Information and technology law course

LECTURE 10 + 12 – 24 AND 31 OCTOBER 2024

FEDERICA CASAROSA – 2024/2025

Conflict between security and privacy

Values protected within cybersecurity

identification and implementation of measures and techniques for the protection of information from

- unauthorized access,
- unauthorized use,
- unauthorized modification,
- unauthorized destruction,
- unauthorized disclosure or disruption

Values protected within cybersecurity

Security

Privacy

Fairness

Accountability

Security

Security is the state of being free from danger or threat

- Safety / security
  - safety is protection against accidental or unintentional danger whereas security is protection against intended harm
- absence of danger or threat

Privacy

informational privacy is about what information about a person is (not) known to, or shared with, others

Distinction between

- confidentiality or secrecy of data and
- control over what data is shared with whom

Fairness

Cybersecurity threats and measures impact differently on people

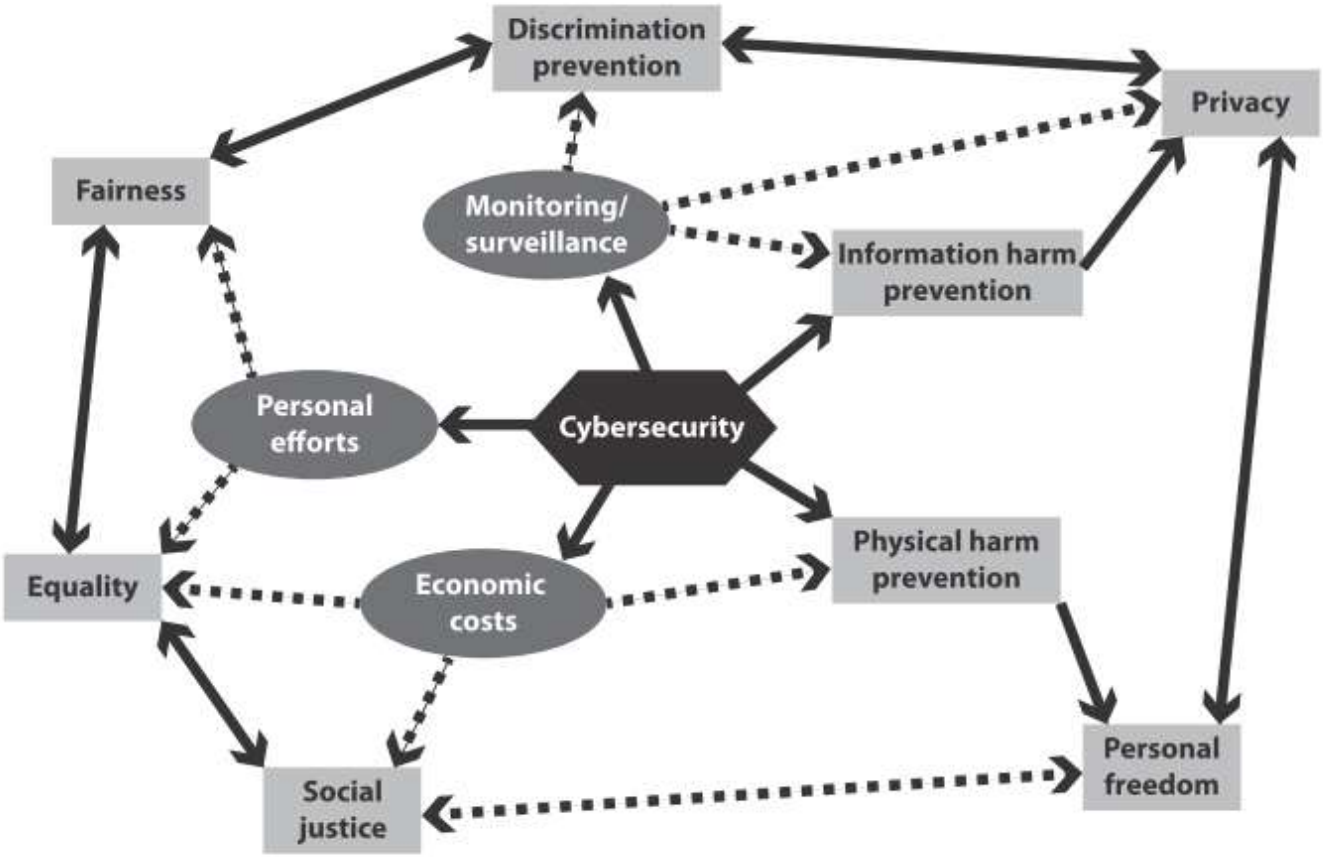
Connected issues of equality, justice, non-discrimination and democracy

