PUBLIC

CounteR

Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection

Project Acronym	CounteR
Project Full Title	Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction, Counter Radicalisation and Citizen Protection
Grant Agreement no	101021607
Project Duration	36 months (starting May 1st, 2021)

Deliverable number 7.1

Data Protection Requirements

Work Package	WP7 Data Privacy & Ethics Requirements
Task	Task 7.1 Data Privacy analysis and requirements
Lead Beneficiary	Eticas Research and Consulting (ETI)
Due Date	31/12/2021
Submission Date	31/12/2021
Deliverable Status	Final version
Deliverable Type	R
Dissemination Level	PU
Document Name	D7.1 Data Protection Requirements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

PUBLIC

Editors

Surname	First Name	Beneficiary
Zamorano	Mariano Martín	ETI
Kapros	Evan	ETI

Contributors

Surname	First Name	Beneficiary
Kapros	Evan	ETI
Zamorano	Mariano Martín	ETI
Galdon Clavell	Gemma	ETI

Reviewers

Surname	First Name	Beneficiary
Tantu	Dana	INS
Trufin	Catalin	AST
Vladuta	Alexandru	SPP

History of Changes

Version	Date	Change	Modified by
0.1	28/10/2021	Index update and review	Evan Kapros, Mariano Zamorano
0.2	17/11/2021	Initial draft sections 1-3	Mariano Zamorano, Evan Kapros
0.3	23/11/2021	Second draft	Mariano Martín Zamorano
0.4	29/11/2021	First review	Sarah Cannataci, Michael Zammit
0.5	03/12/2021	Third draft integrating review	Mariano Martín Zamorano
0.6	14/12/2021	Second review	Dana Tantu, Catalin Trufin
0.7	20/12/2021	Final version integrating review	Mariano Martín Zamorano
0.8	31/12/2021	Final version	Mariano Martín Zamorano
1.0	31/12/2021	Version reviewed and approved	Dana Tantu, Catalin Trufin

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

Executive Summary

The CounteR Project will develop a system (the 'System') to automate Big Data to detect radicalisation online. LEAs and other competent authorities will use the System to prevent and tackle radicalisation of individuals and groups. By clustering data online and avoiding using personal and sensitive identifiers as a basis for data classification the System expects to reduce adverse outcomes of data processing. However, the System policy involves several issues related to its potential for algorithmic discrimination function creep and privacy violations. Moreover, due to its complex data processing including the reuse of personal data online the System has a complex inscription in data protection and criminal investigation legal frameworks. In order to define the normative and legal boundaries for the design of the System this Deliverable (the 'Deliverable') reviews applicable legal provisions and sets requirements for the System to be considered by design and default. Based on literature and legal review and the analysis of case study, the Deliverable also made recommendations for operationalising such EU and national requirements into the system design and operation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

List of Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
D	Deliverable
DoA	Description of the Action
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
EECC	European Electronic Communications Code
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
GA	Grant Agreement
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
LOPDGDD	Organic Law on Data Protection and Guarantee of Digital Rights
ML	Machine Learning
NLP	Natural Language Processing
NIS	Network and Information Security directive
SNA	Social Network Analysis
T	Task
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101021607

1 Introduction

This deliverable sets the data protection requirements **for the CounteR System development.** The document identifies and discusses applicable legal definitions for the system design together with ethical principles and standards that should drive its concept and implementation. Tensions between these legal frameworks and the actual deployment of the system are addressed. In particular, the analysis is contrasted to a case study and translated into suitable recommendations for the CounteR implementation.

The CounteR project is aimed at supporting the **detection and tackling of radicalisation online in the EU**. With this purpose, it develops an **early alert platform** for processing data from a variety of sources using data mining techniques and AI. The platform will collect posts, texts, and images/videos from the surface/deep/dark web and social media using user-defined keywords, areas of interest, or user accounts to proceed with ML-based analytics. The system concept combines NLP technologies with a robust theoretical background on the psychology of radicalisation to provide a complete solution for LEAs to understand and address related processes. On this basis, CounteR enables specific actions against threat activities such as propaganda, fundraising, recruitment and mobilization, networking, information sharing, planning/coordination, data manipulation, and misinformation.

The CounteR system will **support LEAs analysing online content and its surrounding community** as well as related risk factors when conducting criminal investigations. The information gained by the system will also allow LEAs and other community stakeholders to implement prevention programs and employ counter-narrative rather than relying solely on surveillance. In addition, the CounteR system will support information sharing between European LEAs and foster collaboration between various agencies by providing an open platform that prioritizes harmonized information formats.

One key added value of the CounteR development is its design aimed at automatically monitoring contextual factors related to radicalisation rather than targeting and surveilling individuals. In this way, the system concept seeks to ensure **respect to the right to privacy and** mitigate **risks of criminalisation.** In addition, the approach should support **end-users in proportionately preventing data misuse**.

However, CounteR still entails many challenges, including specific technical and legal requirements for automated processing of big data, reuse of social media data, personal data classification and support for policing online. These issues can be mirrored into two interrelated ethics and legal requirements for using online data for policing investigations on the one hand and for ensuring privacy rights on the other hand. Big Data, AI, and insight tools have significantly impacted how **surveillance** is done, including further invasiveness and disproportionate impacts on disadvantaged populations when conducting policing surveillance (Brayne, 2017). Negative externalities of this data processing include **privacy violations, algorithmic discrimination or false positives** leading to unfair treatment. Along these lines, adverse outcomes of automated surveillance include **processing and exposing pseudo-identifiers and personal data** disseminated online, prompting threats for privacy and facilitating identification (Sweeney, 2000; Ratha et al., 2015). Therefore, a proper **balance between rights to security and privacy** while respecting human rights must be ensured by

design and default. This deliverable provides a legal and ethical framework addressing all these issues and establishes the general system data processing and implementation boundaries.

1.1 Briefing of the system current architecture, functionalities and their legal implications

In its current state, the CounteR System will be used to support **intelligence gathering and threat assessment**. By conducting analysis of large amounts of data coming from various sources, this system will allow officers to determine if a specific person/group/organization targets one or more different subjects and initiate a gathering process.

As pointed out in D1.1, in real scenarios, CounteR will process data from **offline and online** databases. Among its online processing capabilities, the system will analyse different data formats, including **text or images/videos**, to conduct **detection and recognition of behaviours and activities**. Two approaches will be used in this regard. On the one hand, CounteR will process data coming from **social media**. Examination of these datasets will require the intervention of intelligence officers to establish proper associations between detected activities and groups or individuals. On the other hand, officers will **screen surface/deep/dark web environments** to collect data of interest. Data subjected to scrutiny includes publicly available data related to a specific protected subject, an event at which one or more protected figures attend, the location where a dignitary works/lives/attends a meeting and the routes used by a protected figure and any other relevant information. As with social media, investigators will establish hypotheses about potential links between these actions and specific persons, groups or communities.

CounteR **Operational Scenarios are divided into proactive and reactive modes**:

- **Proactive**: This mode aims at identifying terrorist online communities, by categorizing malicious content shared online.
- **Reactive**: This mode provides functionalities to allow a precise removal of inappropriate content with a human-in-the-loop approach.

When using algorithms for processing **heterogeneous data sources for conducting threat detection and classification based on AI, problems can arise**. Data initially gathered will be personal (and sensitive) data to be correctly pseudonymized so individuals can be reidentified when required, thus remaining personal. This means that issues to be considered when framing legal and ethical requirements for CounteR include:

- Need for ensuring access control (i.e., unexpected problems with authentication systems used by LEAs for CounteR);
- Need for ensuring data minimization (i.e., through automated anonymization techniques);
- Algorithmic discrimination (i.e., derived from user Interaction);
- Performance issues (i.e., number of wrong detections);
- Problems in examining diverse data types (i.e., lack of adaptation to data characteristics).

Requirements framing considers these implications for narrowing down the legal scope of the system and setting actionable protocols and recommendations.

1.2 Relation with other tasks and deliverables

CounteR has 11 Work Packages (WPs). This Deliverable is carried out as part of **Task 7.1 and it is part of WP7**, which is dedicated to **legal and ethical requirements**. The project WP structure can be classified into five main categories:

A. Firstly, those concerning technical and scientific development of the solution (WPs 1 through 6);

B. Secondly, the WP enabling the solution to be ready for the market (WP8), through a set of pilots involving real cases scenarios;

C. Thirdly, the WP supporting dissemination and exploitation (WP9) to carry out activities during the project and to plan the actions after the project to bring about the expected impact;

D. Fourthly other supporting activities to carry out European guidelines and procedures (WP10).

E. Lastly, one WP which will address the Ethics Requirements of the project needed after the Ethical Screening.

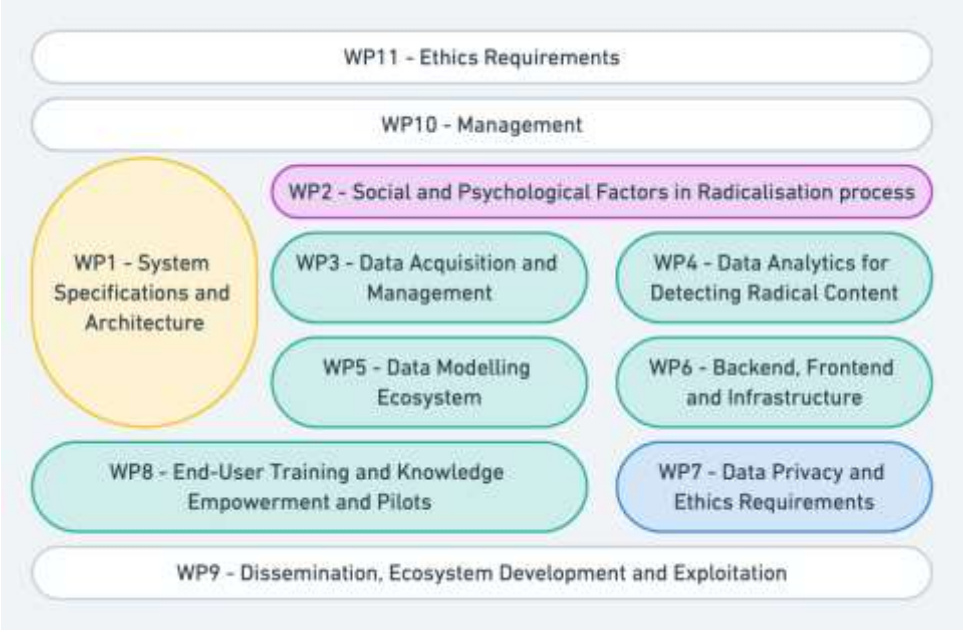

Figure 1 - CounteR Work Packages Structure

Although WP7 ensures **transversal integration of ethical and legal aspects** into all of these registers and WPs, its Tasks will focus on ensuring compliance by design (WP1-WP6) and proper alignment of social and psychological factors within CounteR technology development and validation (WP2 and WP8). In the Grant Agreement, Task 7.1 is described as follows:

"Systems for fighting radicalisation online, often developed by states and supranational organisations, have become very important in the last years due to the growing use of ICT in transnational communication. Both recent findings concerning the geopolitical impact of online radicalisation strategies and the evolution of the European legal framework on data protection have forced organizations to develop "by-design" prevention systems and focus on security controls and protocols.

Taking this into account, a ***thorough revision of the legal framework on data protection and cybersecurity issues*** *in the studied field will be carried out in D7.1. In this way, this task will identify and* ***frame the requirements and principles*** *that should guide the proposed solution (WP1and 6), both in terms of its technical challenges, as well as in terms of supporting LEAs to develop appropriate management strategies. In order to accomplish that aim, we will go through the most pivotal regulations that affect the questions approached in the project. Those are, among others, the regulations listed down below:*

- *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.*
- *General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC).*
- *DIRECTIVE 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.*

The review of the applicable legal framework will not be limited to the mere enumeration of legal texts that are relevant for the proposal. Instead, D7.1 will ***spot all the most salient precepts and will apply them to the reality of the CounteR system*** *and research project with the aim of ensuring legal compliance. Aspects already addressed by cyber-based crime regulations, such as the complex jurisdictional aspects of illegal activities committed online or the "alegal" character of many of the infractions occurred in this context, will be particularly analysed. In order to do so and to frame the scope, adaptability and sustainability of the CounteR system, relevant EU case studies and jurisprudence in this domain will be examined."*

Therefore, this deliverable focuses on framing and analysing the **system requirements for implementation** (I.e., privacy by design in real scenarios). Instead, D1.3 "Review of relevant supranational/ EU/ national laws and regulations" and deliverables in WP11 will provide an in-depth analysis of requirements for compliance with EU legal applicable provisions and the EC requirements **during the research project** (I.e., data processing during algorithmic training). Lastly, the thorough presentation of data protection and other requirements, even applied to a hypothetical implementation of CounteR, provides elements for developing and analysing other research-oriented WPs and documents, such as D11.1_H Requirement no. 1, and D11.2_POPD Requirement no. 3, or D10.3: Data Management Plan.

