Information and technology law

LECTURE 1 – 23 SEPTEMBER 2024

FEDERICA CASAROSA – 2024/2025

Structure of the course

Main topics

- Definition of cybersecurity law
- The role of EU in cybersecurity regulation
  - Competence – governance structure
- EU Legislation
  - NIS directive and NIS 2 directive
  - Cybersecurity act
  - Cyber resilience act
  - AI Act
  - European Health Data Space regulation
- Interplay between security and data protection
  - GDPR
  - Data act
- Security and data protection in different technologies
  - IoT, Cloud computing, smart cars, digital wallet
- Cyber crime

Exams and presentation for attending students

Oral exam on all the topics of the course

Only for students attending the course (at least 70% of lectures – 14 sessions)

- group presentation (max 3 people) addressing one of the topics of the course in the last sessions of the course
  - Selection of topics by mid April

Definition of cybersecurity law

Categories of cyber-threats

Cyber-attacks have grown rapidly in scale, scope, and sophistication

Four different and overlapping threat-categories:

- Cyber War
- Cyber Espionage
- Cyber Terrorism and Cyber Vandalism
- Cybercrime

Cybersecurity

Cybersecurity is a term that covers a wide range of activities aimed at preventing and mitigating cyber-threats

It can be divided into

- Network and information security,
- fight against cybercrime, and
- cyber defense.

Cybersecurity law

According to J. Koos (*Defining Cybersecurity law*, 103 Iowa L. Rev. 985 (2018))

In order to define cybersecurity law we must answer five fundamental questions :

- (1) What are we securing?
- (2) Where and whom are we securing?
- (3) How are we securing?
- (4) When are we securing?
- (5) Why are we securing?

Cybersecurity law

(1) What are we securing?

- promote the **confidentiality**, **integrity**, and **availability** of information, systems, and networks.
- Cybersecurity is not confined only to data security
- Cybersecurity focuses not only on the protection of data, but also on the systems and networks of the public and private sector.

Cybersecurity law

Confidentiality: prevention of unauthorized disclosure of information

Integrity: guarantee that the message that is sent is the same as the message received and that the message is not altered in transit

Availability: guarantee that information will be available to the user in a timely and uninterrupted manner when it is needed regardless of the location of the user

Cybersecurity law

(2) Where and whom are we securing?

- Should law be focused only on on bolstering the security of military and civilian government systems?
- Should the laws apply also to private-sector cybersecurity?
  - Does Internet design provide for a different infrastructure for public and private sector?
    - NO!
- Any effective cybersecurity law regime will seek to secure both the public sector and private sector.

Cybersecurity law

(3) How are we securing?

- Hard law or soft law ?
  - Coercive laws deter inadequate cybersecurity whereas cooperative laws that provide incentives for companies and government agencies to invest in cybersecurity.

Cybersecurity law

(4) When are we securing?

- Should law focus on events that already have occurred, or should it attempt to build resilience to prevent future attacks?
- There is a need for a forward looking approach

Cybersecurity law

(5) Why are we securing?

- Three distinct types of harm that cybersecurity law should seek to avoid (or at least mitigate):
  - (1) harm to individuals
  - (2) harm to business interests
  - (3) harm to national security.

Added relevant features

Flexibility and adaptability of measures

Importance of human factor

Update vis-à-vis changing risks

Cooperation and Information sharing