LAW AND DATA SIMPLE (FOR REAL)

GABRIEL ROVESTI

1 TABLE OF CONTENTS

Disclaimer

This year of the course was made by professors Andrea Pin and Fiorella Dal Monte, subsequent to the material of the courses held by Elisa Spiller and Pin itself – for which I gathered the notes/exams present in Telegram and elsewhere for our MEGA, of course including this file. Hope this can be useful overall, given the quality of the present themes and also its exam.

Prof. Pin started to be present in the latest version done by Elisa Spiller, so in 2022-2023; years before, only prof. Spiller did the course herself, so some reference in older notes and older syllabuses are taken as titles/sections/quotes, just to give you here the full/complete experience of this course as possible only reference material, as I tried multiple times to do with my files.

Additional considerations, phrases and materials are retained and based on existing lectures, existing links of the 2023-2024 Moodle, compared with previous editions of the course and also integrating the older notes files of Law and Data which are great in their own right.

I actually wrote a ticket to add this exam in my study plan, then watched/skimmed through some lectures in order to gather some context (I don't think from what I saw they are worth attending honestly), but mostly it's my work re-elaborating the slides and the present material.

About the exam: cross questions and open questions, you have also examples here in MEGA, found between the Moodle and Telegram. Feel free to reach me to give me feedback about this file contents; also, if you want, feel free to thank me, it doesn't kill me that much.

2 LECTURE 1 - THE STRUCTURE OF LEGAL ORDERS (4-10)

(Note: This is the beginning of Prof. Andrea Pin's part)

There is an immediate contrast between two concepts: traditional legal frameworks and the more contemporary, technology-driven concept of "code" or programming as a regulatory mechanism. This duality might discuss how traditional laws enacted by governmental and legal bodies interact with, or differ from, the regulations and controls imposed by software and technology (i.e., "code").

- Traditional law (The Law): the body of rules and regulations that are formally enacted by legislative bodies or through common law and interpreted by courts

- The Code: refers to software, algorithms, and programming that effectively regulate or control behavior in digital spaces. This concept was popularized by Lawrence Lessig's principle that "code is law," suggesting that software and technology can enforce rules just as legal statutes can but operate in the realm of digital interactions

A question naturally arises: *how do we regulate digital technologies?*

2.1 THE ROLE OF LAW IN TECHNOLOGY

There are different *phenomena* to consider:

- Technological Sovereignty refers to a nation's ability to control and manage its own technological ecosystem without external influence
    - This involves policies and laws that govern the development, implementation, and security of technology to ensure it serves national interests

- The Splinternet describes the fragmentation of the global internet into divergent, closed segments as countries impose local regulations that restrict/alter Internet and services.
    - This reflects how laws can create separate digital territories, impacting global communication and commerce
    - The divergence of legal systems when it comes to regulating the web push people (e.g.: to go deep in the dark or use VPN), so illegality is freedom
    - The Regulatory State and the Technocratic Institutions in the US and in the EU often have regulatory, executive, and judicial powers

- The Brussels Effect is the phenomenon where European Union regulations become de facto standards for global companies because it is easier or more practical to comply with these strict rules universally rather than creating region-specific practices
    - This showcases the EU's indirect influence on global regulatory practices

But also different *problems*:

- Intellectual Property (IP) issues arise as technology enables the easy dissemination and reproduction of copyrighted material without authorization, leading to conflicts over copyright, patents, trademarks. Law plays a role in defining IP rights and scope of enforcement

- Economic disincentives to technological developments can occur when heavy regulation or stringent legal environments stifle innovation
    - For instance, stringent data protection laws might limit how data can be used in AI research, potentially slowing advancements in this field

- The "Matthew Effect", borrowed from sociology, refers to the adage "the rich get richer, and the poor get poorer"
    - In a technological context, this effect can be seen where dominant players in the tech industry gain disproportionate resources and influence, often exacerbated by patent laws and market dynamics that disadvantage smaller competitors

2.2 MAIN LEGAL MODELS

What are **legal systems**?

- *People* = all the participants in the legal system, from the citizens subject to the laws to the lawmakers who create them and law enforcement
- *Laws* = formal norms and directives that govern behavior within the society
- *Institutions* = governmental bodies and structures that create, enact, interpret, enforce laws.
    - These include legislatures (such as parliaments or congresses) that pass laws, courts that interpret and apply the law, and executive agencies that enforce the laws

There are two main legal models:

- **Civil law**
    - Formal validation of administrative acts by the parliaments enact legislation
    - Written – all laws are divided according to classic codification
        - We use *codes/statutes* here, so comprehensive books designed to give a universal and precise meaning to concepts, uniforming them
    - Only legislative enactments are binding
    - Judges are investigators of law and apply it
    - Court specific to the underlying codes
    - Less freedom of contract
    - Examples of countries with civil law systems: France, Germany, Spain, Latin America

- **Common law**
    - Not written – based on doctrine of legal precedents (stare decisis)
    - Judges make law by adjudicating cases
    - Juridical decisions are binding – not only the apply the law but also make law through decisions, which become precedents for future cases
    - Freedom of contract
    - Less prescriptive
    - Everything is permitted if not prohibited
    - Pragmatism and flexibility are the principles here
    - Examples of countries with common law systems: USA, Canada, Australia
        - Common law countries have narrow – but growing numbers of – statuses

In both civil and common law systems, the **constitution** is the supreme law of the land. It outlines the fundamental principles and framework for governance and the rights of citizens.

- Constitutions typically mandate how laws should be enacted and often include provisions that any law inconsistent with the constitution must be invalidated
- This is upheld through judicial review processes, where courts have the power to strike down laws that contravene the constitution

The two main **models** when it comes to data:

- *United States*
    - It has 50+1 constitutions
    - The Federation has:
        - Limited legislative powers
        - Its own judiciary
    - Each State has
        - Broad legislative powers
        - Its own judiciary
    - In most legislations, the one relevant is state legislation
    - Exception: Federal Trade Commission regulations

- *European Union*
    - Tries to put together 26 different legal systems under a single umbrella
    - Tries to set a minimum standard to be implemented domestically
    - Clear separation between State and Society for general interest
    - EU has:
        - Limited powers
        - The Court of Justice
    - States have
        - Most powers
        - The bulk of the judicial activity
    - Most rules that are relevant are EU rules, implementing conditions for goods and citizens – which many times started clashes and wars

3 LECTURE 2 – COMPARATIVE CONSTITUTIONAL RIGHTS AND GLOBAL REGULATORY AUTHORITY (06-10)

3.1 TWO UNDERSTANDING OF RIGHTS AND CONSTITUTION

Let's start comparing the following:

- **Vertical rights**
  - In the U.S., constitutional rights primarily operate vertically, meaning they are enforced against the government to protect individuals from state actions
  - Traditionally, these "vertical" rights would not apply to actions amongst private individuals
  - This framework emphasizes the protection of individual liberties against overreach by governmental authorities

- **Horizontal rights**
  - In contrast, the EU and China recognize rights that operate both vertically and horizontally
  - Constitutional courts have begun to incorporate "Horizontal" rights, which are rights that can be enforced against non-State, private actors as well
  - This means that rights can be enforced not only against the state but also between private parties, integrating constitutional norms directly into private law

Traditionally, these "vertical" rights would not apply to actions amongst private individuals. Over the recent decades, Constitutional courts have begun to incorporate "Horizontal" rights, which are rights that can be enforced against non-State, private actors as well.

3.2 TYPES OF LAWS

The EUCoJ is an organ that provides a code for laws and a reference when legislation is developed. First, we talk about the constitution of the EU Legal System. First, we do a distinction:

- Member States (MSs)
  - Have their own constitutions
  - Autonomous and shared competencies
- EU
  - No formal constitution, there is only primary law
  - Autonomous politics

Now, we will distinguish the main ones:

- **EU Treaties**: Highest level and these are foundational legal documents that establish the EU and its institutions, setting out broad principles and objectives
    - Highest legal legislation, like a constitution

Then, we have the *rules*, which are of two types:

- **EU Regulations**: These are binding legislative acts that apply uniformly across all EU member states without needing transposition into national law, thereby creating immediately enforceable rights upon enactment
    - These create immediately enforced rights

- **EU Directives**: Unlike regulations, directives require member states to achieve certain results but leave them discretion as to how. After the implementation deadline, directives can have direct effect if their provisions are clear, precise, and unconditional.
    - Binding legislation as regards the results to be achieved addressing MS (Member State) with instructions to implement domestic laws
    - It gives more methodological margin of maneuver
    - However, after the deadline, sufficiently precise rules are immediately enforced
    - If MS fail to implement directives, actors can claim to the CoJ that values are violated. Directives are equally balanced with regulations (not inferior)

Remember *regulations are different from directives*:
- Regulations
    - Directly applicable
    - Once approved and entered into force, they produce immediate legal effect over EU citizens, since there is the same law applied for all member states
- Directives
    - Not directly applicable
    - Need to be transported into national LSs (Legal Sources) with a domestic law margin of discretion of the MSs in the transposition

3.3 POWER OF EU – COURT OF JUSTICE, REGULATORY STATE, TECHNOCRATIC INSTITUTIONS

Why is the EU so powerful then?

- **"Direct effect" doctrine (DE)**
    - This is when there's no need to wait for domestic parliaments or courts to implement a new EU law
    - As soon as possible the law is passed and valid, the law is applied to everyone in EU
    - It enables individuals to immediately invoke a European provision before a national or European court

ECJ first articulated this doctrine in Van Gend en Loos case, establishing EU article provision had to be clear, negative obligation, unconditional, no reservation for states a not dependent to state measures.

Written by Gabriel R.

From Wikipedia, I would quote the following to link the concepts:

"In Van Gend en Loos it was decided that a citizen was able to enforce a right granted by European Community legislation against the state – the question of whether rights could be enforced against another citizen was not addressed. In Defrenne v. SABENA the European Court of Justice decided that there were two varieties of direct effect: vertical direct effect and horizontal direct effect, the distinction drawn being based on the person or entity against whom the right is to be enforced."

- **"EU law supremacy" doctrine**
    - Primacy is the general applicable EU law supremacy. When domestic and international law contradict and do not comply, the regional legislation is superior
    - Courts enforce EU law when domestic law conflicts with it
    - Establishes that EU laws override any conflicting national laws

Why the Court of Justice of the EU (CJEU) is so important?

The CJEU has three main principles:

- Privacy
- Compatibility
- Scrutiny

The **rule of law** establishes that the *law's mandate has supremacy above any other principle or person*. There's one EUCoJ where EU Law is dealt by MS Courts and legislation.

- Every time there's a clash and provisions collide, domestic judges suspend proceeding, reach out to EUCoJ for a judgment that will make the MS judge apply the law over domestic ones
- This inexpensive procedure unifies and simplifies the convenience of the regulation
- The principle of the effective of the judiciary review establishes the totality of the protection under law amongst all MS and within them
    - Meaning that every public and private power must be subjected to the interpretation and scrutiny of the EUCoJ court according to the correctness of their activities
- The sharing of jurisdiction makes measures against mutiny in both MS and EU courts
- The EUCoJ checks the domestic compatibility of the treaties
    - Which correspond to the MS constitution

A **preliminary ruling** is a decision of the European Court of Justice (ECJ) on the interpretation of European Union law that is given in response to a request (a preliminary reference) from a court or a tribunal of a member state.

- A preliminary ruling is a final determination of European Union law, with no scope for appeal
- ECJ hands down its decision to the referring court, which is obliged to implement the ruling

This is done from Article 267 (which will be explored) of Treaty on the Functioning of the European Union: *"The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning:*

(a) the interpretation of the Treaties;

(b) the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union"

Written by Gabriel R.

The preliminary ruling procedure is as follows:

- A domestic case starts
- The local judge thinks that EU law is involved
- EU law is ambiguous
- The local judge suspends the proceedings and requests of CJEU to issue a preliminary ruling
- The domestic trial resumes and the local judge will enforce the EU rule as interpreted by CJEU

Regulatory states and technocratic institutions play a crucial role in modern governance, particularly in the oversight and regulation of complex sectors such as commerce, privacy, and technology. These bodies often possess a blend of powers typically associated with separate branches of government, enabling them to enact, enforce, and adjudicate regulations efficiently.

