1. Record Nr. UNINA9910918695503321

Autore	Hewage Chaminda
Titolo	Data Protection : The Wake of AI and Machine Learning
Pubbl/distr/stampa	Cham : , : Springer, , 2025 ©2024
ISBN	9783031764738 3031764730
Edizione	[1st ed.]
Descrizione fisica	1 online resource (309 pages)
Collana	Intelligent Technologies and Robotics Series
Altri autori (Persone)	YasakethuLasith JayakodyDushmantha Nalin K
Disciplina	005.8
Soggetti	COMPUTERS / Internet / Online Safety & Privacy MATHEMATICS / Probability & Statistics / General TECHNOLOGY & ENGINEERING / Electronics / General
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Sommario/riassunto

This book provides a thorough and unique overview of the challenges, opportunities and solutions related with data protection in the age of AI and ML technologies. It investigates the interface of data protection and new technologies, emphasising the growing need to safeguard personal and confidential data from unauthorised access and change.
The authors emphasize the crucial need of strong data protection regulations, focusing on the consequences of AI and ML breakthroughs for privacy and individual rights. This book emphasizes the multifarious aspect of data protection, which goes beyond technological solutions to include ethical, legislative and societal factors. This book explores into the complexity of data protection in the age of AI and ML. It investigates how massive volumes of personal and sensitive data are utilized to train and develop AI models, demanding novel privacy-preserving strategies such as anonymization, differential privacy and federated learning. The duties and responsibilities of engineers, policy makers and ethicists in minimizing algorithmic bias and ensuring ethical AI use are carefully defined. Key developments, such as the influence of the European Union's General Data Protection Regulation

(GDPR) and the EU AI Act on data protection procedures, are reviewed critically. This investigation focusses not only on the tactics used, but also on the problems and successes in creating a secure and ethical AI ecosystem. This book provides a comprehensive overview of the efforts to integrate data protection into AI innovation, including valuable perspectives on the effectiveness of these measures and the ongoing adjustments required to address the fluid nature of privacy concerns. This book is a helpful resource for upper-undergraduate and graduate computer science students, as well as others interested in cybersecurity and data protection. Researchers in AI, ML, and data privacy as well as data protection officers, politicians, lawmakers and decision-makers will find this book useful as a reference.