
Ethical and Social Issues and regulations in Digital Systems

**Part of this material is based on Laudon& Laudon, Management
Information Systems, Chapter 4**

1

Agenda

- Ethical principles and IT
- Societal aspects
- Laws and regulations

2




Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems

- Ethics: **individual** judgement in decision making
- Society: reaching **consensus** on behaviors as a community
- Legal: **laws** are proposed, discussed, approved

4.3

Copyright © 2014 Pearson Education, Inc.

3




Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems
Understanding Ethical and Social Issues Related to Systems

- **Advances in data analysis techniques**
 - Profiling
 - Combining data from multiple sources to create dossiers of detailed information on individuals
 - Nonobvious relationship awareness (NORA)
 - Combining data from multiple sources to find obscure hidden connections that might help identify criminals or terrorists
- **Mobile device growth**
 - Tracking of individual cell phones

4.4

Copyright © 2014 Pearson Education, Inc.

4



Management Information Systems
 Chapter 4: Ethical and Social Issues in Information Systems

- **Basic concepts**
 - **Responsibility:**
 - Accepting the potential costs, duties, and obligations for decisions
 - **Accountability:**
 - Mechanisms for identifying responsible parties
 - **Liability:**
 - Permits individuals (and firms) to recover damages done to them
 - **Due process:**
 - Laws are well-known and understood, with an ability to appeal to higher authorities


4.5
Copyright © 2014 Pearson Education, Inc.

5

Ethics

©2025 Riproduzione riservata – Digital Technology

6




Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems
Understanding Ethical and Social Issues Related to Systems

- **Ethics**
 - Principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors

4.7 Copyright © 2014 Pearson Education, Inc.

7



Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems
Understanding Ethical and Social Issues Related to Systems

- **Information systems and ethics**
 - Information systems raise new ethical questions because they create opportunities for:
 - Intense social change, threatening existing distributions of power, money, rights, and obligations
 - New kinds of crime

4.8 Copyright © 2014 Pearson Education, Inc.

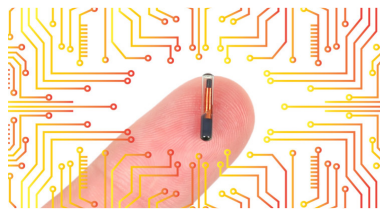
8

An example for discussion

Implantable RFIDs

<https://www.youtube.com/watch?v=DSmr-yuLLr4>

What if your company offers to microchip you? (2018)



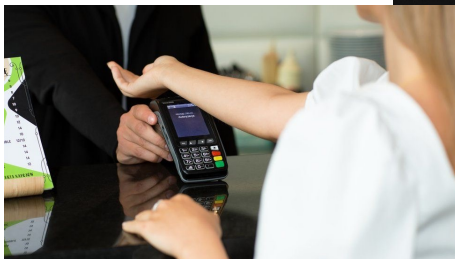
©2025 Riproduzione riservata – Digital Technology

9

9

Microchip implants

source: <https://www.bbc.com/news/business-61008730> April 2022



©2025 Riproduzione riservata – Digital Technology

10

10

What about other possible uses?

- <https://ceo-insight.com/innovation/can-chips-improve-your-health/> (Jan. 2020)
- Example Rapid identification to access medical records in emergencies
- Voluntary vs involuntary
- Need for laws
- In 2004, the US Food and Drug Administration (FDA) approved the use of [Applied Digital Systems microchip implants to store medical information](#). In 2018, the use of medical implanted tags offering continuous monitoring was also approved by the FDA to monitor blood glucose levels in diabetic patients.

©2025 Riproduzione riservata – Digital Technology 11

11

Papers

- The murky ethics of implanted chips
IEEE Spectrum, 2007
- Chipping at work, Iowa Law Review, 2018
- <https://ilr.law.uiowa.edu/print/volume-104-issue-3/chipping-in-at-work-privacy-concerns-related-to-the-use-of-body-microchip-rfid-implants-in-the-employeremployee-context/>

©2025 Riproduzione riservata – Digital Technology 12

12

Worried about identification?

