

CRIMES CIBERNÉTICOS E A INFOÉTICA

CYBERCRIMES AND INFOETHICS

Rondineli Gama Saad

Universidade de São Paulo, USP
SciELO Brasil

E-mail: rondineli.saad@usp.br

ORCID: 0009-0004-2527-0821

RESUMO

Este trabalho analisa os crimes cibernéticos a partir da INFOÉTICA desenvolvida por Luciano Floridi, compreendendo-os não apenas como ilícitos técnicos ou jurídicos, mas como fenômenos que afetam estruturalmente a integridade da infosfera contemporânea. A pesquisa adota abordagem qualitativa, de natureza teórico-analítica, fundamentada em revisão bibliográfica e análise interpretativa de casos empíricos relacionados à privacidade, desinformação, propriedade intelectual, acesso à informação e segurança digital. O referencial teórico articula as contribuições de Floridi (2013; 2023) com autores como Helen Nissenbaum, Shoshana Zuboff, Manuel Castells, Lawrence Lessig, Cass Sunstein e Wardle e Derakhshan. A análise demonstra que os cinco pilares éticos da INFOÉTICA operam de forma interdependente, produzindo impactos simultâneos sobre diferentes dimensões da vida social, política e institucional. Os casos examinados evidenciam que práticas como vigilância digital, ataques ransomware, exploração massiva de dados, desinformação automatizada e conflitos envolvendo inteligência artificial generativa ultrapassam o domínio tecnológico e comprometem condições fundamentais de confiança, participação e estabilidade informacional. Conclui-se que abordagens exclusivamente técnicas ou regulatórias são insuficientes para enfrentar a complexidade dos crimes cibernéticos, exigindo modelos de governança capazes de articular ética, tecnologia e gestão da informação na preservação da integridade da infosfera.

Palavras-chave: INFOÉTICA; ética da informação; crimes cibernéticos; infosfera; governança informacional; segurança da informação.

ABSTRACT

This study analyzes cybercrimes through the INFOETHICS developed by Luciano Floridi, understanding them not only as technical or legal offenses but as phenomena that structurally affect the integrity of the contemporary infosphere. The research adopts a qualitative, theoretical-analytical approach, grounded in a literature review and interpretative analysis of empirical cases related to privacy, disinformation, intellectual property, access to information, and digital security. The theoretical framework brings together the contributions of Floridi (2013; 2023) and authors such as Helen Nissenbaum, Shoshana Zuboff, Manuel Castells, Lawrence Lessig, Cass Sunstein, and Wardle and Derakhshan. The analysis demonstrates that the five ethical pillars of INFOETHICS operate interdependently, producing simultaneous impacts on different dimensions of social, political, and institutional life. The cases examined show that practices such as digital surveillance, ransomware attacks, large-scale data exploitation, automated disinformation, and conflicts involving generative artificial intelligence go beyond the technological domain and compromise fundamental conditions of trust, participation, and informational stability. It is concluded that exclusively technical or regulatory approaches are insufficient to address the complexity of cybercrimes, requiring governance models capable of integrating ethics, technology, and information management to preserve the integrity of the infosphere.

Keywords: INFOETHICS; information ethics; cybercrimes; infosphere; information governance; information security.