1.3 Methodology

This report seeks to establish the legal and ethical framework for CounteR technological development and implementation. A **systematic finding and ascertainment of law** in the **online policing area** has been conducted with this purpose. Various laws and legal frameworks and literature have been identified, reviewed, and analysed to determine relevant legal requirements and ethical principles that should guide the solution addressing their tensions and enactments in specific data processing scenarios or CounteR practices and procedures. Moreover, WP1 deliverables, literature and relevant guidelines on **ethics of technology** concerning the use of innovative solutions in online policing have also been reviewed. The ethics analysis is aimed at ensuring that CounteR concept and design goes beyond legal compliance.

Our approach to legal analysis has combined a primary focus on **doctrinal legal research methodology** (or so-called "black letter" methodology) with a preliminary **operationalization of provisions and requirements** (Hutchinson, 1999). Two processes have been followed for this purpose. Firstly, we have composed a descriptive and detailed analysis of legal rules found in primary sources (cases, statutes, or regulations). Secondly, we have carried out an inductive examination by considering legal tensions, contextualization within CounteR scenarios and case studies. This register of the analysis looks into how the law and ethical concern moulds and affects CounteR technology implementation. It employs socio-technical studies methods to answer the questions and ethical dilemmas.

Lastly, a **case study qualitative analysis** has been used to explore the addressed phenomenon in a particular context through various data sources (Baxter & Jack, 2008). The Spanish case has been analysed under the light of two instruments, the scoping of its specific legal framework greatly defined by EU regulations on data protection and policing, and the examination of a specific policy implemented in the country close to the CounteR domain. This aims to hypothesise specifics of CounteR deployment in different EU scenarios and extract elements for legal analysis. However, it should be noted that this examination seeks to illustrate the functioning of the general EU normative framework. Therefore, it is not aimed at operationalizing legal requirements at the EU level since this process will be addressed in other Tasks concerning demonstrations and input based technological design.

1.4 Deliverable structure

The document is structured in 7 sections as follows:

- **Introduction -** this section introduces the goals and methodology of the deliverable and provides a brief overview of the system features and characteristics;
- **CounteR legal frameworks and requirements** - this section identifies and describes data protection and criminal law provisions relevant for CounteR;
- **CounteR ethical framework -** ethics values guiding the System development are summarized and problematized;
- **CounteR approach and national case study -** this section narrows down the legal and ethical approach based on the Spanish case analysis;

- **Summary analysis -** this section summarizes identified requirements and principles and discuss their implications;
- **Conclusions, requirements and recommendations -** this section provides overall findings and recommendations based on the identified requirements;
- **References -** a complete list of references is provided.

2 CounteR Legal Frameworks and Requirements

This section reviews four relevant legal frameworks for developing CounteR solutions **at the EU level**, including **data protection, policing, cyber security and AI**. The analysis starts from the overarching data protection requirements provided by the Regulation (EU) 2016/679, General Data Protection Regulation (GDPR). It continues with those provisions regulating the use of online data for criminal investigation purposes, which are a necessary exemption for different requirements in the GDPR. After this, the section introduces fundamental norms or standards concerning two dimensions that should be transversally considered. Firstly, those provisions that pose requirements for cybersecurity that affect CounteR deployment. Secondly, those concerning automated (personal) data processing with a criminal investigation or radicalisation analysis purposes. All these provisions are addressed in light of its implications for CounteR and in order to set an EU standard for its development.

2.1 Data protection requirements: the GDPR

Data protection can be defined as the normative framework setting **rules for the processing of personal data**. This framework covers norms from the fields of data protection, data security and data privacy. In a more practical sense, it defines how to safeguard data from corruption, compromise or loss while protecting data subjects' rights.

The EU Charter of Fundamental Rights states that citizens of the Union have the right to **have their personal data protected**. The GDPR is the primary Regulation in this domain at the EU level. Its provisions, including data security and the notification of personal data breaches, set out requirements for organizations to follow whenever they process personal data. It also confers rights to individuals in respect of their personal data. In both senses, the domain addressed by the GDPR can be considered broader than cybersecurity.

According to the GDPR, **"processing"** means any process including personal data, including collecting, using, anonymizing, storing, transferring, accessing and deleting personal data (I.e., the removal of data as part of CounteR reactive mode functionalities). Moreover, the concept of **"personal data"**[1] refers to any information relating to an identified or identifiable individual (a "data subject") and that can allow his/her direct or indirect identification. The following sections will summarize those principles and provisions in the GDPR affecting how CounteR collects and processes personal data.

[1] GDPR, Article 4, provides the following examples: *"name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data."*

2.1.1 Data governance and legal basis for the processing of personal data

In order to establish legal boundaries and requirements for CounteR development, requirements for data **governance and distribution of responsibility in the processing of personal data** established in the GDPR must be considered. According to this law, the **data controller** is the natural or legal person (including public authorities) in charge of ensuring that the purposes and means of personal data processing are respected (Art. 4, GDPR). This figure is responsible for the proactive setting of technical and organizational measures for data management. Moreover, the controller must conduct other activities, such as the systematic register of processing activities, which is particularly relevant in the case of special categories of data (Arts. 9 and 82 to 84) or the provision of information to citizens and organizations regarding the processing. In CounteR, the data controller, possibly the LEAs managing the system, will therefore be responsible for personal data collected before, during and after its implementation. However, it should be noted that third parties may collect data to be processed by the CounteR System (i.e., social media companies). Therefore, **LEAs may not always act as controllers.**

Furthermore, the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Arts 4, 8) are defined as **processors**. These actors or entities can share personal data with other processors under the authorization of the controller. According to the GDPR (Art 28), a binding document must define the conditions for the relation between the controller and the processor(s). In CounteR, data is expected to be exchanged between LEAs acting as data controllers, other LEAs or public authorities under specific conditions.

The third relevant actor involved in data governance is the **Data Protection Officer** (DPO), who needs to be designated when processing a certain amount of personal data, or when the processing is a special kind of entity (Article 37.1). The DPO monitors the organization for whom it is designated, to assess whether the organisation is processing personal data concerning data subjects (including staff, customers, providers or any other individuals) in compliance with the GDPR.

When deploying CounteR, **each data governance scheme and legal framework in place** will determine specifics of the operationalization of requirements for the management of personal data. Therefore, governance depends on national and European legal frameworks. These case-specific aspects also concern the responsibility of controllers based in Europe in their relationships with third parties in third countries who may act as data processors established in Article 44 of the GDPR.

To fulfil the principle of **lawfulness, fairness and transparency** (see in Section 2.1.2 below), Chapter 6 of the GDPR requires any organization processing personal data to have a valid legal basis for this activity. Depending on the processing scenarios, lawful processing can **be based on one or more of the six legal bases for processing provided by the GDPR**:

- Consent;
- Performance of a Contract;
- Legitimate Interest;
- Vital Interest;
- Legal Requirement;
- Public Interest.

In CounteR, the processing of personal data by controllers and processors might be conducted on the basis of (Art. 6 GDPR) **explicit consent** (a). To fulfil this basis, data subjects must know the controller(s)/processor(s) identity, what data processing activities they intend to conduct, the purpose of the data processing, and they should be properly informed regarding their right to withdraw their consent at any time. However, in several scenarios, for instance, when the system is used to conduct online investigations, this will not be possible. Therefore, the legal basis for the processing should be one or more of the following conditions contemplated in the GDPR:

> *"b. processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
> *c. processing is necessary for **compliance with a legal obligation** to which the controller is subject;*
> *d. processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;*
> *e. processing is necessary for the performance of a task carried out in the **public interest or in the exercise of official authority** vested in the controller;*
> *f. processing is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."*

The processing of personal data as part of radicalisation detection and response will be primarily based on basis d), e) and f), and may fall outside the scope of the GDPR, as we will see below.

2.1.2 GDPR principles and requirements

The following seven key principles in the GDPR mirror requirements to be observed by controllers and processors when processing personal data.

> **Lawfulness:** Article 5.1 (a), "*personal data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."*

In CounteR, **lawful processing** is that which is carried out on the basis for processing established in Article 6.1 of the GDPR. Moreover, it requires that personal data are processed in a lawful, fair and transparent way in relation to data subjects. One key element for this system development and implementation is that many of its purposes and forms for processing **do not fall under informed consent**[2]. Therefore, processing must fulfil conditions for public interest or legitimate interest legal basis and applicable policing regulations.

[2] *However, in some contexts and situations, data subjects must be informed regarding the purposes for which their data will be processed to be considered genuinely informed and lawful (see Articles 13 and 14 GDPR). In this case, it is still open (a) whether the CounteR System will be providing the information set out in Art. 14, and (b) how it will be providing such information.*

Purpose limitation: Article 5.1 (b): "*personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')."*

Therefore, the principle of purpose limitation indicates that data must be **collected to meet specific and clearly defined goals**. In CounteR, this involves that personal data collected by the system is only used to **detect radicalisation online**. This requires establishing proper technical mechanisms to avoid any kind of function creep[3]. Often new uses for technologies or data beyond what was originally envisaged or legitimated lead to violate conditions for consent. CounteR must integrate mechanisms to avoid all forms of function creep.

Data minimisation: Article 5.1 (c): *"personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."*

The principle of data minimization establishes that collected data should **not be more than what is strictly necessary** in order to achieve the purpose of the processing. In CounteR, this implies that the system must be designed to meet its function while keeping personal data collected online and stored in data controllers' databases for this at a minimum by methods such as automated deletion and anonymization.

Accuracy: Article 5.1 (d): "*personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')."*

According to this principle, data must **be not only accurate but aligned with reality,** which needs to be judged in relation to the processing purposes. Specific data subject's rights in the GDPR regulation serve to enforce this principle. For instance, a data subject has the right to the controller to erase or rectify her data (Arts 16 and 17 of the GDPR). Therefore, features, technical capabilities and protocols in CounteR must allow quality control and data editing to ensure these rights.

Storage limitation: Article 5.1 (e): *"personal data must **be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')."*

[3] *"Function creep" means using information for a purpose that is not the initially specified purpose*

Along these lines, personal data should **not be kept for any longer than is reasonable for achieving the purposes** for which they were collected in the first place. The period can be longer if the data are being processed for one of the purposes in 89 GDPR (public interest, scientific or historical research purposes, and statistical purposes). Therefore, once the CounteR system is implemented, its controller may need to put in place technical and organisational measures to safeguard the data subject's rights and freedoms related to legal data retention periods.

Integrity and confidentiality (Security): Article 5.1 (f): *"personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

This means that CounteR developers and implementers must ensure that the system can provide **technical and organizational support for safeguarding personal data**. Both the need for conducting a proportionality analysis in order to set the boundaries for these measures and the inclusion of concrete data protection techniques to be used are mentioned in Articles 25 and 32 GDPR:

Article 25, GDPR, on the need of i**ntroducing security measures**: "*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself,* ***implement appropriate technical and organisational measures, such as pseudonymisation,*** *which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet these requirements*."

Article 32, GDPR, on possible forms of **securing personal data**: "*the* ***pseudonymisation and encryption of personal data****; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*."

Lastly, the **accountability principle** involves controllers and processors taking responsibility for their processing of personal data and ensuring compliance with the all above principles.

Accountability: Art 5, 2: *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

Moreover, data protection measures must be accompanied by **documentation and recording processes** allowing them to demonstrate compliance. In CounteR implementation, specific mechanisms for data processing monitoring, such as login control for end-users, will have to be established following this principle. Moreover, the system must allow to trace back the activity of a specific user or determine who/when/how data was manipulated. Audit data must not be manipulated under any circumstance by any category of users (even with root access) to have non-repudiation principle valid for CounteR.