We now consider the following:

- USA: The Federal Trade Commission
  - Founded in 1914
  - Central consumer protection body in the United States that regulates anti-competitive, deceptive, and unfair business practices (focus: antitrust laws, consumer protection)
  - Through its regulatory powers, the FTC enacts broad directives and rules that govern market behavior – investigates, enforces, litigates

- EU: The Privacy Authority
  - Collective framework of national Data Protection Authorities (DPAs) responsible for enforcing data protection laws, enforcing GDPR (General Data Protection Regulation)
  - Each member state has own authority
  - DPAs have the authority to conduct investigations into data breaches and compliance failure and can issue decisions on violations including fines and orders

- At the State Level: Privacy Authorities
  - Local privacy authorities exercise similar powers to oversee and enforce regional data protection laws, which must align with overarching EU regulations like the GDPR
  - These authorities ensure that both EU-wide/local data protection standards are met
  - Example: California Privacy Protection Agency
  - Growing trend as states enact own privacy laws

Such institutions often have different kinds of *powers*:

- *Regulatory*: Create rules, set standards
- *Executive*: Enforce regulations, issue fines
- *Judicial*: Hold hearings, make rulings

From here – European Union is based, as we said on the rule of law.

- This means that every action taken by the EU is founded on treaties that have been approved democratically by its members
- EU laws help to achieve the objectives of the EU treaties and put EU policies into practice

There are *two main types* of EU law – primary and secondary.

- Treaties are the starting point for EU law and are known in the EU as **primary law**
- The body of law that comes from the principles and objectives of the treaties is known as **secondary law**; it includes regulations, directives, decisions, recommendations and opinions

So, to conclude from slide:

- Primary laws of EU
    - Treaty of EU
    - Treaty on the functioning of EU
    - EU charter of fundamental rights
- Secondary laws
    - EU regulations
    - EU directives

4 LECTURE 3 – EVOLVING DIMENSIONS OF PRIVACY, THE CASE OF EU AND THE PROBLEM OF DATA: DEBATING AN OP-ED (11-10/13 -10)

Here, just for readers' notes: An op-ed is an essay or guest column published in the opinion section of a newspaper. These are called op-eds because they usually appear opposite the editorial page.

4.1 CHINA

China has different regulatory framework. Normally, there is a general piece of legislations laying out broad principles reflecting the agenda of the leading party and much of the job is deferred by and to the government(s). There are objectives, goals, tasks, and values with no exact rules.

It is based on the following:

- The Central State and the Local Government
- The Communist Party's Rule
- Regulating by principles and instructions

On the topic of privacy, China has the *Personal Information Protection Law ('PIPL')* entered into effect on November 1, 2021, and is China's first comprehensive data protection law. It's basically China's take on GDPR and contains may of the same principles: territorial scoping, personal information protection, data protection, openness and transparency, etc. Some quite good read on this here.

4.2 EU CONVENTION AND EU COURT OF HUMAN RIGHTS

EU's Charter of Human Rights is a treaty that has a list of rights and limitations, which are *broad* and *unstrict*.

It was born in 2000 and brings together the most important personal freedoms and rights enjoyed by citizens of the EU into one legally binding document.

The rights to consider here are the following *articles* (quoting their texts integrally):

- Art. 8
  - 1. *Everyone has the right to respect for his private and family life*, his home and his correspondence
  - 2. *There shall be no interference by a public authority* with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

- Art.10
    - 1. *Everyone has the right to freedom of expression*. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises
    - 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary

So, in a nutshell for both:

- Art 8. Right of privacy. Right to enjoy private and family life insulation from the rest of society. There must be a place where public-private authorities cannot have access to
- Art 10. Freedom to receive info, of expression within a societal pluralistic worldview, and to hold opinions without interference

The **European Court of Human Rights (EUCoHR)** has different *powers*:

- It intervenes after the exhaustion of domestic remedies
- It addresses complaints against States
- Its rulings establish obligations, but hardly have direct effects within state jurisdictions

This intervenes to address rules according to international obligations and complaints against States after the exhaustion of domestic remedies, but it hardly has DE (Direct Effect) within MS jurisdiction due to it being time consuming and expensive.

- The way cases are framed put private entities suing public MS when rights are violated
- The behavior of the court is to give priority to the different MSs so to avoid controversies and abuse of powers, so the interested MS must fix the problem by addressing the issue to avoid reputation problem within the others

Countries can temporarily ask for suspension, which means to ask courts to suspend liberties for a limited amount of time.

- Laws must not be *ambiguous* because all limits need to be known
- Due to the verity of uses which change with the context (when, who, where)
    - Prohibitions must have a legitimate and clear specific purpose to not be infringed

4.3 Development of Privacy & Dignity and Paradoxes

Data is factual information (such as measurements or statistics) in digital form output by a sensing device used as a basis for reasoning, discussion, or calculation; and that can processed.

The evolution of **privacy** as a legal concept is traced through a series of historical, legal, and societal changes, demonstrating how privacy has transitioned from a focus on physical spaces to encompassing personal information and the integrity of individuals.

Written by Gabriel R.

This is the most common concept when data is talked about, but let's retrace some steps.

- The narrative begins with the seminal 1890 Harvard Law Review article by Warren and Brandeis, which articulated privacy as a right to be "let alone" and set the groundwork for privacy law

Some cases to be quoted here (from old notes file, reported for completeness, since I guess they were discussed somehow):

- *Boston (1819)*
    - All the ancient tools that would protect people and their properties weren't sufficient since cheap journalism made those shields ineffective
    - Privacy was born when two lawyers, which one of them (Mr. Warren) was bothered by the fact that his Boston Bahamian of a wife had her picture taken and information gathered for the tabloids regardless of legal obstructions, drafted an article that was published in the Harvard Law Review about no public authority within intimacy
    - Intimacy is within the aim of property, which makes it impossible for private actors to break into. Privacy is a way of saying private powers don't have the right to break into properties and share with others private lives
    - A person's house is a place in which even public authorities need consent, as jurisdiction is separate from common property. There must exist physical (the idea of the protection of place of residence and property) and non-physical (information) possibilities for people to live private lives, which is worthy of protection

- *Friedrichsruh (1898)*
    - Keizer Chancellor of the German Empire Otto von Bismarck was the prominent protagonist and self-assorted unifier of Germany and its rise to power in the late 19th Century
    - He died of sickness in his bed and his family wanted to protect his image with a modest funeral. The family closed the house from anyone entering the house, but two photographers bribed the servants and took pictures of the dead Chancellor, and the media took hold of it
    - Even though major disrespect against public dignity and honor is detached from privacy, privacy is a response to similar necessities and problems because it covers areas that individuals would like to be protected or insulated

As societal norms and technologies evolved, privacy concerns expanded beyond simple intrusion into personal spaces to encompass broader issues of data and personal autonomy.

- This shift is vividly illustrated by significant legal cases such as Griswold v. Connecticut and Roe v. Wade in the United States
    - *Roe v Wade (1973)*
        - This decision centered around women's right to bodily privacy and the capacity of the individual to make an autonomous decision about one's own body
        - Individuals must make their own ideas of their own lives without intrusion of third-party powers, making the idea of privacy overwhelming the idea of dignity

- *Griswold v Connecticut (1965)*
  - Artificial contraception measures were illegal in the Connecticut and a case went to the Supreme Court of the US, which said that intimate relationships are covered by privacy
  - Public authority cannot legislate when it comes to intimacy of private actors

This encompasses different *means*:

- From places to people
- From protecting people with private powers
- To protecting people from public powers
- From people to information

Furthermore, the development of digital technologies and the internet introduced new complexities to privacy, exemplified by the "Barbra Streisand Effect" (good summary here and for privacy here), where efforts to suppress information about one's private life inadvertently lead to wider dissemination.

- Some municipalities in California subsidized aerial photography of the coastal area. Being that it was of Hollywood-centered area, photographs were taken of Barbara Streisand's house, and she was preoccupied that her wealth would become public
- This was a breach of safety and privacy, so she filed a complaint to the local court. Before the complaint was filed, her picture was downloaded only 4 times. However, the files of the application and complaint were published online
- By claiming privacy rights, she worsened her situation as millions downloaded the pictures
- The paradox is whether to protect or let things go because of secondary and unwanted effects
  - On the one hand, privacy loses protection when it is claimed
  - On the other hand, ethical obligations and duties on privacy do not fall on the shoulders of spreading information

In an era dominated by social media, the Streisand effect has found new avenues for expression. Social media platforms serve as virtual town squares, amplifying information at unprecedented speeds. Attempts to suppress content through takedown requests or legal actions often result in the Streisand effect taking center stage.

In EU, everyone has the right to respect for his private, family life, home and communication, gaining *protection* for his/her personal data.

- It must be processed *fairly*, for specific *purposes* and on the basis of the *consent* of the person
- Everyone has the right to access the data concerning him/her and to access / to rectify it

EU strategy tried overtime to adapt and use different legal frameworks so to address the evolving dynamics between human-technology and technology-technology interactions. As technology changes rapidly and pervasively, law attempts to provide stable conditions for these changes, though it often varies by jurisdiction.

- In terms of legislation, the EU has introduced significant regulations that impact the digital market, notably affecting how technologies comply with these laws
- This is part of the "Brussels Effect," where EU regulations influence global market practices due to its substantial market share, thus setting standards that have transnational effects
- The EU digital strategy is not just about creating immediate legal changes but is a long-term plan that evolves from strategies to policies and finally into mandatory laws

Written by Gabriel R.

4.4 STRUCTURE OF PROPORTIONALITY

Privacy is not a *shield*. Depending on the jurisdiction, other interests can prevail over the proportionality of privacy. The **proportionality** measurement has been a core problem when it comes to law because it is unknown how the scrutiny assessment can be implemented. Furthermore, the law's scope is that of a legal regime were data's definition is non-exhaustive (read here).

- Proportionality scrutiny involves a thorough assessment of whether a specific governmental or private action that impacts privacy is legitimate
- In many legal systems, privacy is not an absolute right but one that must be balanced against other societal interests, e.g., intellectual property rights can supersede privacy rights

In Europe, there's a test that has been designed to assess the balance of privacy and other competing interests to assess the legitimacy of a solution. The four technical steps that one needs to go through to see if the structure of proportionality exists are the following:

1. Lawful measure?
2. Legitimate goal?
3. Least restrictive?
4. Benefits > damages?

The proportionality test assesses data security measures within legal and political frameworks, adjusting for judicial and technological changes over time. It ensures legislation is transparent and rigorous by incorporating technical expertise from data scientists and cybersecurity experts. This helps balance sophisticated interests, making the regulation of technologies accurate and informed.

Why the Proportionality Test is so *important*?

- It shapes judicial assessments
- It forces parliaments and executives to incorporate the proportionality analysis
- It allows authorities without democratic legitimacy to address political issues
- It incorporates technical considerations into legal analysis
- It pushes private companies that deal with data to incorporate privacy analysis

An *example* follows here: Costeja Gonzalez v. Google Spain (C-131/12)

- This involved Mario Costeja Gonzalez, who argued that Google's search results on his name, linking to outdated articles about his financial troubles
    - This infringed on his privacy and damaged his reputation
- Costeja Gonzalez sued Google Spain in courts, a proceeding sent to the EUCoJ for an opinion
    - The EUCoJ addressed the issue of the facility of obtaining unimportant info. The judgement made a series of serious accusations, mainly that privacy has been violated as search engines can retrieve a lot of information.
- The decision said that it's almost impossible to eliminate information but, being that Google makes possible atemporal horizontal flat information virtually exist forever, information publicly retrieved from past acts shouldn't be a publicly available personality trait.

Search engines have become power sources of information which jeopardize how we decide and structure ever-fading memory and, since it's impossible to log off from the proxy monopoly of Google, Google violated the right of privacy which entails the right to be forgotten with past information not effecting the privacy of the present.

Written by Gabriel R.

