

How legislation deals with emerging cybercrime: A digital security perspective in Ireland

Cathrine Friend

Cybercrime legislation in Ireland is still in its infancy and needs an effective and consistent constitution and framework to ensure accountability and action. Cybersecurity today faces difficulties and controversies that go beyond technology capabilities; the normalization of cybercrime, personal and international communication and trade obstruction, information validity concerns and purposeful misuse. Therefore, defining cybercrime legislation through a legal review of current Irish legislation of technology related crimes and understanding the experiences of digital security practitioners with relevant legislation is important for civil, criminal and national security. This research addressed professional experiences and opinions of security practitioners in the field of cybercrime legislation through qualitative surveys and interviews as well as a review of current legislation in Ireland. Primary emergent themes were professional and public awareness and education, perception of seriousness and prioritization of resources for more “serious” crimes, jurisdiction, technology use and accountability. Secondly, this research has explored themes in current legislation in Ireland under data access and harmful communication. This cross-discipline research will contribute to Irish psychological and legal understandings of cybercrime regulation and technology use today and ultimately, create recommendations from academics and practitioners to improve current legal approaches to cybercrime regulation.