- Think of tracking applications

©2025 Riproduzione riservata – Digital Technology 13

13


Mobile application data

- An MIT study by de Montjoye et al. (2013) showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database

de Montjoye, Yves-Alexandre; César A. Hidalgo; Michel Verleysen; Vincent D. Blondel (March 25, 2013). "Unique in the Crowd: The privacy bounds of human mobility". Nature *srep*. doi:10.1038/srep01376

©2025 Riproduzione riservata – Digital Technology 14

14




Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems

Understanding Ethical and Social Issues Related to Systems

- **A model for thinking about ethical, social, and political Issues**
 - Society as a calm pond
 - IT as rock dropped in pond, creating ripples of new situations not covered by old rules
 - Social and political institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, laws
 - Requires understanding of ethics to make choices in legally gray areas

4.15 Copyright © 2014 Pearson Education, Inc.

15



Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems

- Ethics: **individual** judgement in decision making
- Society: reaching **consensus** on behaviors as a community
- Legal: **laws** are proposed, discussed, approved

4.16 Copyright © 2014 Pearson Education, Inc.

16




Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems

- Ethics: **individual** judgement in decision making
- Society: reaching **consensus** on behaviors as a community
- Legal: **laws** are proposed, discussed, approved

4.17 Copyright © 2014 Pearson Education, Inc.

17

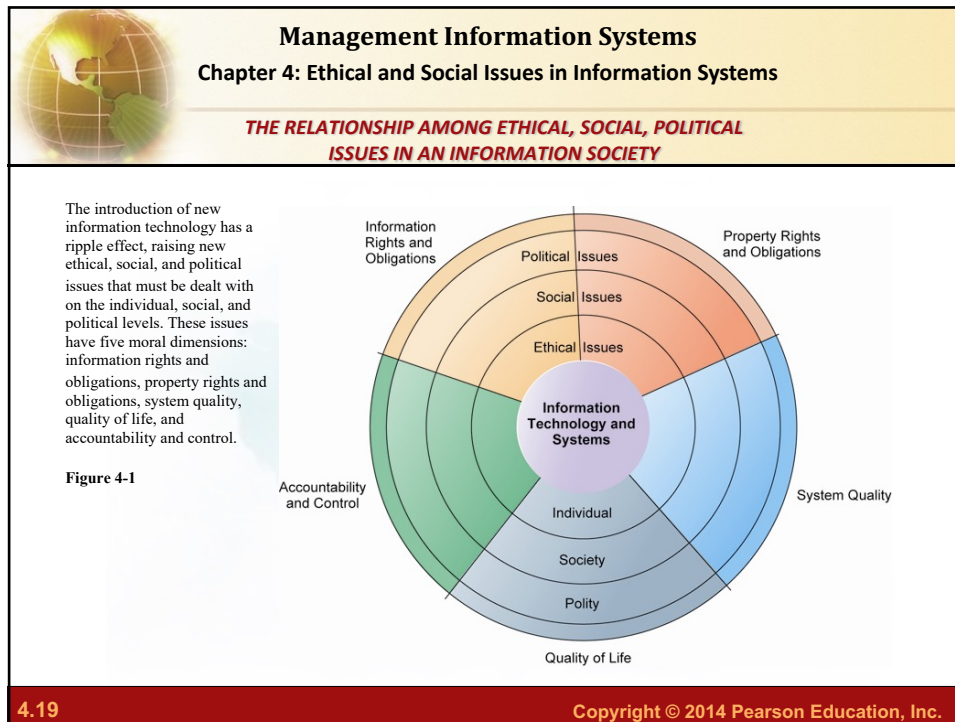


Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems
Understanding Ethical and Social Issues Related to Systems

- **Five moral dimensions of the information age:**
 - Information rights and obligations
 - Property rights and obligations
 - Accountability and control
 - System quality
 - Quality of life

4.18 Copyright © 2014 Pearson Education, Inc.


18



19

ETHICAL ASPECTS


25

	Management Information Systems
	Chapter 4: Ethical and Social Issues in Information Systems
	Ethics in an Information Society

- **Candidate ethical principles**
 - **Golden Rule**
 - Do unto others as you would have them do unto you.
 - **Immanuel Kant's Categorical Imperative**
 - If an action is not right for everyone to take, it is not right for anyone.
 - **Descartes' Rule of Change**
 - If an action cannot be taken repeatedly, it is not right to take at all.

