1. Record Nr. UNINA9910831004403321

Autore	Carneiro Pacheco de Andrade Francisco António
Titolo	Legal Developments on Cybersecurity and Related Fields / / edited by Francisco António Carneiro Pacheco de Andrade, Pedro Miguel Fernandes Freitas, Joana Rita de Sousa Covelo de Abreu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	9783031418204 3031418204
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (341 pages)
Collana	Law, Governance and Technology Series, , 2352-1910 ; ; 60
Altri autori (Persone)	Fernandes FreitasPedro Miguel de Sousa Covelo de AbreuJoana Rita
Disciplina	005.8026
Soggetti	Information technology - Law and legislation Mass media - Law and legislation Law - Europe Criminal law Data protection IT Law, Media Law, Intellectual Property European Law Criminal Law and Criminal Procedure Law Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Legal Developments on Cybersecurity and Related Fields: Introductory notes and presentation -- PART I – CYBERSECURITY, CYBERDEFENCE AND LAW -- Getting critical. Making sense of the EU security framework for cloud providers -- Cyber operations targeting space systems. Legal questions and the context of privatisation -- A legal assessment of the concept of risk in reversible operations through cyber and electronic means -- Knowledge management and continuous improvement in cyberspace -- Information security metrics: challenges and models in an all-digital world -- Cyberterrorism and the Portuguese counter-terrorism act -- PART II – CYBERSECURITY AND LAW: SPECIFIC TOPICS -- Towards cybersecurity regulation of software

in the European Union -- The importance of the computer undercover agent as an investigative measure against cybercrime: a special reference to child pornography crimes -- Post-Mortem data protection and succession in digital assets under Spanish law -- The suitability of the regime oftechnological measures for copyright protection in the face of modern cybersecurity risks -- Digital signatures and quantum computing -- No words needed? Emojis as evidence in judicial proceedings -- PART III – CYBERSECURITY, ETHICS AND FUNDAMENTAL RIGHTS -- Bug bounties: ethical and legal aspects -- Profiling and cybersecurity: a perspective from fundamental rights' protection in the EU -- Legal developments on smart public governance and fundamental rights in the digital age -- Biometric signatures in the context of Regulation (EU) nr. 910/2014 and the general data protection regulation: the evidential value and anonymization of biometric data -- Cybersecurity issues in electronic communications and some insights on digital literacy and technological infrastructures' demands – anticipations of the European Digital Decade through the lens of a Declaration on digital rights and principles.

Sommario/riassunto

This book presents a fresh approach to cybersecurity issues, seeking not only to analyze the legal landscape of the European Union and its Member States, but to do so in an interdisciplinary manner, involving scholars from diverse backgrounds – ranging from legal experts to ICT and engineering professionals. Cybersecurity requirements must be understood in a broader context, encompassing not just conventional aspects, but also emerging topics. This can only be achieved through an interdisciplinary approach. Indeed, cybersecurity should be consistently considered in relation to cybercrime and/or cyber defense, while examining it through the lens of specific domains that are intertwined with various legal fields. Moreover, it is crucial to uphold ethical standards and safeguard fundamental rights, particularly regarding personal data protection. By adopting this comprehensive perspective, the significance of cybersecurity in the exercise of public authority becomes apparent. It also plays an essential role in upholding the fundamental values of both individual Member States and the EU as a whole, such as the rule of law. Moreover, it fosters trust, transparency, and effectiveness in market relations and public administration interactions. In turn, the book draws on the expertise of its authors to provide insights into ICT components and technologies. Understanding these elements holistically is essential to viewing every "cyber" phenomenon from a legal standpoint. In addition to the holistic and interdisciplinary approach it presents, the book offers a captivating exploration of cybersecurity and an engaging read for anyone interested in the field.