards whenever information technology would be used for processing information relating to individuals.\(^{13}\)

If privacy is a concept and a right, then data protection is not only a separate right but in a way it is also a legal process by which the right to informational privacy is upheld. Data protection on the other hand, is procedural and legalistic in nature as it refers to policy, legal and administrative aspects of personal data processing.\(^{14}\)

The European Court of Human Rights considers the mere storing of personal information as an interference with the right of privacy, whether or not the state subsequently uses the data against the individual (Court of Human Rights, Amann v. Switzerland).

---


In the frame of the General Data Protection Regulation (GDPR) implemented in May 2018, the impact on the data protection process relates to the areas of legal and compliance (legislation), the technology, and the data itself. The main axes of actions and objectives of the GDPR\textsuperscript{15} are the following:

- GDPR establishes the rules relating to the protection of natural persons with regard to the processing of personal data, and rules relating to the free movement of personal data.
- GDPR sets a frame that protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

In the scope of the revised GDPR is that it is applicable to the either fully or partially automated processing of personal data and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The GDPR is not applicable to the processing of personal data for the following cases:

- in the course of an activity which falls outside the scope of EU law;
- by the Member States when carrying out activities which fall within the scope of GDPR’s Chapter 2 of Title V (General Provisions On The Union’s External Action and Specific Provisions on the Common Foreign and Security Policy), relating to “Specific provisions on the common foreign and security policy’’;
- by a natural person in the course of a purely personal or household activity;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

\textsuperscript{15} Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018

Deliverable no.: D11.1
Version: V1.0
Date: 03/08/2018
Furthermore, in the scope of the GDPR is that for the processing of personal data by the Union institutions, bodies, offices and agencies, it is the Regulation (EC) No 45/2001 that applies; this in combination with other EU legal acts that are applicable to such processing of personal data, shall be adapted to the principles and rules of this Regulation in accordance with Article 98 ("Review of other Union legal acts on data protection").

Additionally, the GDPR shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

The GDPR impacts many areas, such as the aforementioned legislation, technology, and data. In terms of legal and compliance functions, the GDPR introduces new requirements and challenges as mentioned above. To accommodate the directives of the GDPR, many organisations will require a Data Protection Officer (DPO) who will have a key role in ensuring compliance. A renewed emphasis on organisational accountability will require proactive, robust privacy governance, requiring organisations to review how they write privacy policies, to make these easier to understand, as non-compliance will result in heavy penalties (up to 4.0% of global turnover).

The impact of the GDPR on technology implies changes to the ways in which technologies are designed and managed. Documented privacy risk assessments will be required to deploy major new systems and technologies. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced incident response procedures. The concept of “Privacy By Design” has now become embodied in law, with the Privacy Impact Assessment expected to become commonplace across organisations over the next few years. And organisations will be expected to look more into data masking, pseudo-anonymisation and encryption.

In the frame of the data, individuals and teams tasked with information management will be challenged to provide clearer oversight on data storage, journeys, and trace. Having a better grasp of what data is collected and where it is stored will make it easier to comply with new
data subject rights, such as rights to have data deleted and to have it ported to other organisations.

3.3 The right to Communication Secrecy

Privacy and freedom of communication are strictly interrelated, at least in the European approach. The European Convention on Human Rights (ECHR), guarantees everyone’s “right to respect for his private and family life, his home and his correspondence” (Art. 8). The Charter adopts in Art. 7 the same wording with the exception of the term “correspondence,” which is replaced by “communications,” in order to “take account of developments in technology”\textsuperscript{16}. In recent years the prevalence of the expression “telecommunications” has been steadily replaced by the term “(electronic) communications,” which, in the wording of the relevant European Union regulatory framework, refers to the “conveyance of signals on electronic communications networks” (Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services). The use of this expression makes it clear that the form and the content of any communicative exchange is as central to [tele] communications as the technological system in place to enable it. An exchange of signals or data between technological devices includes or generates mechanisms to monitor and store the information being exchanged. The digitalization of data and communication structures makes it possible to scrutinize and manipulate previously unimaginable amounts of information.

Communicating with others and using communication services falls within the protected zone of (communicational) privacy. Governmental regulations that chill communication or inhibit the use of communications services amount to an interference with an individual’s right to

\textsuperscript{16} EU Charter, Art. 7 Explanatory Notes.
respect for their private life\textsuperscript{17}. As asserted by the European Court of Human Rights in the case Malone vs. United Kingdom, data related to the source, the destination, and in general to the conditions of communication are an “integral element of the communications made.” The Court has recently accepted (Copland vs. UK) that information derived from the monitoring of internet use should be similarly protected under Art. 8 of the ECHR.\textsuperscript{18} The relevant European statutes, which regulate the use of such transactions, cover traffic data either “in a technology neutral way,” (i.e. the e-Privacy Directive, which addresses traditional circuit-switched telephony as well as packet-switched internet transmission) or in a functional way (i.e. the Data Retention Directive, which dealt with any data necessary to identify the subscriber or user, as well as the source and the destination of a communication). The informative value and the usability of traffic data is extremely high as they can be analyzed automatically, combined with other data, searched for specific patterns, and sorted according to various criteria\textsuperscript{19}.

The claim to anonymity, inherent in the right to privacy, is essential to freedom of communication via electronic networks, but, at the same time, it runs against public policy objectives. Privacy also comprises one’s ability to remain anonymous in certain contexts, such as the use of technology without revealing one’s name\textsuperscript{20}. Anonymity, in the context of this discussion, should not only shield individuals while speaking or reading, but also when physically or electronically roaming about, interacting, and transacting through networks\textsuperscript{21}. As

\textsuperscript{17}Data Protection Working Party. 2005. Opinion 113/2005 on the proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services. Available at \url{http://ec.europa.eu}.


electronic communications leave “digital traces,” communications surveillance also has a disturbing effect on the right to anonymity.

Surveillance potential expands exponentially through data collection, storage, and mining as communication technologies become more interconnected and are used more extensively and intensively. Increasingly law enforcement authorities and security agencies seek to exploit the interactivity of information communication technologies to identify risky individuals and the networks in which they operate. The convergence of communications and information technologies over the past few decades has led to more diverse and sophisticated technologies being used for personal communications while governments and law-enforcement agencies have gained an unprecedented ability to engage in powerful surveillance.

The legal apparatus reflects new powers, investigative methods, and procedures, all supported by a new technological environment. The far-reaching impacts of communications surveillance on rights and liberties cannot be assessed without considering the technological mechanisms that enable the monitoring of systems as well as the deep changes in communicational exchanges that these mechanisms support or initiate. Another aspect that has to be taken into account is the potential impact on trust on technology. The risks of unlawful or arbitrary surveillance and interception of the digital communication technologies can discourage innovation and undermine the opportunities presented by the digital economy, as the protection of privacy is seen as critical for trust, that is a particularly important tool in the global online environment for reducing uncertainty and enabling reliance on others.

The necessity to fight against terrorism had previously led to the introduction of data retention regimes permitting state surveillance of communications for security purpose. The Data

---


Retention Directive was introduced as an urgent counter-terrorism measure responding to the terrorist attacks in Madrid (2004) and London (2005). Despite concerns about the compliance with fundamental rights, it was rapidly adopted under huge political pressure and entered into force in 2006. The Data Retention Directive required Member States to oblige telecommunications and internet service providers to retain traffic and location data regarding fixed and mobile telephony, internet access, email communications, for a period of at least six months and no more than two years, and to make it available on request to law enforcement authorities for the purpose of investigation, detection and prosecution of serious crime and terrorism. However, the CJEU in the Digital Rights Ireland case declared the Data Retention Directive to be invalid on the basis that it entails an unjustified interference with fundamental rights 24.

According to the ECHR, communications surveillance is unacceptable, unless it fulfills three fundamental criteria set in Art. 8 (2): (1) a legal basis, (2) the need/necessity of the measure in a democratic society, and (3) the conformity of the measure with the legitimate interests of national security, public safety, or the economic well-being of a country, prevention or disorder of crime, protection of health or morals, or protection of the rights and freedoms of the others. The provision reflects the tension between individual and community and the need to take into account the interests of society without infringing upon the intrinsic value of privacy in a democratic society. The CJEU, in its Tele 2 and Watson judgment 25 decided that national legislation, such as that relating to the retention of data for the purpose of combating crime, falls within the scope of European law. In its Digital Rights Ireland ruling 26 with which it...

---


25 CJEU (Grand Chamber), Judgement of 21 December 2016, Joined Cases C-203/15 (Tele2 Sverige AB) and C-698/15 (Watson), ECLI:EU:C:2016:970, para. 73.

26 CJEU (Grand Chamber), Judgement of 8 April 2014, Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Seitlinger and others), ECLI:EU:C:2014:238
invalided the Data Retention Directive (2006/24), the CJEU further specified how these conditions must be interpreted.

3.4. Balancing security and freedoms

A first major issue that extensive preventive surveillance measures raise relates to the “reverse of the rule”, i.e. the shift from a constitutional state guarding against the threat of specific risks in specific situations toward a security-orientated preventive state, which acts operatively and proactively. The “data retention” approach and the extension of PNR policies to EU\textsuperscript{27} indicate a transformation from the traditional constitutional model of gathering conclusive evidence of wrongdoing of suspect individuals toward intelligence gathering, which may be carried out against individuals at random, who themselves are is no longer perceived as a principally law-abiding citizen, rather as a potential threat” or “as an exchangeable element in a principally dangerous environment”\textsuperscript{28}.