2.1.3 Other relevant GDPR requirements in CounteR

This subsection further details key GDPR requirements concerning CounteR system development and implementation based on functionalities, goals and data processing.

2.1.3.1 Profiling and automated decision making

Besides requirements regarding data governance and following requirements aligned with the seven above principles, other GDPR provisions must be considered in CounteR. One particular aspect of being considered is its automated processing of personal and sensitive personal data. The system will conduct **profiling and be supported in automated decision-making** to produce alerts and classify data subjects' data online. GDPR introduces specific requirements for these processes going beyond privacy implications. In the GDPR, profiling means both the generation and use of profiles. Article 4 defines it as follows:

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

According to GDPR Article 22, "*The data subject shall have the right not to be subject to a decision based solely **on automated processing, including profiling,** which produces legal effects concerning him or her or similarly significantly affects him or her.*" Therefore, the norm poses limitations to automated decision making and profiling in this framework. In inferring and predicting processes supported by AI technologies, profiling can produce personal data and classify these data on a discriminatory basis. Article 22 may only concern a limited range of automated decisions. Nevertheless, CounteR must foresee and integrate mechanisms for ensuring human intervention in certain decision-making activities, classifying individuals and groups (for instance, based on their preferences and behaviours) that involve data subjects' risks' rights.

Moreover, CounteR profiling will be based on a predictive method "to identify 'unknown' individuals who may be of interest to law enforcement and border management authorities" (Fundamental Rights Agency, 2018: 18). As examined by the Fundamental Rights Agency (FRA), behavioural analysis conducted within law enforcement is accompanied by the classification of individuals based on their visible physical traits, such as age, gender, or ethnicity. In order for this type of profiling to be lawful, it must be conducted following **specific safeguards, including having an objective and reasonable justification** for the profiling and data-driven risk analysis.

2.1.3.2 Reuse of personal data and online privacy

In case further processing of the personal data is no longer for original purposes, organizations need to have a lawful basis under Article 6 of the GDPR detailed above. Furthermore, as the personal data processed by CounteR will share or reuse is likely to include criminal offence data, its controller will need to meet the requirements of Article 10 GDPR: "Processing of personal data relating to criminal convictions and offences".

> *"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out **only under the control of official authority** or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."*

Therefore, only legally authorized LEAs and official authorities **may be allowed to reprocess personal data collected by third parties** (I.e., social media providers) for new purposes (I.e., monitoring radicalisation online) using the CounteR System. However, this processing must be conducted under the conditions set by applicable EU and national legislation concerning criminal investigations. Furthermore, appropriate and proportional safeguards must also be taken, including privacy-enhancing technologies for ensuring purpose limitation.

2.1.3.3 Additional applicable data privacy requirements

Anonymisation and pseudonymisation are two concepts addressed by GDPR to make data processing fit legitimate purposes and protect the data subject's privacy. Anonymised data is introduced in Recital 26 of the GDPR in the following terms:

> *"The principles of data protection should therefore not apply to anonymous information, namely information which **does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable**. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."*

Differently from the former EU 95/46/EC Directive, which did not mention pseudonymised data (so data was either identifiable (personal) or non-identifiable data), the GDPR introduced a **middle ground by formalising the notion of pseudonymised data**. Pseudonymised data, also Recital 26, is defined as follows:

> *"Personal data which have undergone pseudonymisation, which **could be attributed to a natural person using additional information** should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."*

This middle ground has been a notable innovation of the GDPR, and it is crucial for the CounteR concept and implementation. It provides more instruments and strategic approaches to data controllers to protect datasets (Kotschy, 2016). In this regard, pseudonymization has been presented as a legal pathway to ensure a balance between systems functionality and the social value of data with the need of protecting privacy (Brasher, 2018). However, to ensure this balance, it is crucial to mitigate **risks for reidentification when applying pseudonymization techniques**.

Together with anonymization and pseudonymization, the GDPR requires organizations to implement other technical and organizational measures to protect data and safeguard individual rights. This is framed under the concept of data protection by design and by default. It means integrating data protection into organizations processing actions and business practices, from the design step and through the lifecycle. In particular, Articles 25(1) and 25(2) of the GDPR outline obligations concerning data protection by design and by default.

Article 25(1) regarding data protection by design:

> *"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures,* ***such as pseudonymisation,*** *which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."*

Article 25(2) specifies the requirements for data protection by default:

> *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are* ***not made accessible without the individual's intervention to an indefinite number of natural persons****."*

2.1.3.4 Additional data security requirements

As part of the above detailed appropriate technical and organizational measures to ensure organizations process personal data securely, the GDPR (Arts 6, 32 and 34) includes **encryption**. Encryption is a mathematical function that encodes data so that only authorised users can access it. This measure will be suitable depending on the nature and risks of CounteR processing activities. An encryption policy should be put in place to govern its methods and timing to ensure the proper implementation of this technique. The policy should define the most suitable way to implement encryption in data transfer and storage. Lastly, **an incidental policy for residual risks of encryption** should be available.

2.1.3.5 Processing special categories of personal data

Article 9 GDPR prohibits the processing of special categories of personal data, which are defined as follows:

> *"Processing of 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 prohibited.**"*

However, several EU laws or national legislations can entail **exceptions to this prohibition**. For example, special categories of personal data can be processed by virtue of the GDPR when the processing is necessary to **protect the data subject's vital interests** or another person if the data subject is physically or legally incapable of giving consent. Also, when the processing relates to personal data, which are manifestly made public by the data subject, such as publishing them on his/her own website. Lastly, another relevant exemption for CounteR is the establishment, exercise or defence of legal claims.

2.1.4 GDPR national implementation and exemptions

Although GDPR is directly effective in the Member States without implementing legislation, **Member States can develop their own legislative instruments on this basis**. Such laws can also implement specific data protection requirements in some matters and areas, always if aligned with the GDPR principles. Reasons for adaptation or interpretation of requirements can include the need to process personal data to comply with a legal obligation, particular data processing policies based on public interest or tasks conducted by an official body in a specific country.

Moreover, as privacy or data protection rights are not absolute, it is vital to notice that various CounteR based policies and activities **may fall entirely outside the GDPR's scope**. The GDPR defines the general rules for personal data processing and can hence be viewed as *lex generalis*. In international law and some specific cases, if two laws govern the same factual circumstance, a law ruling a particular subject matter (*lex specialis*) overrides a law governing only global issues (*lex generalis*). Along these lines, the Directive 2016/680 setting the rules for processing personal data within the law enforcement domain can be understood as *lex specialis* (de Hert and Papakonstantinou, 2016). Therefore, the processing of personal data can be conducted under the GDPR rules or satisfy the criteria of the law enforcement purposes under national transpositions of the Law Enforcement Directive (LED) (2016/680) described in the following section.

2.2 Applicable policing regulations: the Law Enforcement Directive

The Directive 2016/680[4], which entered into force in 2018, explicitly **regulates data processing by police and criminal justice authorities in the EU**. The Directive is aimed at ensuring compliance with the fundamental right to privacy when processing citizens data by police and judicial authorities for law enforcement purposes. Under the Directive, personal data of crime victims, witnesses and suspects must be adequately protected. Along these lines, Article 4 of the Directive mandates Member States to consider the above **7 GDPR principles in the processing of criminal data**. It also promotes cross-border cooperation in the fight against crime and terrorism.

Under this Directive, the purposes of the **processing can be the prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties** (Articles 2(1) and 1(1) which can be justified under **public Interest** (Article 35). The scope of the Directive also includes automated processing (Arts 2, 2 and 3):

> *2.This Directive applies to the processing of personal data wholly or partly by automated means, 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.*
> *3.This Directive does not apply to the processing of personal data:*
> *(a)in the course of an activity which falls outside the scope of Union law;*
> *(b)by the Union institutions, bodies, offices and agencies.*

The applicability of this legal regime needs to be **assessed on a case-by-case and national basis.** This depends on local definitions of competent authorities and how the data collection purposes are defined and secured. To define competencies and responsibilities in CounteR based online policing in a particular country, forms of data processing within specific systems will have to be considered. For example, cases include local police storing information of the platform in their servers which could be framed as being ‘"on behalf of" Law Enforcement Authorities qualifying them as "data processors" under the Directive 2016/680 (Caruana, 2017). Still, in case that the data controller of the CounteR System is a **competent national authority, and the purposes of the processing are the prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties** (Articles 2(1) and 1(1), then the processing falls under the LED. Competent authorities include the police, national courts, and other judicial authorities, prosecution, customs and border guards. Depending on the country, other authorities may be specialized agencies having investigatory powers or other departments with similar competences.

In this regard, data collected with prevention purposes under the GDPR may have to be used to resolve other criminal offences or conduct criminal investigations making a strict application of the purpose limitation principle difficult. Directive 2016/680 thus allows the use of data for purposes **other than those for which they have been gathered** as long as the processing is in line with the following requirements:

---

[4] *Named as: “On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA”*

- the general purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- the controller is authorized to process such data by law;
- the processing is necessary and proportionate (Article 4(2));
- relevant national competences and regulatory frameworks.

The LED (28) mandates competent authorities to process personal data **in a safe manner** and establishing mechanisms for ensuring **security and confidentiality**:

> *"In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an **appropriate level of security and confidentiality,** including by preventing unauthorised access to or use of personal data and the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected."*

Moreover, Article 34 indicates a wide range of data processing operations and data processing purposes falling under the Directive, including **automated processing**. It also points out that its requirements for data processing in the Directive also apply to sharing personal data between competent authorities and third parties.

> *"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, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by **automated means or otherwise**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction. In particular, the rules of this Directive should apply to the **transmission of personal data for the purposes of this Directive** to a recipient not subject to this Directive. Such a recipient should encompass a natural or legal person, public authority, agency or any other body to which personal data are lawfully disclosed by the competent authority."*

However, in line with the GDPR, the Directive mandates data subject to have the right not to be subject to a decision evaluating personal aspects based **solely on automated processing** and which produces adverse legal effects concerning, or significantly affects, them (Art 38). This is vital for CounteR, since the system should allow human intervention concerning outcomes of data processing leading to concrete policing actions related to radicalisation prevention or response. In this regard, data subjects' rights also include the right to be informed about the processing or challenging the decision.

Furthermore, requirements concerning **non-discrimination** are also integrated into the Directive, including data processing and profiling leading to adverse consequences (Arts 11, 3; 23; 51; 61).

2.2.1 National implementation of the Directive provisions

EU “directives” are legislative acts setting out policy goals for Member States, but each EU member can develop its own laws on how to reach those goals. In the LED, this has been translated into a **variety of implementations and legal frameworks defining how to conduct criminal investigations online**. This must be considered in terms of standards for CounteR development and implementation. Under data protection general rules defined by the GDPR and LED, CounteR should allow modularity and adapt to national contexts.

2.3 EU cybersecurity legislation

This section will introduce provisions and elements from the **Directive (EU) 2016/1148** -concerning measures for a high common level of security of network and information systems across the Union (**NIS**)- and the **Cybercrime Directive** (2013/40/EU) affecting the CounteR system implementation. In addition, the European Electronic Communications Code (EECC) (Directive (EU) 2018/1972) and the EU Cybersecurity Act (Regulation (EU) 2019/881) implement many of these Directives’ provisions. Together with the GDPR and the LED, these texts represent the key regulatory framework for fighting crime online and online privacy (Markopoulou et al., 2019).

Before addressing these norms, a distinction between **cybersecurity, cybercrime and data protection jurisdictions** must be established, although they often overlap. Cybersecurity is defined in the Cybersecurity Act (Regulation (EU) 2019/881) as "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by **cyber threats***". In EU law and policy, ‘cybersecurity' can also cover other matters such as cyber defence policy, which is relevant for CounteR systems framing and analysis. A different concept is **cybercrime**, which is regulated by the Cybercrime Directive, and covers "***attacks against information systems***" and prescribes rules in relation to, for example, illegal access to information systems, illegal system interference, illegal data interference and interception. EU cybercrime law and policy also cover other crimes where computers or IT systems are a primary tool, such as sexual exploitation of children online and child pornography, and fraud and counterfeiting of non-cash payments.

