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

There can be attacks to devices we now have connected to the internet and can be attacked by malicious actors. Interventions of legislation are needed to avoid the presence of vulnerabilities in the first place.

Categories of cyber-threats

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

Four different and overlapping threat-categories:

- Cyber War = cyber attacks to a nation that can create problems to infrastructures, government and cause deaths.
- Cyber Espionage
- Cyber Terrorism and Cyber Vandalism
- Cybercrime

Problem: as soon as you have regulations and legislations we have the tools to prevent cyberwar in advance.
But defining cyberwar is difficult: you need to know who carries out the attack and sanction them
It includes espionage to extract sensitive data, sabotage by stealing and destroying info or denial of service for core operations and sensitive websites.

The fact that you can attack without being there physically makes liability more difficult, it's difficult to ALLOCATE responsibilities.

Cyber war refers to the use of digital attacks by one nation or group to disrupt the computer systems of another nation or group. These attacks typically aim to cause significant damage to infrastructure, such as power grids, financial systems, military networks, or communication systems, with the intent to weaken or destabilize the opponent. Cyber war can involve activities like hacking, espionage, sabotage, and misinformation campaigns. It is considered a modern form of warfare, with potentially widespread consequences but often without the physical destruction seen in traditional warfare.

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, (how they are protected)
- fight against cybercrime, and
- cyber defense. (interplay between stakes)

Cybersecurity law

Connected to CIA. C = protect what should not be available to anyone
I = content won't be changed
A = if allowed, need access all the time to something

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.

↗ Not only focus on the content (of communication or else)

Cybersecurity law

Confidentiality: prevention of unauthorized disclosure of information

↳ ex: attack to the network when doc knows to change insulin dose

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

WE ARE SURE OF AUTHENTICITY OF MESSAGE AND SENDER

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? We can't think of something sector specific

- 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. = overall system

Take the example of cloud computing offering service to military. Sector specificity does not work.

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.

Hard law: some legal docs adopted by the government of a state that can be national or international. There are requirements and sanctions for non compliance. Soft law: the recipients of this type of rules will feel compelled to comply but do not receive a sanction if they aren't.

Hard is a strong intervention, there is the need of a system that enforces them. Tech is running faster than the law so guidelines are easier to manage because they do not require parliaments action.

Legislation should look at the environment and look at how it is inclined to comply. If we have companies with a level of security and no inclination a regulation is necessary. In softer structures, guidelines show a target that needs to be reached.

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

Be able to be resilient. 0 risk is not possible: control known risks, then if something happens we avoid disrupting events.

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 (companies have stopped for 2 days)
  - (3) harm to national security.

Added relevant features

- Flexibility and adaptability of measures
- Importance of human factor *
- Update vis-à-vis changing risks *2
- Cooperation and Information sharing *3

adaptable is the case: some sectors have different problems than others. Ex. doctor more prone to open attachments from colleagues.

↑ Hard law is easy but law is usually outdated.

↓ Flexibility: if I say "use this", for example cryptography algorithm, if the cracks what then it is gone over.

* Take into account that most problems come from humans making mistakes.

*2 impact assessment has to be recurrently to be aware of changing risks.

*3 One organization might not want to share their security problems to avoid reputation damage, but it needs to be pushed to incentivize learning from mistakes. EX: unknown vulnerability.

Reporting cybersecurity incidents should be incentivized.