The legitimization of the democratic state depends upon its success in balancing the various public objectives, i.e., freedom and security, under the terms and within the limits of core democratic values. The main challenge concerns the material and procedural precautions, law

\textsuperscript{27} In December 2015, the EP and the Council negotiated Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes (EU PNR Directive). According to Art. 1 (a) and (b) of the Directive, air carriers ought to transfer PNR data of passengers who are flying from outside the Union to the EU to EU Member States. The data is then collected, used, retained and exchanged by and between Member States. Member States may apply the PNR Directive to intra-EU flights too according to Art. 2 (1) of the EU PNR Directive. Pursuant to the Directive, Member States have to set up Passenger Information Units (PIUs) in order to manage the collection, storage and process of PNR data.

makers law enforcement officials have to adhere to in order to guarantee security without infringing fundamental rights.

In Art. 8 (2) ECHR, reasons of justification for interferences with Art. 8 (1) ECHR are stipulated. According to this provision, interferences with Art. 8 (1) by a public authority are only allowed if they are in accordance with the law and necessary in a democratic society, for instance, in the interest of national security. In conjunction with the requirement of ‘necessary in a democratic society’, further vital interests of States are listed such as public safety or the economic well-being of a country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of other. The derogation provided in Art 52 (1) allows limitations on the exercise of the rights rights and freedoms recognised [by this Charter] only if “provided for by law and [they]] 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”.

The early case law on balancing of national security with privacy can be found mostly in the jurisprudence of the ECtHR. The ECHR expressly puts forward the possibility of balancing between privacy and national security or public safety. The European Court of Human Rights in its case law has specified the requirements to be met. The three criteria that must be satisfied to ensure that any interference with privacy is in compliance with Article 8(2) are that the interference must be: a). in accordance with the law; b) in pursuit of one of the legitimate aims in 8(2); c) necessary in a democratic society.

The law authorizing the interference in the above analysed rights has to meet the standards of accessibility and foreseeability inherent in the concept of the rule of law, so that persons can regulate their conduct according to the law (Court of Human Rights, Malone v. U.K., Kruslin v.
France). Conditions, safeguards for the individuals, and implementation modalities must be sufficiently summarized, in order to succeed the “quality of law” test²⁹.

Proportionality, a key principle in European constitutional law, requires a further assessment of the necessity of the measure and its suitability to achieve its aims. Even if necessary is not synonymous with indispensable... it implies a pressing social need” (Court of Human Rights, Handyside v. U.K.). As “pressing social need” the jurisprudence points to the following considerations: a) Is the measure seeking to address an issue which, if left unaddressed, may result in harm to or have some detrimental effect on society or section of society? b) Is there any evidence that such a measure may mitigate such harm? c) What are the broader views of society on the issue in question? d) Have any specific views/opposition to a measure or issue expressed by society been sufficiently taken into account?

The CJEU has equally dealt with the issue of conflicts and balances between public security and data protection in its early case law. One of the most obvious cases in this regard is the case Parliament v. Council and Commission, also known as the Passenger Name Record (PNR) case (2006), which led to the annulment of decisions relating to the PNR agreement. The grounds on which the adequacy decision were annulled was due to the fact that the processing of personal data, transferred on the basis of PNR agreement, did not fall within the scope of the DPD because it constituted “processing operations concerning public security”.

The main characteristic of the jurisprudence in the earlier phase was that the European Courts did not lean towards a preference for protecting privacy, in its multifold nature (informational,


³⁰ Following the grounds for annulment action, brought by the EP, the CJEU annulled the decision on which the PNR agreement was concluded, as well as the adequacy decision on the transfer of PNR to the USA, as it did not fall within the scope of application of the Data Protection Directive 95/46/EC.
communicational), but instead balanced the two values, privacy and security in a rather neutral manner, which allowed to rely on the concrete a factual background of the cases, leading to the result that, in the majority of cases, public security still prevailed over privacy. It was exactly in the context of the gradual awareness of the existence of mass surveillance measures and their gradual escalation in order to meet the challenges of new “asymmetric” terrorist threats, that the European courts, notably the CJEU, increasingly began to tilt the balance towards the protection of privacy rather than security. That was the case in the judgement Digital Rights Ireland (2014) that annulled the Directive 2006/24/EC on the retention of data. Although the CJEU underlined that the “objective of that directive is [...] to contribute to the fight against serious crime and thus to public security” it regarded the interference with the fundamental rights to privacy and data protection as disproportionate. The CJEU reaffirmed its strict stance towards data retention measures in Tele2 Sverige (2016) where it found incompatibility of the national data retention measures with the EU privacy legislation. In these seminal the CJEU acted as a catalyst of policy change by striking a different balance between data protection and public security as the EU legislator.

The judgments of the European Courts have shown that the reasons of justification for using security measures must be strong. The usage of security measures may only be justified in cases of serious offences such as organised crime, terrorism and other grave breaches of law.

According to the “constitutional framework” security measures and the exchange of personal data must be restricted to what is absolutely necessary and that the principle of proportionality is adhered to. This approach puts certain limitations with regard to mass surveillance and the exchange of bulk data that affect individuals who are not involved in serious offences. Accord These overarching criteria ought to guarantee targeted surveillance and a targeted exchange of personal data in contrast to mass surveillance and a transferal of bulk of data. One central problem with. Hence, innocent persons may be put under general suspicion. More specifically, the ECtHR and CJEU demand that legal provisions that allow security measures and the transferal of personal data are precise and targeted with regard to the measures, persons affected, competent authorities and the crime that ought to be prevented or investigated. There
have to be clear and precise criteria that stipulate under what circumstances a security measure is used or discontinued. It has to be clear which persons are affected and why. There has to be a direct link between the measure applied with regard to a person and the specified crime that ought to be fought against.

As noted by Sampson and Lyle “each case will depend on its own merits. Whether the processing will satisfy the legal requirements will depend on many things but following the principles outlined earlier, as a minimum, should be the priority before any processing takes place. Each crisis, each crime and each investigation or prosecution will be unique, so prescriptive advice is not realistic or appropriate.”

In any case, the objective pursued must be balanced against the seriousness if the interference, which is to be judged taking into account, inter alia, the number and nature of persons affected and the intensiveness of the negative effects. Restrictions must be limited to a strict minimum: Legislators are required to minimize the interference by trying to achieve their aims in the least onerous way (Court of Human Rights, Hatton v. U.K.). The necessity and proportionality have to be clearly demonstrated by considering that privacy is not only an individual right of control over one’s information, but moreover a key element of a democratic constitutional order (German Federal Constitutional Court, Census Decision 1985). These restrictions persist even where incursions into privacy rights have been justified by states on grounds of national security or prevention or detection of crime as evidenced by a number of prominent ECtHR cases [ECtHR Weber v. Germany (2006) and Klass v,Germany( 1978)]

The degree of suspicion of a person is crucial criterion while deciding whether the use of security measures is appropriate or not. There has to be concrete evidence or a concrete

---

probability that the person concerned has committed a serious crime or will commit such a crime in the foreseeable future. The legislation ought to be precise regarding which competent authorities can use surveillance measures or access and use personal data. It ought to be specified which serious crimes are sought to be prevented or investigated to ensure that the security measures or the personal data are only used for a specific purpose. Furthermore, the courts demand procedural precautions that should guarantee that the use of surveillance measures and the exchange of data are legitimate. The application of security measures in a lot of cases should be subjected to the prior obtaining of a judicial authorization/warrant. Continuous scrutiny by an independent control mechanism has to be provided in case of secret surveillance measures.

In its opinion 01/2014 the Article 29 Data Protection Working Party has emphasised the importance of the concepts of necessity and proportionality when interfering with human rights in relation to processing personal data. The WP29 provides practical guidance to LEAs and state that specific attention should be paid to: a) the legal basis for the measure, particularly under Article 8(2) ECHR; b) the specific issue to be tackled such as the seriousness of the issue and social and cultural issues; c) the reasons behind the measure which are closely linked to decisions about data retention, minimised collection and data quality; and d providing sufficient evidence to support the reasons for choosing the measure32.

---

4. The Council of Europe’s Recommendation and Guidance

Under the instruments of ECHR and the Charter, rules and guidelines have been issued that specifically relate to processing of personal data for law enforcement purposes. These include, in particular, Council of Europe Recommendation R(87)15 of the Committee of Ministers to Member States, Regulating the Use of Personal Data in the Police Sector (1987).

The Convention for the Protection of the Individuals with regard to Automatic Processing of Personal Data (Convention 108) has created ambiguity by including an exclusion from its provisions for security purposes. Recommendation NoR (87)15 resolved this by explicitly subjecting police data to the same data protection regime as other personal data. Recommendation (87)15 regulating the use of personal data in the police sector provided a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided by Article 8 of the European Convention on Human Rights and by the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data (Convention 108). “Given the increased activities of police forces in the lives of individuals necessitated by new threats to society posed by terrorism, drug delinquency etc, as well as a general increase in criminality, it was felt even more necessary to establish clear guidelines for the police sector which indicate the necessary balance needed in our societies between the rights of the individual and legitimate police activities when the latter have recourse to data-processing techniques.