The main piece of legislation on cybersecurity is the NIS Directive, which primarily aims to **improve cybersecurity**. It covers obligations to manage risks posed to "*the security of network and information systems*", which is defined as "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (*Art 4, 2). This Directive entered into force in May 2018, and it is the first comprehensive piece of European legislation specifically aimed at **protecting critical infrastructures** such as airports, connecting bridges or railways (Davis Michels & Walden, 2018, p.3). In order to achieve this, the European legislator has taken a risk-based approach similar to that of the GDPR[5]. This means that the NIS Directive does not require the affected organisations to implement specific policies or security measures. Instead, it obliges them to **consider the risks that their activities** involve and put in place preventative measures that are proportional to their likelihood and the potential damage they could cause. The obligations imposed by the NIS Directive can be divided into two different categories:

a) **Safeguarding obligations**: they require organisations to put in place appropriate and proportionate security measures.
b) **Information obligations**: they require the sharing or disclosure of information.

The two first points of Articles 14 and 16 shown below are helpful as far as understanding the obligations placed upon relevant operators:

Article 14. Security requirements and incident notification:

*"1. Member States shall ensure that **operators of essential services** take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.*
2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services."

[5] *Still, it should be noted that the enforceability of the GDPR as a regulation is entirely different to the NIS directive, since it is just a Directive and not a Regulation.*

Article 16. Security requirements and incident notification:

> *"1. Member States shall ensure that **digital service providers** identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:*
> *(a) the security of systems and facilities;*
> *(b) incident handling;*
> *(c) business continuity management;*
> *(d) monitoring, auditing and testing;*
> *(e) compliance with international standards.*
> *2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents **affecting the security of their network** and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services."*

In terms of the subjective scope of the regulation, the figure of operator of essential services is defined in article 4(4) of the NIS Directive:

> *"'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)."*

This is an important aspect for CounteR, since LEAs using the System may fit this category. In fact, CounteR might circumstantially be an instrument to conduct investigations related to cyber-attacks. In this regard, point 62 of the Directive also mentions that:

> *"Incidents **may be the result of criminal activities the prevention, investigation and prosecution** of which is supported by coordination and cooperation between operators of essential services, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage operators of essential services and digital service providers to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA."*

As a Directive, this piece of legislation required Member States to transpose it via a national legislative act. Member States play a vital role in determining which organizations are to be considered "operators of essential services" according to Article 5 of the NIS Directive.

The **Cybercrime Directive 2013/40** includes additional rules harmonizing the criminalization framework and penalties for several offences aimed against information systems. To this end, it proposes **common definitions** for illegal access to information systems and illegal system interference. Aspects covered include **regulation of malicious software** designed to take remote control of a network of computers (so-called botnets). The Directive also proposes **coordination mechanisms** for responding to threats involving advanced technology. It calls for improving the fight against cybercrime by setting more all-embracing international cooperation between judicial and law enforcement authorities. To this end, as stated in Article 13, EU countries must have an operational national "*points of contact available 24 hours a day and seven days a week*". Moreover, Member States shall also "*ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer.*" As we can see, since the intentional criminal offences addressed by this piece of legislation are attacks against information systems, it does not have direct implications for CounteR. However, in specific scenarios and conditions, **CounteR may contribute to identifying and punishing these activities** by enabling effective, proportionate and dissuasive criminal penalties as stated in the Directive.

In brief, the most critical regulations within the cybersecurity and cybercrime domains and their main implications for CounteR are:

Table 1 - Cybersecurity provisions and general implications for CounteR

Legislation	Scope	Implications for CounteR
The NIS Directive ((EU) 2016/1148) -Commission Implementing Regulation (EU) 2018/151 clarifies and complements some of its rules.	It provides EU scope rules and requirements for enhancing cybersecurity across Member States in key areas.	As the GDPR and the LED, it requires taking proportional organizational and technical measures to protect both systems and personal data. This includes the releasing of relevant information about the systems security and related events.
The Cybercrime Directive (2013/40/EU)	It provides standards for criminal law and policies of the EU member states in the area of attacks against information systems. For this purpose, it sets minimum rules concerning the definition of criminal offences.	It frames the potential usages of CounteR as a tool for contributing to fighting criminal activity online related to radicalisation.

Overall, the EU legal framework on cyber security does not pose specific restrictions or requirements for the development of CounteR, but it represents a guideline to be considered for its implementation.

2.4 AI requirements and standards

AI is a growingly important domain for regulatory and political authorities. In April 2021, the European Commission published a draft regulation on artificial intelligence (AI), representing a transversal regulatory framework comprising any AI system performed in the EU, whether the provider is based in the continent. The draft regulation broadly defines AI as a set of software frames comprising machine learning, expert and logic systems, and Bayesian or statistical approaches. The **implications of using AI in CounteR** will be examined in this section in light of these comprehensive legal text requirements. It should be noted that many of the requirements and measures proposed in this section must be considered as best practices given both the open nature of many of IA ACT proposal provisions and the use of the highest standard approach to the interpretation of such requirements.

In section 1.2, the IA ACT proposal details that its provisions are "*without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems*." Other supplementary elements concern expanding the regulatory framework relating to aspects such as algorithmic discrimination or automated biometric identification. It should be noted that the draft regulation not only represents a comprehensive standard for algorithmic fairness but, also, we may expect that this draft regulation will be passed by when CounteR is deployed.

The **draft regulation categorizes AI systems** based on their **risk in three different levels** that correspond to prohibited AI uses -for those considered unacceptable-, high-risk AI uses, and systems with limited or low risk.

Prohibited AI uses in Title II comprises all those AI systems that contravene Union values or infringe human rights.

> *"The prohibition covers practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour. The proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use* ***of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement*** *is also prohibited unless certain limited exceptions apply."*

Secondly, **high-risk AI uses** include those concerning applying AI technology as a product's safety component and if it is covered by one of **19 designated pieces of EU single market harmonization** legislation (e.g., aviation, cars, medical devices). When the existing single market harmonization legislation covers the product where the AI system is integrated, the draft regulation indicates that the product is already obliged to undergo a third-party compliance assessment. Moreover, these compulsory third-party conformity inspections will include the AIA's obligations after the draft regulation is passed.

Other cited high-risk systems for safety or fundamental rights are:

- Critical infrastructure where the AI system could put people's life and health at risk;
- Educational and vocational settings where the AI system could determine access to education or professional training;
- Employment, worker management and self-employment;
- Essential private and public services, including access to financial services such as credit scoring systems;
- **Law enforcement;**
- Migration, asylum and border control, including verifying the authenticity of travel documents;
- The administration of justice.

As we can see from the above list, **CounteR will likely be integrated into the category of AI high-risk systems once the draft regulation is passed**. Therefore, according to the regulation, LEAs or other organizations in charge of the system will be required to meet a set of technical and regulatory requirements **before the system can be implemented**. There are three main aspects to be considered:

- Mechanisms such as **algorithmic impact assessments** will have to be implemented to ensure an unbiased system;
- This kind of solution needs to set a **governance mechanism and operational protocols** to ensure that the entire system's data life cycle and outcomes can be verified and traced back;
- Acceptable levels of **transparency and understandability** for those subjects affected by the systems and appropriate human oversight over the system generally will have to be ensured, in line with the GDPR provisions.

Furthermore, it should be noted that all **conformity assessments** for high-risk AI applications must be **obtained ex-ante**. These responsibilities are distributed and targeted to providers, importers, distributors and implementers. According to this, in CounteR, these assessments will have to be conducted by partners within the project as part of technical validation and demonstrations and also by local law enforcement authorities before implementation. Along these lines, the EC proposal indicates that **technical and auditing requirements for High-Risk AI** include:

- Testing the system to detect any hazards and devise suitable mitigation measures;
- The capacity of the system to verify that the system runs consistently for the designated end (i.e., tests made against prior metrics);
- Building and sustaining a risk management system for the whole system lifecycle;

- Setting proper data governance controls so all training and validation processes are error-free and representative;
- Full technical documentation, including around AI model, system architecture and data life cycle;
- Logging while the system is running should be automated and as complete as possible;
- Transparency concerning the system goals and outcomes should be translated into communication that users can easily interpret;
- Regular human oversight is required to prevent or minimize risks to safety or fundamental rights.

Lastly, another important point is reflected in section 3.5 of the draft Regulation on Fundamental rights, which states:

> *"The **obligations for ex ante testing, risk management and human oversight** will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls."*

In this regard, following the High-level expert group on artificial intelligence set up by the European Commission (2019), AI systems should comply with four principles: **Respect for human autonomy, Prevention of harm, Fairness and Explicability**. As we have seen above, even though many of these principles are requirements enforceable by law, properly adhering to them requires going beyond compliance from a proactive and preventative approach (Floridi, 2018).

3 CounteR Ethical Framework

This section reflects both relevant **ethical principles and values** to be considered in the design and deployment of the CounteR system. Moreover, it provides an analysis of tensions between these values and others concerning the System development, such as public security or mutual care.

3.1 Ethical principles guiding the solution

Several **technologies are currently being used in police investigation activities**, ranging from biometrics, data management software, data mining, algorithmic systems, and other tools, including robotics. Purposes behind these systems' data management include surveillance of people and places, imaging, communication to support decision-making, and database systems registering criminal activity (Requena, 2004; Custers and Bas Vergouw, 2015). In many cases, these technologies have been shown to enhance policing and online investigation by competent authorities (Roman et al., 2008; Danziger and Kraemer, 1985; Ioimo and Aronson, 2003). Given their relevance for current policing action, intelligence methods and technologies have actually modified the overall policing approach in some countries (Guidette & Martinelli, 2009; Ratcliffe, 2008, 2016).

However, in this scenario, intelligence-led policing seeking to foster a more “proactive” style of crime prevention has brought new societal challenges (Innes, Fielding, & Cope, 2005; Innes & Sheptycki, 2004; Fyfe et al. 2017). For Requena (2004), the new technological scenario can lead to several **issues or unwanted effects in the policing domain**, such as confusion between public and private spaces, contested monopoly of surveillance attributions from the State or internal resistances and tensions in police organizations in implementing technological tools. Related issues revealed by the literature include the lack of preparation and efficient adoption of police technologies, which has had different negative social externalities for citizens' privacy, liberty or integrity (Koper et al., 2015, Manning, 1992; Chan, 2001; Harris, 2007; Garicano and Heaton, 2010; Byrne and Marx, 2011). In order to anticipate these problems, technological developments in policing should not only align with legal requirements but also consider the **ethical connotations** related to these forms of social impact.

Framing CounteR from the ethics perspective will allow us to go beyond legal compliance when understanding what the system is permitted to do. **Ethics** have often been defined as **moral standards** guiding individuals’ behaviour, actions, and choices (Poonia et al., 2009). Therefore, we will consider what the CounteR system is prompted and required to do in moral terms from this perspective. These standards intervene and adopt different forms in citizens' behaviours, perceptions and social habits and norms. From a broad societal perspective and understanding ethics as value-driven, the following values must guide CounteR development:

- **Liberty**: as stated above, data-intensive technologies can potentially infringe upon different types of freedoms by spreading various personal identifiers. Moreover, data mining systems can turn into instruments to support surveillance, creating "soft checkpoints'' away from criminal events and sites (Razac, 2009). In this context, legally conceived as the right to be free, in CounteR, liberty should be translated into mechanisms, tools and features ensuring freedom of speech, assembly and association and expression. The system should also

guarantee personal property and other externalities such as arbitrary arrest due to false positives.

- **Autonomy**: this ethics' value concerns the relative capacity to make informed decisions without external physical or unfair symbolic coercion. In the socio-technical domain, self-govern action requires assessing the level of control held by users, who should be able to understand and anticipate relevant technological decisions (Brey, 2005). In CounteR, this requires ensuring that both end-users and citizens are able to be aware of data processing concerning their licit activities online and proportionally react to system actions.
- **Integrity and privacy**: Intrusion on individuals' autonomy, privacy and liberty can affect their self-worth and dignity (Dillon, 1995). One critical dimension of CounteR in this regard is its capacity to use sensitive data from sources such as social networks, which can expose people's identities and sensitive data. In a broad understanding of the privacy concept, this form of exposure can lead to all sorts of consequences, ranging from stigmatization to other events, even threatening persons' lives (González Fuster and Kloza, 2016).
- **Equality and justice**: according to this value, technology developments should treat users and citizens fairly to avoid worsening existing inequalities. Issues in this regard range from the digital divide to the discriminatory distribution of benefits and risks in algorithmic treatment. In CounteR, this means that the systems should not systematically disadvantage protected groups such as minors or ethnic minorities (Monahan, 2002; Woolgar, 2002).
- **Democracy and misuse**: Another critical value in the relation between science, technology and society is democracy. Democracy concerns collective decision-making and control over technology. In this regard, any technological innovation with public implications should be designed considering social acceptability, power relations and needs. In CounteR, it is also important to consider mechanisms so any misuse attempting against democracy can be avoided.

