PREVENTING RADICALISATION THROUGH OSINT TOOLS: RECOMMENDATIONS FOR LAWFUL PROFILING

EDITED BY
VIRGINIA CINELLI
STEFANO BELLINA

AGENFOR
INTERNATIONAL

INTRODUCTION

The increasing interest of Law Enforcement Agencies (LEAs) and private companies in **prevention** has driven to the development of new analytical tools and indicators capable of detecting and identifying suspect criminals and, consequently, preventin them from committing a crime. These techniques are often based on the **criminal profiling paradigm**, a method that originated in the mid-90s, according to which investigators – in addition to the traditional method of evaluating crimes with physical evidence – are expected to use the outcomes of the investigation (i.e. offline and online data mining and storage) to profile the individual who most likely committed the given crime (Dean, 2007; Dinant, Lazaro, Lefever, Rouvroy, 2008: 3).

Although these techniques are applied to any type of crime, they are extensively used to identify individuals who might become radicalised or engage in terror-related crimes, especially online. A clear example are the violent extremist risk assessment tools (e.g. COVR, ERG22, MAPPA, VERA) specifically developed for radicalisation cases, together with Open Source Intelligence (OSINT) tools currently used by public and private bodies to identify radical profiles online by analysing the content they publish (Bianchi, Ladu and Bianchi, 2019). Yet are these methods trust-worthy? Is profiling necessarily helpful in cases of radicalisation or could it be dangerously misleading?

Without hiding the advantages of these new tools, this article highlights the risks related to their use, in particular regarding **legal violations** (e.g. freedom of expression) and **misleading results**, and finally argues that it would be more fruitful to shift the focus on the **situational factors** that may lead a person to become radicalised (i.e. meso and macro factors) rather than variables specific to the individual themselves.

ASSETS AND LIMITS OF THE OSINT TOOLS

OSINT methods and other innovative assessment tools certainly improve the policing activity both in its strategic and tactical responses. As a general benefit, such tools come to be very useful in collecting **heterogeneous and extensive amounts** of data from different sources on a scale that a human would be incapable of (Cinelli, V. 2020). In the specific analytical phase, of particular interest in cases of radicalisation and terror-related crimes are the **graphical representations** and **link analyses** that could represent the individual network and detect figures such as "recruiters", "ideologues", or simply other "at-risk individuals". Other beneficial techniques refer to the **verification of digital sources** such as photos or videos or the **scenario awareness**. Examples of relevant tools that could be applicable to terror-related crimes could be: the functional end-to-end product **MEDUSA®** (2019), developed to fight against serious crimes, is among the most-used OSINT tools within international police forces to extensively monitor media sources, identify the origin of any kind of message, its dissemination and the audience's reactions to it; the graphical link analysis tool Maltego (undated) developed by the German private company Maltego Technologies Ltd for gathering and connecting information for investigative tasks (Maltego, undated); the predictive analysis software used by the French National Gendarmerie **I2 Analyst Notebook** (IBM, 2019); and the software **Huntsman SPIDA** which mainly focuses on data extraction (Pointduty, undated).

In the investigative field, such tools are of highly beneficial for LEAs, specifically allowing them to **effectively investigate relationships** between criminal networks, quickly tracing crimes back to suspects. Yet in absence of a crime, as it is in the case of radicalisation, the collection and processing of personal data on natural persons that these tools carry out risk **violating** some of the **fundamental rights** included in the European Charter of Human Rights such as privacy and data protection, freedom of expression and information, protection against discrimination in

the exercise of rights and freedoms (E.U. Charter of Human Rights, art. 8, 10, 14); often use **indeterminate criteria** that can lead to prejudice, politicisation or discrimination and risk to be based on **not corroborated information** and, finally, lead to **false positive results** (Babuta, Oswald and Rinik, 2018).

THE OPPORTUNITY: LAWFUL PROFILING FOR LEAS

In order to overcome such risks, and therefore ensure a beneficial application of OSINT tools within the framework of radicalisation and terror-related crimes, two actions should be carried out. Firstly, LEAs should ensure that their **profiling** activities are **lawful** and **admissible** by meeting four criteria. Namely, they must have a **legal basis** in national or European law, that stipulates possible limitations of the fundamental rights and its correlated standards (i.e. clarity, predictability, quality); they must have a **legitimate**, **appropriate** and **legally valid purpose**; they must be **necessary** and ensure a **fair balance** between the purpose and the means of the preventive activities.

These principles are stressed heavily by the Court of Justice of the European Union (2012) that considers the collection of data in the context of "monitoring" and profiling without judicial authorisation as an interference with the **Articles 7** and **8** of the Charter of Fundamental Rights of the European Union. Equally, the European Commission declared any profiling that “does not pursue a legitimate aim or if there is no reasonable relationship of proportionality between the means employed and the aim pursued" as illegal (European Commission against Racism and Intolerance, 2017).