This Recommendation has become the effective standard on the issue: it is expressly referred to in various European police co-operation instruments, including the Schengen and Europol

---

33 Article 9, paragraph 2, of the Convention 108 makes it possible for member states to derogate from the Convention’s basic data protection principles in the interests of, inter alia, “the suppression of criminal offences”

34 Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector – Explanatory Memorandum -par. 4
treaties and associated regulations, and is also regularly invoked in recommendations by the Parliamentary Assembly of the Council of Europe and its Committee of Ministers, by the Working Party, and the European Parliament\textsuperscript{35}. Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance.

However, the report “Recommendation R(87)15 – Twenty five years down the line\textsuperscript{36}” considering the key changes that occurred between 1987 – 2010 suggested that while the Principles included in the Recommendation of the 1987 remained valid and useful, they were formulated in a non-binding and sometimes insufficiently detailed way that significantly impeded its usefulness.

The major societal and sectorial changes outlined suggest that the amount of personal data collected, and the risks of its abuse have increased significantly and that Convention 108 and R(87)15 are no longer a proportionate response to current levels of risk. The Rapporteus suggested that increased risks require binding legislative instruments for European states, sufficiently detailed to be meaningful to relevant practitioners.

As response to these findings the Council of Europe has recently (February 2018) issued a “Practical guide on the use of personal data in the police sector” based on the assessment that although the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level a preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level. The present Guide was therefore prepared to highlight the most important issues that may arise in the use of


\textsuperscript{36}Council of Europe, Report: Recommendation R (87) 15 – Twenty-five years down the line drafted by Professor Joseph Cannataci and Dr. Mireille M. Caruana (2013)
personal data in the police sector and to point out the key elements to be considered in that context.

This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance. the Guide intends to give orientations for practical situation the police may face in its everyday operation and acknowledges that the lawful collection and use of personal data for law enforcement purposes are crucial in the interests of national security and for the prevention of crime or maintenance of public order.

5.1. A short history and goals of the new framework

The ratification of the Treaty of Lisbon back in 2009, constitutes a turning point in the relationship between data protection and the EU Justice and Home Affairs field. The Treaty of Lisbon along with Article 16 TFEU has created a new legal basis for data protection, which also covers police and judicial cooperation in criminal matters.

As Directive 95/46/EC did not apply to the processing of personal data in the course of an activity which falls outside the scope of European Community law and the Framework Decision 2008/977/JHA does not regulate internal data processing activities of law enforcement, the Police and Criminal Justice Data Protection Directive bridges this legislative gap. The DIRECTIVE (EU) 2016/680, which forms part of the data protection reform package, repealed the Council Framework Decision 2008/977/JHA.

The Directive is some leaps ahead of Council Framework Decision 2008/977 / JHA since: it concerns both the cross-border and national processing of personal data and aims to improve Member States' mutual work in the combat against terrorism and other criminal offenses in the EU; it ensures that personal data transmitted from outside the EU by law enforcement bodies of criminal law should be adequately protected; it provides that the agreements by the Member States are to be revised in accordance with the Directive's provisions; it sets major principles.


38 Even though the Framework Decision was a welcome first step in the regulation of the scattered field of data protection in the police and criminal justice sector, its limited scope and lacking data protection standards prevented the instrument from providing a sufficient and comprehensive level of regulation in this area. As it did not cover domestic data processing and was not entirely in line with prior legal instruments, which the Decision allowed to remain unaffected and even take precedence, the instrument has proven to be inadequate in light of article 16TFEU and ineffective at mending the increasingly fragmented and inconsistent landscape of data protection in the area of law enforcement and criminal justice. As further discussed below, it now remains to be seen if the newly introduced Directive shall be able to correct these flaws.
for the processing of personal data, just when it is needed, in a proportionate manner and in accordance with a particular objective.

The Data Protection Directive on Police Matters repeats the principles of the data protection law established already in the Directive 95/46/EC. The difference is that for the first time the Union directs these principles to apply also in the field of police matters. As emphasized by Van Lieshout et al., if viewed from a non stricto sensu legal research point of view, the field of EU Justice and Home Affairs is evidently faced with the fundamental contemporary question of reconciling privacy and security.

This Directive seeks to uniform the protection of personal data and to facilitate the exchange of data between member states competent authorities. The point is to enable effective judicial cooperation in criminal matters, although it steps into the member states’ sovereignty. The Directive strengthens individual rights, and adapts novelties introduced by the GDPR into the law enforcement field, (see, for example, the cases of data protection impact assessments or data protection by design and by default). The Police and Criminal Justice Authorities Directive harmonises the laws in the Member States in respect of the exchange of information between police and judicial authorities, whilst leaving discretion in specific areas (for example, penalties for breach of the Directive) in order to respect the different legal traditions of the Member States.

5.2 The scope of the Directive

The Data Protection Directive on Police Matters is for "the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of

criminal penalties, and on the free movement of such data” including the prevention of threats to public security.

The Directive for data protection in the police and justice sectors does not regulate the processing of data in the course of an activity which falls outside the scope of Union law (Article 2(3)). That provision has been interpreted (Recital 14) as relating to activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU. The formulation of that provision is therefore partially contradictory with the inclusion within the purposes set out in Article 1 of safeguarding against and the prevention of threats to public security.

It needs to be pointed out that the notions of ‘national security’ and ‘public security’ should be distinguished under EU law. Caruanna suggests that definitions or interpretations given to these concepts by different States could, and do, differ, resulting in a lack of clarity as to the scope of application of the Directive. The lack of definitional clarity is problematic, and it is necessary to ensure that the exception is not overly used to legitimise the processing of personal data outside the scope of the GDPR and Directive 2016/680. The European Parliament, in a resolution of 12 March 2014, reiterated that Member States must fully respect EU law and the ECHR while acting to ensure their national security. The European Parliament

However, while broad at first sight, the scope of the Directive is restricted in a number of ways. The lack of a clear definition or distinction between ‘national security’, which is a matter falling outside the scope of the Directive, and ‘safeguarding against threats to public security’, which is covered by the instrument, is cause for concern and could result in member states making use of this vague exception to unduly legitimise processing activities without the presence of adequate data protection measures.

The term ‘national security’ is limited to the security of each particular Member State and not of the Union as a whole and that the Union’s competence does not extend to encompass issues of national security


While R(87)15 refers to ‘state security’, the Proposal and the recital of Directive 2016/680 refer to ‘national security’, which terms are however generally used interchangeably.
recalled a ruling of the CJEU, according to which “although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable” (Case C300/11, ZZ v Secretary of State for the Home Department, 4 June 2013).

The Directive applies on two cumulative conditions: one relative to the identity of the processor (“a competent authority”) and one relative to the purpose of the data processing (which must be related to crime prevention, investigation, detection or prosecution). The Directive does not explicitly define the different purposes but relies on national laws. Criminal investigation purposes as well as criminal intelligence purposes can therefore fall within the scope of Directive 2016/680.

“Competent authorities” may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive (..)” (Recital 11). In conclusion, the concept of competent authority is not restricted to a strict administrative law notion of public authority. However, as pointed by recital 11, for the Directive to apply the processor should be bound with a public authority by a contract or any other legal act that gives him the authority to collect data for such purpose and to act in practice as an “agent” of the public authority for the purpose of data processing. In all the other cases, the stricter framework of GDPR applies.


46 “A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive”.

47 Jougleux P., Leventakis G, Mitrou L. Community policing in the light of the new European Data Protection Legal Framework 2018
Caruana points out\textsuperscript{48} that Member States define the activities of their authorities, in relation to law enforcement or merely administrative purposes, differently; thus, the same data processing operation could be covered by the GDPR in one Member State, but by national laws based on the Directive in another. In fact, it has recently been considered that ‘[i]n some Member States the FIUs set up under the Anti-Money Laundering Directive are administrative authorities, while in others they are considered as law enforcement authorities’ (Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680). This distinction matters as processing in the context of administrative offences is covered by the GDPR, while processing in the context of criminal offences is covered by the Directive.

The Directive will actually regulate processing of personal data by Member States and not only intra-Member States exchanges of data. However, it is still far from ensuring maximum harmonization of data processing in the criminal field. That is confirmed by Article 1(3), which states that the Directive for data protection in the police and justice sectors shall not preclude Member States from providing higher safeguards than those established in the Directive for the protection of the rights and freedoms of the data subject. The Directive allows for significant space for Member State differentiation. Nevertheless, in terms of consistency, Directive 2016/680 merely provides for so-called minimum harmonisation (Article 1(3)). It is important to bear in mind that it is nevertheless the responsibility of the EU legislator, under the TFEU (Art.16), to ensure high standards of data protection and not to leave this to the Member States individually\textsuperscript{49}. Thus, the real added value of the Directive will depend on a large extent on its transposition into national law and its implementation by the national competent authorities.

\textsuperscript{48} Caruana M. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement, International Review of Law, Computers & Technology 2017,

\textsuperscript{49} European Data Protection Supervisor Opinion 6/2015. A further step towards comprehensive EU data protection, recommendations on the Directive for data protection in the police and justice sectors, 28.10.2015
5.3 The principles

The processing of personal data must be **lawful, fair and transparent and used for specific purposes mentioned in law.** The purpose for the processing should be explicit and legitimate, and determined when that data is collected. Individuals should be informed of the possible risks, rules, safeguards, and rights in relation to the processing of their personal data and how to use their rights.

