**TRENDS IN SHARED SECURITY DATA**

**Abstract**: The current paper seeks to explore the development of the legal framework related to the European Data Strategy in the field of security and related to the exchange of datasets between law enforcement authorities. The text will delve into and compare the categories of open data and data available in open-source intelligence investigations.

**Keywords**: data; interoperability; open data; security

A Europe of innovation, a Europe for citizens - these are some of the guiding messages derived from the strategic documents adopted in the framework of the last European Commission mandate (2019-2024), and the European Data Strategy1 is no exception. In this respect, improving interoperability between different sectors is emerging as one of the key challenges for the European Union by the end of the decade, as this is evident both in the systematic ring-fencing of funds and in the dynamic development of harmonised legislation in the field, aiming to impose uniform standards to ensure the sharing of data (for example - Regulation (EU) 2024/9032).

Of particular interest is the strengthening of interoperability capacity within the area of freedom, security and justice in the European Union (EU). The creation of the so-called EU Innovation Hub for Internal Security3, bringing together the leading EU agencies and institutions with competence in the sector and the Commission's vision of developing Common European Data Spaces4 provide the basis for enhanced cross-border cooperation tailored to the operational needs of law enforcement authorities. A key opportunity, from a legal and ethical perspective, is the alignment of the requirements and rules for the creation and dissemination of datasets in the security sector by the law enforcement authorities themselves, the definition of a more limited scope of openness of the data in relation to generally applicable policies, and stricter requirements for the technological systems ensuring the creation and interlinking of datasets in view of the applicable pan-European and national legal framework for the respective hypothesis within the security sector (Scerri, Tuikka, Vallejo, Curry 2022, p. 340). The European Parliament Resolution on the fundamental rights implications of big data5 should also be recalled here and the recommendation set out in its paragraph 29 that the procurement of data processing models, tools and programmes should be formulated and verified in a way that ensures that the processing of personal data is limited to the minimum necessary and that the principles of non-discrimination and privacy are respected. It is extremely challenging not only for businesses, but also for law enforcement authorities to handle data sets in full compliance with the EU legal framework due to the systematic perception of data protection as a fundamental principle (Kusak 2022, p. 214).

While there are a number of risks to using large data sets for national and alliance security purposes - including the creation of "bias" in automated systems based on statistically available information as a result of pre-existing structural discrimination (Crawford, Schultz, pp. 103-104); the possibility of de-anonymization of data (Bormida 2021, p. 76; Boté, Térmens 2019, p. 331), or the contradictions arising when granting access to databases containing biometric data (Hert, Gutwirth, pp. 5-7), among others, innovation in the field should be encouraged, and rules already long known to law enforcement agencies, such as allowing data to be exchanged only for law enforcement purposes and where assurances are created that the receiving party will also use it for the same purpose (Hert, Gutwirth 2006, p. 4), can be applied to them. The requirement to achieve interoperability, otherwise aimed at covering the widest possible range of interested organisations, should here be looked at as intra-sectoral because of the particular protection of information that can be segregated and would be useful to law enforcement entities in the form of shared data.

Effective countering of cybercrime and the development of digital forensics are among the main reasons to strive for the development of shared datasets for law enforcement purposes. For example, human trafficking, pornography, child pornography, homicides, drug dealing, terrorist activity, the cybercrime market, and cryptocurrency exchanges are the top eight most common crimes that can be investigated with the help of analytics programs such as the so-called Surface Web, Deep Web, and Dark Web (Nazah, Huda, Abawaju, Hassan 2020, pp. 171800-171801, 171802). The collecting, interpreting, and verifying the credibility of data on the Internet, on the other hand, is a self-contained process (Böhm, Lolagar 2021, p. 325) that can be secured in a variety of ways, but often for law enforcement agencies themselves, open data work and "open source" based investigation prove to be highly effective mechanisms precisely in the fight against cybercrime and crimes mediated in the virtual environment (Ivanjko, Dokman 2019; Yadav, Kumar, Singh, p. 12420). Information becomes valuable to investigations when it is collected in a timely manner and for a specific purpose, and when it is explored within a broad context of related data (Williams, Blum 2018, p. 8, 10) - precisely the goal pursued by the development of shared datasets for law enforcement purposes.