4.26	Copyright © 2014 Pearson Education, Inc.
-------------	--


26

	Management Information Systems
	Chapter 4: Ethical and Social Issues in Information Systems
	Ethics in an Information Society

- **Candidate ethical principles (cont.)**
 - **Utilitarian Principle**
 - Take the action that achieves the higher or greater value.
 - **Risk Aversion Principle**
 - Take the action that produces the least harm or potential cost.
 - **Ethical "No Free Lunch" Rule**
 - Assume that virtually all tangible and intangible objects are owned by someone unless there is a specific declaration otherwise.

4.27	Copyright © 2014 Pearson Education, Inc.
-------------	--

27



Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems
Ethics in an Information Society

- **Five-step ethical analysis**
 1. Identify and clearly describe the facts.
 2. Define the conflict or dilemma and identify the higher-order values involved.
 3. Identify the stakeholders.
 4. Identify the options that you can reasonably take.
 5. Identify the potential consequences of your options.

4.28


Copyright © 2014 Pearson Education, Inc.

28

SOCIETY

©2025 Riproduzione riservata – Digital Technology

29



Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems
Ethics in an Information Society

- **Professional codes of conduct**
 - **Promulgated by associations of professionals**
 - Examples: AMA, ABA, AITP, ACM
 - **Promises by professions to regulate themselves in the general interest of society**
- **Real-world ethical dilemmas**
 - **One set of interests pitted against another**
 - Example: right of company to maximize productivity of workers versus workers right to use Internet for short personal tasks

4.30 Copyright © 2014 Pearson Education, Inc.

30

ACM Code of Ethics and Professional Conduct Association for Computer Machinery

- <https://www.acm.org/code-of-ethics> (as of 2025)
 - For computing professionals

1. GENERAL ETHICAL PRINCIPLES

- 1. Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing
 - Human rights, minimize negative consequences of computing
- 2. Avoid harm
- 3. Be honest and trustworthy
- 4. Be fair and take action not to discriminate
- 5. Respect the work required to produce new ideas, inventions, creative works, and computing artifacts
- 6. Respect privacy
- 7. Honor confidentiality.

©2025 Riproduzione riservata – Digital Technology 31

31

ACM Code of Ethics and Professional Conduct Association for Computer Machinery

- <https://www.acm.org/code-of-ethics> (as of 2025)
 - For computing professionals

2. PROFESSIONAL RESPONSIBILITIES.

Principles about competence, quality of work

Include in particular:

- Access computing and communication resources only when authorized or when compelled by the public good
- Design and implement systems that are robustly and usably secure

©2025 Riproduzione riservata – Digital Technology 32

32

ACM Code of Ethics and Professional Conduct Association for Computer Machinery

- <https://www.acm.org/code-of-ethics> (as of 2025)
 - For computing professionals

3. PROFESSIONAL LEADERSHIP PRINCIPLES

Emphasizes social responsibility, public good

Includes

- Computing professionals should be fully aware of the dangers of oversimplified approaches, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and their contexts, and other issues related to the complexity of their profession
- for systems that become integrated into the infrastructure of society
 - Continual monitoring of how society is using a system will allow the organization or group to remain consistent with their ethical obligations outlined in the Code

