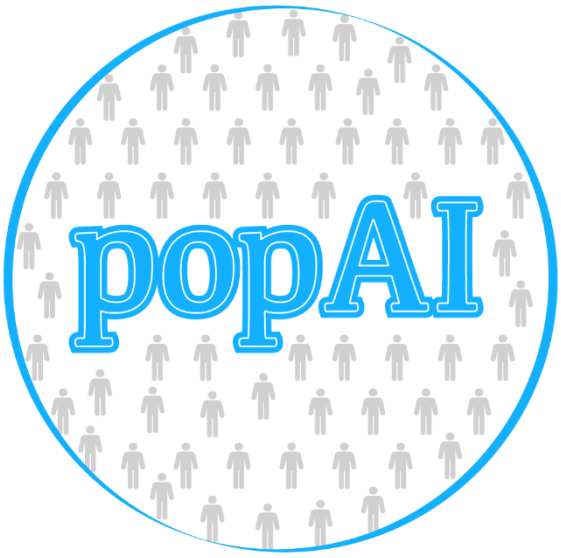

A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D2.1: Functionality taxonomy and emerging practices and trends

Grant Agreement ID	101022001	**Acronym**	pop AI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	**Duration**	24 Months
Project URL	https://www.pop-ai.eu/		
Document date	01/03/2023		
Nature	R = Document, report	**Dissemination Level**	PU = Public
Authors	Konstantinos – Giorgos Thanos, Marilena Sinni, Dimitris Kyriazanos (NCSRD)		
Contributor	Francesca Trevisan (ETI)		
Reviewers	Pinelopi Troulinou (TRI), Andreas Ikonomopoulos (NCSRD)		

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101022001.

Executive Summary

During the recent years there have been made essential advancements in the field of AI and its applications including Security sector and LEAs operation. In this sector, AI progress results in augmented methods of LEAs operation, that exploit the high performance of AI algorithms in human cognitive tasks, such as image/sound comprehension, multi – criteria decision making, etc. These innovative solutions lead to more effective LEAs procedures that rely on the human – machine cooperation, capable of performing much quicker and more accurate the LEAs cognitive and decision-making tasks, and making use of the vast volume of information that can be available for each use case. The inevitable outcome is a constant increase of the number of AI applications in LEAs use cases, continuing research and progress on the performance of these applications, including new algorithms, new data sources, new technical tools such as updated software but also new infrastructures (e.g. cloud technology, GPU optimizations). The large growth of AI involvement in LEAs functionalities, along with the corresponding implications, points to the necessity of deep study and analysis of each AI technique contribution in multi-perspective way, in order to assess the performance of these systems and to understand whether their use complies to ethical and legal requirements of AI in LEA domain. Considering the chaotic number of such use cases, it is needed a systematic, complete and clear organization of LEAs functionality along with their corresponding relations to AI techniques, data sources and potentials sources of controversies. The purpose of this deliverable is the demonstration and analytical presentation of the proposed LEAs functionality taxonomy. This document addresses the necessity of developing a structural organization of LEAs functionalities along with the respective AI technology and implications. The result is a full multi – discipline LEAs functionality taxonomy where abstract functionality categorization, LEAs operations, technical specifications and other ethical and legal implications are binded in an efficient multi-facet structure which is capable of exposing functionalities hierarchy from different perspectives.

Table of Contents

List of Figures

List of Tables

List of Terms & Abbreviations

Abbreviation	Definition
LEA	Law Enforcement Agency
AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
DNN	Deep Neural Networks
SVM	Support Vector Machines
k-NN	k-Nearest Neighbours
DT	Decision Trees
NN	Neural Networks
SVR	Support Vector Regression
HMM	Hidden Markov Model
FC	Fully Connected
SOM	Self Organizing Maps
PNN	Probabilistic Neural Networks
CNN	Convolutional Neural Networks
RNN	Recurrent Neural Networks
LSTM	Long Short Term Memory
GRU	Gated Recurrent Unit
BERT	Bidirectional Encoder Representations from Transformers
GPT	Generative Pre-trained Transformer
EU	European Union
PNR	Passenger Number Record
NLP	Natural Language Processing
CV	Computer Vision

1 Introduction

1.1 Law Enforcement – Challenges - Trends

Law enforcement Agencies (LEAs) operates in several application domains that include surveillance, forensics/analytics, communications and prevention and investigation of crime incidents or malicious acts. As years pass, demand on LEAs' functionality performance increase constantly, given the fact that the availability of sophisticated technical means (such as AI) increase year by year, which not only leverage the efficiency of crime prevention and mitigation procedures but also strengthening the law violation methods. In this regard, the use of Artificial Intelligence (AI) and in general, state of the art technological means (such as facial recognition, biometrics validation, automated negotiators (chatbots), autonomous drones, etc) into LEAs operations increases. These technological methodologies exploit a vast amount of data (public or restricted, sensitive or non-sensitive, multi-discipline) that potentially draw attention not only from technological or security point of view but also from societal, ethics and legal perspective. The large growth in AI involvement in LEAs functionalities, along with the corresponding implications, points to the necessity for studying and analysing each AI technique contribution in multi-perspective way in order to assess the performance of these systems and to understand whether their use complies to ethical and legal requirements of AI in LEA domain. Considering the large number of such use cases, there is a need for a systematic, complete and clear organization of LEAs functionalities along with their corresponding relations to AI techniques, data sources and potentials sources of controversies. In this regard, an extended LEAs functionality taxonomy is proposed that is divided in four tiers that comprise general functionality categories, areas of applications, data sources and functionality cases linked with AI technologies and respective implications.

2 Purpose and Scope

This deliverable demonstrates and analytically presents the proposed LEA functionality taxonomy. This document points out the necessity of developing a structural organization of LEA functionality along with the respective AI technology and implications, explains how this complements AI introduction to LEA operation and increases its efficiency. Moreover, it describes the methodology for developing the proposed taxonomy and finally the document concludes with a detailed description of the taxonomy blocks and the entire architecture.

3 Approach for Work Package and Relation to other Work Packages and Deliverables

D2.1 is the outcome of task T2.1 that focuses on developing functionality taxonomy of LEA-related-to-AI techniques along with the corresponding implications. In this regard, the methodology followed is listed in the table below.

Description of Work	Proposed Action
• Tech specs of different solutions - differences between apps & functionalities/data inputs/databases - relations between concepts • How algorithms are developed for security usage (incl. data sources, providers, models) • Special attention on actual practices and results not only on future or commercial expectations • Identification of consolidated and emerging practices and trends existing and potential risks, specifically in terms of data availability and quality, algorithm training impact. • For data availability provide comprehensive regulatory access framework, complying to both (a) EU legal and ethical standards as well as on (b) public acceptance and positive sentiment • Addressing the data set availability and AI algorithm training challenge within the EU as part of the mapping and assessment process while providing a comprehensive regulatory access framework complying to both EU legal and ethical standards as well as on the public acceptance and positive sentiment.	1. Determine information sources 2. Distinguish/Clear related resources 3. Construct taxonomy 4. Internal evalution/validation 5. Finalization

D2.1 is related to D2.2 and D2.3 that describe in an extended manner the legal and ethical frameworks regarding each functionality. Moreover, D2.1 also exploits the outcomes of D3.1 in order to ensure a realistic conceptual connection of the proposed functionality taxonomy and the several use cases and security context AI is being used.

3.1 Methodology and Structure of the Deliverable

The following sections are structured following a conceptual coherence stating the necessity for taxonomy and ending with the taxonomy description. In this regard, section 4 focuses on the problem definition along with the corresponding state-of-the-art. Moreover, it describes the methodology steps followed in order to realize this taxonomy, taking into account, not only literature references, but also feedback from relevant parties (within the consortium and external resources) to AI technology, LEA, ethics and legal frameworks referring to AI applicability and controversies. Section 5 describes each block of the taxonomy and concludes with the taxonomy itself. Finally, the document concludes with section 6 referring to the respective implications regarding functionalities and the corresponding conclusions.

4 Taxonomy development methodology

During the recent years there have been made essential advancements in the field of AI and its applications including Security sector and LEAs operation. In this sector, AI progress results in augmented LEAs practices, that exploit the high performance of the AI algorithms in human cognitive tasks, such as image/sound comprehension, multi – criteria decision making, etc. These innovative solutions lead to more effective LEAs procedures that rely on the human – machine cooperation, capable of performing much quicker and more accurate the LEAs cognitive and decision-making tasks, and making use of the vast volume of information that can be available for each use case. The outcome is a constant increase of the number of AI applications in LEAs use cases, continuing research and progress on the performance of these applications, including new algorithms, new data sources, new technical tools such as updated software but also new infrastructures (e.g. cloud technology, GPU optimizations). Despite the high-performance increase, these advancements provoke several critical issues and controversies that regard the nature and usage of AI in LEAs sensitive operations (such as human biometrics processing, crowd surveillance, etc), which potentially have societal, political and legal implications as well.