The European Court of Justice ruled in favor of Gonzalez in 2014, establishing the "Right to be Forgotten," which allows individuals to request the removal of links to outdated or irrelevant personal information that infringes on privacy without serving a public interest

- This case highlighted the need for *proportionality assessment*
    - Balancing individual privacy rights against the public's right to access information
- The ruling has significant implications for search engines in Europe
    - Reshaping index/accessibility of interests involved delisting irrelevant information

There are also *legal and technical problems* risen from the previous, but generally we delight these:

- *Intellectual property problem*
    - The market and the burden of data is based on information as costs and resources
    - Since the EU is very protective of people's rights, European citizens have the right to know about the details of a software, which such lack of protection discourages development and stifle software progression
- *Transposing proportionality assessment into search engines*
- *Privacy-boring paradox*
    - The increase of privacy increases the boringness of the internet
- *Gaming the system*
    - Put together a transparent process while avoiding personal gain through indexing, but opting the system has consequences

4.5 ART 17 GDPR THE RIGHT TO ERASURE ("TO BE FORGOTTEN")

To complete this set, the full article so to have everything properly understood:

- *1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*
    - *a. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
    - *b. The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*
    - *c. The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
    - *d. The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*

- *2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.*

- *3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:*
    - *a. For exercising the right of freedom of expression and information;*
    - *b. For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
    - *c. For reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);*
    - *d. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e. for the establishment, exercise or defence of legal claims*

5 LECTURE 4 - PRIVACY & DATA MINIMIZATION: THE STRUCTURE OF THE GDPR. WHY IT IS INSUFFICIENT AND THE AI ACT (18 -10)

5.1 THE LOGIC OF PRIVACY IN THE US AND THE EU

Here, we will distinguish between:

- US
    - *State by state basis*
        - Privacy laws in the US vary significantly from state to state, leading to a patchwork of regulations that can create inconsistencies and complexities for businesses operating across multiple states
    - *Information logic*
        - This primarily focuses on the use and dissemination of information rather than explicit privacy protections
    - *Internet monopoly*
        - Concerns about internet monopolies highlight issues related to data control and privacy breaches, with significant power in hands of a few tech companies

- EU
    - *"One stop shop" logic*
        - This allows companies to deal with only one supervisory authority for privacy matters across all EU states, which is the country of the headquarters rather than the authority of 28 European states
    - *"Opt-in" logic*
        - Unlike the US, the EU heavily relies on "opt-in" logic, requiring explicit consent from individuals before their data can be processed. This fosters greater individual control over personal information
    - *Privacy by design and Privacy by default*
        - By design = prevent and do not correct, incorporating privacy into the project, with maximum functionality, safety, visibility and security
        - By default = companies should deal with the personal data to the extent necessary and sufficient for the intended purposes and for the period strictly necessary for those purposes

To concretely differentiate the two paradigms here (from older notes):

- **European Union paradigm**
    - "Opt-in" option
    - An individual needs to provide explicit consent to share and process data
    - Otherwise, the company cannot gather any data except only the necessary data for service. EU requires the option of consent
    - Cautiously, necessity in a frame where the client doesn't overshare

- **American paradigm**
    - "Opt-out" option
    - The company states that it's collecting clients' data, and they can get out or say if they don't want their info to be collected
    - The amount of data has skyrocketed since the 2008 World Economic Crisis, a new market that boosts the economy with new markets filled with jobs and wealth by the exchange of data because
    - Therefore, sharing data is encouraged because this triggers the creation of potential positive ramifications for the economy

5.2 Pros, Cons and Consequences

Privacy approaches need some *thinking* behind them:

- *Pros*
    - Strong privacy protections *can increase consumer trust and compliance* with international data protection standards
    - Proactive privacy measures *prevent breaches and minimize risks* associated with data handling
- *Cons*
    - Stringent privacy regulations *can impose heavy burdens on businesses*, particularly small and medium enterprises, due to *compliance costs and operational complexities*
    - *Excessive privacy could stifle innovation*, especially in data-driven sectors like technology and marketing

Too much privacy may have inadvertent consequences:

- Over-emphasis on privacy can lead to reduced data availability, impacting areas such as research and development, where data sharing is crucial
- It may lead to inefficiencies in services where personalization is key to user experience, such as healthcare and digital services

5.3 The Importance of Privacy Design and of Going Beyond It

Privacy design is crucial in today's data-driven world. There are many challenges when implementing privacy protection, the value and burden of data, consequences of opt-in systems, unique privacy issues in healthcare, and how AI regulations are expanding the scope of privacy considerations.

- *Time-consuming privacy protection*
    - Implementing comprehensive privacy measures can be resource-intensive and slow down business processes
- *Information as cost and resource*
    - Viewing information both as a cost (due to compliance) and a resource (in terms of value generation) illustrates the dual nature of data in the digital economy.
- *Consequences of the opting-in system*
    - Requiring users to opt-in for data processing can lead to lower participation rates, affecting data collection and the effectiveness of digital platforms

Written by Gabriel R.

- *Healthcare conundrum*
    - Balancing privacy with the need for data in healthcare can be challenging, as excessive privacy measures might hinder medical research and patient care services
- *AI act*
    - The discussion extends into regulatory approaches for AI, suggesting a need to look beyond traditional privacy protections to address ethical and societal impacts of artificial intelligence

6 LECTURE 5 – NAVIGATING AI RISKS AND THE SOCIAL CREDIT SYSTEM IN THE EAST AND THE WEST (25 -10)

6.1 LLM & PRIVACY: THE NOTION OF "RISK"

The **AI Act**, which is still in development, aims to regulate foundation models by enforcing strict data governance measures, so to ensure right and values of UE on those models. These include:

- Assessing the suitability of data sources for training AI to avoid biases and respect standards
- The provision of expectations between actors permits a positive behavior with the AI and related systems by establishing pillars with the complaint of production and the guaranteeing satisfactory compensation
- Requiring transparency in the use of copyrighted training data by making summaries of its use publicly available, provisioning info to users and giving transparency

For sake of completeness, here you see an excerpt of that (remember, "still in the making"):

- *1c) 'foundation model' means an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks;*
  ...
- *Foundation Model providers will ... process and incorporate only datasets that are subject to appropriate data governance measures for foundation models, in particular measures to examine the suitability of the data sources and possible biases and appropriate mitigation*
- *.. train, and where applicable, design and develop the foundation model in such a way as to ensure adequate safeguards against the generation of content in breach of Union law in line with the generally-acknowledged state of the art, and without prejudice to fundamental rights, including the freedom of expression*
- *... without prejudice to Union or national or Union legislation on copyright, document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law*

The Act assigns applications of AI to three risk categories.

- First, *applications and systems that create an unacceptable risk*, such as government-run social scoring of the type used in China, are banned
- Second, *high-risk applications*, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements
- Lastly, *applications not explicitly banned or listed as high-risk* are largely left unregulated

The EU AI Act could become a global standard, determining to what extent AI has a positive rather than negative effect on your life wherever you may be.

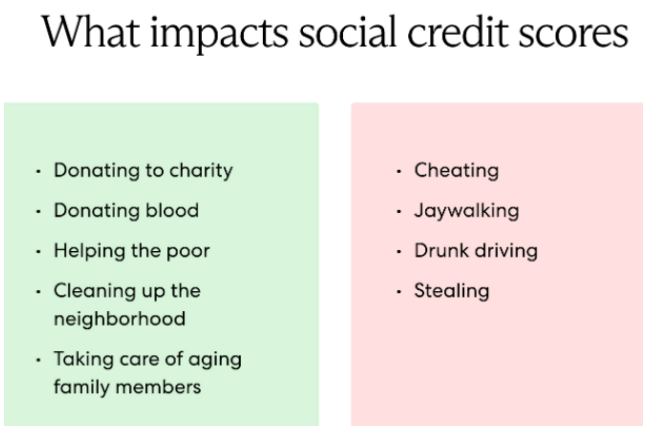
- *If an AI application makes a wrong decision or one that unfairly privileges or harms a human being, whose responsibility will it be?*

There are 4 levels of risk: unacceptable (subliminal techniques/biometric remote authentication), high (safety, school, welfare, making "conformity assessment"), limited (transparency obligations), minimum (antispam filters, IA games).

Written by Gabriel R.

6.2 SOCIAL CREDIT SYSTEM: FEATURES AND PROBLEMS

Social Credit Systems (SCS) are national credit ratings and blacklists, mainly developed by the government of China. Imagine: every action you take, every interaction you have, every movement you make – all reduced to a single rating on a five-point scale. A higher rating opens the door to good opportunities/special benefits, while a low rating can keep you shut off from the rest of society.



The government's optimism about this project, which has grown over the years, rests almost entirely on the technological element, which serves a threefold function here:

- First, it enables direct, widespread and effective monitoring, not based on simple data entry by one (corruptible) official but rather on multiple channels of data sourcing;
- Second, it allows this big data network to be created and managed and information to be easily shared with all authorities involved;
- Third, it allows for automatic adjustment of the consequences arising from this system on the one hand by "crediting" the score in real time and on the other hand by allowing all offices involved to "read" the score and determine what services the citizen or company is entitled to

The social credit initiative calls for *the establishment of a record system* so that businesses, individuals and government institutions can be tracked and evaluated for trustworthiness.

There are multiple forms of the social credit system being experimented with, while the national regulatory method is based on whitelisting (termed redlisting in China) and blacklisting.

- In Eastern contexts, particularly in countries like China, the Social Credit System aims to foster public good by monitoring and assessing the behaviors of individuals and communities.
    - The system integrates data from various sources, using AI to rank and incentivize societal harmony and collective responsibility
    - This centralized approach aids in administrative and legal processes by providing detailed situational profiles that can influence laws and regulations
    - The gathering of multiple sources in a centralized way incorporates AI tools within the administrative / judicial systems, giving information about people according to the status' score to public administrations to set principle / translate them into law

- Conversely, in Western societies, Social Credit Systems often target individual and private sector risks, such as financial reliability and health insurance qualifications
    - These systems are *more fragmented, generally driven by private entities* aiming to mitigate risks associated with personal interactions and behaviors
        - *Big companies*, to get information, *apply strategies to bypass and workaround problems that have been legally placed to protect privacy* (such as AI-based tools that search through the web)
        - Liberty relies on multiple actors that go their own ways, but companies in imperfect systems are not good at sharing information, making the personal portrait less real
    - *Legal frameworks in the West attempt to curtail the reach of SCS due to privacy concerns*, with some systems being restricted or banned due to their invasive nature and the potential for bias
        - EU is trying to prohibit scoring on people by prohibiting disclosing confidential information
        - In the US, there are constraints to check the whole makeup of society and to modify the market, which try to balance the system by nudging institutions to pay for social costs and accept disadvantaged minorities less

The People's Republic of China created the social credit system – which is sometimes referred to as SCS, SoCS, or China's ranking system – to function as a unified record system that measures businesses, individuals, and government entities to evaluate their trustworthiness.

- China's social credit system gives individuals, businesses, and government entities a credit score based on their trustworthiness
- A poor credit score comes with penalties like reduced access to credit and fewer business opportunities
- Corporations seeking to fix a poor credit score must apply to do so

So, we will try to answer the following *questions*:

- Which are the key issues of a Social Credit System-based model?
    - *Privacy*
        - Perhaps the most significant issue with SCS is the extent of personal data collection involved, which raises severe privacy concerns
    - *Transparency and accountability*
        - There is often a lack of transparency about how data is collected, processed, and how scores are calculated
    - *Discrimination and bias*
        - Algorithms used in SCS can perpetuate existing societal biases. They may unfairly penalize certain groups based on flawed data or biased processes
    - *Loss of individual autonomy*
        - By penalizing certain behaviors and incentivizing others, SCS can lead to a loss of personal freedom, with individuals feeling pressured to conform
    - *Legal and ethical issues*
        - SCS intersects complexly with legal frameworks, often challenging traditional notions of legality and ethics, particularly concerning data protection and individual rights

Written by Gabriel R.

- Which are the main achievements?
    - *Enhanced public accountability*
        - By linking actions to consequences transparently, it encourages compliance with norms and standards
    - *Improved financial trustworthiness*
        - In the financial sector, SCS can enhance trustworthiness by providing more accurate assessments of credit risk
    - *Promotion of socially desirable behaviors*
        - SCS can effectively incentivize behaviors deemed beneficial for society, such as environmental stewardship, charitable contributions, and civic engagement
    - *Efficiency in resource allocation*
        - By better understanding the behaviors and trustworthiness of individuals and entities, resources such as loans, government services
    - *Economic and social stability*
        - By encouraging a trustworthy, rule-abiding society, SCS can contribute to overall economic and social stability

There are also different <u>problems</u> to list here:

- *End of the separation between private and public*
    - *Issue*
        - SCS often blurs the lines between private life and public oversight. By collecting extensive personal data, these systems can lead to a situation where private behaviors are subjected to public evaluation and consequences
    - *Impact*
        - This encroachment can lead to societal discomfort and resistance, as individuals may feel their private lives are unfairly scrutinized

- *Biases*
    - *Issue*
        - Bias in SCS can arise from the data used, the design of algorithms, or the application of the system. Since these systems often rely on historical data, there is a risk of perpetuating existing societal biases
    - *Impact*
        - Biased systems can result in unfair treatment of certain groups, leading to discrimination and social inequality