4. COMPLIANCE WITH THE CODE.


©2025 Riproduzione riservata – Digital Technology 33

33

LEGAL FRAMEWORKS

©2025 Riproduzione riservata – Digital Technology 34

34



Management Information Systems


Chapter 4: Ethical and Social Issues in Information Systems

The Moral Dimensions of Information Systems

- **Information rights: privacy and freedom in the Internet age**
 - **Privacy:**
 - Claim of individuals to be left alone, free from surveillance or interference from other individuals, organizations, or state; claim to be able to control information about yourself
 - **In the United States, privacy protected by:**
 - First Amendment (freedom of speech)
 - Fourth Amendment (unreasonable search and seizure)
 - Additional federal statutes (e.g., Privacy Act of 1974)

4.35
Copyright © 2014 Pearson Education, Inc.

35



Management Information Systems
Chapter 4: Ethical and Social Issues in Information Systems

The Moral Dimensions of Information Systems

- **European Directive on Data Protection:**
 - Companies must inform people information is collected and disclose how it is stored and used.
 - Requires informed consent of customer.
 - EU member nations cannot transfer personal data to countries without similar privacy protection (e.g., the United States).
 - U.S. businesses use *safe harbor* framework.
 - Self-regulating policy and enforcement that meets objectives of government legislation but does not involve government regulation or enforcement.

4.36 Copyright © 2014 Pearson Education, Inc.

36

Privacy

**Introduction to the
General Data Protection Regulation
(EU)**

A legal framework

https://www.garanteprivacy.it/web/garante-privacy-en/home_en

37

Regulation (EE) 2016/679:

- Entered into force in May 2016
- Applied in May 2018
- Repeals Directive 95/46/EC
- Allows Member States some flexibility
- Draft Bill for implementing certain provisions of the GDPR
- The Bill replaces Law 138(I)/2001
- Updates under discussion

©2025 Riproduzione riservata – Digital Technology 38

38

Outlining the GDPR:

- Protection of individuals
- Free movement of data in the EU
- Balance data protection against other fundamental rights
- Balance against public and legitimate interests
- Regulatory tool

©2025 Riproduzione riservata – Digital Technology 39

39

Where are our data?

- Collected through interactions with different organizations
 - E.g. schools, doctors, insurance companies, banks, on line shopping
- Other sources
 - Telephone
 - Social networks

©2025 Riproduzione riservata – Digital Technology

40

Data Collection and Privacy

- **Monitoring software:** collecting info about employees at work
 - Screens, e-mail, number of typed characters, length of breaks, used files
- **Monitoring Web Site access**
 - Visited sites, clickstream analysis, origin of visits, used hw and sw
- **Tracking applications**
 - GPS, smartphones apps
- **Cookies**
 - Store info about users
 - Initial goal: save user's preferences, maintain sessions
 - Others: monitoring users' habits [and preferences](#)
 - Can be blocked (but service may be [no longer available](#))

©2025 Riproduzione riservata – Digital Technology

41

Privacy law

- Responsibility and accountability
- General Data Protection Regulation (GDPR) (EU)
 - it does not require any enabling legislation to be **applied** by national governments
 - regulates **also** transfer of personal data to third **parties and non-EU Countries**

©2025 Riproduzione riservata – Digital Technology

42

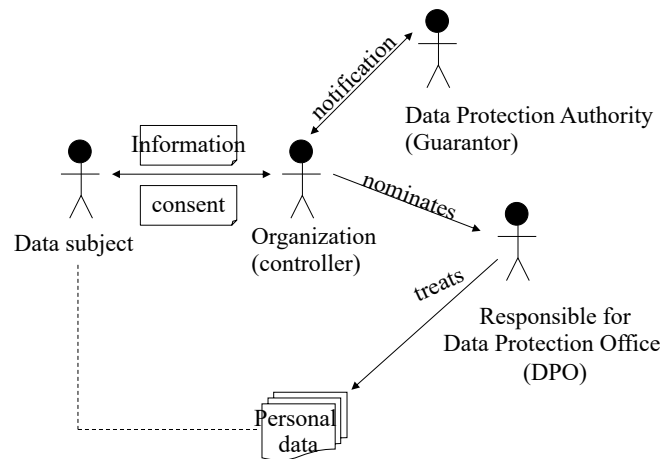
Some definitions

- **Personal data:** any information relating to an identified or identifiable data subject
- **Data subject:** a natural living person
- **Controller:** the owner of the data
- **Processor:** acts on behalf of the controller
- **Special categories:** health, race, religion and other special categories (**sensitive** data)
- **Processing:** collection, storage, disclosure, transfer, profiling and other processing operation
- **Profiling:** analysis/ prediction of behavior

