National Conference on Recent Advances in Science, Engineering, Humanities, and Management (NCRASETHM - 2024)
28th January, 2024, Banquet, Noida, India.

CERTIFICATE NO : NCRASETHM /2024/C0124145

IMPACT OF NATIONAL AND INTERNATIONAL LEGAL FRAMEWORKS TOWARDS CYBER CRIME

AMSHALA SHANKARAIAH

Research Scholar, Ph. D. in Law
P.K. University, Shivpuri, M.P., India.

ABSTRACT

National and international legal frameworks play a crucial role in combating cybercrime, shaping strategies to prevent, detect, and penalize such offenses. National laws are essential for defining cybercrime and establishing legal guidelines for prosecution. Countries often create stringent regulations to protect data privacy and ensure that law enforcement can respond effectively to cyber incidents. For example, legislation like the General Data Protection Regulation (GDPR) in the European Union has set global standards for data protection, influencing legal frameworks worldwide. Similarly, in countries like the United States and India, laws such as the Cybersecurity Information Sharing Act and the Information Technology Act establish regulations for addressing online fraud, hacking, and data breaches. On an international level, cooperation is necessary to combat cybercrime that transcends national borders. Frameworks like the Budapest Convention on Cybercrime, the first international treaty addressing internet crimes, facilitate collaboration among nations to tackle global cyber threats. Such international agreements foster cross-border investigations and data sharing, essential for pursuing cybercriminals who operate in multiple jurisdictions. However, the effectiveness of these frameworks depends on the willingness of nations to cooperate and harmonize laws, which can be challenging due to differing legal systems and priorities. Despite advancements, continuous efforts are needed to strengthen these frameworks and adapt them to the evolving nature of cyber threats.