The member states shall make sure that personal data is:

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive compared to the purposes why they are processed;
- accurate and kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; and
- processed so that the data’s security is ensured, including protection against unauthorized or unlawful processing and against accidental loss or damage.

In order to be lawful, such processing should be necessary for the performance of a task **carried out by a competent authority for the above-mentioned law enforcement purposes.** The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamentals Freedoms. Personal data are to be adequate and relevant for the purposes for which they are processed.

The data controller must prove he complies with the above set rules (accountability). Additionally, article 5 explicitly calls for the introduction of a periodic review of the need for
the storage of personal data or for the implementation of appropriate time limits for storage enforced by procedural measures. The stored personal data must be reviewed and erased periodically after appropriate time limits. The concept of purpose limitation is an important principle. It has two main aspects: data should only be used for limited purposes and it should only be retained for a limited amount of time.

The right of presumption of innocence, as ordered by the Charter of Fundamental Rights should not be threatened in the data processing especially when establishing different categories of data registries for natural persons.

Different data subjects should be distinct from each other, such as persons suspected of committing a crime, persons convicted of a crime, and victims, and other parties such as witnesses. (see also Recital 31).

Facts based personal data must be separated from data which is based on personal assessments. The competent authorities should not make available nor transmit inaccurate and incomplete personal data and they should verify the quality of the data before processing. When personal data is sent to other authority, the receiver should be able to evaluate its accuracy, completeness, and reliability. If incorrect personal data is transmitted or transmitted unlawfully, the recipient must be notified and the data should be corrected or erased or the processing restricted.

5.4 The legal basis

The data subject´s consent does not provide a legal basis for processing personal data by competent authorities. A national competent authority may process personal data if that is necessary for performing its tasks according to the objectives set in the Directive´s Article 1(1). These must also be based on member state law, which specifies the objectives of the processing, it´s purposes and the processed personal data. The competent authorities may process personal data for other purposes than the ones´ set in the Article 1(1), if it fulfils the conditions of the Article 9.
Sensitive personal data can be processed if it is strictly necessary, with safeguards and where authorized by law to protect the natural person’s interests, or if the data subject has made the data public herself. A decision which is based on automated processing and produces harmful effects to the data subject, should be authorized by the law of the data subject and provide appropriate safeguards for her.

Following article 10, particular attention shall be paid to the processing of special categories of special data. By broadening the traditional categories of sensitive data such as religious beliefs, health data, political opinion and racial origins by the inclusion of genetic and biometric data, the Directive takes notice of recent technological developments and creates an adequate regime awarding special protection to the processing of certain data which might result in a greater impact on the data subject’s life. Processing of particularly sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only under well-defined and restrictive conditions.

5.5 The rights of the data subjects

The third chapter of the Directive regulates the protection and exercise of data subject rights. A clear set of rules and procedures is established through the introduction of a number of rights belonging to the data subject, the restrictions applicable thereto and the modalities for the exercise and communication thereof by and to the data subject.
Following article 13, the information made available to the data subject must include the identity of the controller and the data processing officer, the purposes of the processing and the possibility to lodge a complaint with the supervisory authority or request rectification or erasure of personal data. Under article 14, data subjects are given the right to access personal data concerning them and to obtain knowledge of ongoing processing activities involving their personal data.

Additionally, article 16 grants data subjects the opportunity to obtain the rectification or erasure of their personal data as well as, in certain cases, restrictions on its processing. Their personal data can be corrected when inaccurate and erased in case of a legal obligation or infringement of certain data protection standards.

Nonetheless, these rights are not absolute and their exercise is subject to a number of limitations in order to protect the integrity and confidentiality of criminal investigations and procedures. The obligation on the controller to make information available to the data subject may be restricted, delayed or omitted by law if such a measure is necessary and proportionate in a democratic society with due regard for fundamental rights and legitimate interests of persons concerned, and serves to avoid obstructing legal and criminal procedures, protect the rights and freedoms of others or safeguard national or public security. According to article 15, data subjects’ requests for access to data or the rectification and erasure thereof may be refused on the same grounds, on the added condition that they are informed of the refusal without undue delay, are made aware of their right to lodge a complaint against the decision and are given the reasons for the refusal unless doing so would undermine one of the abovementioned purposes.

Directive 2016/680 further provides for every data subject to have the right to an effective judicial remedy in accordance with Art.47 of the Charter. The Directive provides ‘for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them’ (Art.53(1)). Where the DPA does not handle a
complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Art.52, the data subject shall have the right to an effective judicial remedy (Art.53(2), and recital (85)). Directive 2016/680 also provides for the right of a data subject to an effective judicial remedy against a controller or processor ‘where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions’ (Art.54).

5.6 Other obligations of data controllers and processors

The fourth chapter of the Directive introduces a number of new obligations on data controllers and processors.

Following article 19, it is up to the controller to provide appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the Directive, taking into account both the nature and purposes of the processing as well as the potential risks for the freedoms of the data subjects. Supplementing this, the controller shall be tasked with the implementation of appropriate data protection policies when proportionate to the nature of the data processing activities.

Under article 20, data controllers shall be required to implement the principles of data protection by design and by default. As for the design part, technical and organizational measures will have to be adopted to implement necessary safeguards into the processing acts themselves, while data protection by default shall require built-in mechanisms ensuring that only personal data necessary for a specific purpose shall be processed, stored and made accessible.
At the more technical level, articles 24 and 25 establish the requirements of recordkeeping and logging which require data controllers to maintain records and logs of the data processing and are set to support the demonstration of compliance with data protection rules and improve the transparency, accountability and effective supervision of processing activities. These requirements shall assist with the establishing of the justification and lawfulness of processing activities as well as determining the identity of the person consulting, disclosing and receiving the data.

In order to ensure compliance with the objectives of the Directive, the logs and records shall be made available to supervisory authorities upon their request. In the event that a method of processing is considered likely to cause a high risk to the rights and freedoms of individuals, article 27 requires the controller to conduct a prior assessment of the impact of the processing activity on the protection of personal data, hereafter referred to as a Data Protection Impact Assessment (DPIA). These impact assessments must take into account the rights and legitimate interests of data subjects and concerned persons, as well as include the envisaged operations, applicable data protection safeguards, potential risks to freedoms and the measures used to manage them. As DPIA's take into consideration wider consequences for the rights and freedoms of data subjects while contributing to the accountability of controllers and the proper compliance with data protection obligations in the Directive, they shall play an especially important role in the management of new surveillance and processing technologies.

Following articles 26 and 28, data controllers and processors are under a general obligation to cooperate with supervisory authorities and provide the necessary information for the fulfilment of their enquiries. In the event that a particular type of processing using new technologies or procedures involves a high risk to data subject rights, or a data protection impact assessment reveals that processing activities would result in such a risk in the absence of special measures taken by the controller, this provision requires the controller or processor to consult the supervisory authority prior to the processing and disclose the results of the DPIA.
Recital 52 of Directive 2016/680 provides some guidance to assess the level of risk of a processing. The purpose of the processing is one of the factors, besides the nature, scope and context of the processing. Determining whether a subsequent processing of personal data for a law enforcement purpose constitutes a ‘high risk’ processing requires a case-by-case analysis. Therefore, it could be that the further processing of personal data would constitute a ‘high risk’ processing in a context of criminal intelligence because of the risk of mass surveillance, whereas the same processing performed in a criminal investigation context would not.\footnote{Jasserand C., Law enforcement access to personal data originally collected by private parties: Missing data subjects’ safeguards in directive 2016/680? Computer Law and Security Review 24 (2018), pp. 154 ff.}

The supervisory authorities may also establish a list of processing operations requiring such prior consultation by default to ensure that these particular operations do not escape scrutiny. Additionally, these provisions determine that the authorities must also be consulted during the legislative process on data processing and are capable of using their powers discussed in section 3.5.2 to halt processing activities which infringe on the Directive.

Under articles 32 through 34 of the Directive, data controllers must appoint a publicly designated Data Protection Officer (DPO)\footnote{To consider if the Consortium should “nominate” a DPO for the purposes of the project. In some projects this is a requirement posed by reviewers.} to assist in the protection of personal data. These officers are required to be involved in all issues relating to data protection in a proper and timely manner, and be provided with the necessary resources to carry out their tasks effectively. Among these tasks are the informing and advising of the controller, monitoring compliance with data protection legislation, participating in data protection impact assessments, cooperating with supervisory authorities and acting as a contact point for data subjects and other actors with concerns related to data protection. While the introduction of highly qualified DPO’s contributes to a higher degree of data protection expertise and closer compliance with data protection rules, the fact that courts and other judicial authorities may be exempt from this obligation creates a potentially problematic situation where such actors may not be
assisted by a data protection expert in the exercise of their duties. Furthermore, the considerable differences between the Directive and the GDPR as well as the lack of rules on independence, confidentiality and conflicts of interest are regrettable and could erode the effectiveness of the data protection officers.

5.7 Independent oversight

An important element of the EU data protection model, embedded also in the Charter, refers to the establishment of an independent supervisory authority entrusted with the task of monitoring the application of data protection law within the respective Member State. The Directive permits assignment of this role to the authority established for similar purposes under the GDPR.