©2025 Riproduzione riservata – Digital Technology

43

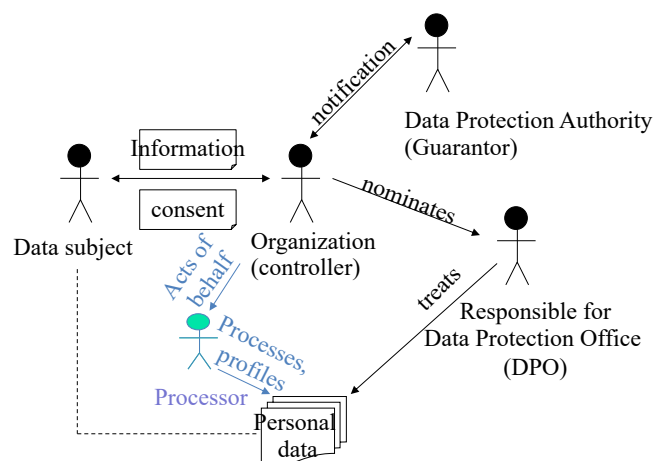
General principles of privacy laws



©2025 Riproduzione riservata – Digital Technology

44

General principles of privacy laws



©2025 Riproduzione riservata – Digital Technology

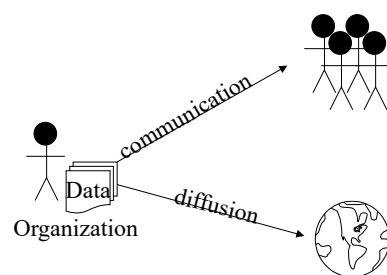
45

Appointment of Data Protection Officer (DPO) Article 37:

Mandatory for controller & processor when:

- Public authority or body
- Core activities consist of operations that require **regular** and **systematic** monitoring of data subjects on a **large scale**
- Core activities require processing of **special categories** of personal data or **criminal convictions and offences**, on a large scale

General principles



Data protection principles Article 5:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability: The controller is obliged to demonstrate compliance with all of the above principles

©2025 Riproduzione riservata – Digital Technology

48

General principles

- **Minimality (proportionality)**

Personal data may be processed only as long as they are adequate, relevant and not redundant wrt the purposes for which they are collected and/or further processed.

Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate or incomplete data, wrt the collection purposes or wrt further processing, are erased or rectified.

Data should be kept in a form which does not allow the identification of data subjects and not for longer than necessary for collection purposes or wrt further processing.

Member States shall put in place appropriate protection measures for personal data stored for longer periods for historical, statistical or scientific use. (art. 6).

- When **sensitive personal** data (can be: religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply (art. 8).
- The **data subject may object** at any time to the processing of personal data for the purpose of direct marketing. (art. 14)

©2025 Riproduzione riservata – Digital Technology

49

Lawfulness of processing Article 6:

- With Consent
- Without consent when:
 - Contractual obligation
 - Legal obligation
 - Vital interest
 - Public interest
 - Overriding legitimate interest

©2025 Riproduzione riservata – Digital Technology 50

50

Rights of data subjects Articles 12-22

- Transparent information provided when data collected from the person, or from a third party
- Right to access my own data (free of charge)
- Rectification of inaccurate/ incomplete data
- Erasure (right to be forgotten): when data are no longer necessary or consent is withdrawn or person objects for legitimate grounds or data have been unlawfully processed or there is legal obligation for erasure or data collected in relation to information society services