Apparently, the continuing assimilation of AI in LEA operations, result to an essential need for keeping track of each operation, how AI contributes, what information is consumed, how much it is pervasive, what is the legal framework that concern each use case and to what extent AI could be publicly accepted. Consequently, an AI enhanced LEA functionality (for instance “Licence Plate Recognition”) should be examined from technical perspective (what algorithms are used, what data are needed and corresponding classification level, etc), Legal perspective (what is the legal framework that concerns each functionality, do the means that are used follow legal native and EU level regulations, etc). This study is mandatory for:

- **Civil Society / EU citizens**: Safeguarding citizens fundamental rights and human-centric innovative progress in public security characterized by effective and continuous advancing LEAs operations that respect human rights and retain public acceptance.
- **LEAs performance**: Examine strengths and weaknesses of LEAs functionalities and adopt effective technological solutions which exploit AI capabilities, that increase LEAs performance and totally aligned however with Legal and Ethics standards.
- **Technology providers** (including Research communities and related industry): Defining technological constraints and best practices in order to leverage research on LEAs functionality and provide innovative ethical and legal by design solutions.

In this regard, D2.1 aims to develop a multi-aspect taxonomy of LEAs functionalities that reflects the basic aspects of LEAs functionality use cases, application area, AI technology that is used and respective data sources. Moreover, the taxonomy presents in an effective and clear way, any critical features for further elaboration from Societal and/or Legal Perspective. To this end, T2.1 splits the taxonomy built in three major steps: (a) Information sources collections and clarification, (b) Taxonomy development, (c) End users’ evaluation and validation along with taxonomy finalization.

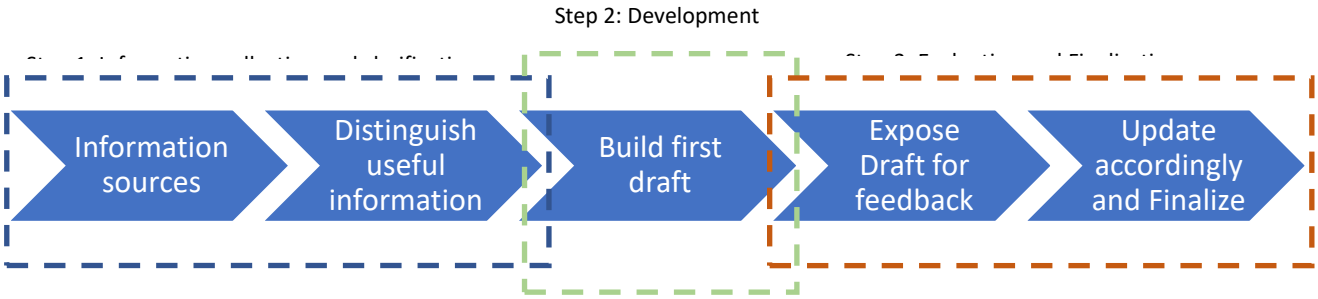

Figure 1 Taxonomy development methodology flow

Although the methodology steps correspond to a traditional approach of information and requirement determination following a development phase and final evaluation, each step has evolved in an agile manner having a consortium task force contributing – evaluating – updating, iteratively, at each step.

Step 1: ***Information sources & resources clarification***

During this step, information was collected from resources related to LEA functionality taxonomy/categorizations, AI applications in LEA operations, related AI algorithms along with the corresponding data sources. Moreover, the study included examination of related EU funded projects, official studies concerning AI involvement in LEAs and security in general. The information sources collected were organized in eight categories:

- **Scientific Publications**: Collection of publications in scientific journals, conference/workshops proceedings and scientific book chapters.
- **Articles-other publications**: Articles other than scientific publications, mostly posted on internet electronic journals and magazines.
- **Official studies – results**: Official reports published by related to LEA policies and functionalities area, AI scientific field and EU stakeholders.
- **Legal Framework**: Information resources related to legal regulations and framework that regard AI technology application in LEA and security operations.
- **Ethical Frameworks LEA & AI**: Information resources related to ethical implications and potential controversies of AI application in LEA operations.
- **EU-funded projects & Initiatives**: Present and past EU – funded projects as well as independent or official institutional initiatives that examine the cooperation of AI technologies and Security functionalities and operations.
- **Advocacy Groups**: Collection of organizations that perform research and studies on digital technologies and AI applications from Legal, Ethics and EU Policies perspective.
- **Case studies**: Collection of information resources comprising of AI application in LEA operations

The entire collection of information resources is listed in ANNEX 1.

.

Step 2: *Taxonomy development*

The collected information resources were evaluated and ranked based on their relevance – type of resource (official or unofficial) and publication date. Beginning with the highest ranked sources, there were distinguished the different functionalities mentioned along with the corresponding information regarding technology used (Data sources, Data Availability, Algorithmic techniques), Maturity Level, area of application and related impact (Legal/Ethics implications). The different functionalities were examined in a comparative manner among the collected information resources trying to be in agreement with the most significant and essential functionality categorizations that have been proposed in the literature while also maintaining coherency with the resource plurality. In this regard, initially a first draft of taxonomy criteria was developed along with taxonomy hierarchical levels and categories, including sets, subsets and supersets of the collected functionalities. Moreover, in a collaborative manner, through online documents and partner meetings the proposed taxonomy was presented – received feedback – updated – presented again for comments until an agreement was reached among the participating partners that included WP3 representatives as well.

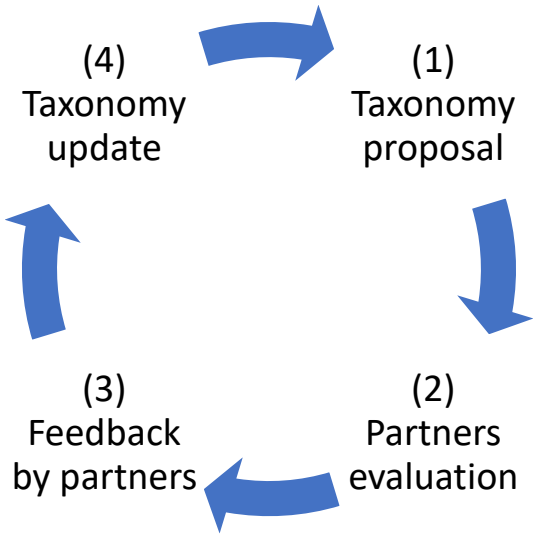

Figure 2 Taxonomy development agile procedure

Step 3: *Evaluation and Validation*

The first draft of the taxonomy was presented during the 1st pop AI online Workshop "AI in support of Civil Security: functionalities and controversies mapping" that took place on 15th March 2022. The workshop comprised, among others, of representatives of LEAs, RTOs, AI and Security experts. During the meeting we had the opportunity to demonstrate in detail the taxonomy structure, the choices made during the development procedure and presented how the proposed taxonomy could be adapted to the "ClearView AI" use case in Sweden. The goal was for the proposed taxonomy to be exposed and evaluated based on: (a) taxonomy classes, (b) taxonomy structures, (c) completeness, (d) usability, (e) taxonomy realism . The received feedback was noted and used for updating and finalizing the taxonomy as presented in detail in the following sections.

5 Law Enforcement functionalities taxonomy

5.1 Taxonomy description

The proposed taxonomy is a functionality oriented structure with a 4-tier hierarchy comprising of (a) high-level categories of functionalities, (b) an area of application of each functionality, (c) the functionality themself along with the related meta – information regarding the technical implementation of each functionality (algorithms, systems, etc), maturity level and potential impact, and the related data sources. The block diagram of the taxonomy is depicted in Figure 3, where each tier corresponds to a hierarchy level presented in a top-down logic.