The supervisory authority (or several, each with a separate task, adequate resources, and public annual budget) monitors the application of the rules adopted based on this Directive. Member states have already established the supervisory authority under the Directive 95/46/EC and the GDPR and the tasks under the new Directive may be transferred to this authority. The supervisory authority handles the data subjects’ complaints and investigates the matter, or transmits it to the competent authority, and then it informs the data subject of the progress and the outcome. The authorities’ tasks and powers to perform should be equal in each member state. They should be able to bring the Directive’s violations to the attention of the judicial authorities or to engage in legal proceedings.52

The Data Protection Authority has got no specific power under Directive 2016/680 to impose penalties. Under the GDPR the DPA is provided with the “corrective power” and the power to

impose an ‘administrative fine’ (pursuant to Art.83), depending on the circumstances of each individual case (Art.58(2)(i)). Under the GDPR, Member States must also lay down the rules on other penalties applicable to infringements of the Regulation, in particular for infringements which are not subject to administrative fines pursuant to Art.83, and take all measures necessary to ensure that they are implemented (GDPR, Art.84(1)). This is a case of relative weakness of the DPA with regard to processing operations carried out under the Directive, when compared to the position under the GDPR.

5.8 Relation to GDPR

The reform process has not ensured that uniform data protection rules apply in all areas of EU law and it has as a result given rise to problems regarding the delimitation between Directive 2016/680 and the GDPR. Directive 2016/680 applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art.2(1) and Art.1(1)). However, Member States define the activities of their authorities, in relation to law enforcement or merely administrative purposes, differently. This may have as result that the same data processing operation could be covered by the GDPR in one Member State, but by national laws based on the Directive in another.53

The Directive and the GDPR supplement each other as they operate in different sectors but cooperate in the areas where they overlap. The line separating processing under the GDPR or under the Directive may at times become extremely thin.54 Recital 11 of Directive 2016/680


evokes the scenario of personal data collected for a law enforcement purpose and further processed for a non-law enforcement purpose. In that case, the further processing is covered by the GDPR. Recital 19 of the GDPR, that builds a bridge between the GDPR and the Directive 2016/680/EU describes the other-way around scenario and provides for the applicability of Directive 2016/680 to the further processing by law enforcement authorities of personal data initially collected for a non-law enforcement purpose. The further processing of personal data held by private parties falls within the scope of Directive 2016/680 if the data is further processed for a law enforcement purpose.

A police authority may have to apply both legal instruments: the GDPR while processing personnel or non-law enforcement related files, and the Directive for the detection, prevention and prosecution of crime. The GDPR applies when a competent authority lawfully discloses personal data to a recipient who is not a competent authority defined by the Directive. When the competent authority has collected personal data for one of the Directive purposes, the GDPR applies when that data is processed for other purposes than the ones named in this Directive.

5.9 Relation to other legal instruments

The European Union has adopted instruments in the field of judicial cooperation in criminal matters before adopting this new Directive. These specific provisions of acts should stay unaffected. These are for example, the provisions in the Prüm Decision or the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU. The Directive states in its Recitals that the Commission should evaluate the relationship between this Directive and those acts adopted before it. The Commission should evaluate the need for adjusting and if necessary to make proposals to create coherent legal rules of those provisions.
with this Directive. This is to ensure that the protection of personal data is guaranteed equally everywhere in the EU.

More specifically Art. 62(6) of the Directive 2016/680/EU states that the Commission must review, within one year of the expiry of the period for transposition, other EU acts which regulate the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, in order to assess the need to align them with the Directive and ‘to make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive’
6. The legal framework for the fight against terrorism


In June 2013, the Justice and Home Affairs Council has presented the package of 22 measures against foreign terrorist fighters proposed by the EU Counter-Terrorism coordinator\textsuperscript{55}. This package was the basis of future actions such as the reinforcement of the Schengen Framework, the Passenger Name Record System (PNR), the prioritization of information sharing and operational cooperation and, in line with the two instruments analysed above, the criminalization of certain conducts usually associated with the activity of foreign terrorist fighters. The European Council asked the Commission to assess if the EU Decision on combating terrorism needed an update, following the reports of Eurojust about existing gaps in the prosecution of foreign terrorist fighters\textsuperscript{56}.

The phenomenon of foreign terrorist fighters has deeply influenced criminal law. An international answer to the global nature of terrorism has been regarded as necessary;\textsuperscript{57} this also means that the European Union and its Member States must strengthen cooperation with third countries, including with a view to securing and obtaining electronic evidence. The need to reinforce the Union's legal framework on combating terrorism and to review the existing legislation in order to ensure full compliance with international obligations and standards required action of the Union's legislature.

The EU Council and the Parliament approved on 15 March 2017 the EU Directive on combating terrorism. The legal basis of this EU Directive is article 83.1 of the TFEU, according to which “the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism...”

According to article 1, this new legal tool establishes “minimum rules concerning the definition of criminal offences and sanctions in the area of terrorist offences, offences related to a terrorist group and offences related to terrorist activities. The Directive categorizes the offences in three groups: terrorist offences (article 3); offences relating to a terrorist group (article 4) and offences related to terrorist activities (articles 5 to 12). Article 20 establishes rules on investigative tools and confiscation, providing that Member States shall ensure that effective investigative tools, such as those which are used in the fight against organised crime or other serious crimes, are also available to persons, units and services responsible for investigating or prosecuting the terrorist offences laid down in the Directive. Moreover, national competent authorities shall freeze and confiscate, in line with Directive 2014/42, the proceeds derived from and instrumentalities used or intended to be used in the commission or contribution of any of the offences referred to in Directive 2017/541.58

Article 23(1) states that the Directive shall not have the effect of modifying the obligations in respect fundamental rights and fundamental legal principles as enshrined in Article 6 TEU. “[The]Directive respects the principles recognised by Article 2 TEU, respects fundamental rights and freedoms and observes the principles recognised, in particular, by the Charter, including those set out in Titles II, III, V and VI thereof which encompass, inter alia, the right to liberty and security, freedom of expression and information, freedom of association and

---

58 A. Caiola points out that this will give an important tool to judicial and police authorities dealing with the repression of terrorist acts. See A. Caiola, The European Parliament and the Directive on combating terrorism. ERA Forum (2017) 18:409–424 DOI 10.1007/s12027-017-0476-1
freedom of thought, conscience and religion, the general prohibition of discrimination, in particular on grounds of race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, the right to respect for private and family life and the right to protection of personal data, the principles of legality and proportionality of criminal offences and penalties, covering also the requirement of precision, clarity and foreseeability in criminal law, the presumption of innocence as well as freedom of movement as set out in Article 21(1) of the Treaty on the Functioning of the European Union (TFEU) and in Directive 2004/38/EC of the European Parliament and of the Council (1). This Directive has to be implemented in accordance with those rights and principles taking also into account the European Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and other human rights obligations under international law” (Recital 35).

This symbolic specific commitment to the protection of fundamental rights and freedoms is of high importance especially with regard to counter terrorism intelligence and data exchange actions, including the processing of personal data of an often sensitive nature. Recital 25 stresses the need to strengthen the existing framework on information exchange in combating terrorism: “Member States should ensure that relevant information gathered by their competent authorities in the framework of criminal proceedings, for example, law enforcement authorities, prosecutors or investigative judges, is made accessible to the respective competent authorities of another Member State to which they consider this information could be relevant”. However, the Directive is clear: personal data processing “is subject to Union rules on data protection, as laid down in Directive (EU) 2016/680 of the European Parliament and of the Council (1) and without prejudice to Union rules on cooperation between competent national authorities in the framework of criminal proceedings, such as those laid down in Directive

---

59 This provision is not actually necessary since fundamental rights and the EU Charter apply by virtue of primary law. The European Parliament insisted in having this provision in the operative part of the Directive in order to stress the importance of protecting and safeguarding fundamental rights and freedoms when combating terrorist offences. Several instruments, and not only the EU Charter of Fundamental Rights, are recalled in Recital (33) of the Directive, which has to be implemented taking also into account the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the International Convention on Civil and Political Rights, and other human rights obligation under international law.
2014/41/EU of the European Parliament and of the Council (2) or Framework Decision 2006/960/JHA” (Recital 25).

6.2. Counter-tools and considerations

In terms of the counter tools that can be engaged for the prevention stage, there is a wealth of information available part voluntarily or with some discretion leaving “tracks” that can be followed and evaluated for their validity. Information Technology tools as well as digital instruments that can monitor and identify suspicious activities in terms of financial transactions, traveling (hence a link to possible frequent traveler / flyer and therefore to PNR systems), participation in fora and social media platforms promoting radical ideas.

The ability to monitor the communications of entire groups and nations on a mass scale is now a technical reality, posing new and substantially more sensitive human rights issues. Recent reforms of surveillance laws undertaken across political systems with significant checks and balances, demonstrate how easily surveillance capabilities can outstrip the ability of laws to effectively regulate them. In non-democratic and authoritarian systems, the power gained from the use of surveillance technologies can undermine democratic development and lead to serious human rights abuses.