©2025 Riproduzione riservata – Digital Technology 51

51

Rights of data subjects Articles 12-22

- **Restriction of processing**: contested accuracy or unlawful processing or legal claims or decision is pending on exercised right to objection
- **Data portability**: receive data that I have given, in human or machine readable form & ask to transmit these data to other controller, when processing is based on consent or contract
- **Objection** (including profiling): when processing is based on public interest or legitimate interest
- **Object to decisions** based solely on automated processing, including profiling

©2025 Riproduzione riservata – Digital Technology 52

52

Responsibilities of controller & processor Cooperation with DPA & security Art.31,32

- The controller & the processor & where appropriate their representatives shall cooperate with the DPA, on request
- They must implement appropriate security measures, taking into account state of the art technology, costs and possible risks

©2025 Riproduzione riservata – Digital Technology 53

53

Minimal measures for digital data (1/2)

- a) Authentication
- b) Management of data access credentials
- c) Authorization system
- d) Periodic update of access rights

©2025 Riproduzione riservata – Digital Technology

54

Minimal measures 2/2

- e) Protection of electronic systems
- f) Procedures for keeping backup copies and restoring them
- g) Encryption of sensitive data

©2025 Riproduzione riservata – Digital Technology

55

Responsibilities of controller & processor

Data breach notification Article 33

- The controller notifies the DPA about data breach within 72hrs unless there is no risk
- Justification required, after 72 hrs
- The processor informs the controller about data breach immediately
- The notification includes: nature of breach, number of persons affected, risks involved, measures taken or considered to be taken to mitigate risks

©2025 Riproduzione riservata – Digital Technology 56

56

Security and cloud computing

“The government or company that manages the data, the data transfer and the data handling on the cloud must designate the cloud provider responsible for treatment”

Geographical localization constraints must be considered



©2025 Riproduzione riservata – Digital Technology

57

Data management outside EU

- The privacy code prohibits in principle the "even temporary" transfer of personal data to an extra-European state if the destination or transit Country of data does not ensure an adequate level of protection
- This can happen if public cloud services are used
- The data controller must also consider the geographical location of the data

©2025 Riproduzione riservata – Digital Technology

58

TOWARDS REGULATIONS

©2025 Riproduzione riservata – Digital Technology 59

59

An example - Google Analytics (GA)

- Google Analytics is not illegal for most countries in the EU and it's not illegal in the US or any other country.
- Declared illegal in Austria, France, Italy (2022 directive of Garante della Privacy), Denmark, Finland, Norway and Sweden.

Why is Google Analytics illegal in some countries of the EU?

- IP addresses are considered personal data

- GA3 not usable anymore in EU

In GA3 the IP is sent natively from the browser to the server. A lot of Google's servers are based in the US, which is outside of the EU. Thus violating GDPR.

©2025 Riproduzione riservata – Digital Technology 60

60

Google Analytics GA4

- GA4
 - Server-side Google Tag Manager (SGTM)
 - enable the "Redact visitor IP address" option, it ensures user IP addresses are not captured, mapping IPs onto cities / countries
 - Redaction of **parameters**, emails,...
 - Opt-in: explicit users consent is necessary

If you are using Analytics data with a Google service, such as Google Ads, Play, Display & Video 360 or others, and *you take no action*, only end users outside the EEA will be included in audiences used by your linked advertising products starting early March, 2024.

The Garante has not confirmed GA4 is GDPR compliant.
Responsibility of possible GDPR violations on companies using it.

©2025 Riproduzione riservata – Digital Technology 61

61

European data strategy

- Principles
- A path towards regulations
- Facilitate the flow of – non-personal – data
- New technologies

©2025 Riproduzione riservata – Digital Technology 62

62

EU Commission proposes new rules and actions for excellence and trust in Artificial Intelligence – proposed April 21, 2021

- The new **AI regulation** will make sure that Europeans can trust what AI has to offer. Proportionate and flexible rules will address the specific **risks** posed by AI systems and set the highest standard worldwide.
 - 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm
- <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- March 2024 **AI ACT**
<https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

2 May 2024 – The AI Act Explorer has now been updated with content from the European Parliament's '[Corrigendum](#)' version from 19 April 2024.
The content of the Act is unlikely to change any further.