Accountability

Connected issues of transparency, openness and explainability

Two possible scenarios:

- situations in which someone (allegedly) harms someone else, or infringes on the rights of that person
- situations in which there is a power imbalance between two agents and in which the more powerful is in the position to introduce rules or measures that may harm the less powerful ones


Discrimination prevention
Privacy
Fairness
Monitoring/ surveillance
Information harm prevention
Personal efforts
Cybersecurity
Physical harm prevention
Equality
Economic costs
Social justice
Personal freedom

Privacy v security

Sometimes security is attained at the cost of privacy

Sometimes security helps to achieve privacy

Privacy requires some degree of cybersecurity

Sometimes, privacy is attained at the cost of security

Sometimes, privacy contributes to security

GDPR – Data protection

Legal sources

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 04.05.2016, pp. 1-88.

Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196),

- Decreto legislativo 10 agosto 2018, n. 101.

Personal data – definition

Personal data are defined as information that identifies or makes identifiable, directly or indirectly, a natural person and that can provide information on their characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc.

- Data allowing direct identification and data allowing indirect identification
- Sensitive data and judicial data
- New data?
  - Data relating to electronic communications, geolocation data

Actors – definitions

Data subject is the natural person to whom the personal data relate (Article 4(1)(1) GDPR)

Data Controller is the natural person, public authority, company, public or private body, association, etc., who takes the decisions on the purposes and means of processing (Article 4(1)(7) GDPR)

Data processor is the natural or legal person whom the controller requires to perform specific and defined tasks of management and control on its behalf of the processing of data (Article 4(1)(8), GDPR)

Scope of application of GDPR

Regulation (EU) 2016/679 governs the processing of personal data

irrespective of whether or not it is carried out in the EU,

- either when carried out by data controllers or data processors established in the EU or in a place subject to the law of an EU Member State by virtue of public international law,
- or when the controller or processor is not established in the European Union but the processing activities concern
  - the offering of goods or the provision of services to the said data subjects in the European Union, irrespective of whether payment by the data subject is compulsory
  - the monitoring of their behaviour to the extent that this behaviour takes place within the European Union.

Rights of the data subject - 1

Right to access personal data

- The data subject has the right to ask the data controller
  - Whether his/her personal data have been processed, and if so
  - to obtain a copy of such data
  - to be informed about:
    - (a) the purposes of the processing; (b) the categories of personal data processed; (c) the recipients of the data; (d) the storage period of the personal data; (e) the origin of the personal data processed; (f) the identification details of the person processing the data (data controller, data processor, designated representative in the territory of the Italian State, recipients); (g) the existence of an automated decision-making process, including profiling; (h) the rights provided for by the Regulation

Rights of the data subject - 2

Right to rectification, erasure, restriction of processing, portability of personal data

- The data subject may request from the data controller that personal data be:
  - rectified (because they are inaccurate or not updated), possibly by supplementing incomplete information;
  - erased,
  - restricted in their processing
  - transferred to another data controller, if the processing is based on consent or on a contract concluded with the data subject and is carried out by automated means.

Right to be forgotten

right to erasure of one's personal data in an enhanced form:

Obligation for data controllers (if they have "made public" the personal data of the data subject) to inform other data controllers processing the deleted personal data of the erasure request, including "any link, copy or reproduction" (Art 17(2)).

Rights of the data subject - 3

Right to object

- You may object to the processing of your personal data:
- for reasons related to the particular situation of the data subject, to be specified in the request;
- (without having to state the reasons for the objection) when the data are processed for direct marketing purposes.