While actions to demotivate and prevent radicalization through reduction of exploitation and prevention of the availability of “material” that attracts people may be proposed, it is important that this is not crossing the line of inhibiting freedom of speech or expression of ideas that leads to a reverse propaganda by thinking of it as “raising awareness”.
In the line of prevention, a counter tool can be the legislation itself which can alter the rules for precursor inhibition such as the EU precursor law (REGULATION (EU) No 98/2011), which regulates the concentrations with which some chemicals are sold to the public, and which states that suspect transactions of some chemicals should be reported. Of course, when changing a product through legislation, the consequences must be examined like whether this chemical has a different toxicity (i.e. the safety of the product to users and the environment), is the legal status of this chemical different to the previous state, etc?  

In the frame of **detection**, numerous technologies have been developed worldwide following the terrorists’ attacks over the last decade. The deadly attacks in Brussels highlighted the vulnerability of Europe’s airports and transport systems. European Union officials, responded with intense organization to the difficult task of how to increase security while retaining the openness of society, and have convened meetings to discuss public transport security.

Facial recognition software, scanners that detect weapons and cameras that spot nervous people are some of the technologies proposed to secure public places, but some would require greater acceptance of surveillance in Europe. It is important that surveillance is active unobtrusively while not interfering to people flows, keeping hold ups that create crowds to minimum, as they can themselves become new targets. Another counter process proposed is for example the screening of the passengers at the entrance to airports, as has been implemented already in locations like Istanbul.

Technology experts claim that technology cannot solve the problem on its own, but techniques such as facial recognition able to pick out known suspects could assist although technologies as such must go through social acceptance, which will be translated and supported by a legal frame. It is also strongly supported that security agencies should share more information, in

---

60 [TNI, Market Forces: The development of the EU Security-Industrial Complex, 25 August 2017]
compatible formats, which is rarely the case at the moment, in order to make the technologies more effective.

One technology proposed as a non-intrusive counter tool for example, is the Passive Millimetre Wave technology, a technology that monitors naturally occurring energy from passengers, rather than requiring them to queue up and pass through a scanner that shines a beam at them. It is claimed that concealed weapons can be found at a distance of up to 15 meters. However, any such technologies would still rely on security people on the ground able to respond in seconds. 61

Israel’s Suspect Detection Systems (SDS) utilizes thermal surveillance cameras able to point out suspects in a crowd by spotting unusual body heat (behavioural indicators), signaling nervousness, which of course must be combined with agents on the ground. It is proposed that if such a system is set up at the entrance of a terminal (airport, train, bus, concert arena etc) to mark out potential terrorists, it is imperative that security personnel is available on the spot to intercept them. It is clear from the aforementioned examples that, while technologies may be enablers, it is important that personnel that is trained is available and participates actively. Similar case is the use of animals, for example dogs, which are very effective in the detection (and mitigation) phase but which are only as effective as their escort / handler; it is the ability and efficiency of the trained personnel that maximizes the output of the counter tool, in this case the dog. 62

Technologies have been developed for post or in the vicinity of attack phases, where mitigation takes place. Counter tools based on the recent development of network dynamics allow authorities to contact smartphone-holders in the vicinity of a suspected terrorist incident and commandeer the cameras on their smartphones. This is a counter tool that can be activated after there is an initial attack and a pursuit of suspects, or when an attack has not yet happened.

but a suspect has been reported for example. This kind of counter tool utilization however, requires consent by the owner of the smartphone, implying a different role by the civilian community, engaging to a more active participant, almost a “first-responder”, which though requires the analogous legal frame to enable such network to be activated, including a mentality shift of the civilians. This kind of approach must be carefully evaluated as definitions of the civilians’ role in an event are crucial since they become an active and responsive “counter-tool”.

Other technologies that can be used for phases of prevention, as well as detection and mitigation are the UAV / drones, serving as surveillance counter tools. The UAVs can provide audio as well as video surveillance capabilities but can accommodate for stand-off detection if equipped properly.

It becomes clear from all aforementioned technologies and procedures that great consideration must be placed on the development and use of counter-tools and methods. Attention and focus must be placed on the design of the tools and measures that do not infringe on the privacy and data protection of the individuals or groups. Following are some case studies based on the technologies described and the respective legal frame.

6.3 Case Studies

6.3.1 RPAs as surveillance tools and the rights to privacy and data protection

Although of different sizes and specifications, all RPAs (Remotely Piloted Aircraft) carry photographic equipment, and due to their flying capabilities they have the ability to carry out
wide-range surveillance. In this perspective UAVs are widely regarded as novel threat to privacy as they are designed and built for surveillance and potentially extensive and intrusive data collection.

The use of drones for surveillance purposes poses issues that are similar to these posed with regard to video surveillance. However, a question of major importance for the assessment of drones is if and how UAVs change the nature of surveillance. The common argument that RPAs technology is comparable to “traditional CCTV systems” or “aerial surveillance through helicopters” and consequently does not contribute anything new in terms of surveillance does not take into consideration the complexity of drones. It seems that they represent a substantial change to surveillance capabilities and respectively new dimensions to surveillance threats that already exist.

RPAs expand the scope of surveillance with regard to the visual spectrum for contributing additional content to support surveillance: due to the advanced CCTV equipment they offer new angles enabling ground level obstruction while avoiding ground-level congestion. In this respect, RPAs change also the notion of place as they may expand the place under surveillance while enabling mobile surveillance. While normal CCTV systems are fixed and confined to public or publicly accessible places, RPAs offer new capabilities for visual surveillance as they

---


64 See the petition that the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center (EPIC) and 32 other NGOs have submitted to the U.S. Federal Aviation Administration

65 Commission Nationale de l’Informatique et des Libertes (CNIL), Drones, innovations, vie privée et libertés individuelles. La Lettre Innovation et Prospective de la CNIL. Decembre 2013


68 Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada- A Report to the Office of the Privacy Commissioner of Canada (April 2014)
do not require access to the premises to be monitored. Drones may become more intrusive as they penetrate and monitor places that are normally inaccessible\textsuperscript{69}.

The capture of the broader environment that objects or targets of surveillance are situated seems to be an inherent characteristic of drones technology and concept. Surveillance is becoming both highly specific and diffuse\textsuperscript{70} and raises further privacy considerations with regard to the fact that this instrument can register indiscriminately information concerning a large number of people.

In its Communication the European Commission underlines that “...Remotely Piloted Aircraft Systems (RPAS) operations must not lead to fundamental rights being infringed, including the respect for the right to private and family life and the protection of personal data. Amongst the wide range of potential civil RPAS applications a number may involve collection of personal data and raise ethical, privacy or data protection concerns, in particular in the area of surveillance, monitoring, mapping or video recording”\textsuperscript{71}.

The European Group on Ethics in Science and New Technologies underlines that privacy concerns are exacerbated by developments in drone miniaturization: “Due to their small size they can access confined spaces and navigate their interiors more effectively than ground robots, all without those under observation knowing they are there”\textsuperscript{72}.

\textsuperscript{69} Commission Nationale de l’Informatique et des Libertés (CNIL), Drones, innovations, vie privée et libertés individuelles”, La lettre innovation et prospective de la CNIL, No.6, Paris, 2013, p. 4.

\textsuperscript{70} Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada- A Report to the Office of the Privacy Commissioner of Canada (April 2014)


\textsuperscript{72} European Group on Ethics in Science and New Technologies, Opinion No 28 - Ethics of Security and Surveillance Technologies, May 2014, p. 54
Privacy concerns are expressed also in relation to the continuous character of surveillance that RPAs enable. Emerging aerial platforms combine increasing endurance and the ability to monitor an area to effectively create continuous surveillance of any given area73.

RPAs have some of the main characteristics of the so called "smart surveillance": a) a qualitative broadening and a quantitative increase of the types of data that can be collected, b) increasing analytical and processing power tools, c) the convergence of surveillance systems and assemblages74. By combining an RPAs video footage with ground-based surveillance technologies like location trackers and conventional CCTV recordings on the ground establishes new possibilities for profiling individuals on the basis of their movements, behavior and contacts, thus opening up whole new dimensions of personal surveillance75.

The use of RPAs interferes also with the right to data protection, a right that has been increasingly recognized by the European Court of Human Rights in its case-law under Article 8 of the European Convention on Human Rights. In EU law the Charter establishes the right to data protection. Article 8 of the Charter codifies the key data protection principles laid down in pre-existing data protection law (Directive 95/46/EC) and now in the GDPR (Article 5): legitimate purpose, consent as legal basis, right to access and rectification as well as the existence of an independent authority will control the implementation of these principles. The basic data protection principles and rules therefore now have, effectively, constitutional

---

73 International Working Group on Data Protection in Telecommunications Working Paper on Privacy and Aerial Surveillance 54th Meeting, 2-3 September 2013, Berlin (Germany). Also CNIL (see above)....


75 Report on surveillance technology and privacy enhancing design, SURPRISE Project (D.3.1), 2013, p. 22
status. The Charter is binding both for EU institutions as well as Member when implementing Union law (Article 51 of the Charter).

Privacy and data protection are closely linked but they are not identical. Data protection serves the protection of private life but the relevant rules apply also to personally identified information which does not falls under the scope of “private life” even in its broad interpretation. Data protection rules are applicable, whenever personal data are processed. The dimensions of privacy examined briefly above (communicational, informational, location privacy) indicate the interplay between privacy and data protection. However, it has to be mentioned, that unlike privacy laws, personal data protection legislation exists across a breadth of instruments including international conventions, bilateral agreements, and European Union instruments, (treaties, directives, framework decisions) and this framework gives more legal certainty as the privacy law.