To the extent possible, depending on its goals and means, a technological solution should ensure mechanisms to avoid issues affecting the above ethical value principles. In this regard, a **precautionary principle,** which provides a framework for decisions under uncertainty, should be taken. This means considering strategies to anticipate and minimize potentially severe or irreversible risks. Therefore, the desirability of CounteR must be weighted considering complete scientific certainty or consensus over its potential beneficial or harmful effects on individuals.

3.2 Ethical dilemmas to be considered in CounteR

This section will introduce issues to be considered in CounteR's design in relation to potential **ethical issues or dilemmas**. This exercise aims to operationalise the above principles into specific issues where decision-making problems between two possible ethical-moral imperatives, neither of which is unequivocally acceptable nor preferable, will need to be conducted. While situational conflict will cover multiple casuistries in the actual implementation of CounteR, issues presented below show how acting according to one imperative could result in transgressing the other.

- **Balance between public safety and privacy**

As we have seen above, data management within online intelligence is conducted under public interest claims and legal basis. The benefits of big data analysis, ranging from disease control to the development of "smart grids", have been underlined (Omer and Polonetsky, 2012). However, it has been mentioned that ensuring the population's safety against unforeseen threats such as terrorism often boosts tensions with other ethical principles such as privacy. This balance assessment can be accessed from different ethics approaches, envisioning equal treatment (utilitarian approach), overall impact and capacity to serve the community (common good approach) or development of new civic and moral habits (virtue approach). From all these philosophical perspectives, proportionality analysis will focus on different actors and outcomes but having above moral values as general guidelines. This dilemma is fundamental for CounteR development, and it will be addressed by mitigating risks on individuals by design through the community hubs approach based on data pseudonymization.

- **Balance between the inclusion of new data analysis techniques and harm on individuals**

The processing of big data and the searching of threats online (particularly within the Dark Web) can prompt unexpected outcomes such as unwilling spreading misinformation or the unwanted revelation of data subjects' identity (including his/her privacy, autonomy and integrity). This issue should be tackled by introducing security techniques and methods ensuring safe intervention and protection of third parties. CounteR concept seeks to reach this equilibrium by automatically hiding personal information.

- **Balance between unorthodox investigation method (i.e., revictimization of vulnerable people) and achievement of policing goal**

In some cases, operations in the Dark Web require the intervention of victims in order to ensure proper detection of criminals or the sharing of victims' sensitive data with similar purposes. The revelation of these victims' identities or information concerning related individuals can involve infringing fundamental rights and put their integrity in danger. Other methods involve entrapment, which can be used as part of online police operations to provide individuals specific opportunities to commit a crime. Thereby, LEAs can use different baits to have a vital role in turning users into criminals. Some authorities have framed this method as acceptable if there is evidence of previous criminal intent (Vitkauskas & Dikov, 2012: 59). These issues are not expected to be operationalized through the CounteR system since, although based on LEA's task definition, search and detection will not be conducted using these methods.

- **Balance between online intelligence and allowing harm**

As Hadjimatheou (2017) pointed out, there are some scenarios where LEAs can facilitate crime, such as developing sites or online tools to share illicit goods. In consequence, some criminal activities can happen under LEA's watch in the context of more ambitious operations. Our dilemma relates to how LEAs should act in both facilitation and detection processes in these cases. Something similar happens when officers who witness severe crimes on the Dark Web have to pass them in the context of more strategic goals. In CounteR, this process may relate to the operations based on data collected by the system. However, it does not concern its overall concept and goals.

As we can see from the above analysis, CounteR ethics dilemmas primarily concern how the system will **set proportionality between its surveillance capabilities to strengthen public safety and the values of individuals' privacy, integrity, and autonomy**. Addressing these values allows us to visualize how CounteR should go beyond legal compliance when projecting its design and implementation. Furthermore, this approach provides LEAs, ISPs and other authorities in charge with instruments to understand the ethical implications of its use.

4 National case study: Spain

In this section, we will describe the **Spanish case study** in order to gain a more specific and operational understanding of legal requirements for CounteR implementation. The case study aims to provide an example helping to illustrate and extend the legal analysis based on a specific national EU scenario. While no comparative or operational perspective is introduced or sought to be achieved, this analysis is oriented towards providing project partners with pertinent information and examples concerning national fitness and constraints in the system's design.

4.1 The data protection and criminal legal framework at the national level: The Spanish case

Following the rationale established in section 2, the examination of relevant legal texts in Spain is divided into two blocs, those provisions regulating data protection and those concerning policing online. We mainly refer to the national transposition and interpretation of EU level provisions examined above in both cases.

4.1.1 Data protection framework in Spain

The **LOPDGDD (Organic Law on Data Protection and Guarantee of Digital Rights)** adapts the EU GDPR to the Spanish framework. While the LOPDGDD only applies in Spain, the GDPR applies worldwide as long as the protected data belongs to the European Union's residents.

There are other significant differences between the GDPR and the LOPDGDD. The Spanish law is more **exhaustive and includes additional rights**, both personal and in the workplace. In addition, new obligations are included regarding the processing of personal data in cross-border procedures, and it establishes guarantees for biomedical research beyond personal protection. In this way, the LOPDGDD brings new features that are relevant from the CounteR perspective, among which are the following:

- ***Minimum age***

The minimum age from which consent can be given is **set at 14 years** (Art. 7). Therefore, it is a possibility, not an obligation, that individuals from 14 years of age and older consent. In the case of minors under 14 years of age, their parents or legal guardians must give this consent and be able to withdraw data of children within the minority of age.

- ***Processing of deceased person data***

Article 27 of the LOPDGDD regulates the **right to access, rectify, or delete a deceased person's data** (Art. 27). Some individuals and organizations may contact the person in charge of data treatment in order to request access to the personal data of deceased persons and, where appropriate, their rectification or deletion. This right can be exercised by people linked for family or de facto reasons. This can also be done by institutions or persons that the deceased had expressly designated for this. Moreover, legal representatives of minors and the Public Prosecutor's Office, legal representatives of people with disabilities, and the Public Prosecutor's Office can also request this access under

certain conditions. Therefore, this provision expands the groups of people who can access that data compared to the GDPR.

- ***Special categories of data***

The **conditions under which special categories of personal data** can be processed are established in Articles 9 and 28.2(c) of the LOPDGDD, which are stricter than those established by the GDPR. Categories of data particularly protected by the LOPDGDD are ideology, religion, beliefs, racial or ethnic origin, health, and sex life or orientation. Moreover, genetic and biometric data are specially protected.

The LOPDGDD indicates that exemptions for the prohibition of this data processing include the ones defined by the GDPR, such as the necessity to fulfil obligations and exercise specific rights of the person responsible for the treatment. Moreover, it includes fundamental public interest reasons. In this regard, in CounteR, special categories of personal data may be **processed by LEAs or other public authorities under public interest**.

However, as mandated in Article 89.1 GDPR, under the LOPDGDD (Art. 26), treatment of sensitive data under public interest must be subject to the **appropriate rules and safeguard the rights and freedoms of the interested parties**. These will make available technical and organizational measures to guarantee respect for the principle of minimizing personal data. Such measures may include pseudonymisation, provided that such purposes can be achieved in this way.

Article 9 of the LOPDGDD indicates in this regard:

> *"The data processing referred to in letters g), h) and i) of article 9.2 of the Regulation (EU) 2016/679 based on Spanish law must be covered by a rule with the force of law, which may establish **additional requirements related to its security and confidentiality**.*
> *In particular, said rule may protect the processing of data in the field of health when required by the management of health care systems and services and social, public and private, or the execution of an insurance contract of which the affected party is part."*

- ***Exemptions in the LOPDGDD***

The LOPDGDD has been modified by the publication of the Organic Law on the protection of personal data processed in cases of criminal offenses and penalties (LO 7/2020, of May 26), which entered into force on June 16, 2021. Specifically, modifications were made to Articles 2, 44 and additional provision 15 of the LOPDGG. On this basis, Article 2,2, LOPDGDD will not apply to the following matters:

> *"2. This Regulation does not apply to the processing of personal data:*
> *a) in the exercise of an activity that does not fall within the scope of Union law;*
> *b) by the Member States when they carry out activities falling within the scope of Chapter 2 of Title V of the TEU;*
> *c) carried out by a natural person in the exercise of exclusively personal or domestic activities;*

d) by the competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offenses, or the execution of criminal sanctions, including protection against threats to public safety and their prevention. "

All this, without prejudice to the provisions of sections 3 to 5 of Article 2 GDPR, so that:

"3. Regulation (EC) No. 45/2001 is applicable to the processing of personal data by the institutions, bodies and agencies of the Union. Regulation (EC) No. 45/2001 and others Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with its article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31 / EC, in particular its rules relating to the liability of intermediary service providers established in its articles 12 to 15.
5. The processing of data carried out on the occasion of the processing by the Public Prosecutor's Office of the processes of which it is competent, as well as that carried out for those purposes within the management of the Fiscal Office, will be governed by the provisions of the Regulation (EU) 2016/679 and this Organic Law, without prejudice to the provisions of Law 50/1981, of December 30, regulating the Organic Statute of the Public Prosecutor's Office, Organic Law 6/1985, of July 1, of the Judicial Power and of the procedural norms that are applicable to it ".

- ***Authorizations/notifications required for international transference of personal data***

The persons responsible and in charge of the treatment may carry out international data transfers **without the need for an authorization from the Spanish Data Protection Agency, provided that** the data processing complies with the provisions of the GDPR, and the following cases are met a) Recipient declared of adequate level by the European Commission; b) In the absence of an appropriate decision, and with the following guarantees:

"A legally binding and enforceable instrument between the authorities or public bodies, b) Binding corporate rules and c) Standard data protection clauses adopted by the Commission; d) Standard data protection clauses adopted by a control authority and approved by the Commission; e) Codes of conduct, together with binding and enforceable commitments of the person in charge or the person ***in charge of the treatment in the third country*** *to apply adequate guarantees, including those related to the rights of the interested persons, f) Certification mechanisms, together with binding commitments and of the controller or the person in charge of the treatment in the third country to apply adequate guarantees, including those related to the rights of the interested persons."*

In the **absence of a decision of adequacy and adequate guarantees**, international transfers are allowed if any of the following conditions are fulfilled:

- The interested person has explicitly given their consent;
- The transfer is necessary for the execution of a contract between the interested person and the person responsible for the treatment or for the execution of pre-contractual measures adopted at the request of the interested person;

- The transfer is necessary for the conclusion or execution of a contract, in the interest of the interested person, between the person responsible for the treatment and another natural or legal person;
- **The transfer is necessary for important reasons of public interest;**
- The transfer is necessary for the formulation, exercise or defence of claims;
- The transfer is necessary to protect the vital interests of the person concerned or other persons, when the person concerned is physically or legally incapable of giving their consent;
- The transfer is made from a public registry that, in accordance with Union or Member State law, is intended to provide information to the public and is open to consultation with the general public or any person who can certify a legitimate interest, but only to the extent that, in each particular case, the conditions established by the law of the Union or of the Member States for the consultation are met.

When neither of these exceptions is applicable, a transfer can only be carried out if it is not repetitive, affects only a limited number of interested persons, and is necessary for the purposes of **compelling legitimate interests** pursued by the controller. Moreover, the interests or rights and freedoms of the person concerned should not prevail, and the controller evaluates all the concurrent circumstances in the data transfer and based on this evaluation, offers appropriate guarantees regarding the protection of personal data. In this case, the data controller will inform the transfer control authority. In addition to the information referred to in Articles 13 and 14 of the GDPR, the data controller will inform the interested person of the transfer and of the compelling legitimate interests pursued.