©2025 Riproduzione riservata – Digital Technology

63

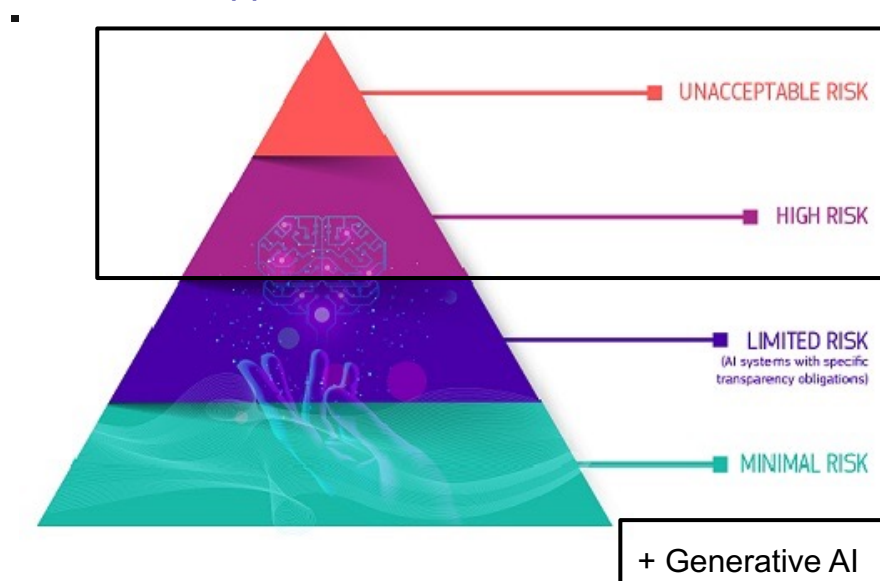
AI Act - Art. 1 (of 113)

- This Regulation lays down:
- (a) harmonised rules for the **placing on the market, the putting into service, and the use of AI systems in the Union**;
- (b) **prohibitions** of certain AI practices;
- (c) specific requirements for **high-risk AI systems** and obligations for operators of such systems;
- (d) harmonised **transparency** rules for certain AI systems;
- (e) harmonised rules for the placing on the market of **general-purpose AI** models;
- (f) rules on market monitoring, market surveillance, governance and enforcement;
- (g) measures to support innovation, with a particular focus on SMEs, including startups.

©2025 Riproduzione riservata – Digital Technology 64

64

Risk-based approach



©2025 Riproduzione riservata – Digital Technology 65

65

Unacceptable risk

Unacceptable risk AI systems are systems considered a threat to people and will be banned. They include:

- **Cognitive behavioural manipulation** of people or specific vulnerable groups: for example voice-activated toys that encourage dangerous behaviour in children
- **Social scoring**: classifying people based on behaviour, socio-economic status or personal characteristics
- **Biometric identification and categorisation** of people
- **Real-time and remote biometric identification systems**, such as facial recognition

Some exceptions may be allowed for law enforcement purposes.

©2025 Riproduzione riservata – Digital Technology 67

67

High risk

1) AI systems that are used in products falling under the **EU's product safety** legislation. This includes toys, aviation, cars, medical devices and lifts..