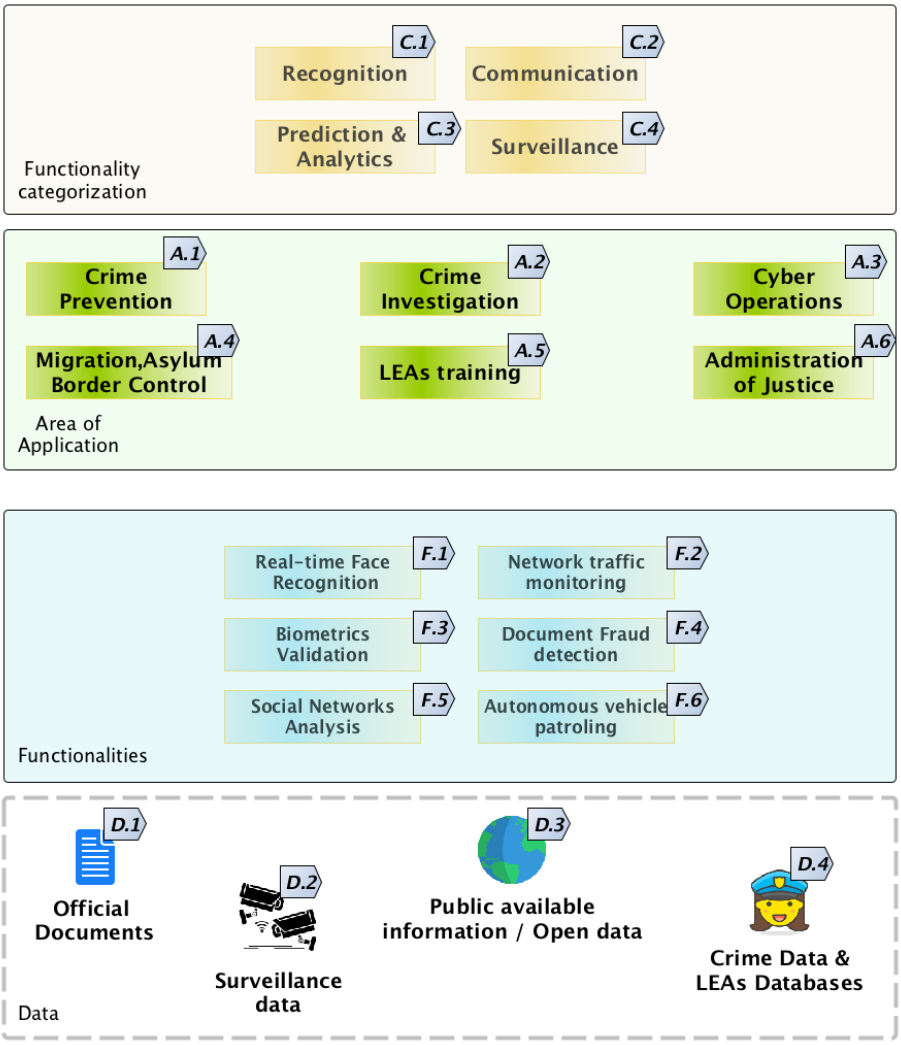

Figure 3 Functionalities Taxonomy hierarchy

5.1.1 Categorization and Encodings

Each hierarchy tier comprises a set of sub-blocks which are the categories of each tier – level (e.g. Functionality Categorization :- {Recognition, Communication, Prediction & Analytics, Surveillance}). Each category block is mapped to a pre – defined unique encoding in order to increase effectiveness in referencing and reduce error rate regarding erroneous duplicates, mislabeling, etc.

Functionality encodings

Encoding	Functionality
C.1	Recognition
C.2	Communication
…	
A.1	Crime Prevention
A.2	Crime Investigation
…	
F.1	Face Recognition
F.5	Social Network Analytics
…	
AIT.17	Computer Vision
AIA.NN.11	LSTM
…	

Functionality node

Figure 4 Functionalities representation

5.1.1.1 Functionality Categorization

This is the top tier of the taxonomy and corresponds to high level categorization of LEAs functionalities. This is a fixed categorization and relies on the Functionalities categorization as proposed in INTERPOL/UNICRI [1] study. The tier comprises of the following categories:

- **Recognition**: This category regards functionalities that regard recognition / identification / verification / validation tasks either real-time or offline. Examples are: voice recognition, suspects identification, etc.
- **Communication**: This category comprises of interaction functionality with humans such as communication robots, translation bots, chatbots, etc.
- **Prediction & Analytics**: This category comprises all the data processing and information analysis and knowledge extraction operations, real – time or offline, such as: Digital forensics, Agent-Based simulations, suspicious behaviour detection, etc.
- **Surveillance**: This category includes all the surveillance patrolling monitoring functionalities, such as: Surveillance drones, patrol robots, AI generated Patrol Live Stream, etc.

5.1.1.2 Area of Application

The second tier corresponds to the Area of Application category of each functionality following the Area of Application categorization as proposed in T3.1 [[2]] and is also a fixed tier. The categories are presented below:

- **Crime Prevention**: Indoor functionalities that contribute to the prevention of potential crime. These functionalities act before a potential crime incident takes place with the aim of determining all the information needed for preventing the crime.
- **Crime Investigation**: Functionalities that contribute after a crime takes place with the aim of determining information that support investigation procedures.

- **Cyber Operations**: Functionalities that regard network cloud and digital communication infrastructures.
- **Migration, Asylum, Border Control:** Functionalities related to migration asylum and border control.
- **LEAs Training**: Training functionalities / educational content providing and skill development.
- **Administration of Justice**: Functionalities that support jural operations.

5.1.1.3 Functionalities

This tier contains a list of all functionalities along with corresponding meta – information:

- **Maturity Level**: This tag corresponds to the readiness level until commercial deployment. It is a fixed categorization reflecting the estimated time for deployment: (a) ***Concept*** *(10+ years to deploy)*, (b) ***Lab Prototype*** *(5-10 years to deploy)*, (c) ***Prototype for evaluation in real conditions*** *(2-5 years to deploy)*, (d) ***Approved*** *(ready to deploy)*
- **Related Data Sources:** Related data sources, databases that are consumed by the referred functionality
- **Related Algorithms**: Refers to the AI algorithms realized at each functionality. As described below, AI algorithms are organized in a tree-based hierarchical structure in order to reflect the dependencies among the several algorithm labels as referred in literature. More information is given below in the *5.1.1.5* AI Technologies subsection.
- **Impact/Other**: This tag is about related information to Impact (Legal/Ethics implications), or other information related to the functionality and the connection with the other blocks or tags (e.g. data availability, security issues, etc).

5.1.1.4 Data

The Data tier refers to the related Data sources/databases for each functionality. The main categories that are used within the taxonomy are:

- **Official Documents (PNR, IDs, etc):** This type corresponds to information and data related directly or indirectly with official documents that had been issued by official authority
- **Surveillance Data:** This data type corresponds to all data that come from surveillance devices (cameras, sensors)
- **Publicly Available Information/ Open Data**: This category refers to the all publicly available (free or paid).
- **Crime Data/ Police Database**: Datasets that are related directly or indirectly with crime incidents and in general private police data.

5.1.1.5 AI Technologies

In literature, LEA functionalities usually refer to AI technologies and the corresponding algorithms appear as keywords. Although this set up can provide full reference among the several functionalities and the respective algorithms, an incoherence problem still remains, because in this way there is no

information about the relation among the algorithms. For example, let's examine the two following functionalities: (a) F.9 – Licence Plate Recognition (AI algorithms: SVM and others), (b) F.17 – Improving Police / Community Relations (AI algorithms: NLP (Chatbots), (c) F.21 – Video and Photo Surveillance (AI algorithms: DNN). Apparently, the above functionalities refer to AI algorithms using a different keyword for each algorithmic approach. In this example there are three AI algorithmic techniques, namely: SVM, NLP and DNN. SVM corresponds to a specific AI algorithm, NLP refers to an AI technique, that comprises several algorithmic approaches, such as Naïve Bayes, Hidden Markov Models (HMMs), DL (or else DNN) and more specifically transformer algorithms such as BERT, T5, etc. HMM, Naïve Bayes and SVM correspond to traditional ML but transformers to DL terminology. Moreover, HMM and Bayes are probabilistic models while SVM is a regression model. HMM, Naïve Bayes Model, SVM, DNN (BERT, T5) are supervised ML algorithms and needless to say that all of the above correspond to AI techniques. In this regard, for the proposed taxonomy to reflect these dependencies which are forwarded to the functionalities themselves, it is proposed that algorithms are organized in a tree – based hierarchical form, where each algorithmic technique links to supersets as parent nodes and to subsets as child nodes. The benefit of this set up is that each functionality is mapped to algorithmic approaches which inherit the relation to other algorithmic approaches. This approach supports the capability reflection of potential relations among functionalities at an algorithmic level.