The right to data protection will only protect individuals when the RPAs collect personal data. This differs from the right to privacy which protects people monitored by drones in a systematic way or through the means of intrusive payloads regardless of whether data is collected. The collection of images, videos, sounds, and the geo-localization data related to an identified or identifiable natural person that has been collected and processed by data processing equipment embedded in UAVs technology is subject to the application of European data protection law.

A significant requirement that has to be met with regard to fair processing of personal information is transparency. Covert collection and/or monitoring may lead to abuses, errors and harms for the persons concerned. Opaque data collection and processing interferes with the right of individuals to informational self-determination, i.e the right to know and (co-)

---


determine, at least in principle if and to what extent the others will collect data about him/her. Transparency of processing is a logical extension of the requirement that personal data shall be processed “fairly and lawfully”. Transparency serves also to counter the information asymmetries between individuals and controllers. Even if individuals have not the opportunity to consent to the processing it is important that they are at least informed when their data is being processed.

The EU data protection framework is securing transparency for the data subject by way of the controller’s obligation to inform him/her, and for the general public by way of notification. Specifically, the transparency principle imposes the data collector/controller to notify the data subject of the personal information collected, whenever data is obtained from the data subject, or from any other means (Art. 13 and 14 of the GDPR). Data subjects have to be informed about the purpose of processing the identity of the controller, the categories of data processed as well as the recipients thereof.

As confirmed by Art 29 Data Protection Working Party, the domestic provisions on video surveillance have been generally considered to be applicable to the processing of personal data related to the use of drones together with the relevant data protection rules, such as notification and the data subjects’ right to be informed: They should be aware of the fact that video surveillance is in operation, even where this surveillance is related to public events. Individuals concerned have to be informed in a detailed manner as to the places monitored. Art. 29 Data Protection Working Party does not require the data controller to specify the precise location of the surveillance equipment but it demands however that the context of surveillance is to be clarified unambiguously.

Art. 29 Data Protection Working Party emphasizes that data subjects would hardly be aware of this kind of processing as it is difficult to notice drones, because of their small size and the altitude of operation. Furthermore, the Working Party states, it is difficult, if not impossible, even for individuals noticing such devices, to know who is observing them and for what purposes. Mostly, the collection of personal data by RPAs (will) take place without the knowledge of the affected data subjects with the consequence that individuals won’t know how they could enforce their rights.

The European RPAs Steering Group points out that “generally speaking, “citizens will expect RPAS to have an ethical behaviour comparable with the human one, respecting some commonly accepted rules” 81. Concerns and mistrust are fed also by the idea of an “autonomous” machine that is fully governed by its own artificial intelligence” 82. Other ethical impacts relate to the potential “dehumanization of the monitored” as the distance between the controller of the RPA and the monitored person diminishes the sense of moral responsibility and accountability for the actions of drones 83.

Whereas the use of drones for military or law enforcement purposes has evoked some limited public debate, there is no similar debate about civilian uses of RPAs’ technology and surveys relating to public perceptions about the impact of drones deployment. It is reasonably expected that people may conceive the positive effects of the use of RPAs in the context of civil protection, namely in monitoring, preventing and alert and post-crisis management system for natural disasters. Furthermore, the risk that operators of RPAs show a “playstation mentality” of which

81 European RPAS Steering Group, “, p. 44.

82 Ilse Griek, Andres van der Linden & Terence Berkleef, Drones & Human Rights: Emerging Issues for Investors

operators of RPAs have been accused in war scenarios, is extremely low in civil protection missions.

6.3.2 Profiling Online Social Networks (OSN) Users as a Surveillance Tool

Several inherent features of Internet (especially Web 2.0) supported technologies and platforms (e.g., digitization, availability, recordability and persistency of information, public or semi-public nature of profiles and messages) encourage not only new forms of interaction, but also novel surveillance tendencies via behavior and sentiments’ detection and prediction. Any content uploaded online can be accessed, recorded, stored and retrieved “without respect for social norms of distribution and appropriateness”[84] Such sites and interaction platforms are, by design, destined for users to continually follow digital traces left by their “friends”, “followers” or persons they interact with often by simply consuming or commenting user-generated content. As noted by Lampe et al., OSNs are founded on the premise of surveillance, where individuals are not only allowed but expected to “track other members of their community”[85]. While users’ content visibility increases, the architecture of the majority of Web 2.0 applications allows exposing content to unwanted and/or invisible audiences.

The combination of Web 2.0 technologies, user-generated content and the growth of ICT (data warehousing, data mining, broadband internet access etc.) has enabled fast and efficient processing of vast amounts of information. Thus, novel and invasive Open Source Intelligence (OSINT) techniques have been developed by researchers and practitioners along with military organizations in order to extract user/usage patterns and correlations between seemingly unrelated data (namely psychosocial characteristics and OSN usage patterns). OSINT refers to


intelligence collected from publicly available sources, such as websites, web-based communities (i.e. social networks, forums, blogs) and publicly available data. Such techniques facilitate the extraction of knowledge when this is not easily accessible.

The following key points must be taken into consideration, since the quality of the results of the surveillance is directly connected to the quality of the gathered data:

- Uncovering data location: It is required to have knowledge of the locations from where the appropriate data can be gathered.

- Sources pre-processing: The pre-processing of the useful and the irrelevant sources of information is important, so as to avoid collecting outdated or useless data.

- Results refining: After having generated conclusions over the subject of interest, it could be useful to further process the results in order to focus on the required knowledge and provide with further analysis of the subject’s parameters. A process of meta-training on the collected data could reveal secret connections or correlations between the parameters of the dataset.

Users’ data/user generated content in OSNs is publicly available, since most of the communicating individuals neglect to use any privacy mechanisms, even if offered, or they are not even aware of or willing for. Even when users do not fail to utilize the offered privacy mechanisms, it is possible to obtain their data indirectly through “crawling”, namely the process of collecting web-based data by utilizing automated techniques and specialized software. Therefore, one could gather personal information even without having legitimate direct access to the target’s online profile by crawling either the medium per se, or other users that communicate with the target user.

Although the processing of such data may be used for fair purposes, so as to provide the user with a more personalized user experience, user’s privacy may be easily infringed. The knowledge extracted using OSINT may be utilized for purposes ranging from profiling for targeted advertising (on the basis of analysing online features and behaviour of the users) to
personality profiling and behaviour prediction for purposes such as employee screening, counter intelligence, threat prediction or forensics analysis. Online media and user generated content-mining provides support for decision makers to detect, track or even predict opinions and attitudes.

Governments also seek to use the informational goldmine of online social media to extract implicit, previously unknown and potentially useful information and to discover or infer previously unknown facts, patterns and correlations. Governments are interested in doing more than simply identifying individuals but furthermore in accumulating as much data about their citizens as they can. Web 2.0 technological features combined with voluntary exposure to an indefinite audience in OSNs give rise to traditional surveillance as Government is enabled to form patterns and correlate data, combine information, find causal rules and statistical regularities and generate mass user profiles on the base of identifying patterns. The privacy/surveillance relevant application of user-generated content mining is the determination of correlation between characteristics and patterns and the respective classification of individuals. The surveillance potential has to be considered also in view of Big Data technologies, which augment(s)/increase(s) knowledge discovery. What makes Big Data technologies and applications surveillance-relevant is not the size as such but the possibility to


aggregate and correlate distinct and hidden (massive) data sets. OSN users may be soon overwhelmed by the increased level of sophistication and the pervasiveness of predictive and real-time large-scale software\textsuperscript{91}.

Data mining of OSN crawled data may have far reaching implications when we refer to the surveillance context. Governments may make extensive use of Big Data for surveillance purposes, such as the case of US Government’s PRISM program that involves the US NSA collecting and analyzing foreign communications collected from a range of sources, including OSN companies \textsuperscript{92}. When referring to Big Data possibilities, Podesta points out that the Dept. of Homeland Security will now be able to take on new kinds of predictive and anomaly analysis while complying with the law and subjecting its activities to robust oversight\textsuperscript{93}. Thus, data management complexity for social networking sites and service providers has significantly escalated\textsuperscript{94}. The observation of the behaviour and characteristics of individuals through mining of large quantities of data may infringe fundamental rights, let alone the determination of correlation between every-day activities and political beliefs, between characteristics and patterns and the respective classification of individuals. The risk to stigmatize groups of persons or persons, as part of a group life, is high. As noted by the German Federal Constitutional Court (Rasterfahnuung Urteil of the Bundesverfassungsgericht, 04.04.2006, 1 BvR 518/02, 23.05.2006), data profiling means a higher risk of becoming the target of further (official) criminal investigations and suffering stigmatization in public life \textsuperscript{95}. Studies conveyed


\textsuperscript{93} Podesta, J., ‘Big data: Seizing opportunities, preserving values.’ Executive Office of the President. Report (2014)


how profiling and the widespread collection and aggregation of personal information increase social injustice and generate further discrimination against political or ethnic minorities or traditionally disadvantaged groups. On the other side online social media data mining seems to be the “future, if not the present of law enforcement and security “thus enabling governmental agencies to extract information from an individual’s every day interests, affiliations and online activities. Largely and permanently available and accessible information allows diving detailed portraits and profiles. Online social media data mining is proved to be more efficient than “traditional” forms of surveillance as it allows identifying past or even future wrongdoers whom the government would otherwise never have been able to detect. Despite the usefulness of such methods, concerns about privacy and personal data protection lead to significant public debate about the scope and barriers of surveillance. In particular after E. Snowden’s disclosures public concerns and fears are steadily augmented and become more severe as data mining as analysed in this paper may not be based on any individualised suspicion resulting in invasive surveillance that can target everyone.

