NEW TECHNOLOGICAL SOLUTIONS TO HELP PREVENTION AND INVESTIGATION IN PRISON

EDITED BY
STEFANO BELLINA

AGENFOR
INTERNATIONAL

INTRODUCTION

Today, we are witnessing a continuous and **exponential development** of digital technologies that has affected the way crimes are committed as well as investigated (Mijatović, 2019). As is the case with many other contexts, prisons have been influenced by such advancements – especially for what concerns the increased difficulty in controlling inmates' illegal actions and illegal communication with the outside world, as well as in relation to the technologies to prevent inmates from committing additional crimes. There is a need for an urgent update, partly already underway, of the methods used in prison facilities, both from a preventive and an investigative point of view.

The following article reflects on the change that digital and communication technologies can and have brought to the **security** and **prevention** sectors, specifically examining three innovative techniques currently used in prison: Open Source Intelligence tools (OSINT) to collect and analyse data; wiretapping microphones; and drones and counter drone systems.

DIGITAL FORENSICS

Considering the vast amount of data circulating in prisons and the consequent difficulty for operators to monitor them clearly and comprehensively, the **support** that technologies can provide in this regard - e.g. data mining for preventive security measures generated by **mobile data** forensics in investigations - is a real asset for the expansion of intelligence analysis. As an example, only through an analysis of the telephones illegally owned by the inmates, officers can detect existing **criminal networks**, criminals' connections, hierarchies between suspects, group dynamics and movements (Agenfor International, 2020).

Telephones introduced illegally in prisons and used by inmates are, in fact, common and valuable sources of data. As it might be

the case for inmates convicted of organised crime or terror-related crimes, phones in possession of this kind of inmates can be exploited by Law Enforcement Agencies (LEAs) for the **analysis** and **monitoring** of criminal chains between different detainees, family, or kinship networks. Indeed, "artificial intelligence and big data analytics, combining the aforementioned **OSINT** and **Human Intelligence** (HUMINT) can help better filter and prioritise mass data on suspects and share and compare data with other police forces, intelligence agencies and courts for more accurate prediction techniques" (Agenfor International, 2020).

As the CEO and CO-founder of **SecurCube** Nicola Chemello (2020) explains, if a phone exchanges traffic via a cellular network, there is a log that allows investigators to trace a series of information, such as the geographical trace of the call, the International Mobile Subscriber Identity (MSI) - a number that uniquely identifies each mobile phone user, and the International Mobile Equipment Identity (IMEI) - a code that uniquely identifies each mobile terminal, thus allowing the owner of the phone to be **instantly traced**. These records are **unchangeable** and are a source of fundamental importance for preventive and investigative purposes for LEAs, making a range of related information available to them that can be used for investigative purposes.

LEGAL INTERCEPTION OF CONVERSATIONS IN PRISON

Another prison scenario that could benefit from technology refers to legal interception of visitors' conversations. In this sense, as Sasha Bianchi (2020), Sales Manager of the private enterprise **AREA**, states: a **fixed pattern** must be followed in order to conclude the investigation effectively, which mainly consists in sending the wiretapping in real time to the Public Prosecutor's Office, watching the interviews from the headquarters of the judicial police and finally drafting the transcripts, which are, in the Italian context, always to be delivered to the Public Prosecutor's Office.

The microphones are installed inside the tables in the room where the meeting takes place, so that they are not visible at all, and help by cameras fixed inside the room, it is possible to **intercept live** any kind of conversation, which as already mentioned, in addition to being seen by the judicial police, is sent live to the Public Prosecutor's Office, via a wireless link. At the end of the interview, the judicial police officers take care of transcribing in full the conversations observed, so that the document can then be handed over to the Public Prosecutor's Office.

DRONES AND COUNTER-DRONES SYSTEMS

Finally, the use of Unmanned Aerial Systems (UAS) – also known as drones – and related counter-drones technologies be analysed. Drones are a widely used tool in prisons for making **illegal deliveries**, such as drugs or money, as well as for planning escapes or collecting data on inmates. Such tools are generally "small and difficult to detect by conventional surveillance means, as they do not follow traditionally examined trajectories" and it is often the case that "payloads carried by UAS devices in the prison system have been made to look like permitted objects" (Russo, 2020).