The proposed AI techniques categorization is split in two tree taxonomies: (a) AI algorithms where we propose a categorization based on algorithmic approach characteristics, (b) AI tasks categorization of AI problems, borrowed by JRC study AI definition [[3]] which correspond to the AI goals that are approached by the pre-mentioned AI algorithms. For instance, we have the AI task "NLP: Natural Language Processing" which is approached by the AI algorithmic family "Transformers". AI algorithms categorization divided AI approaches in two main groups: Expert systems which contain the algorithms that rely on given expert knowledge modelled either in the form of rules set or graph model, and the Machine Learning group which comprises the AI data driven approaches (Figure 5). On the other hand, AI tasks categorization splits AI practices in eight main groups as met usually in practical applications of AI:

- **Reasoning**: Data processing and comprehension resulting to knowledge representation
- **Planning**: Determining optimal routes and policies based on pre – defined goals and requirements.
- **Learning**: Cognitive learning tasks such as knowledge extraction, prediction, automated systems, etc
- **Communication**: Tasks regarding the communication of humans with machine. Characteristic example of this category is NLP.
- **Perception**: Tasks responsible for comprehending audio and image data.
- **Integration/Interaction**: This category comprises the autonomous intelligent systems, such as Agent-based simulations, Robots, etc
- **Services**: Other intelligent tasks that operate as supporting services to users (e.g. decision support systems, recommender systems, etc)
- **AI Ethics/Philosophy**: Tasks aiming to ensure Ethical and Fair usage of AI (Fairness, Privacy, etc)

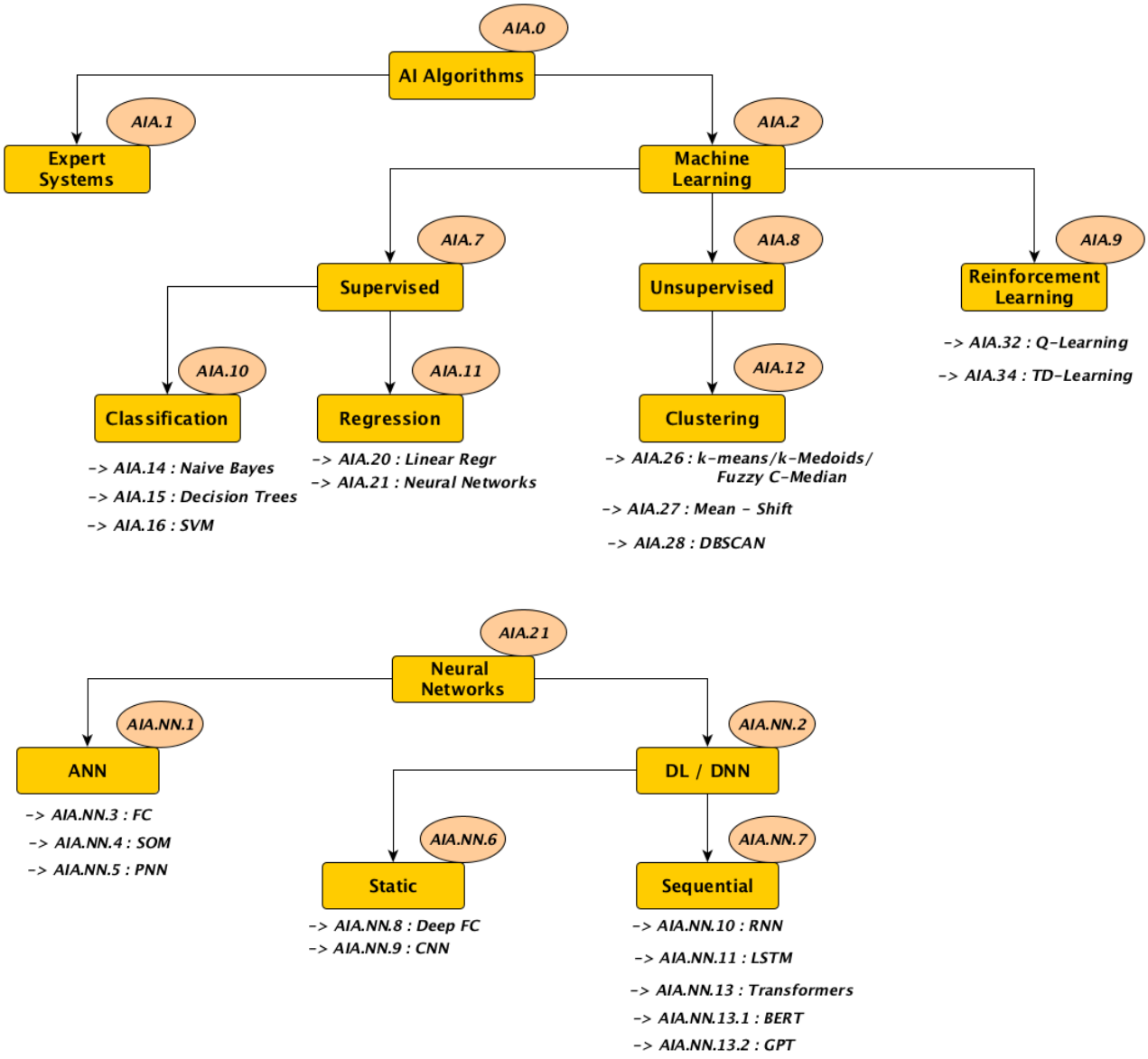

Figure 5 AI Algorithms taxonomy (sample) (up), Neural Networls span taxonomy (sample) (down)

The corresponding encodings are related with the the type of categorization it represents. AI alogirhmic approach are encoded with the string “AIA.X” (e.g. “Machine Learning”:AIA.2, “Q-Learning”:AIA.32). Moreover the specific category of Neural Networks, due to the fact that it spans in a signigificant depth, it is mapped with a dedicated encoding string, “AIA.NN.X” (e.g. Deep Neural Networks (DNN):AIA.NN.2). On the other hand AI Tasks are encoded with the string :AIT.X (e.g. NLP:AIT.16). Moreover, the AI Tasks taxonomy includes references to the AI algorithms taxonomy, however it should be noted that these references are not exhaustive. It includes only a subset of these references based on the examined literature. In Figure 6 it is presented an example of AI Tasks representation. The full taxonomies and the corresponding references in the taxonomy excel document are presented in section 5.2.

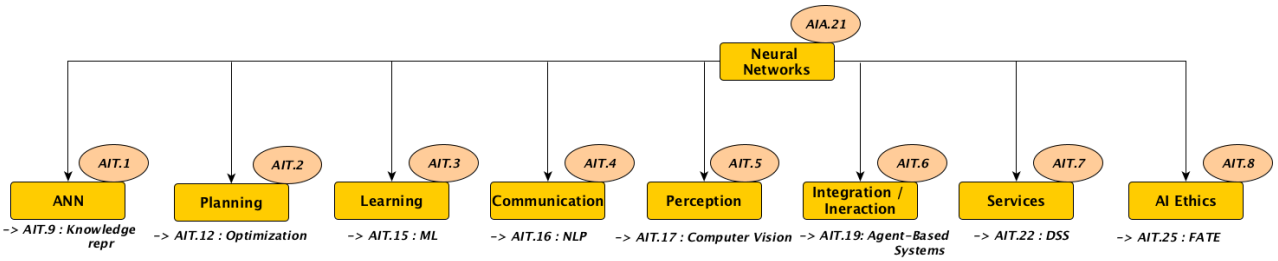

Figure 6 AI Tasks taxonomy (sample)

5.2 Taxonomy tables

The following tables provide a structured, tabular presentation of the proposed taxonomy described in section 5.1. Table **1** includes a list of all the existing law enforcement functionalities that utilize AI, organized in the first column. Subsequent columns contain indexes to Tables 2-6 that follow, as explained in the text following Table 1.

Table 1 Functionalities table

Encoding	Functionalities	Related Category (mandatory)	Related Algorithms	Related Data	Related Area of Application	Maturity Level (where available)	Reference (mandatory)
F.1	Real-time Face Recognition	C.1	AIT.17	D.2, D.3	A.2, A.3	P	
F.2	Network Traffic Monitoring	C.4	AIT.15	D.2, D.3	A.3, A.1, A.2	A	
F.3	Biometrics Validation	C.1	AIT.17	D.4, D.3, D.1	A.1, A.4	P	
F.4	Document Fraud Detection	C.3	AIT.16	D.2, D.3, D.1	A.1, A.2, A.4	E	
F.5	Social Networks Analysis	C.2,C.3	AIT.15	D.3	A.1,A.2, A.3	A	https://www.policechiefmagazine.org/power-social-network-analysis/ , https://arxiv.org/abs/2002.09485
F.6	Autonomous Vehicle Patrolling	C.4	AIT.21	D.3, D.4, D.2	A.1,A.2	P	https://www.policechiefmagazine.org/implications-of-self-driving-vehicles/
F.7	Deepfake Detection	C.1,C.3	AIT.17, AIT.18	D.3, D.1	A.1,A.2	A	https://www.niessnerlab.org/projects/roessler2019faceforensicspp.html , https://www.euractiv.com/section/digital/ne
F.8	Voice and Video Transcription	C.3	AIT.16, AIT.18, AIT.17	D.2	A.1,A.2	A	https://www.policechiefmagazine.org/product-feature-artificial-intelligence-breaking-into-law-enforcement/ ,
F.9	Licence Plate Recognition	C.1,C.3	AIT.17, AIA.21, AIA.NN.4, AIA.16	D.2,D.3, D.1	A.1,A.2, A.4	A	https://www.policechiefmagazine.org/product-feature-artificial-intelligence-breaking-into-law-enforcement/ , S. Du, M. Ibrahim, M. Shehata and W. Badawy, "Automatic License Plate Recognition (ALPR): A State-of-the-Art Review," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 2, pp. 311-325, Feb. 2013, doi: 10.1109/TCSVT.2012.2203741.
F.10	Cryptocurrency Tracking	C.4	AIT.15	D.2	A.1,A.3	A	https://www.policechiefmagazine.org/product-feature-artificial-intelligence-breaking-into-law-enforcement/