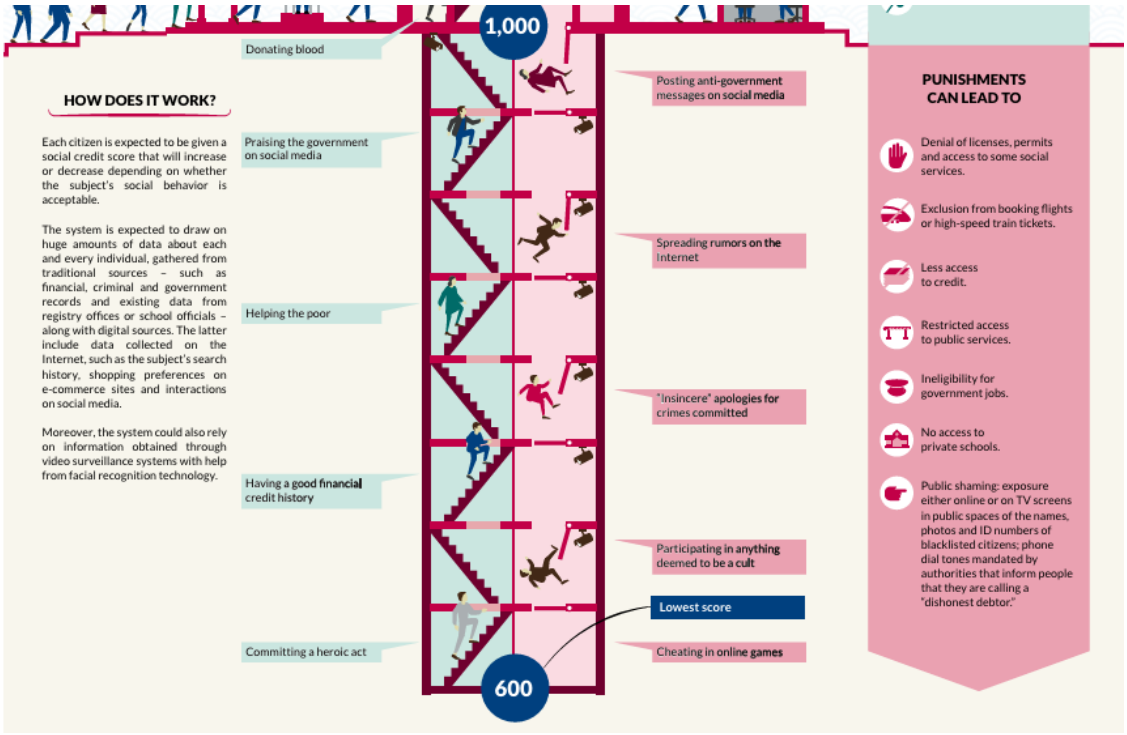
- *Determinism*
    - *Issue*
        - This refers to the reduction of human behavior to predictable patterns that can be quantified and controlled. This deterministic approach assumes that all actions are foreseeable and can be influenced
    - *Impact*
        - This can diminish the perceived agency and free will of individuals, reducing complex human behaviors to mere data points within a predictive model. It can lead to fatalism or apathy among individuals

- *IP protection of software*
    - *Issue*
        - This concerns the proprietary algorithms and software used to collect, analyze, and apply data. There is often a tension between protecting these innovations and the need for transparency about how decisions are made
    - *Impact*
        - Without sufficient transparency, it's challenging to scrutinize or challenge the decisions made by these systems, which can lead to a lack of trust and acceptance

- *Training*
    - *Issue*
        - The training of algorithms in SCS involves using large datasets to model and predict behaviors. This process can be fraught with challenges related to the quality, relevance, and integrity of the data used
    - *Impact*
        - Poorly trained algorithms can lead to inaccurate predictions or failures in the system, affecting its reliability and fairness. Additionally, training these systems requires ongoing effort and adaptation

From here, some useful images on the topic to conclude it properly:

Written by Gabriel R.



6.3 High Risk systems, Social Credit and Biases

This identifies several applications of AI that are considered particularly sensitive due to their potential impact on individuals' rights, well-being, and access to services. These AI systems require careful regulation and oversight because they can significantly affect people's lives.

- *AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score*, with the exception of AI systems used for the purpose of detecting financial fraud (Dutch SyRI)
    - Dutch SyRI (System Risk Indication) is an example of a high-risk AI system that was implemented in the Netherlands
    - It was designed as a risk profiling system used by the government to detect fraud in areas such as benefits, allowances, and taxes

- *AI systems intended to be used for making decisions or materially influencing decisions on the eligibility of natural persons for health and life insurance*

- *AI systems intended to evaluate and classify emergency calls by natural persons* or to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by *police and law enforcement*, firefighters and medical aid, *as well as of emergency healthcare patient triage system*

There are definitely critical issues of data quality and inherent biases that can significantly impact the fairness and effectiveness of these systems.

- *Garbage in, garbage out*
    - This highlights that the quality of the output (decisions, scores, or classifications made by an AI system) is directly dependent on the quality of the input data
    - If the input data is flawed, biased, or of inferior quality, the output will also be compromised
    - This is a significant concern in systems like Social Credit, where data from various sources can vary in accuracy, relevance, and objectivity

- *Bias – how do you fix biases?*
    - Fixing biases in AI systems, especially those as complex and influential as Social Credit Systems, requires a multi-faceted approach
        - Diverse and representative data, so to make it comprehensive and representative of the diverse populations it will impact
        - Regular audits and updates to AI algorithms, checking for biases, thanks to audits or general findings
        - Transparency on the algorithms being used and their factors
        - Ethical AI development, so to adhere to guidelines while respecting privacy and ensuring non-discrimination, upholding human rights
        - Develop and enforce robust legal and regulatory frameworks governing AI systems

7 LECTURE 6 – PRIVACY IN THE DIGITAL AGE, PUBLIC SPACES AND ARTIFICIAL FACE RECOGNITION (03 -11)

7.1 PRIVACY AND THE TYPES OF DATA

There are various classifications of data relevant to privacy concerns, especially in the context of legal and ethical considerations in data handling and processing. Such categories are different according to different consequences and situations regarding processes.

- **Personal data (PD)**
  - Information that relates to an identified or identifiable individual
  - This could include names, addresses, email addresses, and even digital footprints that can be linked to a person

- **Non-Personal data (NPD)**
  - Information that does not relate to an identified or identifiable individual (weather data, stock prices) or data that has been rendered anonymous in such a way that the individual is not or no longer identifiable (pseudoanonymized)

- **Anonymized data**
  - Information which does not relate to a subject data or personal data rendered anonymous in such a manner that the DS is no longer identifiable
  - Anonymous data isn't compliment to frameworks like GDPR as it's outside its scope since it doesn't concern the processing/techniques of such anonymous information

- **Pseudonymized data**
  - Process of personal data in such a manner that the data can be attributed to specific DS without the use of additional information, which is kept separate from the DS
  - Although this type of data cannot be attributed to a specific data subject without the use of additional information, pseudonymization reduces the risks associated with data processing while maintaining the data's utility

- **Synthetic data**
  - Artificially generated information that mimics the statistical properties and patterns of real data without containing any actual personal information from real individuals

7.2 Social Credit & Biases

It has been pointed out that the future is data-driven.

- What this means is that much of the present innovation taking place in domains such as Machine Learning and Artificial Intelligence is fueled by data, which is needed for calibrating the complex models (comprising neural network-based as well as other kinds)
- The larger the volume, diversity and quality of the data, the higher is the quality of the model, leading to better predictions and explanations

Social credit systems are a form of societal management that leverages data and algorithms to assign or deduct points based on an individual's actions.

- These systems aim to manage societal behavior and trust, creating a quantifiable measure of 'good' or 'bad' behavior that can significantly impact an individual's life
- For instance, a high social credit score might grant access to certain benefits, while a low score could lead to restrictions or penalties

Scorings can definitely be influenced by what data is gathered and its quality, since with multiple regulation enforcements, it's increasingly difficult/impossible to obtain data in the quantities required.

- At their core, social credit systems function by collecting vast amounts of data on individuals' behavior. This data is then processed through complex algorithms that assign or deduct points based on the perceived value of the behavior. The resulting score influences or controls access to various services or opportunities
- Several problems: breadth of data collected, opacity of algorithms used, risk of data breaches and misuse of information, issue of consent

Also because of this reasons, privacy frameworks were born. I suggest using this as reading.

7.3 Public Space & AFR

The problem of privacy in public spaces is related to what people expect when they are processed and analyzed without consent (a reading to gather some ideas on this here)

- Even putting social bias at the exploitation of certain systems aside, the process of technological tools transforms public spaces into areas that the transparent aggregation of information overlaps anonymity
- There are many safeguards that put human beings in the context of deployment, but these safeguards miss the social perception that may happen to not be correct
- There's a missing link in between the human-software relationship. The human process of saying that software is reliable and how algorithms work accordingly

Europe exhibits a cautious stance towards the use of Automated Facial Recognition (AFR), reflecting its broader approach to privacy and data protection.

- This is to be used as airports/border control, public safety, banking/payments, ATM access, customer experience, patient identification

Written by Gabriel R.

- Under GDPR Article 22 (Automated individual decision-making), individuals are protected from being subject to decisions based solely on automated processing, including AFR, that have significant legal significant effects on them (article here)
- This protection aims to prevent potential abuses and ensure that decisions that significantly impact individuals' lives involve human oversight and are not left entirely to algorithms

There are however *exceptions to article 22 protections*:

- *Contractual necessity*
    - If using AFR is necessary for entering into or performing a contract between the data subject (DS) and a data controller, and the DS has given explicit consent, Article 22's restrictions do not apply
    - However, the data controller is obligated to implement measures that safeguard the DS's rights, freedoms, and legitimate interests
    - This includes ensuring the possibility of human intervention, allowing the DS to express their point of view, and providing a means to contest the decision
- *Legal authorization*
    - Article 22 also does not apply if the decision is authorized by European Union or Member State law to which the data controller is subject
    - This law must also specify suitable measures to protect the DS's rights and freedoms

The *South Welsh Police case* (see here) illustrates significant differences between human and AI observers in the use of Automated Facial Recognition (AFR) technology in public spaces.

- The police deployed AFR over two years without a robust legal foundation, primarily for analyzing and identifying individuals within crowds, described metaphorically as "a crowd of lambs."
- This indiscriminate scrutiny led to legal challenges, particularly from those who were not directly harmed by the system but recognized the broader privacy implications.
- The court's decision highlighted a critical perspective on public interest, asserting that the deployment of such technology affects everyone, not just those identified by the system
- This case underlines the tension between public surveillance and individual privacy rights. It emphasizes that simply because an area is public does not grant authorities the liberty to deploy invasive technologies that could infringe on privacy.

In response to similar concerns, activists in the U.S. have been pushing against public surveillance systems to prevent a shift in the dynamic between private and public spheres, as well as between individuals and government.

- Several U.S. states have enacted laws to restrict or ban the use of facial recognition technology, reflecting growing resistance to such measures and a proactive stance on protecting personal privacy in public spaces.

7.4 GDPR: Article 22 – Automated Individual Decision-Making

Again, for the sake of completeness, the entire article is below.

- 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including *profiling*, which produces legal effects concerning him or her or similarly significantly affects him or her.
- 2. Paragraph 1 shall not apply if the decision: 1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- 3. is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or 3. is based on the data subject's explicit consent.
- 4. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement *suitable measures to safeguard the data subject's rights and freedoms* and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision

7.5 Politics and echo chambers

Echo chambers create environments where individuals are exposed only to information or opinions that reflect their own beliefs. For more detailed analysis you can explore here.

- This occurs due to a preference for similarity in socially significant attributes, leading to segregated spheres within society
- These chambers isolate individuals from diverse viewpoints, reinforcing in-group biases and behaviors

Technological advancements exacerbate this by facilitating even more selective information exposure, enhancing the natural inclination towards homogeneity.

- This not only polarizes societies by aligning individuals with similar views but also supports political extremes, potentially radicalizing views and disrupting societal harmony
- In contexts like the Capitol attack on January 6th, 2021, such polarization was evident as participants believed they were defending democracy based on their skewed perceptions

The combination of both globalization and technology has a tremendous affect.

- The echo chambers of social media promote the era of political polarization, making populism being a backlash against the global institutionalism of the liberal constitutionalism's rule of law
- Political polarization happens when the political center is weekend and is pushed towards the outside while also the growing of fringe parties and the reduction centrist moderation, making the most extreme voices becoming more dominant

- The *affective polarization* is when ideology as identity becomes something biological, closing the in-group and excluding the out-group. Political polarization turns institutions into partisan ones and politicizes institutions, making people consider these institutions as political

Political polarization destabilizes the basis of judicial systems so, to regain legitimacy, there are 2 strategies

1. Depoliticization of the court (taking politics out of the judiciary and the judiciary out of politics) by taking the constitution away from the courts and curtailing the judiciary's constitutional powers.
2. Balancing the power b/w political inclinations. Since Courts have become political bodies, give voice of every part of politics.

	Depoliticization	**Balancing**
Europe	No political view.	Deal w/ fringes and allow dissenting opinions
US	Stripping authority w/ formalist procedural barriers	Democratizing and disempowering the Supreme Court.
Westminster	No politicians involved and taking away or limiting judicial review over governmental decisions	Supermajority to increase political representation.