In the event that one of these tools is seized and consequently the **data** are **extracted**, such devices can provide a significant source of information for LEAs. In this regard, the use of **counter-drone systems**, which are useful tools for detecting, tracking, identifying and intercepting drones, is crucial.

Counter-drones technologies and the use of cooperative drones by LEAs are an important **deterrent to crime** and are much more effective than the so-called 'passive' methods of law enforcement, i.e. walls and nets, which are easy to circumvent, unlike the new UAV surveillance methods. According to Stefano Russo (2020), Chief Software Engineer at **Italdron**, counter-drone technologies cooperative drones used by LEAs have a very **low acoustic footprint** and are able to intercept any illegal air transport. These instruments are currently used mainly to detect events such as accidents, parades and car traffic (their use has recently been implemented for surveillance purposes at the Shopping Mall in Arese, Milan) but their gradual introduction into prisons would bring countless benefits.

Additional positive aspects of such technologies include the fact that they are controlled from a control room, through which the UAV camera can be viewed and controlled in **real time**, locating and tracking the threat on the ground in seconds. Also, UAV data can be accessed from anywhere, with no need for special infrastructure, only 4g/5g coverage. "Thanks to real-time video processing on a powerful on-board computer, threats can be detected and tracked automatically. Once detected, threats can be precisely geolocated and the detection can be used to trigger alerts", states Russo (2020).

CONCLUSION

Innovative technologies are beneficial for security and especially for high-risk contexts such as the prison environment – their application should therefore be upscaled significantly. While this article has mainly focused on the securitisation of prisons, it is worth noting that within that same environment, technology can and should also be used for educational and rehabilitation purposes. As society changes, the penitentiary system should change in parallel, introducing different ways of communicating or interacting and preparing inmates for the digital world they will later be re-integrated into.

REFERENCE LIST

Agenfor International. (2020). Concept Note. *J-Safe Project.eu.* Retrieved from: https://jsafeproject.eu/webinar-on-new-technological-solutions/.

Bianchi, S. (2020). *Experimental Lab of Penitentiary Forensics* [PowerPoint Slides]. Agenfor International, Italy: J-SAFE project funded under the European Union's JUST-AG GA No. 763714. Retrieved from: https://jsafeproject.eu/webinars/.

Bianchi, S. (2020), *Lawful Interception of families talks in prison environment* [PowerPoint Slides]. Area, Italy: J-SAFE project funded under the European Union's JUST-AG GA No. 763714. Retrieved from: https://jsafeproject.eu/webinars/.

Chemello, N. (2020). *Spot the illegal use of mobile phones* [PowerPoint Slides]. SecurCube, Italy: J-SAFE project funded under the European Union's JUST-AG GA No. 763714. Retrieved from: https://jsafeproject.eu/webinars/.

Mijatović, D. (2019). *Justice in Europe facing the challenges of digital technology* [Conference]. Council of Europe Justice Ministers. Retrieved from: https://www.coe.int/en/web/commissioner/-/justice-in-europe-facing-the-challenges-of-digital-technology.

Russo, S. (2020). *Webinar J-Safe, Italdron Group* [PowerPoint Slides]. Italdron, Italy: J-SAFE project funded under the European Union's JUST-AG GA No. 763714. Retrieved from: https://jsafeproject.eu/webinars/.

Van De Steene, S. (2020). *Dynamic Security & Offender Engagement* [PowerPoint Slides]. Smart Corrections, France: J-SAFE project funded under the European Union's JUST-AG GA No. 763714. Retrieved from: https://jsafeproject.eu/webinars/.

AGENFOR
INTERNATIONAL

FOR MORE INFORMATION ON THIS TOPIC AND ON OUR PROJECTS PLEASE VISIT:

AGENFORMEDIA.COM