In Europe, agencies ground the legitimacy of collecting and analysing information gained through data mining methods by pointing to the fact that such data are manifestly made public by the person concerned (Art. 8 §2e of the European Data Protection Directive), which is the case if people generate content or comment on other users’ content in social networks or media using their real identity and aiming at expressing their opinions publicly. In any case, however, data mining is a form of data processing that has to be fair and based on the grounds provided and required by European Law (mainly informed consent, legal obligation, overridden public interest such as prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the prevention of threats to public security) and subject to the respective procedural guarantees as laid down in national law (warrant, approval by a Data Protection Authority, consultation with the latter authority, etc.).

While reflecting on assessing the lawfulness of online social media data mining the new European data protection regulatory framework has to be taken into consideration: the General Data Protection Regulation (679/2016/EU) that replaces the 1995 Directive and the Police and Criminal Justice Data Protection Directive (680/2016/EU, replaces the 2008 Data Protection Framework Decision. The new framework does not include specific rules on data mining but it regulates profiling (Articles 4 (4), 13 (2f), 21 and 22 of the Regulation and 3 (4), 11 and 24 (1e) of the Directive). The European legislators dealt with profiling within the context of automated decision making: decision-making based on profiling, should be allowed where expressly authorised by Union or Member State law including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision (Recital 71). In the Police and Criminal Justice Data Protection Directive it is explicitly stated that profiling which results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms, should be prohibited.

6.3.3 Communications / Metadata Retention as Surveillance Tool

Access to communications content is a common way of gathering information for criminal investigations and security purposes. However, in the emerging “information society” more relationships and social interactions occur via electronic communications networks. It is not only the content of such information that is useful to the police and the security agencies; data on the use of communications systems are a valuable resource in preventing, investigating, detecting, and prosecuting threats and crimes. Communications data are used to trace and locate the source and route of information as well as to collect and secure evidence: “allowing investigators for example to establish links between suspected conspirators (itemized bill) or
to ascertain the whereabouts of a given person at a given time, thereby confirming or disproving an alibi”\(^{97}\).

The form and the content of any communicative exchange is as central to [tele] communications as the technological system in place to enable it”. An exchange of signals or data between technological devices includes or generates mechanisms to monitor and store the information being exchanged. The digitalization of data and communication structures makes it possible to scrutinize and manipulate previously unimaginable amounts of information. Surveillance potential expands exponentially through data collection, storage, and mining as communication technologies become more interconnected and are used more extensively and intensively. Defenders of the new data-retention measures point out that the Data Retention Directive does not allow the content of communications to be monitored. In the landscape of electronic communications, however, the frontiers between communication data and content (the so called “envelope– content principle”) no longer necessarily reflect a distinction between “sensitive” and “innocuous” information\(^{98}\). Numerous network services cannot be easily categorized by distinguishing between data content and data traffic.

Apart from the difficulties of establishing clear distinctions between content and traffic data, it is disputable if—under changing technological circumstances—the surveillance of content is necessarily more of a privacy invasion than the retention of and access to traffic data. The informative value and the usability of traffic data is extremely high as they can be analyzed automatically, combined with other data, searched for specific patterns, and sorted according to various criteria \(^{99}\). It is worth mentioning that authorities are often, at least initially, only

---


interested in obtaining traffic data (German Working Group against Data Retention, 2007). Without ignoring the particularities of monitored infrastructures and the data being retained, it is important to stress the unique feature of data retention as a method to gather information. Data-retention practices allow law-enforcement authorities to analyze the wealth of data at their disposal and develop models of what constitutes normal and “suspicious” communications networks, identifying individuals for further investigation.

Data retention inevitably affects the right to privacy and confidential communications. The fact that data are retained by private parties (service and network providers) is not decisive in this regard. Instead, what is significant for classifying such practices as interference with personal privacy is that the authorities have the right, as specified by domestic law, to access the data at any time, whether or not the state subsequently uses the data against the individual (see the European Court of Human Rights case Amann v Switzerland).

The data-retention framework represents a significant development in relation to personal security and freedom. That is, surveillance practices, which were once reserved for “suspect” or “deviant” individuals, have been extended to cover the majority of the population, making it increasingly possible to sort, categorize, and target innocent individuals. Data-retention policies mandate the permanent, general recording of the communicational behavior of all subscribers/users, notwithstanding the fact that in the first instance they are not understood to be a source of danger, nor are their communications taking place in an unusually dangerous area.

According to the European Convention of Human Rights, communications surveillance is unacceptable unless a legal basis is provided: unless the measure is “necessary in a democratic society” and serves the legitimate interests of national security, public safety or the economic wellbeing of a country, the prevention of disorder or crime, protection of health or morals, or protection of the rights and freedoms of others. Even if “necessary is not synonymous with

---

indispensable ... it implies a pressing social need” (European Court of Human Rights case Handyside v UK). The objective pursued must be weighed against the seriousness of the interference entailed in the measures. It is not only the practices of collecting and processing telecommunications data that have important social effects and regulatory implications, but the scale of the collection. The seriousness and the impacts of the interference are to be judged by taking into account, inter alia, the competences granted to the security authorities, the number and nature of persons affected, and the intensity of the negative effects that will result. Restrictions on personal freedoms must be strictly minimized and legislators must try to achieve their aims in the least onerous way possible (European Court of Human Rights case Hatton v UK). The necessity and proportionality of any particular measure must be clearly demonstrated, recognizing that privacy is not only an individual right to control one’s information but also a key element of any democratic constitutional order (Federal German Constitutional Court Census case, 1983). The Data Retention Framework was adopted without demonstrating that “the (pre) existing legal framework does not offer the instruments that are needed to protect physical security” 101. Nor was it demonstrated that this large-scale initiative, with its massive surveillance potential, was the only feasible option available to combat crime. Under the current dominant security ideology—which sometimes verges on a security obsession—the need for greater security is presented as a “self-evident fact,” but “security” cannot be understood normatively nor does it allow for the usual constitutional balancing of process and principles.

Generalized data-retention practices conflict with the requirements for proportionality, fair use, and specificity in the European data-protection regulations. In that framework, personal data is not to be collected, processed, or transmitted for the sole purpose of providing a speculative future data resource 102. In light of the increased use of electronic communications in daily life, and the fact that the internet in particular provides an unprecedented ability to

---


store and reveal information, the storage of such data amounts to an “extended logbook” of a person’s behavior and life\textsuperscript{103}.

From the very beginning, the Data Retention Directive has been one of the most controversial pieces of the EU’s counter-terrorism legislation. Debates over its compatibility with fundamental rights and legality in general have raged since the earliest stages of its drafting to the April 2014 judgment by the Court of Justice at the level of both the EU legal order and the national legal orders of the member states. In 2006, Ireland brought a direct action before the Court seeking annulment of the directive by claiming that the directive was adopted on an incorrect legal basis.

The Court of Justice could easily conclude that the obligation on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raised ‘questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter’.

In doing so, the Directive ‘treats everyone as a suspect’, ‘monitors everyone’ and ‘puts everyone under surveillance’, and for this reason the European Court of Justice in a landmark judgment—held that the Data Retention Directive ‘constitutes a particularly serious interference’ with the fundamental right of citizens to privacy. As a consequence, on 8April 2014 the CJEU, sitting in Grand Chamber, declared Directive 2006/24/EC invalid since it violates the right to privacy (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter), read in light of Article 52 of the Charter of Fundamental Rights of the European Union (the Charter). In adopting Directive 2006/24, the EU legislature exceeded the limits imposed by the principle of proportionality. For the first time, the CJEU has declared the full invalidity of the

European data retention regulation due to a violation of fundamental rights as laid down by the Charter.

As a result, the CJEU held that 'the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality' and in so doing the Court rejected the practice of universal surveillance. In fact, the core of the Court’s decision lies in the rejection of mass surveillance and in particular indiscriminate monitoring of ‘the entire European population’, which interferes with fundamental rights, especially the right to privacy and the right to data protection. This main argument of the Court’s decision can also be seen as an indirect warning regarding any future negotiations between the US and EU in this field.

More precisely, according to the Court, the data indicated by Article 5 — ‘taken as a whole’— allow specific and precise deductions to be made regarding the private lives of the persons whose data has been retained, including their habits, movements, activities and relationships. For the Court this result does not comply with the right to privacy, as enshrined in the Charter. Furthermore, the Court established that interference with the rights to privacy could be merely ‘potential’ since ‘it does not matter (...) whether the persons concerned have been inconvenienced in any way’, in the same way that it does not matter ‘whether the information on the private lives concerned is sensitive’.

104 Arianna Vedaschi and Valerio Lubello, Data Retention and its Implications for the Fundamental Right to Privacy
A European Perspective, Tilburg law review 20 (2015) 14-34