ABSTRACT

The transition to a digital information society in the late 20th and early 21st centuries has fundamentally transformed how individuals acquire and disseminate information, express opinions, and interact with one another. This transformation has led to unprecedented volumes of information in digital open sources, with more personal data exposed than ever before.

This new era has significantly boosted the use of open-source intelligence (OSINT) among security and intelligence agencies (SISs) and law enforcement authorities (LEAs). Technological advancements have exponentially increased OSINT capabilities, enabling advanced software tools to browse, collect, merge, and analyse data from the online realm, uncovering patterns and relationships at an unprecedented level. OSINT is now exploited for various intelligence needs, from situational awareness to investigatory and preventive purposes.

However, this new OSINT environment has introduced new concerns, and exacerbated pre-existing ones. Historically, OSINT has been perceived as a discipline with few (if any) privacy-related constraints, due to the open nature of its sources. This perception, formed when OSINT primarily involved the translation of foreign broadcasts and newspapers, has been challenged in light of the new digital environment and the emergence of more complex and sophisticated technological capabilities.

Furthermore, the online environment has intensified challenges related to data reliability and accuracy, particularly with the rise of user-generated content platforms, digital disinformation, and hybrid warfare. In addition, advanced software has introduced issues such as human and algorithmic bias, as well as tool complexity and opacity, challenging the accountability of accurate OSINT outcomes. The reliance by SISs and LEAs on flawed conclusions derived from OSINT can lead to harms to individuals in various ways, such as impacting the right to privacy, right to non-discrimination, right to liberty and free movement, freedom of expression, assembly, and the right to a fair trial.

This dissertation examines these challenges and analyses whether European legislators provide adequate solutions and safeguards to address the privacy and data protection issues associated with modern OSINT practices. To this end, it examines (a) the concept, evolution and state of the art of OSINT practices, (b) the privacy implications

of these practices, (c) the current European landscape addressing these impacts, and (d) proposes several recommendations for policy-makers and practitioners.

Keywords: *OSINT, privacy in open spaces, openly available information, Convention 108, data protection, intelligence services, law enforcement authorities*