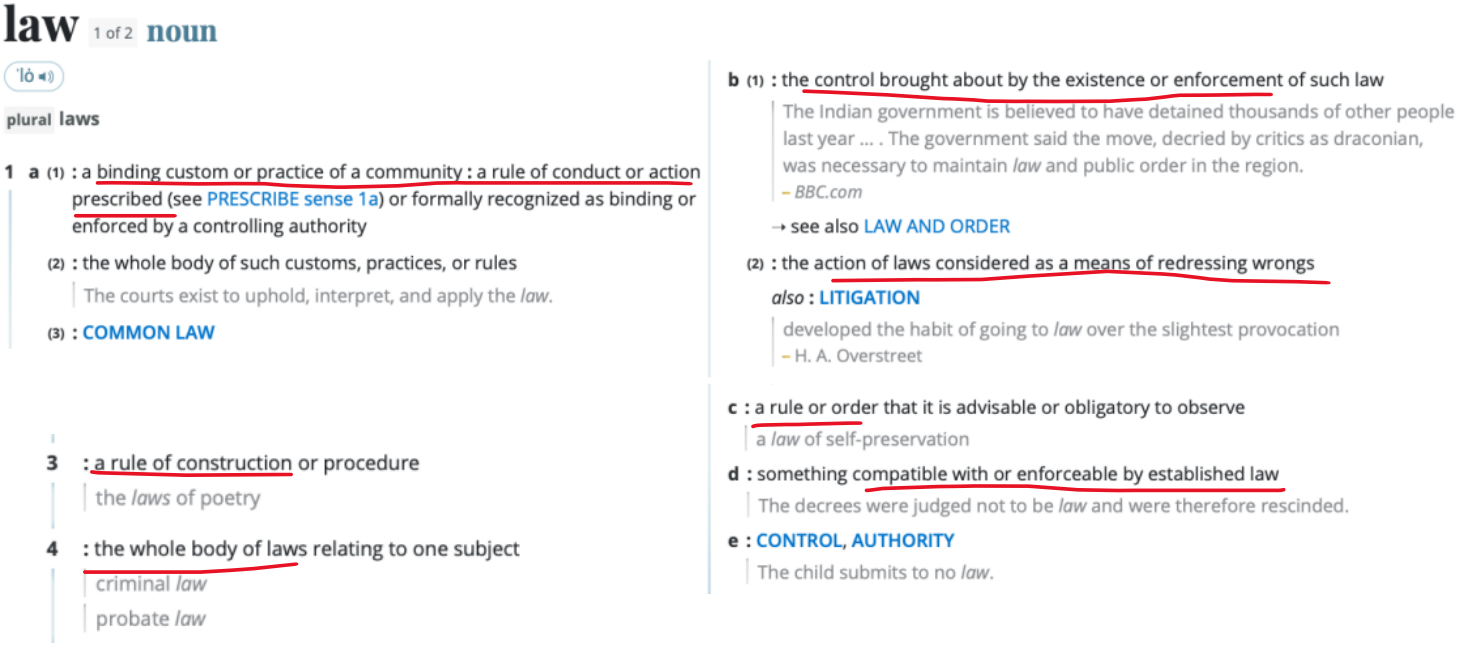
8 LECTURE 7 – BASIC LEGAL NOTIONS (08 -11)

(We finally start to see some structure on these slides, since here begins the part of prof. Fiorella Dal Monte, not slides written in Comic Sans with basically no content so to force you to follow the lesson – something common to most law professors, also for our "Diritto, tecnologia e società" B. Sc. course – but something more coherent and organized, at least in style, also in contents to be honest)

8.1 WHAT IS LAW?

There are multiple definitions which can be given to **law**. Law should be used to prevent wars – make law, not war. Assess the legal situation and trust the rules.

The following definition comes from Merrian-Webster dictionary:



law 1 of 2 **noun**

'lȯ

plural **laws**

1 a (1) : a binding custom or practice of a community : a rule of conduct or action prescribed (see PRESCRIBE sense 1a) or formally recognized as binding or enforced by a controlling authority

(2) : the whole body of such customs, practices, or rules

The courts exist to uphold, interpret, and apply the *law*.

(3) : COMMON LAW

b (1) : the control brought about by the existence or enforcement of such law

The Indian government is believed to have detained thousands of other people last year ... . The government said the move, decried by critics as draconian, was necessary to maintain *law* and public order in the region.
– *BBC.com*

→ see also LAW AND ORDER

(2) : the action of laws considered as a means of redressing wrongs

also : LITIGATION

developed the habit of going to *law* over the slightest provocation
– H. A. Overstreet

c : a rule or order that it is advisable or obligatory to observe

a *law* of self-preservation

d : something compatible with or enforceable by established law

The decrees were judged not to be *law* and were therefore rescinded.

e : CONTROL, AUTHORITY

The child submits to no *law*.

3 : a rule of construction or procedure

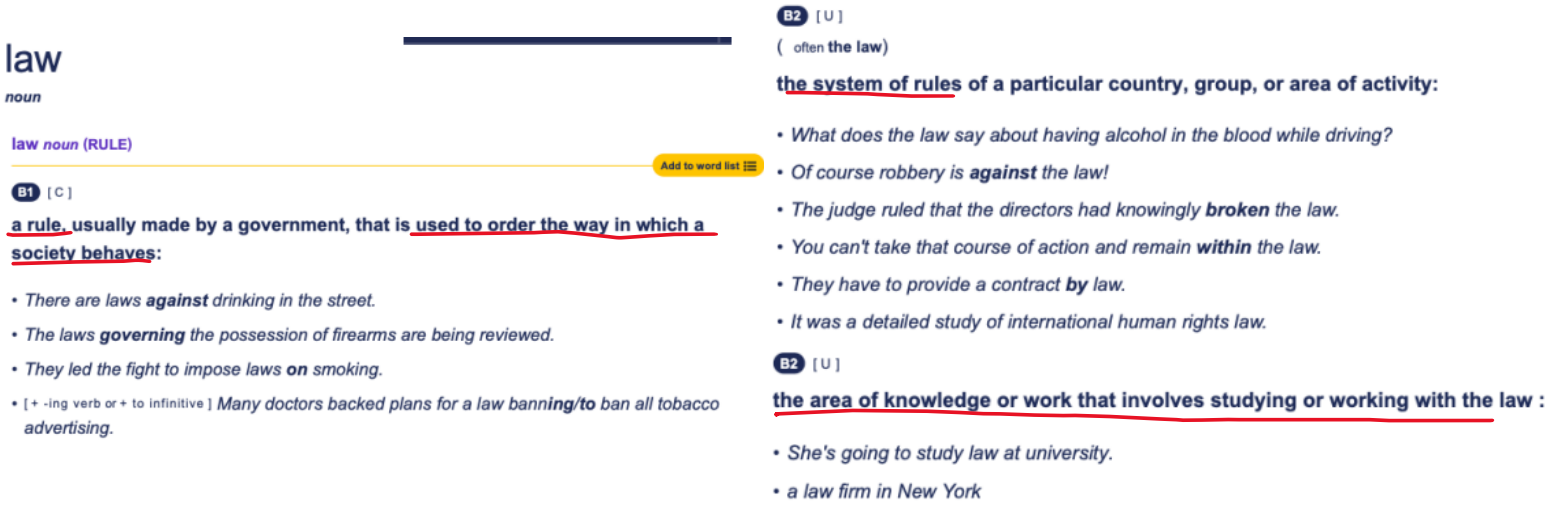
the *laws* of poetry

4 : the whole body of laws relating to one subject

criminal *law*

probate *law*

The following comes from Cambridge instead:



law
noun

law *noun* (RULE)

Add to word list

B1 [C]

a rule, usually made by a government, that is used to order the way in which a society behaves:

- *There are laws **against** drinking in the street.*
- *The laws **governing** the possession of firearms are being reviewed.*
- *They led the fight to impose laws **on** smoking.*
- [+ -ing verb or + to infinitive] *Many doctors backed plans for a law banning/**to** ban all tobacco advertising.*

B2 [U]

(often **the law**)

the system of rules of a particular country, group, or area of activity:

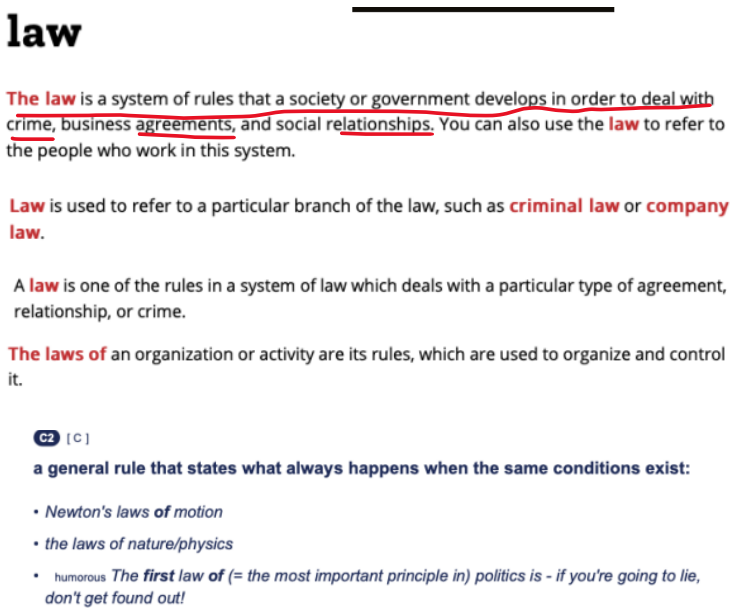
- *What does the law say about having alcohol in the blood while driving?*
- *Of course robbery is **against** the law!*
- *The judge ruled that the directors had knowingly **broken** the law.*
- *You can't take that course of action and remain **within** the law.*
- *They have to provide a contract **by** law.*
- *It was a detailed study of international human rights law.*

B2 [U]

the area of knowledge or work that involves studying or working with the law :

- *She's going to study law at university.*
- *a law firm in New York*

Here, also, the Collins one:



law

The law is a system of rules that a society or government develops in order to deal with crime, business agreements, and social relationships. You can also use the **law** to refer to the people who work in this system.

Law is used to refer to a particular branch of the law, such as **criminal law** or **company law**.

A **law** is one of the rules in a system of law which deals with a particular type of agreement, relationship, or crime.

The laws of an organization or activity are its rules, which are used to organize and control it.

C2 [C]

a general rule that states what always happens when the same conditions exist:

- *Newton's laws **of** motion*
- *the laws of nature/physics*
- humorous *The **first** law **of** (= the most important principle in) politics is - if you're going to lie, don't get found out!*

Immanuel Kant, from The Metaphysical Elements of Justice (finally a good quote inside a Computer Science course, ffs, at least for me guyz) gives the following definition:

"Set of conditions under which the choices of each person can be united with the choices of others under a universal law of freedom"

Google (aka Oxford) gives the following:

"The system of rules which a particular country or community recognizes as regulating the actions of its members and which it may enforce by the imposition of penalties"

8.2 Legal Systems and Separation of Powers

From *H. Kelsen, The concept of the legal order*, in The American Journal of Jurisprudence (translated by S.L. Paulson) we have the following:

«A **legal order** is an aggregate or a plurality of *general and individual* norms that govern human behavior, that prescribe, in other words, how one ought to behave. That behavior is prescribed in a norm or, what amounts to the same thing, is the content of a norm means that one ought to behave in a certain way. *The concept of the norm and the concept of the "ought" coincide*. To prescribe in a norm how one ought to behave is understood here not only as a *command but also as a positive permission or an authorization*.

So, in short: "Legal orders are collections of norms, be it the law of nation-states, supranational entities or international law"

A plurality of norms is an order if the norms constitute a unity, and they constitute a unity if they have the same basis of validity. If the law is positive law, the norms of a legal order are "posited" or "created" through human acts.

Written by Gabriel R.

To say that a norm prescribing how one ought to behave is "posited" (postulato in Italian) or "created" through an act is a metaphorical way of saying that the norm is the subjective meaning of the act. Acts through which the norms of a legal order are posited or created comprise legislative acts, acts constituting legally binding custom, judicial acts, administrative acts, and private law transactions, in particular contracts.

These acts are characterized here as legal acts, and the individuals authorized by the legal order to perform such acts are characterized as legal officials».

The legal system includes *rules, procedures and institutions* by which activities, both public and private, can be carried out through legitimate means (acting like a framework binding disputes using jurisdiction).