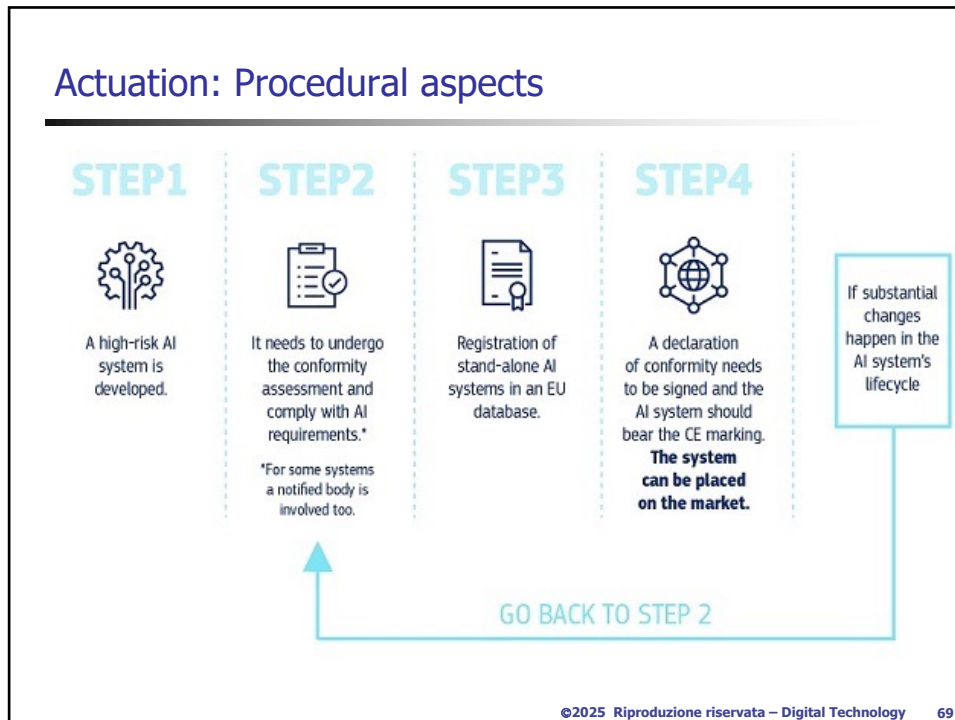
2) AI systems falling into **specific areas** that will have to be registered in an EU database:

- **Critical infrastructures** (e.g. transport), that could put the life and health of citizens at risk;
- **Educational or vocational training**, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- **Employment, workers management and access to self-employment** (e.g. CV-sorting software for recruitment procedures);
- **Essential private and public services** (e.g. credit scoring denying citizens opportunity to obtain a loan);
- **Law enforcement** that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- **Migration, asylum and border control management** (e.g. verification of authenticity of travel documents);
- **Administration of justice and democratic processes** (e.g. applying the law to a concrete set of facts).

©2025 Riproduzione riservata – Digital Technology

68

Actuation: Procedural aspects



69

Strict obligations before they can be put on the market

- **Adequate risk assessment and mitigation systems;**
- **High quality of the datasets** feeding the system to minimise risks and discriminatory outcomes;
- **Logging of activity to ensure traceability of results;**
- **Detailed documentation** providing all information necessary on the system and its purpose for authorities to assess its compliance;
- **Clear and adequate information** to the user;
- **Appropriate human oversight** measures to minimise risk;
- High level of **robustness, security** and **accuracy**.

©2025 Riproduzione riservata – Digital Technology

70

Transparency requirements

Generative AI, like ChatGPT, will not be classified as high-risk, but will have to comply with transparency requirements and EU copyright law:

- **Disclosing that the content was generated by AI**
 - Designing the model to **prevent it from generating illegal content**
 - **Publishing summaries of copyrighted data used for training**
- High-impact **general-purpose AI models** that might pose systemic risk, such as the more advanced AI model GPT-4, would have to undergo thorough **evaluations** and any **serious incidents** would have to be **reported** to the European Commission.
 - Content that is either generated or modified with the help of AI - images, audio or video files (for example deepfakes) - need to be clearly **labelled as AI generated** so that users are aware when they come across such content.

©2025 Riproduzione riservata – Digital Technology 71

71

AI Act application

The Parliament adopted the Artificial Intelligence Act in March 2024. It will be fully applicable **24 months** after entry into force, but some parts will be applicable sooner:

- The **ban of AI systems posing unacceptable risks** will apply **six months** after the entry into force
- **Codes of practice** will apply **nine months** after entry into force
- **Rules on general-purpose AI** systems that need to comply with transparency requirements will apply **12 months** after the entry into force

High-risk systems will have more time to comply with the requirements as the obligations concerning them will become applicable 36 months after the entry into force.

©2025 Riproduzione riservata – Digital Technology 72

72