A distinction should be made here between open data and data collected in investigations based on open-source intelligence (OSINT), the former being progressively regulated at the European Union level6. The open data doctrine builds on the concept on access to public information, that has already been developed over the years (Wessels, Finn, Sveinsdottir, Wadhwa 2017, p. 50), practically deriving principles to which data held by the executive should conform and be made public in order to engage citizens in public processes. Open data is data that can be freely used, reused and disseminated by anyone and, at most, a requirement to attribution and sharing on the same terms can be imposed on developments7 based on it. Open data should be complete, primary-sourced, timely, accessible, machine-readable, non-discriminatory, open-format, and unlicensed or open-licensed8 (Wessels, Finn, Sveinsdottir, Wadhwa 2017, p. 51). The main goal behind the development of open data legislation is to democratize access to high-value datasets to ensure their reuse9. A similar trend, for example, has been observed in other protected categories of data, whose access and reuse are regulated by the Data Governance Act10.

Open-source investigation, on the other hand, is a well-established mechanism for collecting, analyzing, and disseminating data in a way that serves intelligence purposes. If within the 20th century it was mostly centered around the tracking of foreign media in order to obtain strategic information about the enemy's tactical intentions, the last twenty years have seen the so-called "second generation" of OSINT centered around the use of highly effective linguistic, geospatial, network and visual analysis tools. The use of OSINT is applied in a number of scenarios such as situational awareness, terrorist threat risk analysis, investigation of trafficking and smuggling, and online fraud (Yadav, Kumar, Singh 2023, p. 12420).

Handling such large volumes of information requires adherence to high ethical standards and repeated verification of the processed data. Preserving contextual integrity is essential when verifying the credibility of information, especially when it has been collected in the course of an investigation (Forgó et al. 2020, p. 383). Adhering to a standardized system for describing datasets and their origin is also key to tracking potential data compromise during future aggregated analysis (Shanley et al. 2024, p. 2154). As previously stated, privacy and data protection considerations are overriding within European law, and while law enforcement authorities enjoy certain exemptions, the development of shared datasets for sectoral purposes will fall within the generally applicable limitations of both the General Data Protection Regulation11 and Directive (EU) 2016/68012. Thus, within the framework of the TESSERA13 project, in which the Law and Internet Foundation is a participant, a key objective is to define the requirements for interoperability and the ability to share datasets for the needs of law enforcement authorities, as well as to provide recommendations on the introduction of new policies in the field. The challenges related to defining data categories and developing technological models capable of working with them clearly highlight the need for further advancement of harmonised legislation within the third pillar, in order to enable the creation of interconnections between datasets rather than generating 'digital waste'14 from unsupported and unlinked data collections.

In conclusion, the legal and strategic framework for data use in the EU is rapidly evolving in its effort to position the Union as a leader in innovation. However, this dynamic often necessitates the adoption of numerous secondary legislative acts to ensure the correct application of the provisions and, at times, raises concerns about the industry's ability to respond promptly and sustain a comparable level of innovation. Nevertheless, the planned development of the Common European Data Spaces offers significant opportunities for advancing sectoral policies and establishing data handling standards aligned with the needs of sectors such as freedom, security, and justice

**FOOTNOTES:**

1. **COMMUNICATION FROM THE COMMISSION** TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS ”A European strategy for data”, COM/2020/66 final, 19.02.2020, Brussels

2. **Regulation (EU) 2024/903** of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), *OJ L, 2024/903, 22.3.2024*

3. **EU Innovation Hub for Internal Security**. Europol, [online], 04.06.2024. Available on: https://www.europol.europa.eu/operations-services-innovation/ innovation-lab/eu-innovation-hub-for-internal-security

4. **COMMUNICATION FROM THE COMMISSION** TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS ”A European strategy for data”, COM/2020/66 final, 19.02.2020, Brussels; **COMMUNICATION FROM THE COMMISSION** TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS ”Action Plan on synergies between civil, defence and space industries”, COM/2021/70 final, 22.02.2021, Brussels

5. **European Parliament resolution** of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)), *OJ C 263, 25.7.2018, p. 82–89*

6. **Directive (EU) 2019/1024** of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), *OJ L 172, 26.6.2019, p. 56–83*

7. Open Definition: Defining Open in Open Data, Open Content and Open Knowledge. Open Knowledge Foundation, [online]. Available on: https://opendefinition. org/od/2.1/en