- A legal system is a system for interpreting and enforcing the laws
- Plurality of legal systems in light of several and different social groups

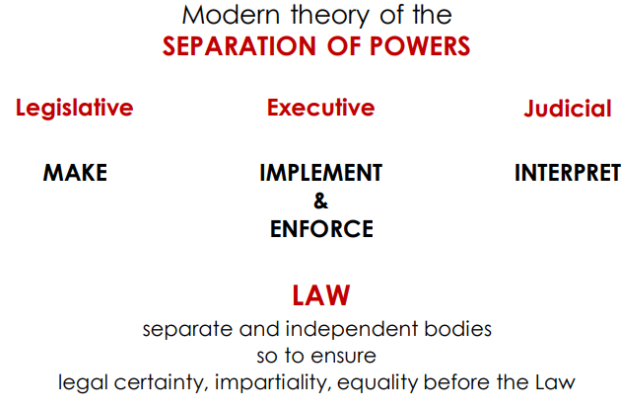
Legal systems operate on the interplay between laws, people, and institutions, where institutions legitimize, enact, and enforce laws.

- The Constitution stands above these laws, ensuring they conform to its mandates and providing the framework for their enactment and amendment
- Laws, articulated by governing bodies such as courts and legislatures, are designed to create predictable and equitable outcomes by establishing clear, binding rules
- These rules may enforce penalties or promote cooperative benefits and must adapt to control behavior effectively within varying jurisdictions, especially in a global context

Examples of what legal systems can be / Where legal systems can be found:

- *States*
  - E.g., Italy, France, USA, India, China, etc.
- *European Union*
  - Legal system encompassing 27 Member States
- *Council of Europe*
  - Legal system including 47 Member States
- *International Legal Order*
  - Special legal system – independent from States
- *World Wide Web*(?)

The following outlines the modern theory of the separation of powers, a fundamental principle in democratic governance:



Written by Gabriel R.

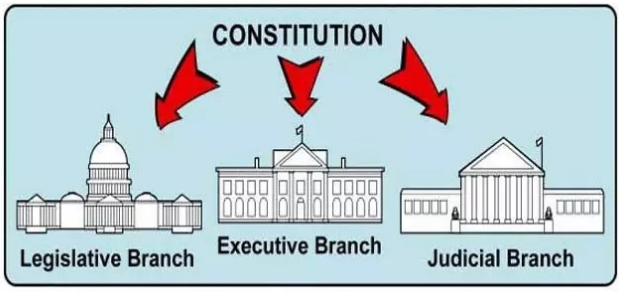
- It divides state power into three *branches*: legislative, executive, and judicial
- The legislative branch is responsible for *making* laws, the executive for *implementing* and *enforcing* these laws, and the judicial for *interpreting* them
- This structure ensures that power is not concentrated in one branch, promoting legal certainty, impartiality, and equality before the law
- Each branch operates independently but interdependently to maintain a balance of power and prevent abuse

9 LECTURE 8 – BRANCHES AND SOURCES OF LAW (10 -11)

9.1 BRANCHES OF LAW

According to what was said in the previous lecture, the theory of separation of powers, developed by Montesquieu in "The Spirit of the Laws" (1748), divides government functions into the three *branches* analyzed just before: legislative, executive, and judicial.

This division ensures that no single branch holds excessive power, promoting checks and balances, legal certainty, impartiality, and equality before the law. Each branch operates independently to maintain a balance and prevent tyranny, as exemplified by the U.S. Constitution (and image below).



The system of checks and balances is designed to limit the power of any single individual, entity, or branch of government.

- This framework ensures that power is distributed and balanced among the legislative, executive, and judicial branches, promoting harmonious and cooperative relationships
- By doing so, it prevents any one branch from becoming too powerful and helps maintain a stable and just government structure
- This system is integral to the functioning of democratic governments, ensuring that laws are made, implemented, and interpreted fairly and impartially.

Talking about the main lecture topic, the branches of law are fundamental, universally accepted, and exhaustive categories that organize legal principles and rules. They are divided into two main types: public law and private law.

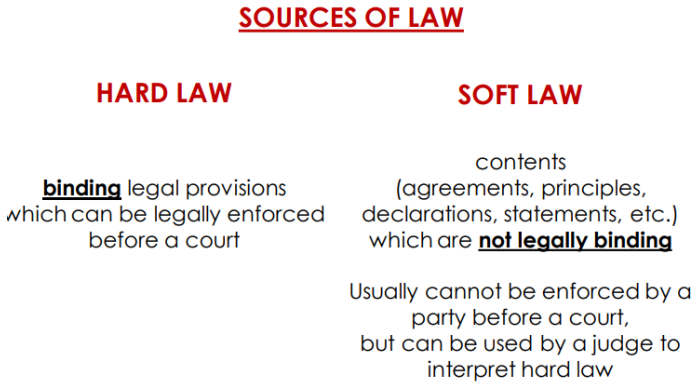
- **Public law** governs the relationship between individuals and the state, ensuring the regulation of public affairs and the protection of individual rights through administrative, constitutional, and criminal law
    - Laws intended for general application
- **Private law**, on the other hand, manages relationships between private individuals and entities, encompassing areas such as contract law, property law, family law, and tort law.
    - Laws enacted for benefit of a particular individual or group

Together, these branches form the comprehensive framework within which legal systems operate.

9.2 SOURCES OF LAW

Sources of law are categorized into the following, as also figure below shows:

- **Hard law** consists of *binding legal provisions* that can be legally enforced before a court, such as statutes, regulations, and treaties
    - These are *mandatory rules* that must be followed
    - The term is common in international law where there are no sovereign governing bodies
    - *Examples* in international hard law are treaties, UN Security Council Resolutions, Customary International Law (international practices)
- **Soft law**, on the other hand, includes agreements, principles, declarations, and statements which are not legally binding
    - Although soft law cannot be enforced by a court, it can guide judicial interpretation and influence the development of hard law by providing frameworks and recommendations
    - *Examples* of soft law include recommendations, guidelines, codes of conduct, non-binding resolutions, and standards



Sources of law include various legal instruments and frameworks that guide the creation, interpretation, and enforcement of legal norms. Examples include:

- *Treaties and conventions*
    - Agreements between states or international entities.
- *Legislation*
    - It comprises constitutions, acts, laws, statutes, regulations, and codes established by governmental bodies
- *Case-law*
    - It refers to judicial decisions that interpret and apply the law
- *Public and private policies*
    - These can influence legal frameworks
- *Doctrine*
    - This involves scholarly writings and theories
- *Fundamental or general principles of law*
    - Those provide foundational concepts
- *Customary law*
    - It arises from long-standing practices and traditions recognized as binding

Written by Gabriel R.

10 LECTURE 9 – EUROPEAN UNION (15 -11)

10.1 DEFINITION AND DIFFERENCES

The **European Union (EU)** is an international organization that has evolved through various treaties since 1952, including the Treaty of Rome and the Maastricht Treaty.

- It comprises 27 member states and represents a new legal order where states have limited their sovereignty for collective benefit
- The EU operates through a complex legal system integrated into the member states' laws, ensuring uniformity and cooperation
- Membership is open to European countries that respect human dignity, freedom, democracy, equality, and human rights
- The Copenhagen Criteria outline political, economic, and administrative requirements for access into the EU (see here on this)

There are some *differences* between how it is composed:

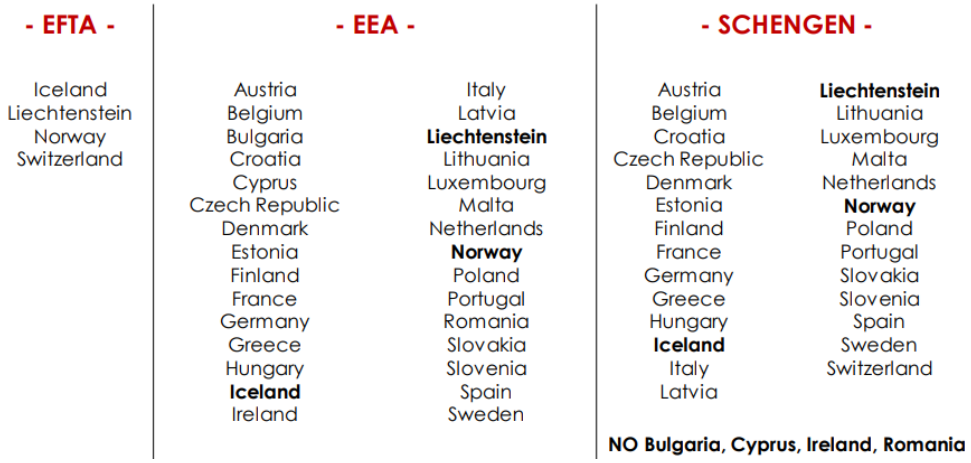
COUNCIL OF EUROPE - CoE -	EUROPEAN FREE TRADE ASSOCIATION - EFTA -	EUROPEAN ECONOMIC AREA - EEA -
Continental level	Regional trade organisation	EU MS + EFTA MS (no Switzerland)
46 Member States	Iceland, Norway, Liechtenstein, Switzerland	Defined by an international agreement (1994) within which the EU single market basic rules apply
Institutions (European Court of Human Rights)	Free trade area → participation in the European Single Market (not in the customs Union)	
	Participation in the Schengen Area	
Strasbourg (France)	Geneva (Switzerland) Bruxelles + Luxembourg	Geographic area

More specifically:

- The **Council of Europe (CoE)** operates with the goal of upholding human rights, democracy and the *rule of law* (compliance to existing legal systems) in Europe
- The **European Free Trade Association (EFTA)** is an intergovernmental organisation established in 1960 by the EFTA Convention, that p*romotes free trade and economic integration between its members*, within Europe and globally
- The **European Economic Area (EEA)** includes EU and EFTA members (excluding Switzerland) under an international agreement from 1994, *ensuring the application of EU single market rule*s across a defined geographic area
    - The single market seeks to guara*ntee the free movement of goods, capital, services, and people*, known collectively as the "*four freedoms*"
    - This is achieved through *common rules and standards* that all participating states are legally committed to follow

We consider here the *members* of such zones, including the following;

- The **Schengen Area** is a zone comprising most EU member states and some non-EU countries, such as Iceland, Liechtenstein, Norway, and Switzerland, which have abolished passport control at their mutual borders
    - This allows for free and unrestricted movement of people across member countries, though not all EU members participate
    - Notably, Bulgaria, Cyprus, Ireland, and Romania are not part of the Schengen Area



10.2 Legal Foundations of EU and Criteria for Application

Here we analyze some cases which are important when analyzing legal foundations of the EU:

«The Community constitutes a new legal order of international law for the benefit of which the states have limited their sovereign rights» ECJ, case 6/64, Costa v. ENEL [1964]

- ECJ, case 6/64, Costa v. ENEL (1964):

This case established the principle of EU law supremacy. Flaminio Costa, an Italian citizen, refused to pay an electricity bill to protest the nationalization of the electricity industry. He argued that the nationalization law conflicted with EU treaties.

The ECJ ruled that EU law takes precedence over national law when there's a conflict. This decision was crucial in establishing since the judgment expressly sanctioned the primacy of Community law over the law of the Member States.

This is important since legal subjects are not only the States, but citizens themselves.

«its own legal system which, on the entry into force of the Treaty, became an integral part of the legal systems of the Member States and which their courts are bound to apply (...)»

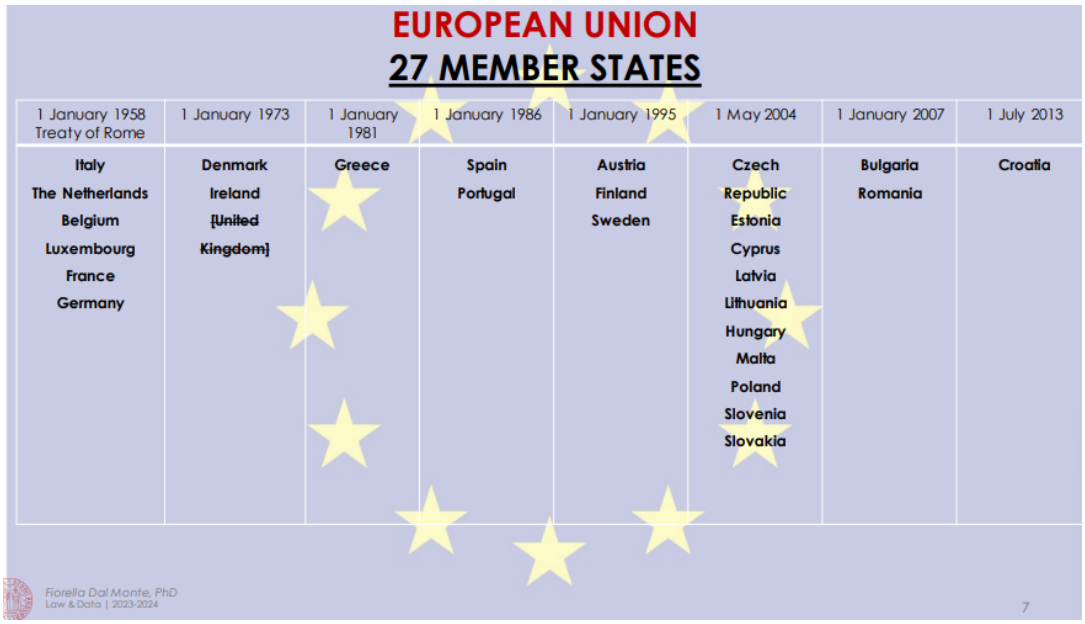
- ECJ, case 26/62, Van Gend en Loos (1963):

This case introduced the principle of direct effect of EU law. A Dutch transport company challenged a tariff imposed by Dutch customs, arguing it violated EU treaty provisions.

