1. Record Nr. UNINA9910629294503321

Autore	Torra Vicenc
Titolo	Guide to Data Privacy : Models, Technologies, Solutions / / by Vicenç Torra
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	9783031128370 9783031128363
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (323 pages)
Collana	Undergraduate Topics in Computer Science, , 2197-1781
Disciplina	323.448 005.8
Soggetti	Data protection - Law and legislation Data protection Cryptography Data encryption (Computer science) Information technology - Moral and ethical aspects Computers and civilization Privacy Data and Information Security Cryptology Information Ethics Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. Introduction -- 2. Basics of Cryptography and Machine Learning -- 3. Privacy Models and Privacy Mechanisms -- 4. User's Privacy -- 5. Avoiding Disclosure from Computations -- 6. Avoiding Disclosure from Data Masking Methods -- 7. Other -- 8. Conclusions.
Sommario/riassunto	Data privacy technologies are essential for implementing information systems with privacy by design. Privacy technologies clearly are needed for ensuring that data does not lead to disclosure, but also that statistics or even data-driven machine learning models do not lead to disclosure. For example, can a deep-learning model be attacked to

discover that sensitive data has been used for its training? This accessible textbook presents privacy models, computational definitions of privacy, and methods to implement them. Additionally, the book explains and gives plentiful examples of how to implement—among other models—differential privacy, k-anonymity, and secure multiparty computation. Topics and features: Provides integrated presentation of data privacy (including tools from statistical disclosure control, privacy-preserving data mining, and privacy for communications) Discusses privacy requirements and tools for different types of scenarios, including privacy for data, for computations, and for users Offers characterization of privacy models, comparing their differences, advantages, and disadvantages Describes some of the most relevant algorithms to implement privacy models Includes examples of data protection mechanisms This unique textbook/guide contains numerous examples and succinctly and comprehensively gathers the relevant information. As such, it will be eminently suitable for undergraduate and graduate students interested in data privacy, as well as professionals wanting a concise overview. Vicenç Torra is Professor with the Department of Computing Science at Umeå University, Umeå, Sweden.