Even though the above authorization framework is flexible, it should be noted that supplementary measures have been adopted by the European Data Protection Board (EDPB). Measures were adopted after the recent judgment C-311/18 (Schrems II) of the Court of Justice of the European Union (CJEU) and they apply to all Member States. These are reflected in the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"[6]. Main modifications include **emphasizing the importance of monitoring the policies and protocols of third-country public authorities** in the exporters' legal assessment to determine whether the third country's legislation and/or practices impinge - in practice - on the effectiveness of the Art. 46 GDPR transfer tool. It also suggests the possibility that the exporter considers in its assessment the practical experience of the importer, among other elements and with certain caveats. Lastly, it clarifies that the legislation of the third country of destination enabling its authorities to access the data shared, even without the importer's intervention, may also intrude on the effectiveness of the transfer tool.

[6] *See: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf*

4.1.2 Criminal law in Spain

In Spain, the "Organic Law 7/2021, of 26 May, on the Protection of Personal Data to prevention, detection, investigation and prosecution purposes of criminal offences and execution of criminal sanctions" is an **almost literal transposition** of the EU LED. Moreover, in Chapter II, the Law provides **identical principles recognized by the GDPR** on the rights of natural persons who are parties to criminal proceedings, such as victims, convicted persons, witnesses and other persons who have some type of participation or presence in them.

In its Preamble, it indicates that **competent authorities** in charge of its implementation in the country are the Security Forces and Bodies; the Penitentiary Administrations, the Deputy Directorate of Customs Surveillance of the State Tax Administration Agency; the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses; and the Commission for the Surveillance of Terrorism Financing Activities. The judicial authorities of the criminal jurisdiction and the Public Prosecutor will also be considered competent.

Also, in line with the GDPR, the text delimits **controllers and processors responsibilities**. Processors and organizations in charge of the treatment will carry out their functions on behalf of controllers, offering guarantees to apply appropriate technical and organizational measures. All of them are obliged to cooperate with the data protection authority within the framework of current legislation.

Moreover, Organic Law 7/2021 (Article 33) obliges those responsible and those in charge of the treatment to keep a **record of treatment activities** with identifying data. These data include the contact details of the person in charge, the purposes or the categories of interested parties, and a record of operations, which will include the collection, the alteration, inquiries and transfers of personal data, among other operations.

As the LED, the Organic Law includes a series of guarantees aimed at protecting the rights and freedoms of those affected in contexts where the authorities process their data for purposes of prevention, investigation, detection or prosecution of criminal offences - especially, linked to the fight against terrorism. Among these guarantees is the **prohibition of treating special categories of personal data. Article 13 mandates that this processing is only allowed if** strictly necessary and the following conditions are met:

a) It has been provided for by a regulation with the force of law or by European Union Law.
*b) It is necessary to protect the **vital interests,** as well as the fundamental rights and freedoms of the interested party or of another natural person.*
*c) Said treatment refers to **data that the interested party has made manifestly public***

Moreover, the Organic Law advocates the prohibition of taking automated individual decisions, including profiling, in line with the recommendations of the European Data Protection Supervisor. Along these lines, **decisions based solely on automated processing** that produce adverse legal effects for the interested party or that significantly affect him or her are prohibited (Article 14). This unless expressly authorized by national or European law. In this case, corresponding appropriate safeguards for the rights and freedoms and the legitimate interests of the interested party must still be in place.

The *Ley Orgánica* also establishes the rights of **access, rectification, deletion and limitation** of treatment for those affected (Art. 23), provided that their exercise does not **hinder an investigation or national security**. Likewise, a series of data retention periods and review periods are foreseen for the processed data. Article 6.2 indicates that personal data must be: "*Kept in a way that allows the interested party to be identified for a period not higher than necessary for the purposes for which they are processed*." Furthermore, it should be noted that the Law goes beyond what is established in the LOPDGDD and the GDPR by establishing a **maximum period of conservation (20 years) and periodic reviews** of the need to preserve the data (at most every 3 years) (Art. 8).

Lastly, the Organic Law attempts to guarantee that the **movement of data can be carried out without restrictions derived from the protection of personal data**. Chapter V is entirely devoted to regulating international data transfers to a third country or international organization, including requirements such as that the transfer is necessary for the purpose of prevention, detection, investigation and prosecution of criminal offences or enforcement of criminal sanctions, including protection and prevention against threats to public safety, and that the personal data be transferred to a competent data controller for these purposes.

4.1.3 The case of the program to detect and prevent the processes of recruitment and radicalisation of inmates (Service Order 3/2018)

As has been pointed out by Espín López (2021: 1), even though all kinds of policing and data management procedures **must follow fundamental rights** recognized in the Spanish Constitution - in particular, "rights to private life" regulated in Art 18-, to comply with Article 299 of the Criminal Procedure Law "*is necessary use means of investigation that are unfailingly restrictive of certain rights fundamental, since **their protection may be exempted from the public interest in the prosecution of crime***"[7]. The Service Order 3/2018 is a good example of this sort of rights restriction falling within the scope of Organic Law 7/2021 and the Criminal Procedure Law.

In the last years, the General Secretariat of Penitentiary Institutions developed different initiatives to detect and prevent the processes of recruitment and radicalisation of inmates, mainly from Muslim communities, in the Centers Penitentiaries. The **Service Order 3/2018[8] led to creating an evaluation methodology and informatic system for measuring the risk of violent radicalism.** This instrument is inspired by international models and experiences such as Vera-2r[9] (Fernández, 2019; González-Álvarez, 2020) and supports decision-making regarding inmates' **treatment, redirecting detection, monitoring, and intervention**. Moreover, it enables further coordination between the different departments of prisons, in particular the areas of security and treatment. Lastly, the instrument seeks to systematize the treatment of violent radicalism within various penitentiary centres. Under these coordinates, in line with CounteR, this system identifies and evaluates three different profiles. On the one hand, it detects the risk of recidivism of those **inmates who have committed crimes of jihadist terrorism**. On the other hand, it detects inmates who are in the process of radicalisation or who are **vulnerable to being caught**.

---

[7] *As also stressed by Moreno Catena, V., Cortés Domínguez, V., Derecho Procesal Penal, Valencia, Tirant lo Blanch, 2019, p. 265.*

[8] *Text https://www.senado.es/web/expedientappendixblobservlet?legis=12&id1=119003&id2=1*

[9] *https://www.vera-2r.nl/*

The system works by processing different inmates' datasets, including information provided by prison staff through **direct observation,** such as their behaviour and participation in various prison programs. This information is charged by the prison Technical Team into the system. Based on extended ground criteria, inmates are classified into **three risk levels (A, B and C),** and this evaluation is **repeated every six months**. Further inmates may be entered into the risk classification process.

The Service Order 3/2018 calls for the entire prison staff to become an "active agent" for the instrument implementation. It should be noted that, as underlined by Aguerri and Fernández (2021), Order 3/2018 indicates that this instrument "**in any case can be considered a static predictor of future behavior**". However, in a certain contradiction with this principle, the document frames its purpose as "the detection and assessment of **variables that may indicate a real risk of commission of acts related to violent radicalism**".

As we can see, the tool developed within the Service Order 3/2018 manages (sensitive) data of suspects and inmates to classify them and assess their evolution according to certain values that will work as parameters selected as Tasks within CounteR. This proactive model, based on questionnaires, allows us to illustrate how data from these individuals is accessed, stored, shared and used to construct profiles within the current legal framework in Spain.

Asserting this policy, aligned with CounteR aims and methods, requires considering its relative alignment with the **principle of proportionality** as integrated into the above regulatory framework (including the Organic Law 13/2015). Along these lines, its implementation involves the need of avoiding "*the arbitrariness of public powers*" as stated in the Spanish Constitution (Art 9.3). According to Espín López (2021: 12), the Spanish jurisprudence offers grounds for this principle. The Spanish Supreme Court indicated in a resolution (*ATS de 18 de junio de 1992, ROJ: ATS 3773/1992, FJ 1*) on interference in the rights fundamental as a consequence of the investigation of the crime that this foundation was the **respect for human dignity**. The proportionality principle is also integrated within several national and international regulations, including the Charter of Fundamental Rights of the European Union (Arts 8, 9, 10 and 11).

Under these coordinates, measures integrated into the Service Order 3/2018 should consider two **main dimensions of proportionality** (Espín López, 2021: 17). Firstly, the **"judgment of suitability"**. This means that judicial powers should determine whether the object of the investigative measure **is appropriate to obtaining evidence** that serves to ascertain a fact apparently criminal (Perelló Domenech, 1997). In this respect, in principle, policies within the Order seem to fulfil this requirement since finding relevant information on violent radicalism within specific target groups should allow properly tackling threatening events. These kinds of proportionality assessments have been examined for Dark Web operations in Europe and worldwide, which require access to several personal data in order to tackle specific crimes (Hadjimatheou, 2017). Secondly, the **requirement of necessity**. It indicates that the measure must be **essential to achieve the objective proposed**. This will occur when there is no other less burdensome measure and the least restrictive of the fundamental right in question is sufficient to achieve the pursued end (Espín López, 2021: 18). Assessing the Order under this prism requires a technical and overarching analysis of available security policies able to address the issue at hand. This indicates that the same sort of exercise should be followed by CounteR development and implementation.

5 Summary analysis

This section translates the above requirements and principles into a **specific roadmap for CounteR technical development and operational deployment**. Legal and ethical issues are firstly considered from their overall interrelations and forms of convergence into a general approach and then discussed under the light of their overarching tensions and ways to approach them.

5.1 CounteR legal and ethical approach

A legal and ethical approach to CounteR development and implementation means a set of **organized requirements and principles to ensure both legal compliance and mitigate risks for adverse social impact**. As we discussed in previous sections, such an approach can be established at two levels. Firstly, the standard and EU legal normative framework that is defined by applicable laws and standards within this jurisdiction. In this regard, most ethics values described in Section 3 are embedded into studied regulations in the form of specific rights. This includes the right to privacy, consent and equal treatment. Secondly, we have a more specific and operational approach focusing on general implications of the national jurisdiction and problematized under the light of contextual issues to be considered by design.

From a general standpoint, **rights set out in the EU Charter of Fundamental Rights** must be recognized as a framework for CounteR development. These rights are bestowed on individuals and groups by their moral situation as human beings. However, given the above-explained exemption framework leading to the relative "suspension" of certain rights during the implementation of CounteR on the basis of public interest, the main focus of our legal framework is integrated by **data protection and policing provisions**.

Pillars of our legal approach are GDPR, the policing Directive, identified ethical principles and specific proportionality assessments conducted by each national actor as summarized in the image below.

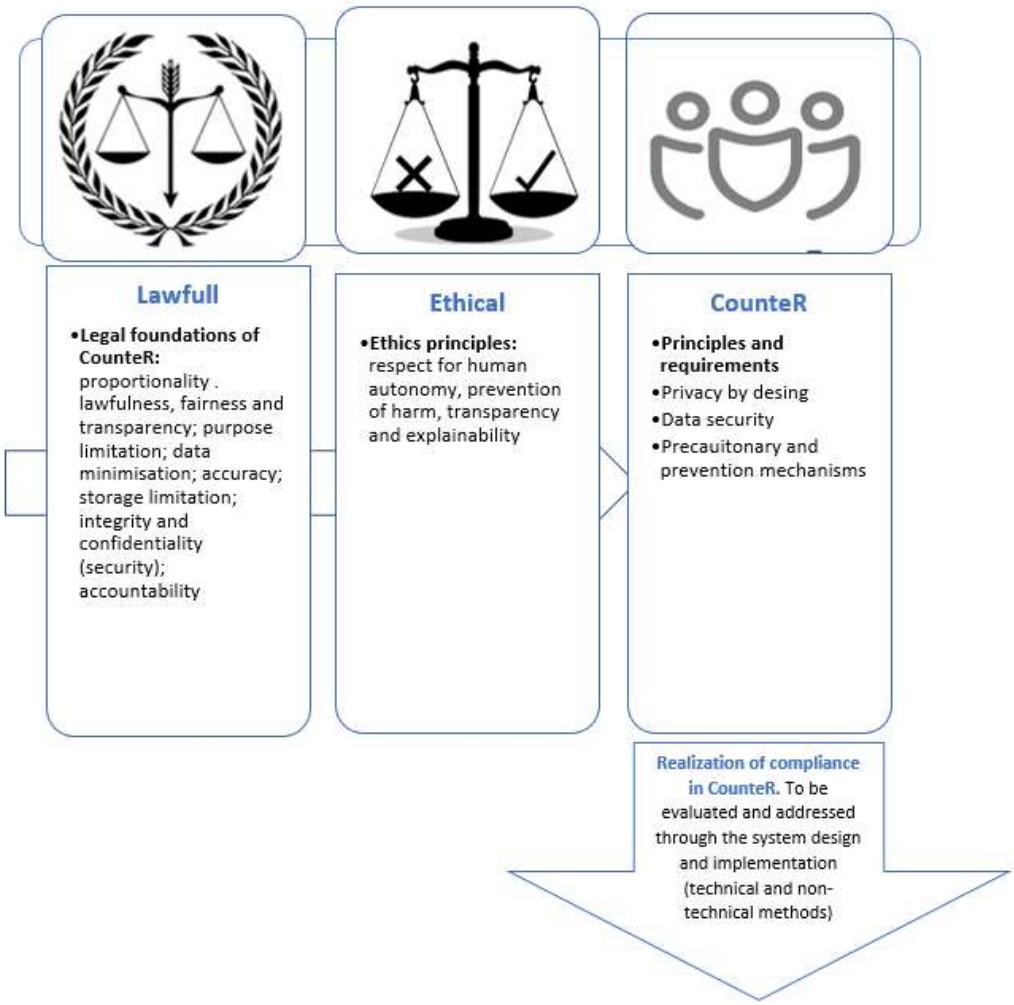

Figure 2 - Counter legal and ethics framework

Source: own elaboration.