F.11	Anti-money laundering	C.3, C.4	AIT.26, AIT.15, AIA.NN.2	D.2	A.1, A.3	A	http://www.artificialintelligenceinsight.org/2019/02/13/how-ai-is-changing-investigations-policing-and-law-enforcement/ , Kute, Dattatray & Pradhan, Biswajeet & Shukla, Nagesh & Alamri, Abdullah. (2021). Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3086230. , https://www.ojp.gov/ncjrs/virtual-library/abstracts/fincen-artificial-intelligence-system-identifying-potential-money
F.12	Predictive Policing: individuals	C.3	AIT.15	D.3,D.5	A.1,A.2	A	http://www.artificialintelligenceinsight.org/2019/02/13/how-ai-is-changing-investigations-policing-and-law-enforcement//
F.13	Predictive Policing: areas or locations	C.3	AIA.NN.1, AIT.15, AIT.16	D.3,D.5	A.1,A.2	A	https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf [p.19], Crime Anticipation System – Dutch police (Netherlands):https://studenttheses.uu.nl/bitstream/handle/20.500.12932/39398/OosterlooSerena_thesis_def.pdf?sequence=1&isAllowed=y
F.14	Autonomous Boats	C.4	AIT.21, AIA.2	D.3, D.2, D.4	A.3, A.4	P-->E	https://news.mit.edu/2020/autonomous-boats-could-be-your-next-ride-1026 , https://www.maritime-executive.com/editorials/autonomous-vessels-are-becoming-a-commercial-reality
F.15	Child Sexual Abuse Mitigation	C.3, C.4	AIA.0	D.2, D.3	A.1,A.2,A.3	A	https://www.analyticsinsight.net/top-8-ai-technologies-mitigate-child-abuse-child-trafficking/ , AI-Combating-online-sexual-
F.16	Counter-Terrorism	C.4	AIA.0	D.2, D.1	A.1,A.2,A.3	A	https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf
F.17	Improving Case Clearance Rates	C.3	AIT.15, AIA.NN.2	D.3	A.2,A.6	P [U.S.A]	https://cjtec.org/files/5f5f94aa4c69b [p.7]
F.18	Improving Police-Community Relations	C.2	AIT.16	D.3	A.1	E [U.S.A]	https://www.policechiefmagazine.org/ai-community-police-relations/ , https://cjtec.org/files/5f5f94aa4c69b [p.7]

F.20	Computer Aided Dispatch (CAD)	C.4	AIA.0	D.3, D.4	A.1	A	https://citec.org/files/5f5f94aa4c69b [p.7]
F.21	Gunshot Detection and Mapping	C.1	AIT.15	D.2, D3, D.4	A.2, A.6	A	A. Caragliu, C. Del Bo and P. Nijkamp, Smart cities in Europe. Series research memoranda 0048, Amsterdam: University of Amsterdam, 2009, https://www.theguardian.com/law/2015/jul/17/shotspotter-gunshot-detection-schools-campuses-privacy
F.22	Video and Photo Surveillance	C.4	AIA.NN.2	D.2	A.1, A,4	A	https://citec.org/files/5f5f94aa4c69b [p.5]
F.23	Autonomous drones	C.4	AIT.21	D.2, D.3, D.4	A.1,A.4	A	A. Caragliu, C. Del Bo and P. Nijkamp, Smart cities in Europe. Series research memoranda 0048, Amsterdam: University of Amsterdam, 2009,
F.24	Autonomous Robots [ALIGNER]	C.4	AIT.20	D.2, D.3, D.4	A.1,A.4	P	https://www.europarl.europa.eu/cmsdata/196207/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf
F.25	Critical Infrastructure Protection	C.3	AIA.NN.1, AIA.18, AIA.15, AIA.16	D.2, D.3, D.4	A.3	C	S. Zeadally, E. Adi, Z. Baig and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," in IEEE Access, vol. 8, pp. 23817-23837, 2020, doi: 10.1109/ACCESS.2020.2968045. [p.15]
F.26	AI data (harvesting) and exploitation by LEAs	C.3	AIT.1, AIT.3, AIT.4, AIT.5, AIT.7	D.2,D.3	A.1,A.2	A	MAGNETO http://www.magneto-h2020.eu/
F.27	Criminal Identification Facilitation	C.3, C.1	AIT.18, AIT.16, AIT.17, AIT.15	D.2,D.3, D.1	A.1,A.2	P	ROXANE https://roxanne-euproject.org/
F.28	Information Extraction from Video Footage Analysis	C.3, C.4	AIT.17	D.2	A.1,A.2	P	SURVANT
F.29	Real-time Online Terrorist Content Detection	C.3, C.4	AIT.1, AIT.15, AIT.7	D.2, D.3, D.4	A.3	A	RED ALERT https://cordis.europa.eu/project/id/740688
F.30	Autonomous Border Surveillance [CONTAINS SUBFUNCTIONALITIES]	C.4	AIT.1, AIT.15, AIT.7	D.2, D.3, D.4	A.4	P	ROBORDER + RELATED PROJECTS https://roborder.eu/related-projects/ , i-BORDER Ctrl
F.31	Improve performance of European police officers by developing VR enhanced training	C.3	AIT.24	D.3, D.4	A.5	P	SHOTPROS https://shotpros.eu/
F.32	Autonomous Digital Evidence Collection for Secure Exploitation in Court	C.3	AIT.15, AIT.7	D.3	A.6	P	LOCARD https://locard.eu/
F.33	Retrieval and Analysis of Mobile Phone Data	C.4	AIT.1, AIT.7, AIT.15	D.3, D.2	A.6	P	FORMOBILE https://formobile-project.eu/ , https://formobile-project.eu/downloads/publications-public-deliverables/156-autopod-mobile-semi-automated-data-population-using-case-like-scenarios-for-training-and-validation-in-mobile-forensics-margaux-michel-dirk-pawlaszczyk-and-ralf-zimmermann/file

Each functionality belongs to one or more high level categories in **"Related Category"** column, labelled C.1-C.4, which are presented in **Table 2** and are further analysed in sub-section 5.1.1.1. The **"Related Algorithms"** column provides a classification of each functionality, based on which AI task or algorithm it belongs to. The encoding for AI tasks or algorithms is presented as AIT.X or AIA.X and is explained in Table 6 and the logic behind this categorization is presented analytically in sub-section 5.1.1.5. The next categorization, **"Related Data"**, is based on what kind of data sources are used in each functionality, with encoding D.1-D.4 that is described in Table 4, along with each data source's modality. Sub-section 5.1.1.4 describes each data source or database. **"Related Area of Application"** tier contains the relevant fields of application of each functionality, which follow the encoding A.1-A.6 in Table 3 and are described in sub-section 5.1.1.2. The final category of the functionalities taxonomy is **"Maturity Level",** which refers to the readiness level until commercial deployment. Table 5 shows the encoding translated as time for deployment of each functionality, where C: ***Concept*** *(10+ years to deploy)*, P: ***Lab Prototype*** *(5-10 years to deploy)*, E: ***Prototype for evaluation in real conditions*** *(2-5 years to deploy)*, A: ***Approved*** *(ready to deploy).*

For example **Real-time Face Recognition** functionality (F.1) falls under the C.1: Recognition category, which belongs to the AIT.17:Computer Vision area, which is part of the broader category of AI Tasks, the AIT.5: Perception. The data sources used by this functionality include D.2: Surveillance Data and D.3: Public Available Information/Open Data, and the area of application for Real-time Face Recognition is A.2: Crime Investigation and A.3: Cyber Operations. Finally, this functionality is currently in the P: Lab Prototype stage, which means it is expected to take 5-10 years before it can be fully deployed in the field.