The ECJ ruled that EU law could confer rights on individuals that national courts must protect, even if the national law conflicted with EU law. This decision meant that EU law could be directly invoked by individuals in national courts, effectively making it an integral part of member states' legal systems.

This is important since laws are effective directly without intervention of any other Member State.

There are 27 different member states as you probably know at this point:



For the application for EU membership:

- ART. 2 TEU (Treaty on European Union – see titles and contents of articles here)

«Any European state which respects the common values of the Member States and undertake to promote them may apply to become a member of the Union.

These values include human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities»

- ART. 49 TEU

«Any European State which respects the values referred to in Article 2 and is committed to promoting them may apply to become a member of the Union. The European Parliament and national Parliaments shall be notified of this application.

The applicant State shall address its application to the Council, which shall act unanimously after consulting the Commission and after receiving the consent of the European Parliament, which shall act by a majority of its component members. The conditions of eligibility agreed upon by the European Council shall be considered.

Written by Gabriel R.

The conditions of admission and the adjustments to the Treaties on which the Union is founded, which such admission entails, shall be the subject of an agreement between the Member States and the applicant State. This agreement shall be submitted for ratification by all the contracting States in accordance with their respective constitutional requirements»

So, to summarize:

- Article 49 TEU outlines the procedure for application, requiring the applicant state to address its application to the Council, which must act unanimously after consulting the Commission and receiving the European Parliament's consent

The **Copenhagen Criteria** outline the requirements for a country to join the European Union.

- Political
    - Stability of institutions guaranteeing democracy, the rule of law, *human rights* and respect for and protection of minorities
- Economic
    - A functioning market economy and capacity to cope with competition/market forces
- Administrative and institutional capacity
    - To effectively implement the *acquis communautaire** and ability to take on the obligations of EU membership

The acquis communautaire, sometimes called *EU acquis* and often shortened to *acquis*, is the accumulated legislation, legal acts and court decisions that constitute the body of European Union law that came into being since 1993 – see indices of chapters here.

- The term is French: acquis meaning "that which has been acquired or obtained", and communautaire meaning "of the community"
- This includes all treaties, legislation, regulations, directives, decisions, and the principles developed by the European Court of Justice. It encompasses various policy areas such as single market regulations, environmental standards, consumer protection, and social policies
- New member states must adopt the acquis communautaire to ensure uniformity and compliance with EU standards and practices.

11 LECTURE 10 – HIERARCHY AND SOURCES OF LAW (17 -11)

11.1 HIERARCHY OF SOURCES AND PRIMARY LAW

The hierarchy of sources of European Union law is structured into several *levels* – see more here.

- At the top is **primary law**, which includes the founding treaties of the EU, such as the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)
    - These treaties set the fundamental legal framework and principles of the EU

- Following primary law are **international agreements**
    - These are treaties and agreements that the EU enters into with non-EU countries or other international organizations
    - They are binding on EU institutions and member states

- **Secondary law** comes next, consisting of regulations, directives, decisions, recommendations, and opinions (all legislative/non-legislative acts adopted by EU institutions, which enable the EU to exercise its powers)
    - Regulations are directly applicable in all member states without needing national implementation, while directives require member states to achieve specific results, leaving them the flexibility to choose how to do so
    - Decisions are binding on those to whom they are addressed

- Finally, **supplementary law** includes case law from the Court of Justice of the European Union (CJEU) and general principles of EU law
    - Case law is crucial in interpreting and filling gaps in primary and secondary legislation

11.2 TREATIES

Primary law in the EU consists of **treaties**, the Charter of Fundamental Rights, and general principles established by the European Court of Justice (ECJ). These include:

- Founding treaties
    - These were the ones established the European Communities, which evolved into the European Union (EU)
    - Key treaties include the Treaty of Rome (1957), which created the European Economic Community (EEC), and the Treaty of Maastricht (1992), which established the EU

- Amending (modificativo in Italian) treaties
    - These modify the founding treaties to reflect changes in the EU's structure and policies
    - Examples include the Single European Act (1986) and the Treaty of Lisbon (2007), which streamlined EU operations and expanded its powers

- Protocols annexed to treaties
    - Protocols are documents annexed to the main treaties that provide additional details or specific conditions related to the implementation of the treaties
    - They have the same legal force as the treaties themselves

- Accession treaties
    - Agreements between the EU and countries seeking to join
    - These treaties outline the terms and conditions of membership, including transitional arrangements and adjustments to the existing treaties

The **EU Charter of Fundamental Rights** consolidates the fundamental rights protected in the EU, including dignity, freedoms, equality, solidarity, citizens' rights, and justice (see more later)

- It was proclaimed in 2000 and given the same legal value as the treaties with the Lisbon Treaty in 2009, ensuring that EU institutions/MSs respect these rights when implementing EU law.

The **European Court of Justice (ECJ)** establishes general principles of EU law through its *case law*.

- These principles include proportionality, legal certainty and protection of fundamental rights
- They guide the interpretation and application of EU law, ensuring consistency and fairness in its implementation across all member states
- The ECJ's role is crucial in maintaining the integrity of the EU legal system

Talking about the treaties, we definitely have to talk the principal on which EU is based upon:

- The **Treaty on the European Union (TEU)** (effective since 1993, Maastricht Treaty) outlines objectives, principles, and institutions of EU
    - It sets the fundamental framework for the EU's goals, values, and the main bodies such as the European Parliament, Council, and Commission

- The **Treaty on the Functioning of the European Union (TFEU)** (effective since 1958, Treaty of Rome) provides detailed organizational and functional provisions to achieve EU objectives
    - It includes the procedures for the functioning of EU institutions and covers policies and internal actions necessary to ensure the EU operates efficiently and effectively, aligning member states with EU objectives

Article 2 of the Treaty on the European Union (TEU) establishes that the *EU is founded on values such as respect for human dignity, freedom, democracy, equality, the rule of law, and respect for human rights, including minority rights*.

- These values are common to the member states, promoting a society characterized by pluralism, non-discrimination, tolerance, justice, solidarity, equality between women and men
- These principles are fundamental in guiding the actions and policies of the EU and its MSs

Here we have its original text:

"The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.

These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."

Written by Gabriel R.

Article 3 of the Treaty on the European Union outlines the *EU's aims and objectives*. It seeks to promote peace, its values, and the well-being of its peoples.

- The Union ensures free movement, internal market establishment, sustainable development, scientific advancement, social inclusion, and protection of the environment. It promotes social justice, equality, and solidarity among member states
- The EU also maintains an economic and monetary union with the euro as its currency. In its external relations, the Union upholds its values and interests, contributing to peace, security, sustainable development, and human rights
- The Union pursues these objectives using appropriate means within its conferred competences

Here we have its original text:

"1. The Union's aim is to promote peace, its values and the well-being of its peoples.

2. The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime.

3. The Union shall establish an internal market. It shall work for the sustainable development of Europe based on balanced economic growth and price stability, a highly competitive social market economy, aiming at full employment and social progress, and a high level of protection and improvement of the quality of the environment.

It shall promote scientific and technological advance. It shall combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men, solidarity between generations and protection of the rights of the child. It shall promote economic, social and territorial cohesion, and solidarity among Member States. It shall respect its rich cultural and linguistic diversity and shall ensure that Europe's cultural heritage is safeguarded and enhanced.

4. The Union shall establish an economic and monetary union whose currency is the euro.

5. In its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among people, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter.

6. The Union shall pursue its objectives by appropriate means commensurate with the competences which are conferred upon it in the Treaties"

Article 16 of the Treaty on the Functioning of the European Union (TFEU) states the following:

"Everyone has the right to the protection of their personal data"

- This provision underscores the importance of privacy and data protection within the EU, establishing a fundamental right for individuals
- It forms the legal basis for EU data protection laws, such as the General Data Protection Regulation (GDPR), ensuring that personal data is processed fairly, transparently, and securely. This right is critical in safeguarding individuals' privacy in the digital age

Written by Gabriel R.

11.3 EU CHARTER OF FUNDAMENTAL RIGHTS

The **EU Charter of Fundamental Rights** consolidates the fundamental rights protected within the European Union. It was proclaimed in 2000 and became legally binding in 2009 with the Treaty of Lisbon, giving it the same legal status as the EU treaties. The Charter is divided into several *chapters*, each addressing different aspects of rights:

- 1. *Dignity*: Human dignity is inviolable and must be respected and protected
- 2. *Freedoms*: Covers various freedoms, including respect for private and family life, and the protection of personal data
- 3. *Equality*: Ensures equality for all individuals, prohibiting discrimination
- 4. *Solidarity*: Addresses social and workers' rights, promoting fair and just working conditions
- 5 .*Citizens' rights*: Details the rights of EU citizens
    - E.g., the right to vote and stand in European elections
- 6. *Justice*: Ensures access to justice and fair trials
- 7. *General provisions*: Includes safeguard clauses to protect rights and outlines applications

The Charter is a comprehensive document that integrates and reinforces the protection of fundamental rights within the EU, guiding both EU institutions and member states in their legislation and policies.

Here, its Article 6 quotes:

«The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties»

The general principles of EU law are developed by the Court of Justice over time and are constantly evolving. These include:

- *Legal certainty*
    - Ensures laws are clear and predictable
- *Legitimate expectation*
    - Protects individuals' expectations based on the law
- *Primacy of EU Law*
    - EU law takes precedence over national laws
- *Direct effect of EU Law*
    - Certain EU laws can be directly enforced by individuals in national courts
- *Protection for fundamental rights*
    - As per Article 6(3) TEU, fundamental rights are guaranteed by the EU
        - *"Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law"*

These are legal principles developed by the Court of Justice over time no exhaustive list – under constant development stemming from constitutional traditions of EU Member States.

Written by Gabriel R.

12 LECTURE 11 – EU LEGAL FRAMEWORKS AND INSTITUTIONAL DYNAMICS (22 -11)

12.1 INTERNATIONAL AGREEMENTS

The following *articles* from the Treaty on the Functioning of the European Union (TFEU) outline the EU's competence to engage in international agreements.

- **Art. 216 TFEU** establishes the *EU's ability to conclude agreements with third countries or international organizations when necessary to achieve EU objectives or when provided for in legally binding EU acts*
    - These agreements bind both EU institutions and member states

Its text follows:

«1. The Union may conclude an agreement with one or more third countries or international organisations where the Treaties so provide or where the conclusion of an agreement is necessary in order to achieve, within the framework of the Union's policies, one of the objectives referred to in the Treaties, or is provided for in a legally binding Union act or is likely to affect common rules or alter their scope.

2. Agreements concluded by the Union are binding upon the institutions of the Union and on its Member States».

- **Art. 217 TFEU** specifically *allows the EU to create association agreements involving reciprocal rights and obligations with third countries or international organizations*
    - This enables deeper partnerships and integration

Its text follows:

«The Union may conclude with one or more third countries or international organisations agreements establishing an association involving reciprocal rights and obligations, common action and special procedure»

- **Art. 218 TFEU** describes *the procedure for negotiating and concluding international agreements, involving the Council, European Parliament*, and potentially the *European Court of Justice (EUCoJ)*
    - This ensures proper institutional oversight and democratic legitimacy in the EU's external relations

12.2 SECONDARY LAWS

Secondary law in the European Union refers to the legal acts adopted by EU institutions based on the founding treaties.

