REGULATORY FRAGMENTATION AND CYBER RISK MANAGEMENT IN BOSNIA AND HERZEGOVINA: BETWEEN FORMAL HARMONIZATION AND OPERATIONAL RESILIENCE

Muhamed Ćosić[1*], Edin Alić[2]

[1]Unversity PIM, Faculty of Computer Sciences, despota Stefana Lazarevića bb, 78000 Banja Luka, Bosnia and Herzegovina, drmuhamedcosic@gmail.com
University of Vitez, Školska 23, 72270 Travnik, Bosnia and Herzegovina, edin.alic@unvi.edu.ba

ABSTRACT

The relationship between formal regulatory harmonization and actual cyber resilience in Bosnia and Herzegovina is examined within the context of the contemporary regulatory model of the European Union. Through the GDPR and NIS2, the EU has established a cyber risk management system based on risk assessment, incident reporting obligations, supervision, and managerial accountability. This framework is further developed through sectoral and horizontal acts such as DORA, the CER Directive, the Cybersecurity Act, and the Cyber Resilience Act. In 2025, Bosnia and Herzegovina adopted a new Law on Personal Data Protection, marking a significant step toward alignment with European standards and the normative modernization of the domestic regulatory framework. However, normative modernization alone does not guarantee a higher level of cyber resilience. The complex constitutional structure, fragmentation of competences, the absence of a unified cybersecurity framework, and uneven institutional capacities create an implementation gap between prescribed obligations and their actual enforcement. The analysis shows that resilience depends on effective coordination, professionally and technically capable supervision, operational CERT/CSIRT capacities, a standardized incident reporting system, and the clear integration of cyber risk into organizational governance structures. Without institutional strengthening, functional inter-institutional cooperation, and consistent enforcement of regulations, harmonization remains largely formal, while actual cyber resilience remains limited, partial, and unevenly developed.

Keywords: cybersecurity, regulatory fragmentation, GDPR, NIS2, Bosnia and Herzegovina, Personal Data Protection Agency (AZLP), CERT/CSIRT, risk management.