Table 2 Functionality Categorization

Encoding	Functionality Categorization
C.1	Recognition
C.2	Communication
C.3	Prediction & Analytics
C.4	Surveillance

Table 3 Area of Application

Encoding	Area of Application
A.1	Crime Prevention
A.2	Crime Investigation
A.3	Cyber Operations
A.4	Migration, Asylum, Border Control
A.5	LEA's Training
A.6	Administration of Justice

Table 4 Data

Encoding	Data	Modality

D.1	Official Documents (PNR, IDs, etc)	Text
D.2	Surveillance Data	Image, Network Data, Audio
D.3	Public Available Information/Open Data	Video, Text, Geolocation
D.4	Previous Crimes	Sound, Geolocation

Table 5 Maturity Level

C	Concept
P	Prototype
E	Evaluation
A	Approved

Table 6 Algorithms

AI Tasks

Encoding	Task	Parent
AIT.1	Reasoning	AIT.0
AIT.2	Planning	AIT.0
AIT.3	Learning	AIT.0
AIT.4	Communication	AIT.0
AIT.5	Perception	AIT.0
AIT.6	Integration and Interaction	AIT.0
AIT.7	Services	AIT.0
AIT.8	AI Ethics and Philosophy	AIT.0
AIT.9	Knowledge Representation	AIT.1
AIT.10	Automatic Reasoning	AIT.1
AIT.11	Common Sense Reasoning	AIT.1
AIT.12	Optimization	AIT.2
AIT.13	Schedule	AIT.2
AIT.14	Searching	AIT.2
AIT.15	Machine Learning	AIT.3
AIT.16	Natural Language Processing (NLP)	AIT.4
AIT.17	Computer Vision (CV)	AIT.5
AIT.18	Audio Processing	AIT.5
AIT.19	Agent-Based Simulations	AIT.6
AIT.20	Robots	AIT.6

AIT.21	Automated Vehicles	AIT.6
AIT.22	Decision Support Systems (DSS)	AIT.7
AIT.23	Recommender Systems (RS)	AIT.7
AIT.24	Virtual Environments (Digital Twins)	AIT.7
AIT.25	FATE	AIT.8
AIT.26	Safety	AIT.8
AIT.27	Privacy	AIT.8

AI Algorithms

Encoding	Algorithm	Parent
AIA.1	Expert Systems	AIA.0
AIA.3	Rule Based	AIA.1
AIA.5	Fuzzy Logic (FL)	AIA.3
AIA.6	Logic Based	AIA.3
AIA.4	Knowledge Graphs	AIA.1
AIA.2	Machine Learning	AIA.0
AIA.7	Supervised	AIA.2
AIA.8	Unsupervised	AIA.2
AIA.9	Reinforcement Learning	AIA.2
AIA.10	Classification	AIA.7
AIA.11	Regression	AIA.7
AIA.12	Clustering	AIA.8
AIA.14	Naive Bayes	AIA.10
AIA.15	Decision Trees	AIA.10
AIA.16	Support Vector Machines (SVM)	AIA.10
AIA.18	k-Nearest Neighbour (k-NN)	AIA.10
AIA.19	Discriminant Analysis	AIA.10
AIA.20	Linear Regression	AIA.11
AIA.21	Neural Network (NN)	AIA.10, AIA.11, AIA.12, AIA.9
AIA.22	Support Vector Regression (SVR)	AIA.11
AIA.23	Decision Tree Regression	AIA.11
AIA.24	Lasso Regression	AIA.11
AIA.25	Ridge Regression	AIA.11
AIA.26	k-Means / k-Mediots / Fuzzy C-Median	AIA.12
AIA.27	Mean - Shift	AIA.12
AIA.28	DBSCAN	AIA.12
AIA.29	Agglomerative hierarchical clustering	AIA.12
AIA.30	Gaussian Mixture clustering	AIA.12
AIA.31	Hidden Markov Model (HMM)	AIA.12, AIA.10, AIA.11
AIA.32	Q-Learning	AIA.9
AIA.33	R-Learning	AIA.9
AIA.34	TD-Learning	AIA.9

AIA.NN.1	Artificial Neural Network (ANN)	AIA.21
AIA.NN.2	Deep Learning / Deep Neural Network (DL/DNN)	AIA.21
AIA.NN.4	Self Organizing Maps (SOM)	AIA.NN.1
AIA.NN.5	Probabilistic Neural Networks (PNN)	AIA.NN.1
AIA.NN.6	Static Neural Networks	AIA.NN.2
AIA.NN.7	Sequential Neural Networks	AIA.NN.2
AIA.NN.8	Fully Connected (FC)	AIA.NN.1, AIA.NN.6
AIA.NN.9	Convolutional Neural Network (CNN)	AIA.NN.6
AIA.NN.10	Recurrent Neural Networks	AIA.NN.7
AIA.NN.11	LSTM	AIA.NN.7
AIA.NN.12	GRU	AIA.NN.7
AIA.NN.13	Transformers	AIA.NN.7
AIA.NN.14	BERT	AIA.NN.13
AIA.NN.15	T5	AIA.NN.13
AIA.NN.16	GPT	AIA.NN.13

6 Implications

6.1.1 Technology

There are resource requirements that need to be met in order AI technique be applied efficiently. These requirements refer to data availability, information sensitivity and security, algorithmic complexity specifications resulting to constraints imposed on information system specifications (cloud computing technologies/infrastructure, GPU optimizations, high processing capabilities, IoT architectures, etc) and have significant effect on the applicability and maturity level of each AI enabled functionality, influencing the usability range in application areas and also the time needed each functionality to be ready for deployment. In this regard, each functionality is characterized (wherever applicable) by short comments referring to infrastructure necessities and resource availability.

6.1.2 Ethics / Legal

Each functionality not only has technological implications, but also essential impact that may emerge due to the ethics or legal consequences in case of careless irresponsible use of controversial AI technologies. In this regard, sort references are included at each functionality recording, such as keywords, short comments/phrases or references to respective pop AI deliverables or external resources that point out the ethics and legal frameworks that define each functionality applicability.

7 Conclusions

The large growth of AI involvement in LEAs functionalities, along with the corresponding implications, emerges the necessity of deep study and analysis of each AI technique contribution in multi-perspective way in order to assess performance and Ethics/Legal implications of AI applications in LEA domain. Considering the chaotic number of such use cases, it is needed a systematic, complete and clear organization of LEAs functionality along with their corresponding relations to AI techniques, data sources and potentials sources of controversies. In this deliverable is was presented the proposed LEAs functionality taxonomy, with the aim of developing a structural organization of LEAs functionality along with the respective AI technology and implications. It is a full multi – discipline taxonomy structure, where abstract functionality categorization, LEAs operations, technical specifications and other ethical and legal implications are binded in an efficient multi-facet component, that is capable of exposing functionalities hierarchy from different perspectives. The specific structure is a tool for LEAs practitioners, Security, Engineering and Ethics/Legal researchers and related industry as well, where each party can easily retrieve different functionality aspects from different point of view such as implications, technical specifications, area of application and data sources. As future work the specific taxonomy could be implemented as an online application database, where, in a quick and efficient way, LEAS functionality along with the related information that is stored in the taxonomy can be retrieved and presented in a multi-discipline way and providing also the capability to be extended with more information in a crowdsourcing way where relevant users can share their experience and expertise, making the taxonomy a common knowledge ground for LEAs AI applications domain.

8 References

[1] "Artificial Intelligence and robotics in Law Enforcement", INTERPOL/UNICRI, url: https://www.policechiefmagazine.org/product-feature-artificial-intelligence-breaking-into-law-enforcement/

[2] pop AI deliverable 3.1 – "Map of AI in policing innovation ecosystem and stakeholders"

[3] Joint Research Center (JRC), "JRC Technical Reports: AI Watch Defining Artificial Intelligence – Towards and operational definition and taxonomy of artificial intelligence", European Commission, 2020

ANNEX 1

Information sources table

Official Studies

ID	Title	Author	Reference
OS1	Artificial Intelligence and robotics in Law Enforcement	INTERPOL / UNICRI	http://www.unicri.it/in_focus/on/interpol_unicri_report_ai
OS2	Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights	Policy Department for Citizen's Rights and Constitutional Affairs - DG Internal Policies - EC	https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf
OS3	Artificial Intelligence in Federal Administrative Agencies	Administrative Conference of the United States	https://www.acus.gov/report/government-algorithm-artificial-intelligence-federal-administrative-agencies
OS4	Artificial Intelligence and Countering Violent Extremism	Global Internet Forum to Counter Terrorism (GIFCT)	https://gnet-research.org/2020/09/28/artificial-intelligence-and-countering-violent-extremism-a-primer/
OS5	Artificial Intelligence Applications in Law Enforcement	Criminal Justice Testing and Evaluation Consortium (CJTEC)	https://cjtec.org/artificial-intelligence-applications-in-law-enforcement/
OS6	Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters	European Parliament	https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.pdf
OS7	Artificial intelligence at EU borders: Overview of applications and key issues	European Parliament	https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf
OS8	Guidelines, Recommendations, Best Practices	EDPB	https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-
OS9	LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	EC	https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF
OS10	The EU AI Act	EU	https://artificialintelligenceact.eu/