8. See more at address: https://public.resource.org/8\_principles.html

9. **Directive (EU) 2019/1024** of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), *OJ L 172, 26.6.2019, p. 56–83*

10. **Regulation (EU) 2022/868** of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), *OJ L 152, 3.6.2022, p. 1–44*

11. **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–88*

12. **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016, p. 89–131*

13. The project is co-funded by the European Union under the ISF Programme, GA No. 101145802. The views and opinions expressed in this publication are entirely those of the author and do not necessarily reflect the views and opinions of the European Union or the European Commission. Neither the European Union nor the European Commission is responsible for them.

14. The author's analogy with cosmic waste.

**REFERENCES:**

**Da Bormida, M.** The Big Data World: Benefits, Threats and Ethical Challanges. *Ethical Issues in Covert, Security and Surveillance Research (Advances in Research Ethics and Integrity, Vol. 8).* Leeds : Emerald Publishing Limited, 2021, pp. 71-91.

**Boté, J., Térmens, M.** *Reusing Data: Technical and Ethical Challenges.* 6, 2019, DESIDOC Journal of Library & Information Technology, Vol. 39, pp. 329-337.

**Böhm, I., Lolagar, S.** *Open Source Intelligence: Introduction, legal, and ethical considerations.* s.l. : Springer, 2021, International Cybersecurity Law Review, Vol. 2, pp. 317-337.

**Crawford, K., Schultz, J.** Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review.* 2013, Vol. 55, 93, pp. 93-128.

**De Hert, P., Gutwirth, S.** *Interoperability of Police Databases Within the EU: An Accountable Political Choice?* s.l. : Tilburg University, 2006, Tilburg University Legal Studies Working Paper No. 003/2006, TILT Law & Technology Working Paper Series No. 001/2006.

**Forgó, N., et al.** *An ethico-legal framework for social data science.* 2020, International Journal of Data Science and Analytics, Vol. 11, pp. 377-390.

**Ghioni, R., Taddeo, M., Floridi, L.** *Open source intelligence and AI: a systematic review of the GELSI literature.* s.l. : Springer, 2023, AI & Society.

**Ivanjko, T. Dokman, T.** *Open Source Intelligence (OSINT): Issues and Trends.* 2019. INFuture2019: Knowledge in the Digital Age.

**Kusak, M.** *Quality of data sets that feed AI and big data applications for law enforcement.* s.l. : Springer, 2022, ERA Forum, Vol. 23, pp. 209-219.

**Nazah, S., Huda, S., Abawaju, J., Hassan, M.** *Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach.* 2020, IEEE Access, Vol. 8, pp. 171796-171819.

**Scerri, S., Tuikka, T., de Vallejo, I.L., Curry, E.** Common European Data Spaces: Challanges and Opportunities. *Data Spaces: Design, Deployment and Future Directions.* s.l. : Springer, 2022, pp. 337-357.

**Shanley, D., et al.** *Getting real about synthetic data ethics.* s.l. : EMBO reports Volume 25, 2024. pp. 2152-2155.

**Wessels, B., Finn, R., Sveinsdottir, T., Wadhwa, K.** *Open Data and the Knowledge Society.* s.l. : Amsterdam University Press, 2017. ISBN: 978-94-6298-018-1.

**RAND Corporation (Williams, H.J., Blum, I.).** *Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise.* s.l. : RAND Corporation, 2018. ISBN: 978-0-8330-9883-2.

**Yadav, A., Kumar, A., Singh, V.** *Opensource intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security.* 2023, Artifcial Intelligence Review, Vol. 56, pp. 12407-12438.

**TRENDS IN SHARED SECURITY DATA**

**Abstract:** *The current paper seeks to explore the development of the legal framework related to the European Data Strategy in the field of security and related to the exchange of datasets between law enforcement authorities. The text will delve into and compare the categories of open data and data available in open-source intelligence investigations.*

**Keywords:** *security; data; open data; interoperability*

Information on the author:

Martina Ilieva Bogdanova, Law and Internet Foundation, ORCiD ID: [0009-0001-3485-2362](https://orcid.org/0009-0001-3485-2362)

E-mail: [martina.bogdanova@netlaw.bg](mailto:martina.bogdanova@netlaw.bg)