AI_CITY

ARTIFICIAL INTELLIGENCE AND CITY'S SECURITY THROUGH INTERDISCIPLINARY TECHNOLOGICAL INNOVATIONS

INTERREG Policy Objectives: A Smarter Europe

Specific Objectives: Research and innovation capacities, uptake of advanced technologies

Duration: 4 years
Call Closing: June 7th 2024
Call Information: Interreg programme manual

AI at the service of city's security can help to identify critical events and, in various circumstances, it can act in preventive phase to support the intervention of security forces during an emergency.

What is AI_CITY?

The main goal is to promote a responsible development of AI systems by exploiting the potential offered by technology to respond to the emergency of violence in the cities' contexts.

Identification of local security policies and exchange of experiences

Detection of spy behaviour

Developpement of AI tools

Development of new intervention policies

Project aims

The project intends to exploit the potential offered by AI for preventive and repressive purposes, with the aim of identifying, detecting and monitoring the 'spy' behaviours that can undermine city's security.

Università di Foggia

Giurisprudenza

AI_CITY

ARTIFICIAL INTELLIGENCE AND CITY'S SECURITY THROUGH INTERDISCIPLINARY TECHNOLOGICAL INNOVATIONS

Abstract

For more than a decade, there has been a widespread belief that **video surveillance** makes great contributions to **public security**, both in a preventive (as a deterrence tool) and repressive (as a means of identifying and detecting perpetrators of offences that have already been committed) key.

The most recent developments in digital technology have caught up with and enhanced the device, opening up scenarios that were unimaginable until some time ago: with the help of video surveillance cameras, in fact, it has become possible to **recognise the individual filmed by cross-referencing the images with other personal data and automatically detect suspicious behaviour, recording and reporting it.**

The phenomenon shows itself in all its disruptiveness as a result of recent developments in Artificial Intelligence, which can further improve the performance of machines. Indeed, 'intelligent' video surveillance systems are able to detect human presence (**Human Detection**) in their field of view. This makes it possible to distinguish humans from animals, increasing the efficiency of the intrusion detection system. Furthermore, the intelligent facial recognition function (**Facial Recognition**) identifies the presence of a face in the frame and captures its somatic features, determining the age and sex of the individual as well as the presence of beard, hat and glasses. In addition, artificial intelligence makes it possible to monitor the suspicious behaviour of intruders (**Loitering Detection**) or gatherings on the premises (**Crowd Analysis**).

Despite several attempts to control algorithmic tools and, more specifically, to curb the possibility of real-time biometric recognition, the risk of massive surveillance justified by emergencies in urban areas is becoming increasingly real.

In fact, we should not underestimate the disruptive scope of the **AI Act**, promulgated in March 2024, which - de facto - authorises (under certain conditions) **the use of remote biometric identification systems in real time for the prevention and countering of threats to national security and for the identification of crime 'suspects'.**

The aim of AI_City is to **promote a responsible development of artificial intelligence systems to respond to the emergency of urban violence, acting on local policies** (general guidelines for the promotion of integrated security and pacts for the implementation of urban security) to make cities safer without neglecting fundamental rights.

So, the aim of the project proposal is to strengthen the existing situational prevention tools in order to remove the root causes of deviance and degradation phenomena and to support citizens' participation in the overall improvement of social, housing and service conditions (so-called community prevention) and social prevention interventions aimed at curbing criminogenic factors.

The ultimate aim of the research is to develop - through the integrated action of the different areas involved - a shared operational model that, by exploiting the potential offered by AI, offers **a concrete response** to stem the risk of criminal deflagration right from the first violent manifestations.

The research aims to achieve, in a gradual development, seven objectives:

1) Systematic framing of the phenomenon.

2) Recognition and systematic reconstruction of the relevant national and supranational legislative compendium, with particular regard to existing policies in the areas concerned.

3) Identification of the criminogenic and criminal phenomena of interest.

4) Statistical analysis of the impact of violent behaviour on urban security.

5) Creation of preventive detection algorithms to alert law enforcement agencies in the presence of unequivocal signs of violent behaviour.

6) Evaluation of the legal implications of using AI for preventive and repressive purposes.

7) Improvement of existing policies through the development of an application model that can be implemented in practice.

Reference context

In a context such as the one described above, the legal system seems to respond by means of 'special' legislation aimed at differentiating the rules on video surveillance in

the public and private sectors: if, in the latter case, the Government seems to favour the use of *surveillance* systems as an antidote to urban insecurity, the legislation - at least formally - becomes more rigorous on the public front.

Meanwhile, the public security decree of 2009 (**Decree-Law No. 11 of 23 February 2009**, converted by Law No. 38), in conjunction with the rules marked by the European Regulation 2016/679 (**GDPR,** *General Data Protection Regulation*), while allowing entities to install systems for the protection of urban security in public places or places open to the public, introduces a series of limits to the processing of personal data stored by video surveillance systems for the controllers (the Public Administration that installs the device) and for the data subjects (the citizens), with regard to retention times, processing purposes and the technical requirements of the systems, in accordance with the principle of *accountability* and *privacy by design*.

More recently, **Legislative Decree No. 51/2018,** transposing EU Directive 2016/680, allows Data Controllers, i.e. municipalities in the person of the mayors *pro tempore*, to enter into special '**security pacts**' to legitimise security police bodies to use remote monitoring systems for the needs of preventing or repressing criminal phenomena (Art. 47).

Intervention policy

In accordance with national provisions, on 6 February 2023, **the Municipality of Foggia, in agreement with the Prefecture**, signed an **urban security pact** which, in Article 1, provides for the financing of programmes to set up new video surveillance and video alarm systems to supplement existing systems by adopting standards and equipment capable of establishing a **direct connection with the operational rooms of** the police forces with general jurisdiction.

In addition, the pact envisages **public-private collaboration** to enable the networking of existing video surveillance systems in banks, pharmacies, apartment blocks, tobacco shops, businesses, possibly involving private individuals and organisations.

The project intends to intervene precisely on this policy with the aim of proposing a **socially sustainable*smart city* model.**

In particular, the project aims to:

1) make video surveillance systems more technically and operationally efficient, thanks to the contribution of AI;

2) strengthen urban security by enabling intelligent video surveillance systems to recognise possible threats to public order (so-called spy behaviour), while respecting the principle of data minimisation and the prohibition of 'live' identification

3) make the operation of smart video surveillance systems compliant with GDPR rules (in relation to processing, anonymisation and psudonymisation, storage, technical requirements);

4) strengthen the transparency profile in the management of information flows;

5) prevent sanctions arising from unlawful processing of personal data;

6) envisage adequate solutions for a 'responsible' use of data extracted from surveillance cameras in criminal proceedings;

7) promote solutions to ensure a balance between security and the protection of individual rights.

Interreg Policy Objectives: A Smarter Europe
Specific Objectives: Research and innovation capacities, uptake of advanced technologies
Duration: 4 years
Call Closing: June 7th 2024
Call Information: Interreg programme manual
References: Prof. Donatella Curtotti – donatella.curtotti@unifg.it
　　　　　　 Dott. Wanda Nocerino – wanda.nocerino@unifg.it