Scientific Publications

ID	Technology	Functionalities Area	Source name	References
SP1	NLP / Automatic Speech/Text, Adversarial Attack, Classification tasks /	NLP / Automatic Speech/Text, Adversarial Attack, Classification tasks / Swarms	NLP / Automatic Speech/Text, Adversarial Attack, Classification tasks / Swarms management/Robotics	https://ieeexplore.ieee.org/abstract/document/9216065
SP2	Computer Vision / Machine Learning	Biometrics identification / verification	A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication	http://dx.doi.org/10.5772/intechopen.76685

Other Publications

ID	Technology	Source name	Reference
O1	Computer Vision / Machine Learning / Speech2Text	Product Feature: Artificial Intelligence Breaking into Law Enforcement	https://www.policechiefmagazine.org/product-feature-artificial-intelligence-breaking-into-law-enforcement/
O2	NLP, Computer vision	Artificial Intelligence Adoption in Law enforcement	https://roxanne-euproject.org/news/blog/artificial-intelligence-adoption-in-law-enforcement
O3	Computer vision	Artificial Intelligence and Law Enforcement	https://www.policemag.com/342341/artificial-intelligence-and-law-enforcement
O4	IoT, Forecasting, Robotics, Intrusion detection	Artificial Intelligence and Security: Current Applications and Tomorrow's Potentials	https://emerj.com/ai-sector-overviews/artificial-intelligence-and-security-applications/
O5	Computer vision, Forecasting	How AI is changing investigations, policing and law enforcement	http://www.artificialintelligenceinsight.org/2019/02/13/how-ai-is-changing-investigations-policing-and-law-enforcement/
O6	IoT, Computer vision, Drones, Forecasting	Opportunities and Challenges from Artificial Intelligence for Law Enforcement	https://www.futuregrasp.com/opportunities-from-artificial-intelligence-for-law-enforcement
O7	Computer vision, Forecasting, Robotics	The Growth Of AI Adoption In Law Enforcement	https://www.forbes.com/sites/cognitiveworld/2019/07/26/the-growth-of-ai-adoption-in-law-enforcement/?sh=95987b0435dd
O8	Malware detection, XAI	Explainable Threat Intelligence: How Automated Static Analysis & Machine Learning Deliver	https://www.bankinfosecurity.com/whitepapers/explainable-threat-intelligence-how-automated-static-analysis-w-5942
O9	Computer Vision / Robotics	AI in police work	https://appen.com/blog/ai-in-police-work/

EU-funded projects

ID	Project name	Dates	Technology	Security Area	Functionalities Area
EP1	RED-Alert	2017-2020	Natural Language Processing Social Network Analysis Complex Event Processing Semantic Media Analysis Artificial Intelligence	Cybercrime/Online terrorism	Social media online activity
EP2	INSPECTr	2019-2023	Big data analytics Cognitive machine learning Blockchain approaches Knowledge discovery techniques		Shared intelligence platform

EP3	MAGNETO	2018-2021	Advanced correlation engine Sophisticated representational model (represent knowledge in an open, standardised manner) Evidence collection platform (heterogeneous data mining and multimedia content indexing) Threat predicition engine by semantic reasoning Augmented intelligence tools	Economic crime/Crime against persons and property/Terrorism/Identity crime
EP4	AIDA	2020-2023	Artificial intellignece and Deep Learning techniques applued to big data analytics Automated data mining Extensive content acquisition Information extraction and fusion Knowledge management and enrichment through novel applications of Big Data processing, machine learning, AI, predictive and visual learning	Cybercrime/Counterterrorism

EP5	INFINITY	2020-2023	Extended reality technologies Automated systems Immersive AR/VR
EP6	ROXANNE	2019-2022	Speech processing - speaker identification and multilingual automatic speech recognition Natural language processing Video and geographical meta-data processing Network analysis

EP7	PREVISION	2019-2021	Visual intelligence modules Data mining modules for crime prevention and investigation Semantic function representation and fusion modules Trends detection and probability prediction modules for organised terrorism and criminal activities Detection modules for cybercriminal activities Situation awareness and HMI modules	
EP8	DARLENE	2020-2023	IoT ecosystem DARLENE cloud Wearable Augmented Reality applications	Anticipation-prevention criminal activites

EP9	SURVANT	2017-2018	Situational awareness framework (geo-registration capabilities and GIS assisted search) Advanced content-based search (using AI and efficient knowledge modelling) Search expansion tools (query building support, search expansion recommendations, iteratuve search functionalities, event evolution prediciton)	Surveillance	Video surveillance analysis
EP10	TRESSPASS	2018-2021	Data from neighbouring countries Person tracking re-identification Data fusion and risk assessment RFID lugagge tracking Real-time behavioutal analysis Passenger trusted mobile app OCULUS contril and command centre Crowd simulation and visualisation Control and simulation VR platform Web intelligence analysis Security personnel mobile app PNR and data from third countries	Border security	Border security checks
EP11	FLYSEC	2015-2018	Intelligent remote image processing Video surveillance Biometrics Open-source intelligence Crowdsourcing Behavioural analysis and cognitive algorithms Mobile applications - positive passenger boarding RFID lugagge tracking	Border security	Aviation security

EP12	D4FLY	2019-2022	Biometric technologies Thermal and multispectral imaging Advanced morphed face detection algorithms through Convolutional Neural Networks Computer vision algorithms Smartphone applications Deep Neural Networks	Border security	Document fraud
EP13	SPIRIT	2018-2021	Integrated Ethics & Privacy Protection Keyword based refined search Keyword based automated search Multi purpose web crawler Content Database System Face extraction and matching Graph visualisation		

EP14	TRUST aWARE	2021-2024	
EP15	ALIGNER	2021-2024	

EP16	STARLIGHT	2021-2025	
EP17	SPIRIT	2018-2021	Integrated Ethics & Privacy Protection Keyword based refined search Keyword based automated search Multi purpose web crawler Content Database System Face extraction and matching Graph visualisation
EP18	TRACE	2021-2024	
EP19	ASSERT	2013-2014	N/A - analysis of good practices to take into to account the societal dimensions of security research

			Analysis automation	Cybercrime
			Data mining	
			Awareness tools	
EP20	CC-DRIVER	2020-2023		
				Social media
EP21	MEDI@4SEC	2016-2018		
EP22	COMPOSITE	2010-2014		

EP23	FORMOBILE	2019-2022	Mobile forensics	Counter-terrorism/crime investigation
EP24	LOCARD	2019-2022	Blockchain technology Cloud and mobile forensics	Digital evidence for juridical work
EP25	SHOTPROS	2019-2022	VR enabled training for law enforcement officers	

EP26	VAST	2020-2023			
EP27	SIENNA	2017-2021			
EP28	4NSEEK	2019-2021		Child exploitation	
EP29	iBorderCtrl	2016-2019	Emotion AI at borders		
EP30	GRACE				