Data processing

Any processing of personal data must comply with the following principles

- Lawfulness, correctness and transparency of the processing, with regard to the person concerned
- purpose limitation of processing, including the obligation to ensure that any further processing is not incompatible with the purposes of data collection;
- data minimization: i.e., data must be adequate relevant and limited to what is necessary in relation to the purposes of the processing;
- accuracy and updating of data, including the timely deletion of data that are inaccurate in relation to the purposes of processing;
- storage limitation: i.e., data must be kept for no longer than is necessary for the purposes for which they are processed;
- integrity and confidentiality: it is necessary to ensure the adequate security of personal data being processed

Lawful data processing – legal basis

- Consent
- fulfilment of contractual obligations
- vital interests of the data subject or of third parties,
- legal obligations to which the holder is subject,
- public interest or exercise of public authority,
- overriding legitimate interests of the data controller or of third parties to whom the data are disclosed.

In the case of special categories of personal data, processing is prohibited, subject to specific conditions.

Consent

Validity of consent:

- the data subject has been informed about the processing of personal data (Articles 13 or 14 of the Regulation);
- has been expressed by the data subject freely, unambiguously and, if the processing pursues several purposes, specifically with regard to each of them.

The request is distinct from others addressed to the data subject

Consent need not be "documented in writing", nor is "written form" required

Information about data processing

It must be provided to the data subject before processing, i.e. before the data are collected.

The content is provided for in Articles 13 (1) and 14 (1)

- Identity of the data controller
- purpose of processing
- rights of the data subject
- contact details of the DPO
- legitimate interest
- Possible transfer to third countries
- period of data retention
- Right to lodge a complaint with the supervisory authority.
- Possible automated decision-making process

The information is in principle given in writing and preferably in electronic format

It must be comprehensible and transparent to the data subject, through the use of clear and plain language.

Data transfer to third countries

The transfer of personal data to countries outside the European Union is prohibited, except in the following cases:

- adequacy of the third country recognised by a decision of the European Commission;
- in the absence of a Commission adequacy decision, appropriate contractual or contractual safeguards
- in the absence of any other prerequisite, use of exceptions to the prohibition of transfer applicable in specific situations

Data protection Supervisory Authorities

- the Article 29 Working Party has become the European Board of Supervisors (EDPB)
- National supervisory authorities
  - The Italian Data Protection Authority
- One stop shop mechanism

The tasks and powers of the Supervisory Authorities

Monitoring and supervision (Art. 57 GDPR)

Advisory functions (Art. 57)

Investigative powers (art. 57 and 58)

Handling complaints (art. 77 GDPR)

Corrective powers (Art. 58 par.2 GDPR)

Complaints in case of violation

Complaint before Supervisory authority

- preliminary investigation and possible formal administrative procedure that may lead to the adoption of
  - Remedies
  - Administrative sanctions

The decision of the supervisory authority may be challenged in court

Administrative sanctions under the GDPR (Art. 83)

Administrative sanctions imposed by the DPA

The principles of administrative sanctions

Two groups of fines under the GDPR :

- ✓ up to 10/million or 2% of the annual global turnover if higher;
- ✓ up to 20/million or 4% of the annual global turnover if higher

The accountability principle in the data protection field

- The meaning of the principle

Controller and processors are obliged to ensure that the processing of personal data complies with the relevant rules and must be able to prove compliance at any time (art. 5 par. 2 GDPR)

- Data controller-focused
- Risk-based approach
- The 'elements' of accountability

The accountability principle under the GDPR

- Adoption of **codes of conduct, certification mechanisms, data protection seals and marks** as facilitating tools to prove compliance with the obligations of the controller (Art. 24 par. 3 GDPR) and of the processor (Art. 28 par. 5 GDPR) as well as mitigating factors of administrative sanctions (Art. 83 par. 2 GDPR)

- Records of processing activities (Art. 30 GDPR)

- Technical and organisational measures to ensure a level of security appropriate to the risk (Art. 32 GDPR)

- Notification of a personal data breach to the DPA (Art. 33 GDPR)

- Data Protection Impact Assessment (Art. 35 GDPR)

From ACCOUNTABILITY to LIABILITY

ARTICLE 82 GDPR (Right to compensation and liability)

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation **shall have the right to receive compensation from the controller or processor for the damage suffered.**

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.