CounteR System will collect large amounts of data online from social media and Surface/Deep/Dark Web for law enforcement and ISP purposes. Therefore, within the above general framework and in order to ensure the realization of compliance with identified requirements and principles, there are **essential aspects to be considered by design and default** as well as concerning its operational aspects. Recommendations aligned with these issues are summarized below:

A. Data protection requirements:

- **A.1** Secure and transparent data governance must be established following Art 5.1.;
- **A.2** A basis for processing established in Article 6.1 of the GDPR must be followed;
- **A.3** CounteR must collect personal data in order to fulfil certain and specific goals (I.e., detecting radicalisation online) to ensure purpose limitation (Art 5.1);
- **A.4** CounteR must avoid collecting more data than those which are specifically needed for the system purposes, and particularly, biometrics data, to enable data minimization (Art. 5.1, c) and protect the privacy of individuals;

- **A.5** CounteR must integrate tools and establish protocols to ensure that processed personal data is accurate and reflects reality (Art. 5.1, d);
- **A.6** CounteR must not keep personal data for any longer than is reasonable for achieving the purposes for which they were initially collected in the first place. The storage period must be reasonable in relation to the purposes of the processing. CounteR should develop matching systems allowing removal of personal data from databases as soon as possible to guarantee storage limitation (Art. 5.1, e);
- **A.7** Data security, integrity and confidentiality (Art 5.1, f) must be ensured, and data subjects rights must be secured by CounteR through anonymization, pseudonymization and encryption whenever possible;
- **A.8** CounteR must integrate special technical and organizational measures to protect special categories of data and establish safeguards directed at protecting the rights and freedoms of those employees who will undergo biometric matching;
- **A.9** CounteR must follow the principle of accountability in the GDPR (Arts. 83 and 84) by keeping anonymized records of data processing activities.

B. Criminal law exemptions and requirements

- **B.1** CounteR must be conceived as a tool in governmental power in constitutional democracies so legally authorized and limited by applicable law;
- **B.2** CounteR managers processing criminal offence data will need both a lawful basis, and either “official authority” or a separate condition for processing under Article 10 GDPR;
- **B.3** When CounteR is implemented by “official authorities” purposes of the processing must be the prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties (LED Articles 2(1) and 1(1);
- **B.4** As stated in the LED, all 7 Principles embedded in the GDPR should be taken as a reference for the processing of personal data;
- **B.5** Counter collection of personal data for law enforcement purposes should be limited to what is necessary and proportionate for the prevention of actual danger or the prevention, investigation and prosecution of a specific criminal offence;
- **B.6** Data subjects whose data is processed by CounteR must have the right not to be subject to a decision evaluating personal aspects based solely on automated processing and which produces adverse legal effects concerning or significantly affecting them (Article 38);
- **B.7** CounteR data controllers must actively avoid discrimination and unfair profiling (Art. 11 LED).

C. AI requirements

- **C.1** CounteR AI systems must be human-centric and aimed at the common good, with the goal of improving human welfare and freedom;
- **C.2** CounteR algorithmic model must anticipate risks appropriately and proportionately;
- **C.3** CounteR algorithms must be explainable by offering tools (I.e., automated processing tracking) to ensure the results of the system can be understood by humans;
- **C.4** CounteR AI must ensure equal respect for all users' moral worth and dignity, mainly providing preventative and monitoring techniques and tools aimed at avoiding unfairly biased outputs. Disadvantage treatment of disadvantaged groups, such as people with disabilities or immigrants, must be monitored and actively avoided.

D. Cybersecurity requirements

- **D.1** CounteR must integrate proper and effective cybersecurity tools and organizational concepts to ensure the protection of the system against cyberattacks;
- **D.2** CounteR implementers must conduct system security assessment before deployment;
- **D.3** CounteR must track the security status of the system to inform end users and other authorities properly and in a timely manner;
- **D.4** CounteR interoperability mechanism and overall concept must allow cooperation with other LEAs without exposing sensitive data or affecting privacy rights.

E. Ethics principles and requirements

- **E.1** CounteR must ensure that liberty, autonomy and integrity of data subjects online are respected;
- **E.2** CounteR must take an ethical approach to AI, so it does not represent a risk for democratic processes, values plurality and right to decide of individuals.

F. Lessons learned from the Spanish case study

- **F.1** CounteR must be adaptable to further requirements concerning confidentiality when processing special categories of personal data;
- **F.2** CounteR must ensure special safeguards in the management of children's data according to Members States provisions;
- **F.3** CounteR must allow the removal and rectification of personal data, for instance regarding data of deceased individuals.

5.2 CounteR tensions and alignment with the legal and ethical implementation framework

As addressed above, many considerations need to be taken in CounteR when establishing mechanisms for **processing personal online data with police investigation processes**. Firstly, it should be noted that any processing performed by a competent authority that is not for law enforcement's primary objective will be covered by the general processing regime under the GDPR.

As a general consideration, the system must allow data security and control in order to **ensure data privacy** while providing enough information to **track detected threats** and translate them into identifiable communities and individuals. Moreover, the system should be able to keep secrecy in a criminal investigation while ensuring traceability of data treatment by authorities so they can be held accountable and conduct monitoring of systems. Exposing this data can represent an illegal infringement of privacy rights by putting victims or law enforcement authorities at risk.

In this scenario, CounteR's most challenging elements concerning the above-studied requirements are the **automated processing of enormous amounts of (special categories of) personal data**. While this may be justified in terms of the system functionalities, mechanisms for limiting the scope of such processing must be available. The system should provide quick analysis of big data, which will be achieved through AI systems while ensuring human intervention in decision making involving personal data.

Processing special categories of personal data by competent authorities and with law enforcement purposes is allowed but for reasons of **substantial public interest, among other bases**. Therefore, LEAs are requested to demonstrate that the processing is strictly necessary, satisfies one of the LED or Member States regulations conditions, or is based on consent. Within the framework of CounteR policies, strictly necessary means that the processing has to relate to an **urgent social need**, and the organization using the system cannot reasonably achieve it through less interfering means.

Furthermore, as we examined in the analysis of the EC proposal for an AI regulation, LEAs will need to ensure several **ex-ante validations and protocols** in order to conduct this type of processing, including algorithmic impact assessments confirming AI fairness. In all cases, as stated above, these examinations need to be combined with robust protection of personal identifiers and regular monitoring of AI fairness, for instance, concerning the distribution of false positives.

Within this challenging scenario, certain limitations in the **reuse of personal data** collected with different purposes by other organizations such as social media must be considered. Even if the LED and its transpositions generally cover this sort of reprocessing, a proportionality analysis will need to be conducted to ensure legal compliance. This includes assessing mechanisms to ensure the **anonymity of individuals until there is clear evidence of criminal activity** that can conduct reidentification.

Along these lines, the categorization of individuals by CounteR must be able to follow the LED framework **establishing a clear distinction between personal data of suspects,** persons convicted of a criminal offence, victims or witnesses. Such requirement (Art 6, LED) supports the implementation of the right of presumption of innocence as guaranteed by the Charter and the ECHR, as interpreted in the case-law of the Court of Justice and the European Court of Human Rights, respectively. Accordingly, CounteR forms of classification (see section 1) must be structured in the light of this concept.

Moreover, as we illustrated with the Spanish jurisprudence, this analysis must have the human right to physical and mental integrity as a critical coordinate. As we saw in our review, **ethical values of liberty, autonomy and dignity** are embedded in all regulatory frameworks affecting CounteR deployment in the form of specific citizens' rights and law enforcement responsibilities. Such a normative basis should frame the scope of surveillance processes and the need for data security measures to enable confidentiality, purpose limitation, and reduce the risk of data breaches at minimum.

Furthermore, other elements must be considered when processing sensitive data - or as we saw in the Spanish case, data made "manifestly public" by individuals- under public interest. As part of this proportionality assessment, it should be considered that **evident and direct correlation** should exist between the data processing carried out by the LEA and circumstances where individuals have already perpetrated or are expected to commit a crime (Council of Europe, 2018: 3). This concerns tools and protocols to ensure **robust data pseudonymization** and control over deanonymization keys. Such keys should only be required to conduct identification once a threat or risk of criminal office has been properly verified.

Besides implementing the risk approach characterizing studied provisions, some legal and ethical requirements involve specific references **guiding the system implementation**:

a) One essential aspect in this regard is the need of **ensuring human intervention in algorithmic decision making**.

b) The system must be able to **track and collect relevant data to explain and justify its performance** and ensure its security, such as access logs. LEAs and other organizations managing CounteR are expected to keep logs for at least collection, alteration, consultation, disclosure (including transfers), combination and erasure of personal data. This is key for ensuring both end-users and citizens' rights, supporting lawfulness of processing, self-monitoring by the controller or the processor, internal disciplinary proceedings or other criminal proceedings.

c) Information should be organized to ensure rights to **explainable AI and data subjects' rights** to access or rectification of personal data.

Lastly, data security and privacy by design should also consider cases, such as Spain, where restrictions to the international transfer of personal data under national criminal law can represent more risks in terms of data breaches and function creep.

6 Conclusions and recommendations

This Deliverable identifies and analysis two legal frameworks that must guide CounteR technological development, including **data protection and criminal law**. Moreover, the document provides elements to establish **AI and cybersecurity standards** applicable to the System. Lastly, the analysis of these requirements is also contrasted by analysing **ethical principles** that should frame its design and implementation. The review of these requirements, standards and principles at the EU legal is done through literature and legal review, the discussion of ethics relevant dilemmas and the building and an examination of the Spanish case study to further understand the concrete implications of CounteR implementation at the national level.

While CounteR may fit current legal requirements for the processing of social media and surface/deep/dark web data for law enforcement purposes under certain conditions, it presents many challenges related to its development as a system **ensuring purpose limitation** concerning law enforcement scope action and legal authority. Moreover, increasing **AI requirements and challenges** must be considered by design, such as the need of tracking and properly tackle any disparate impact or treatment on disadvantaged groups when processing data online. Therefore, **data security and privacy are transversal requirements** to be reflected in tools and solutions for properly achieving data minimization, encryption, and robust pseudonymization. Lastly, CounteR must ensure **modularity and adaptability** to integrate requirements at the national level. This concerns, for instance, specific safety measures for the protection of sensitive data.

CounteR partners shall conduct the research activities to develop an online system able to detect radicalisation online. The system must be designed to r**espect human dignity** and the right of the individuals **not to be discriminated against**. Additionally, to the extent and if they are to process any personal data, they shall do so following the applicable European and national rules applicable. The list of requirements in this Deliverable, summarized in Section 5, serves as a handbook for CounteR partners to advise them on the project's ethical and legal requirements, particularly concerning technology development and implementation. Also, this Deliverable serves as a guide for the potential actual future application of CounteR developments by the end-users, which could be used for public interest purposes. However, as detailed above, several measures are **legally required to be taken ex-ante** the potential implementation of CounteR, which actual realization falls out of the scope of the CounteR H2020 research project.