Case studies

ID	Case study: technology	Summary	Country	Date	Sources
CS1	facial recognition/biometrics	Clearview facial recognition software using online public images (news media, public mugshot websites, Facebook, YouTube...). Upload photo and matches to others and provides information to be able to identify person by name. Used by LEAs both in the US and Europe	France, Austria, Italy, Greece, UK - countries concerned	May 21 - Dec 21	https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html - https://www.dw.com/en/privacy-activists-challenge-clearview-ai-in-eu/a-57691756 - https://www.dw.com/en/clearview-ai-controversy-highlights-rise-of-high-tech-surveillance/a-57890435 - https://edri.org/our-work/challenge-against-clearview-ai-in-europe/
CS2	facial recognition/biometrics	Clearview facial recognition app unlawfully used by Swedish Police Authority.	Sweden	Feb-21	https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en
CS3	facial recognition/biometrics	Members of Parliament favour banning AI mass surveillance e.g. facial recognition in public spaces. Call for ban on use of private facial recognition databases and predictive policing based on behavioural data. Call for ban on social scoring systems.	All EU	Oct-21	https://www.actuia.com/english/meps-vote-for-supervision-of-artificial-intelligence-systems-and-against-mass-surveillance/ https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance
CS4	Smartphone Surveillance	1.000 Hungarians protested over allegations government used Pegasus spyware for illegal surveillance of public figures in Hungary (journalists, lawyers, people critical of government). The tool allows control of mobile device, access all data, turn on video/audio.	Hungary	Jul-21	https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state - https://www.rferl.org/a/hungary-pegasus-protest-spyware/31378863.html - https://www.neweurope.eu/article/pegasus-scandal-involves-over-10-countries-and-targets-thousands-via-smartphones/
CS5	facial recognition/biometrics	Civil rights activist took to court South Wales Police as automatic facial recognition technology being used unlawfully. His image was captured on facial recognition van at peaceful protest	UK	Aug-21	https://www.bbc.com/news/uk-wales-53742099
CS6	facial recognition/biometrics	London police department to use live real-time facial recognition to detect criminal suspects with video cameras in streets	UK	Jan-20	https://www.nytimes.com/2020/01/24/business/london-police-facial-recognition.html https://www.bbc.com/news/uk-51237665
CS7	surveillance	Court prohibits police in Paris to use drone to monitor demonstrations and gatherings on public roads. In May 2020, court also ruled drones could not be used to track people in breach of lockdown rules.	France	Dec-20	https://www.bbc.com/news/world-europe-55411695#:~:text=France's%20top%20administrative%20court%20has,covering%20public%20protests%20in%20Paris.&text=In%20May%2C%20the%20same%20court,of%20France's%20strict%20lockdown%20rules. https://www.aa.com.tr/en/europe/paris-police-banned-from-using-surveillance-drones/2085728
CS8	Body cameras	Unlawful use of body cameras in Stockholm's public transport. Ticket inspectors using body cameras that record video and sound. Transport company fined.	Sweden	Jun-21	https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_en
CS9	Smart policing/facial recognition	Hellenic Data Protection Authority investigating lawfulness of smart policing programmme (not yet implemented but under construction) - facial recognition, fingerprint detection	Greece	2020	https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/ https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights?fbclid=IwAR12E9LHk5XZHu2e0Zf8w2axNHFrzvMYIwSLISoDG5aLAdWDWb-Hd-8tVh4
CS10	Security scanners	Overall picture Lot of controversy on body scanners and discussion on these in 2010, 2011 - less discussion since then			
CS11	Security scanners	China-based company Nuctech supply people, cargo and vehicule scanners across Europe. Fears that China could exploit equipment to sabotage key transit points or acess government, industrial or personal data	Europe	Jan-22	https://www.voanews.com/a/security-scanners-across-europe-tied-to-china-government-military/6404710.html
CS12	Security scanners	Gender discrimination and harassment from body scanners. Some scanners used have to be programmed according to sex and staff alerted if shows prosthesis/chest bindings.	UK/Europe	Sep-17	https://www.theguardian.com/money/2017/sep/11/travellers-gender-issue-security-checks-airports-how-staff-respond

CS13	Facial recogntion/biometrics	El Prat airport in Barcelona first airport to test facial recognition in Europe. Allow passenger to use facial recognition at every step of journey: check in, bag drop off, pass through security, board plane. Participation is voluntary and tested on Barcelona-Malaga journies. Passengers need to use AENA app to register facial biometrics and will be used to link to their passport - participant fill in form and consent to participation. AENA responsible for biometric data collected and owner of database (run in accordance with GDPR)	Spain	December 2021	https://www.barcelonacatalonia.eu/en/el-prat-airport-barcelona-will-be-the-first-to-test-facial-recognition-in-europe/ https://findbiometrics.com/aena-vueling-launch-comprehensive-biometric-screening-pilot-barcelona-airport-010406/
CS14	Google Glasses	GG is a brand of smart glasses developed by X (Google). Glasses were announced by Google in 2012, made available on the market in 2014, banned in several places, not accepted by the public, retired from the market in 2015 and in 2016 Google erased all the Google Plus pages on GG. Now there is only available an enterprise version	US	2012-2015	https://docs.google.com/document/d/1Kzkel-jbQXpMPZBoZziz_XAMxqt3hvgiAk-RIdn1x-A/edit?usp=sharing
CS15	Smart meters /smart grids	Despite Smart meters for electricity have received a	US, Europe	2009-ongoing	https://docs.google.com/document/d/18fbv1M90cfR05S6mC5QT1aXswfPeJBe5hiAHnkoapVM/edit?usp=sharing
CS16	Facial Recognition-Live and Remote	Facial recognition provides government with power	Worldwide		
CS17	Biometric mass surveillance	German authorities in Cologne used facial recognition systems outside LGBTQ+ venues, religious venues, doctor's surgeries and lawyers' offices without legitimate justification.	Germany		https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/
CS18	Facial recognition	Police in Poland misused country's facial recognition based COVID-19 quarantine systems to visit the homes of people after they have finsihed their quarantine	Poland		https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/
CS19	Body cameras	Expansion of body cams to be used by police throughout Finland.	Finland		https://yle.fi/news/3-11830091
CS20	Body cameras	Body cam footage being stored on Amazon Cloud by German police.	Germany	2019	https://www.dw.com/en/german-police-storing-bodycam-footage-on-amazon-cloud/a-47751028
CS21	Facial Recogntion	the Social Democrats (SPD), Greens and liberal Fr	Germany	2021	https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/
CS22	Body cameras	An Garda Siochana to roll out body cameras in 2022.	Ireland	2021-2022	https://www.independent.ie/irish-news/gardai-will-wear-b
CS23	Encryption	Campaign against introducing end-to-end encryption in social media	UK	2022	https://noplacetohide.org.uk/
CS24	Encryption	UK watchdog criticises "No place to hide"	UK	2022	https://www.bbc.com/news/technology-60072191
CS35	Encryption	UK governament and coalition of charities against end t	UK	2022	https://www.bbc.com/news/technology-60055270 https://
CS36	Encryption	Case study	EU	2014/22	https://docs.google.com/document/d/1QQrfKv0VPe-3Xo017JB1sMNnzwufv3ySy63evaNwGZE/edit?usp=sharing

Legal Framework

Title	Date	Location	Area of AI	Links
Italy - introduction moratorium on video surveillance	December 2021	Italy	Mass surveillance using facial	https://edri.org/our-work/italy-introduces-a-

Ethical Frameworks LEA & AI

Link	Document name	Responsible (who issued the document
https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment#:~:text=The%20CEPEJ's%20view%20as%20set,on%20Human%20Rights%20(ECHR)%20and	European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment	European Commission for the Efficiency of Justice (CEPEJ)
https://inventory.algorithmwatch.org/	good source for ethical frameworks	

Advocacy Groups

Name	Type of organisation	Topic	Link
Amnesty International	NGO	Digital surveillance technology and	https://www.amnesty.org/en/documents/EUR01/2556/2020/en/
Human Rights Watch	NGO	Digital surveillance technology and	https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-
IPVM	Independent organisation in the field of video	Digital surveillance technology and	https://ipvm.com/reports/patents-uyghur
Fair Trials	NGO	Use of Artificial Intelligence and	https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf
Ireland-Palestine Solidarity Campaign	NGO	Arguing that the Irish and Northern	https://www.ipsc.ie/action-item/stop-gardai-psni-collaboration-with-israels-ministry-of-death-torture-
The Greens/EFA in the European	Political group of the European Parliament	Campaign to ban biometric mass	https://www.greens-efa.eu/en/campaigns/ban-biometric-mass-surveillance
Algorithmic Justic League	Independent organisation active on algorithmic	Algorithmic bias threats to society,	ajl.org/about
AlgoRace	Independent organisation on AI and racism	debate on how AI impact on racialised	https://algorace.org/
AlgoRights	Independent organisation on Human rights and	Human rights and AI	https://twitter.com/algorights
Center for Humane technology	NGO	For a shift toward a more humane	https://www.humanetech.com/
European Digital Rights	collective of NGOs		https://edri.org/
NetBlocks	private business	digital rights, cybersecurity and	https://netblocks.org/
All tech is human	NGO	building responsible etch pipeline	https://linktr.ee/AllTechIsHuman
The Justice Programme	programme of the Open Knowledge Foundation	offer training to activists, lawyers and camp	https://www.thejusticeprogramme.org/
Accountable Tech	private business	fight for social media accountability	https://accountabletech.org/
Cities Coalition for Digital Rights	Network of 50+ cities that help each other in the	protect and uphold human rights on	https://citiesfordigitalrights.org/
WASP-HS	Swedish National Research Program	research challenging AI with	https://wasp-hs.org/
Big Brother Watch	civil liberties campaign	fight for privacy and civil liberities	https://bigbrotherwatch.org.uk/
Fight For Future		digital privacy advocacy group	https://www.fightforthefuture.org/
Privacy Network	association	dissemination, advocacy and debate on	https://www.privacy-network.it/
Open rights group	uk digital campaigning organisation	to preserve and promote rights in the	https://www.openrightsgroup.org/join/
Access Now	organisation	defend and extend digital rights around	https://www.accessnow.org/