Secondly, OSINT tools should be integrated with other factors beyond individual ones. Agreeing with the theory proposed by Doosje et al. (2016), according to which radicalisation is a **multi-factorial process** generally categorised into three levels (i.e. the micro or individual level, the meso level (such as group dynamics or identity) and the macro level (such as the effects of globalisation, conflicts and modernisation), OSINT tools should carry out a **two-level analysis**, firstly focusing on macro and meso root causes and, only when a specific suspect and crime are identified, shifting to analysis on an individual level.

More specifically, in order to analyse meso-factors, an ideal OSINT tool could integrate the identification of the extremist movement the suspect is supporting or the individual's identity context, the mapping of sub-cultural ecosystems, and social geography through case analysis. The latter could explain how subcultures find an adequate path towards violence and, more specifically, towards terror-related crimes, through the visualisation of a model. As per macro-factors, a key element could be identification of critical places (i.e. geographical areas, countries, cities) through an analysis of social indicators such as the increase in the targets of radicalisation or terror-related crimes; the increase in offenders or radicalised individuals in a specific area; the increase of provocations or extremist messages; and the decrease of security forces controls in a specific area. This technique could identify the generators of crime (e.g. political or religious events), the attractors of crime (e.g. places known to terrorists), the crime clearance (e.g. lack of regulation) and crime-neutral areas. By doing so, policing and private actors would not only ensure a proper use of the OSINT tools but they would also have more effective results, avoiding discriminatory security practices that do more harm than good.

CONCLUSION

All in all, the raising interest towards the area of prevention drove to the development of technologies capable of detecting and preventing individuals from committing a crime. This is specifically true when looking at the cases of radicalisation or terror-related crimes, where policing agencies put a major effort into developing indicators to detect radical behaviours and at-risk individuals. While existing OSINT tools, such as MEDUSA®, Maltego, 12 Analyst Notebook and Huntsman SPIDA, seem to be promising, they lack a multi-factorial perspective. This article proposes the other factors beyond individual characteristics be integrated into existing tools, allowing them to cover other root causes of radicalisation such as group dynamics and identity (meso factors) and the effects of international events or phenomena such as globalisation or conflicts (macro factors). This dual and complex analysis,capable of combining qualitative and quantitative data, would extensively avoid false positive cases and discriminatory analysis.

REFERENCE LIST

Babuta, A., Oswald, M. and Rinik Christine (2018). *Machine Learning Algorithms and Police Decision-Making. Legal, Ethical and Regulatory Challenges*, Royal United Services Institutes. Retrieved from: https://rusi.org/publication/whitehallreports/machine-learning-algorithms-and-police-decision-making-legal-ethical.

Bianchi, S., Ladu, M. and Bianchi, S. (2019). Radicalisation: No Prevention Without 'Juridicalisation'. In: Akhgar, B., Wells, D., Blanco, J.M. (Ed.) *Investigating Radicalization Trends*, London, UK: Springer Nature. Retrieved from: https://link.springer.com/book/10.1007/978-3-030-25436-0.

Cinelli, V. (2020). Crime Prevention and Predictive Analysis: The Italian Case, *Agenformedia*. Retrieved from: https://www.agenformedia.com/publication/crime-prevention-and-predictive-analysis-the-italian-case/.

Dean, G. (2007). Criminal Profiling in a Terrorism Context. In: Kocsis, R.N. (Eds). *Criminal Profiling*. Human Press. Retrieved from: https://doi.org/10.1007/978-1-60327-146-2_8.

Dinant, J.M. Lazaro, C. Poullet, Y. Lefever, N. and Rouvroy, A. (2008). *Application of Convention to the profiling mechanism*, Strasbourg: Council of Europe, p. 3. Retrieved from: http://www.crid.be/pdf/public/5945.pdf.

Doosje, B., Moghaddam, F.M., Kruglanski, A.W., de Wolf, A., Mann, L. and Feddes, A.R. (2016). Terrorism, radicalization and de-radicalization. *Current Opinion in Psychology*, 11, pp. 79-84.Retrieved from: https://www.sciencedirect.com/science/article/pii/S2352250X16300811.

European Commission against Racism and Intolerance (2017), *Standards*, Retrieved from: https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/ecri-standards.

European Union Charter of Fundamental Rights, art. 7, 8, 10 and 14, 2012, c362/02.

IBM (2019). *IBM 12 Analyst's Notebook*. Retrieved from: https://www.ibm.com/uk-en/marketplace/analysts-notebook.

Maltego (undated). *Homepage*. Retrieved from: https://www.maltego.com/.

MEDUSA (2019). *Homepage*. Retrieved from: https://www.medusa-labs.com/.

POINTDUTY (undated). *Web Data Collection*. Retrieved from: https://www.pointduty.com.au/SPIDA.

AGENFOR
INTERNATIONAL

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

AGENFORMEDIA.COM