The following Table translates the above requirements into recommendations for the project technical partners and end users. Although the list does not pretend to be exhaustive given the need of detecting issues and appropriate solutions as part of the research process, including the project demonstrations, it provides a **high-level understanding of how legal requirements and ethical principles** should operate in technological conceptualization and design.

Table 2 - Summary table of recommendations

Ethical and legal requirements/ principles	Recommendation
Data protection (security, integrity and privacy)	• CounteR should be designed from a targeted approach to social media and Dark Web data analysis focusing on detecting illicit activity • CounteR should allow the registering and monitoring of its data processing operations by LEAs over time so issues such as function creep can be avoided (this includes a wide set of data ranging from access control such as logs to outcomes of algorithmic processing) • CounteR must integrate editing tools for end users so they can ensure compliance with data subjects rights (I.e., data access, rectification, deletion, etc.) • CounteR must integrate robust authentication and authorization, so access control policies ensure that end users are who they say they are and that they have appropriate access to the System data • All (personal) data registered by the system which is not necessary for its functioning or required for open criminal investigation, in particular sensitive data must be removed deleted as soon as possible (I.e., using methods such as automated deletion and anonymization) • CounteR must provide secure features for the system interoperability with different systems, service providers (such as cloud services) and actors in third countries in order to protect data and ensure admissibility of evidence in Court • CounteR must provide privacy enhancing systems and technologies to ensure data security, quality and availability (I.e., encryption). An incidental policy for residual risks of encryption should be available in the System implementation guidelines • Data controllers must conduct a full Data Protection and Algorithmic Impact Assessment before deployment of CounteR • CounteR must integrate strong systems and techniques for data pseudonymization able to mitigate risks for reidentification (I.e., keys encryption and distribution) taking ENISA (2019) best practices into account
Human rights (integrity)	• CounteR design might integrate mechanisms to mitigate risk of psychological harm to officers involved in operations (this involves actions such as torture and child abuse) • CounteR must integrate tools for mitigating the risks of LEAs sharing images or videos exhibiting victims' sensitive content (such as abuse or torture)

Proportionality assessment	• References should be included in CounteR implementation guidelines on LEA's training regarding requirements for the use of the system when conducting an operation on the Dark Web and with social media data (training should address risks such as re-victimization, entrapment and normalizing serious crime) • CounteR implementation guidelines should also include a clear description of exemptions and scenarios allowing profiling of individuals and reprocessing of personal data, addressing both "judgement of suitability" and "requirement of necessity" analysis to be considered as best practice
Transparency and accountability	• Besides the above detailed registering of data processes, model cards reporting relevant data regarding AI and data operations must be systematically produced by the system to ensure explainability and information • CounteR implementation guidelines should include a code of ethics/conduct for end-users pursuing criminals • CounteR should allow for robust interoperability tools so data controllers (I.e., end users, third parties, etc.) can share data in a secure manner
AI fairness	• The use of AI for live biometric recognition purposes must be avoided within the System • CounteR must provide tools allowing human monitoring and checking of AI, so the accuracy of information and non-discrimination are ensured

Source: own elaboration.

7 References

Aguerri, J., & Fernández Abad, C. (2021). La orden de servicios 3/2018: ¿un instrumento para medir el riesgo de radicalismo violento en prisión? *Estudios Penales Y Criminológicos*, *41*, 361-413.

Baxter, P., Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report,* 13, 544–559.

Brasher, E. A. (2018). Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation. Colum. Bus. L. Rev., 209. Available at: https://cblr.columbia.edu/wp-content/uploads/2018/06/6_2018.1_Brasher_Final.pdf

Brayne S. (2017). "Big Data Surveillance: The Case of Policing". *American Sociological Review,* 82(5):977-1008.

Brey, P. (2005). "Freedom and privacy in ambient intelligence". *Ethics and Information Technology,* 7(3), 157-166.

Byrne, J., & Marx, G. (2011). "Technological innovations in crime prevention and policing. A review of the research on implementation and impact". *Journal of Police Studies,* 20(3), 17–40.

Chan, J. (2001). Technological Game: How Information Technology is Transforming Police Practice. *CriminalJustice: The International Journal of Policy and Practice*, 139–159.

Council of Europe (2018). *Practical guide on the use of personal data in the police sector*. Available at: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

Custers, Bart & Vergouw, Bas (2015). "Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies", *Computer Law & Security Review,* 31 (4), 518-526.

Danziger, J.N., & Kraemer, K.L. (1985). "Computerized data-based systems and productivity among professional workers: The case of detectives". *Public Administration Review*, 196–209.

Dillon, R. S. (ed.) (1995). *Dignity, Character and Self-respect*. New York: Routledge.

Espín López, Isidoro (2021). Los derechos fundamentales a la vida privada afectados por la investigación tecnológica y el fenómeno del entorno virtual, *Journal Boletín del Ministerio de Justicia*, 2244.

ENISA (2019). *Pseudonymisation techniques and best practices*. Greece: European Union Agency for Cybersecurity.

Fernández, C. (2019). "Valoración del riesgo del radicalismo violento en el medio penitenciario". In R. Bermejo e I. Bazaga (Eds.), *Radicalización violenta en España. Detección, gestión y respuesta*, (pp. 253-259). Tirant Lo Blanch.

Floridi, L. (2018). Soft Ethics and the Governance of the Digital, Philosophy & Technology, 31, 1, 1-8.

Fundamental Rights Agency (2018). *Preventing unlawful profiling today and in the future: a guide*. Luxembourg: Publications Office of the European Union.

Fyfe, N. R., Gundhus, H. O. I., & Ronn, K. V. (2017). “Introduction: What is ILP?” In N. R. Fyfe, H. O. I. Gundhus & K. V. Ronn (Eds.), *Moral issues in intelligence-led policing*. Abingdon: Routledge.

Garicano, L. and Heaton, P. (2010).” Information Technology, Organization, and Productivity in the Public Sector: Evidence from Police Departments.” *Journal of Labor Economics*,28(1): 167–201.

González Fuster, G. and Kloza, D. (eds) (2016). *The European Handbook for Teaching Privacy and Data Protection at Schools*. Wellington: Intersentia.

González-Álvarez, J. L., Santos-Hermoso, J. & Camacho-Collados (2020). “Policía predictiva en España. Aplicación y retos de futuro”. *Behavior & Law Journal*, 6(1), 26-41.

Guidette, R., Martinelli, T. J. (2009). “Intelligence-led policing: Strategic framework”. *Police Chief,* 76(10), 132–136.

Hadjimatheou, Kat (2017). *Deliverable 4.3. Policing the Dark Web: Ethical and Legal Issues*. MEDIA4SEC-D4-3-E-NOV17-DarkWebEthicsLegal

Harris, C. J. (2007). “The Police and Soft Technology: HowInformation Technology Contributes to Police Decision Making”. In Byrne, J. and Rebovich, D. (eds), *The New Technology of Crime, Law and Social Control*. Monsey, NY: Criminal Justice Press.

High-level expert group on artificial intelligence set up by the European commission (2019). *Ethics guidelines for trustworthy AI*. Brussels: European Commission.

Hutchinson, Allan C. (1999). “Beyond black-letterism: Ethics in law and legal education”, *The Law Teacher,* 33:3, 301-309.

Innes, M., Fielding, N., Cope, N. (2005). “The appliance of science? The theory and practice of crime intelligence analysis”. *British Journal of Criminology,* 45(1), 39–57.

Innes, M., Sheptycki, J. (2004). “From detection to disruption: Intelligence and the changing logic of police crime control in the United Kingdom”. *International Criminal Justice Review,* 14(1), 1–24.

Ioimo, R.E., & Aronson, J.E. (2003). “The benefits of police field mobile computing realized by non-patrol sections of a police department”. *International Journal of Police Science & Management*, 5(3), 195–206.

Koper, C. S., Lum, C., Willis, J. J., Woods, D. J., & Hibdon, J. (2015). *Realizing the potential of technology in policing: A multi-site study of the social, organizational, and behavioral aspects of implementing policing technologies*. Fairfax, VA: George Mason University Center for Evidence-Based Crime Policy.

Kotschy, W. (2016). The new General Data Protection Regulation-Is there sufficient pay-off for taking the trouble to anonymize or pseudonymize data. Available at: https://fpf.org/wp-content/uploads/2016/11/Kotschy-paper-on-pseudonymisation.pdf

Manning, P. (1992). “Technological Dramas and the Police: Statement and Counter Statement in Organizational Analysis”. *Criminology,* 30, 3327–346.

Markopoulou, Dimitra; Papakonstantinou, Vagelis, de Hert, Paul (2019). “The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation”, *Computer Law & Security Review*, 35, 6.

Monahan, T. (2002). “Surveillance and inequality”. Surveillance & Society, 5(3).

Perelló Domenech, I., (1997). “El principio de proporcionalidad y la jurisprudencia constitucional”, *Jueces para la Democracia. Información y Debate*, 28.

Poonia, A.; A. S., Bhardwaj and G. S. (2009). Dangayach, "Ethical values and practices for cyber society," *2009 International Conference on the Current Trends in Information Technology* (CTIT), pp. 1-5,

Ratcliffe, J. (2008). *Intelligence-led policing. Environmental Criminology and Crime Analysis.* London: Routledge.

Ratcliffe, J. (2016). *Intelligence-led policing*. New York, NY: Routledge.

Ratha, N. K.; Connell, J. H. and Pankanti, S. (2015)."Big Data approach to biometric-based identity analytics," in *IBM Journal of Research and Development,* 59, 2/3, 4:1-4:11.

Razac, O. (2009). “Le bracelet électronique et la virtualisation de l’enfermement”. *Cultures et Sociétés*, (10), 52-57.

Requena, J. (2004). “De la "sociedad disciplinaria" a la "sociedad de control": la incorporación de nuevas tecnologías a la policía”. *Scripta Nova*, 741-798.

Roman, J. K., Reid, S., Reid, J., Chalfin, A., Adams, W., & Knight, C. (2008). *The DNA Field Experiment: Cost-effectiveness analysis of the use of DNA in the investigation of high-volume crimes*. Washington DC: Urban Institute, Justice Policy Center.

Sweeney (2000). “Simple Demographics Often Identify People Uniquely”. *Carnegie Mellon University, Data Privacy Working Paper* 3.

Tene, Omer & Polonetsky, Jules (2012). "Privacy in the Age of Big Data: A Time for Big Decisions." *Stan. L. Rev. Online,* 63.

Vitkauskas, D. & G. Dikov (2012). *Protecting the Right to a fair trial under the European Convention on Human Rights. Council of Europe human rights handbooks*. Strasbourg.

Woolgar, S. (2002). *Virtual society?: Technology, cyberbole, reality*. Oxford: Oxford University Press.

Appendix A: Glossary of terms

Concept	Definition
Anonymization	Anonymous information is data unrelated to an identified or identifiable individual (i.e., data that is not personal data). Therefore, anonymisation is the process of turning personal data into anonymous information so that a person is not (or is no longer) identifiable.
Artificial Intelligence	the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages (Oxford).
Data controller	'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (Art 4, GDPR).
Data processor	"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Art 4, GDPR).
Data Protection Officer	is the individual responsible for ensuring that her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
Informed consent	explicit permission granted by data subjects for the management of their personal data in full knowledge of the possible consequences.
Machine learning	the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data (Oxford).
Personal data	Personal data is information that is associated with an identified or identifiable individual.
Profiling	In general, it defines the registering and examination of a person's psychological and behavioural traits, so as to predict their capacities in a certain domain or to assist in establishing categories of people (classification). From a narrower perspective, it is the process of singling out persons for Law Enforcement Procedures based on predetermined attributes. Racial or ethnic profiling in policing has been defined as "the use by the police, with no objective and reasonable justification, of grounds such as race, colour, languages, religion, nationality or national or ethnic origin in control, surveillance or investigation activities.

Pseudonymization	It is the “processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person” DPA 2018 (Art 4, 5). Consequently, pseudonymisation reduces data protection risk but does not eliminate it.
Sensitive data	“Special category data” is personal data that needs additional protection because it is sensitive (i.e., religious belief, biometrics, gender orientation, etc.) (see Art.9, GDPR).
Third party	As per the GDPR, "third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
Third country	Third countries are states that fall outside the GDPR zone (this includes EU member states plus Norway, Liechtenstein and Iceland).