



UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Privacy and Data Protection

2526-2-F9102Q040

Aims

The aim of the course is to provide an overview of the fundamental concepts related to privacy and data protection, considering both structured data and unstructured content. To this end, the course will address issues related to the secure and privacy-aware dissemination of data, secure and privacy-aware computation, and protection in emerging scenarios (e.g., considering artificial intelligence, machine learning, and online social platforms). Given the intersection between privacy and intellectual property to ensure a correct use of information, for example in generative AI systems, the course will also address the issue of intellectual property protection, as an indispensable complement to a conscious management of data and information.

At the end of the course, the student will be able to: understand the principles and challenges of data protection and intellectual property; analyze cases and identify appropriate tools and methods for their management; apply techniques and solutions for information protection in complex digital contexts.

Contents

- Secure and privacy-aware data dissemination.
- Secure and privacy-aware computations.
- Protection in emerging scenarios.
- Protection of intellectual property.

Detailed program

Secure and privacy-aware data dissemination.

- Anonymization models and techniques

- Syntactic and semantic anonymization
- Data fragmentation models and techniques

Secure and privacy-aware computations.

- Controlled execution of computations respecting data usage restrictions
- Integrity in computation

Protection in emerging scenarios.

- Protection in digital data markets
- Modeling and fulfillment of user requirements
- Query protection (IR systems and generative AI prompts)
- Privacy in online social platforms

Protection of intellectual property.

- Patents
- Trademark
- Copyright and interaction with generative AI systems
- Patent databases (notes)

Prerequisites

Basic notions of computer science and cybersecurity.

Teaching form

48 hours, in-person teaching.

Textbook and teaching resource

Scientific articles and slides available on the course website.

Semester

First semester.

Assessment method

The exam consists of a written test, on the entire program of the course. The test includes closed and open questions, and exercises. The indicative duration of the test is 90 minutes. The evaluation is expressed on a 0-30 scale, and takes into account the correctness, completeness and clarity of the answers to the questions and exercises. During the written test, the use of any material is not permitted.

There are no intermediate tests.

In order to access an exam session, it is necessary to enroll to the session by the official deadlines.

Office hours

By appointment, to be requested in advance by e-mail.

Sustainable Development Goals