- **Article 288 of the Treaty on the Functioning of the European Union (TFEU)** outlines the *typical acts of secondary law*. These are categorized into "hard law" and "soft law" instruments
    - Hard law includes regulations, directives, and decisions
        - Regulations are directly applicable in all member states, directives require national implementation, and decisions are binding on those to whom they are addressed
        - These instruments have legally binding force
    - Soft law comprises opinions and recommendations
        - While not legally binding, they provide guidance and can influence policy and practice within the EU

- Atypical acts, though not mentioned in Article 288 TFEU, include communications, resolutions, white papers, and green papers
    - These are used by EU institutions to communicate policies, propose legislation, or stimulate discussion on specific topics

12.3 INSTITUTIONS OF THE EU: EUROPEAN PARLIAMENT, EU COUNCIL

Article 13 of the Treaty on European Union (TEU) establishes the *main institutions of the European Union*. These institutions form the core of EU governance and decision-making processes. In general, we can define the following:

- The European Parliament *represents EU citizens and is directly elected*
    - It shares legislative and budgetary powers with the Council

- The European Council, composed of *heads of state* or *government*, s*ets the EU's overall political direction but doesn't legislate*

- The Council of the European Union (Council) *represents member state governments*
    - It shares legislative and budgetary authority with the Parliament

- The European Commission *proposes and enforces legislation, implements policies, and represents the EU internationally*

- The Court of Justice of the EU ensures E*U law is interpreted and applied consistently across member states*

- The European Central Bank (ECB) *manages the euro and EU monetary policy*

- The Court of Auditors *oversees EU finances*

Written by Gabriel R.

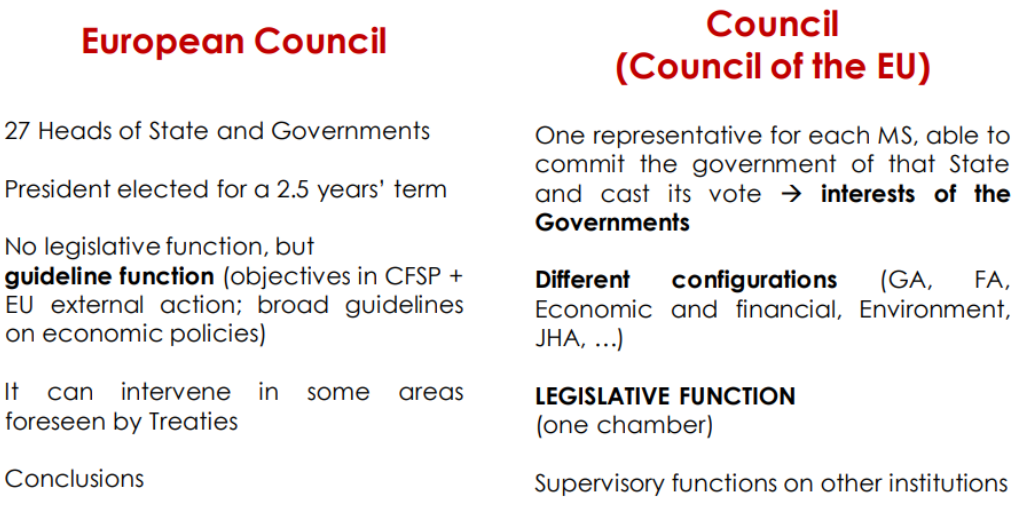
More specifically, on the **European Parliament**, which is the EU's law making body:

- Max 750 members = MEPs (currently 705) – Members of European Parliament
  - Every MS has a different number of MEPs according to its population
- Directly elected by EU voters every five years
- Since 1979 directly elected by EU citizens representing citizens' interests (not MS)
- Groups formed according to affinities in political parties (not upon nationality)
- Strasbourg | Brussels | Luxembourg

It has the following functions:

- *Legislative*
  - Passing EU laws, together with the council of EU, based on EU Commission proposals
  - Deciding on international agreements/enlargements, reviewing Commission's work programme
- *Budgetary*
  - Establishing the EU budget, together with the council, approving EU's long-term budget
- *Supervisory*
  - Democratic scrutiny of all EU institutions
  - Electing the Commission President and approving the Commission as a body
  - Granting discharge, i.e. approving the way EU budgets have been spent
  - Examining citizens' petitions and setting up inquiries
  - Discussing monetary policy with the European Central Bank
  - Questioning Commission and Council
  - Election observations
- *Elective*
  - President of the EU Commission (proposed by the Council)
  - EU Commissioners (proposed by the Commission's President)

This image compares two key EU institutions: the European Council and the Council of the European Union (Council).



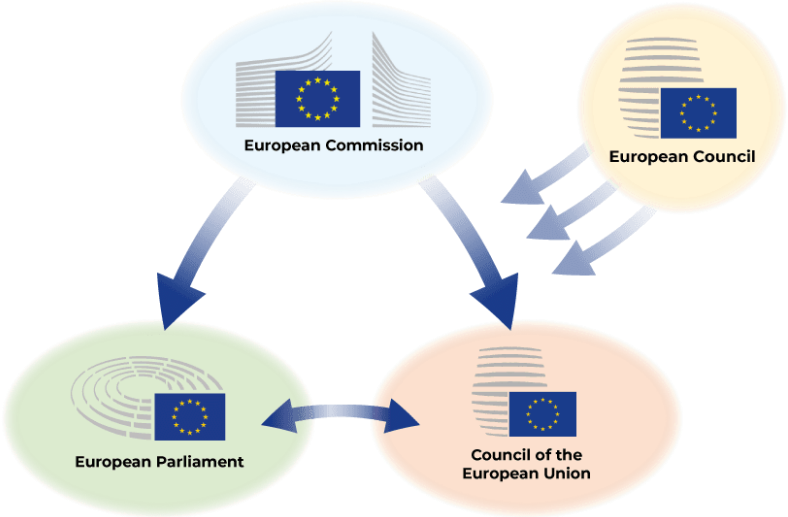
The **European Council** is a collegiate body defining the *overall political direction and priorities of the EU,* being part of the European Union, beside the European Commission.

- It is composed of the heads of state or of government of the EU member states, the President of the European Council, and the President of the European Commission
- While the European Council has no legislative power, it is a strategic (and crisis-solving) body that provides the union with general political directions and priorities and acts as a collective presidency
- The European Commission remains the sole initiator of legislation, but the European Council provides a guide to legislative policy

The **Council of the EU**, often simply called the *Council* but also *Council of Ministers*, comprises one representative from each member state, typically ministers.

- It is one of two legislative bodies and together with the European Parliament serves to amend and approve or veto the proposals of the European Commission, which holds the right of initiative
- The Council of the European Union and the European Council are the only EU institutions that are explicitly *intergovernmental*
    - That is, forums whose attendees express and represent the position of their Member State's executive, be they ambassadors, ministers or heads of state/government

Below, a summarizing enough image on the roles of each and a very nice explanation of the previous ones here (suggested).



13 LECTURE 12 – EU GOVERNANCE COMMISSION AND COURT (24-11)

13.1 EUROPEAN COMMISSION

The **European Commission (EC)** is part of the executive of the European Union (EU) – see here.

- It operates as a cabinet government, with 27 members of the Commission (directorial system, informally known as "*Commissioners*", appointed by the European Parliament – EP)) headed by a President, proposed by the European Council
- The commission is divided into *departments* known as *Directorates-General (DGs)* that can be likened to departments or ministries each headed by a Director-General who is responsible to a Commissioner
- It represents the interests of the EU as a whole, promoting the general interest of the EU by by proposing and enforcing legislation as well as by implementing policies and the EU budget

It has different functions:

- *Legislative* – initiative (proposes and enforces new laws)
- *Executive and administrative* – enforcement of EU law
- *Budgetary* – management of EU budget
- *Supervisory* – on MS (possible breaches of EU law) and on private entities

13.2 COURT OF JUSTICE OF THE EUROPEAN UNION

The **Court of Justice of the European Union (CJEU)** interprets EU law to make sure it is applied in the same way in all EU countries and settles legal disputes between national governments and EU institutions, ensuring countries and EU institutions abide by EU law – see here.

It can also, in certain circumstances, be used by individuals, companies or organisations to act against an EU institution, if they feel it has somehow infringed their rights.

The CJEU is divided into *2 courts*:

- Court of Justice – deals with requests for preliminary rulings from national courts, certain actions for annulment and appeals
    - This is formed by 1 judge from each EU country, plus 11 advocates general
- General Court – rules on actions for annulment brought by individuals, companies and, in some cases, EU governments
    - It's formed by 2 judges from each EU country
    - In practice, this means that this court deals mainly with competition law, State aid, trade, agriculture, trademarks

Both courts are staffed by *judges* and *advocates general*, whose number depends on the number of MS (usually one per MS) 6 years' term – renewable every three years.

Appointed among individuals possessing qualifications required for appointment to the highest judicial offices in their respective countries or jureconsults of recognised competence BUT *independent from their MS*.

Written by Gabriel R.

They have distinct functions:

- *Jurisdictional*: Handles litigation between parties
- *Interpretative/Preliminary rulings*: Provides clarification on EU law, not direct litigation
- *Advisory/consultative*: Offers opinions on EU law matters, also not litigation

The CJEU gives rulings on cases brought before it. The most common types of case are:

- Interpreting the law (preliminary rulings) – national courts of EU countries are required to ensure EU law is properly applied, but courts in different countries might interpret it differently
- Enforcing the law (infringement proceedings) – this type of case is taken against a national government for failing to comply with EU law
- Annulling EU legal acts (actions for annulment) – if an EU act is believed to violate EU treaties or fundamental rights, the Court can be asked to annul it – by an EU government, the Council of the EU, the European Commission or (in some cases) the European Parliament
- Ensuring the EU takes action (actions for failure to act) – the Parliament, Council and Commission must make certain decisions under certain circumstances
- Sanctioning EU institutions (actions for damages) – any person or company who has had their interests harmed as a result of the action or inaction of the EU or its staff can take action against them through the Court

Here are the *types of litigation proceedings before the European Court of Justice (ECJ)* under the Treaty on the Functioning of the European Union (TFEU):

1. **Direct appeals (Article 263 TFEU)**
    a. This allows for the *appeal of acts adopted by EU institutions*, initiated by either public entities like Member States (MS) and other EU institutions, or private individuals against acts directly affecting them without implementing measures
    b. Appeals can challenge competence, validity, or misuse of power and must be filed within 2 months and 10 days

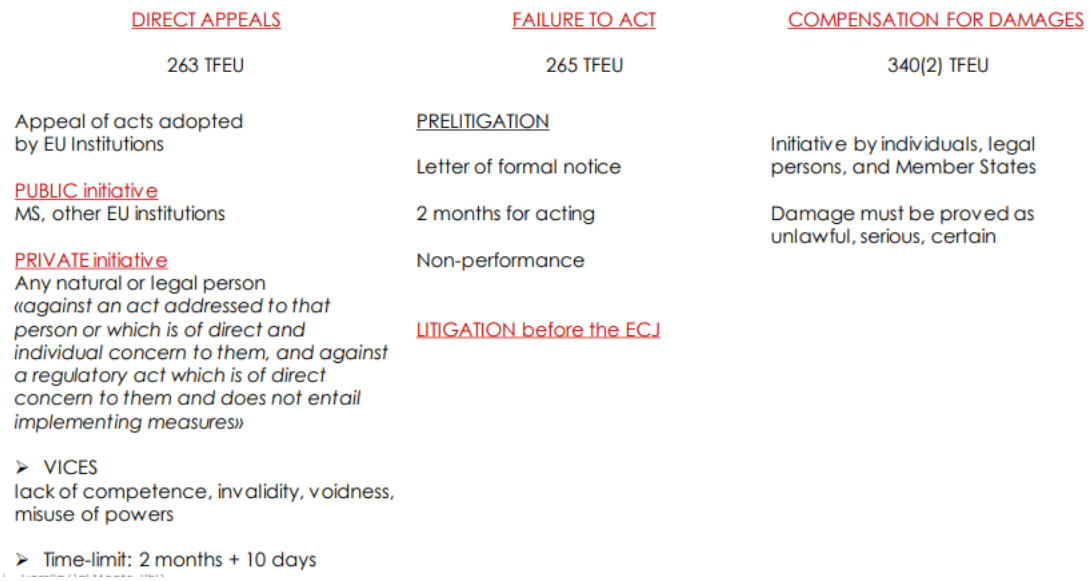
2. **Failure to act (Article 265 TFEU)**
    a. This process begins with a letter of formal notice if an EU institution fails to act, providing them two months to respond
    b. Non-performance leads to litigation before the ECJ

3. **Compensation for damages (Article 340(2) TFEU)**
    a. Individuals, legal entities, or Member States can initiate this for damages proven to be unlawful, serious, and certain

14 LECTURE 13 – PROCEEDINGS AND BODIES OF EU (29 -11)

14.1 PROCEEDINGS BEFORE THE ECJ – LITIGATION AND NON-LITIGATION

Once again, we start from the litigation proceedings before the ECJ (in case, see also this).



Here we give some details about the **non-litigation procedures** involving preliminary rulings by the European Court of Justice (ECJ), not the General Court, under Article 267 of the Treaty on the Functioning of the European Union (TFEU).

There are court affairs which does not form a legal proceeding, but in which the court assists and engages in the procedure of creation, alteration, or extinguishment of personal rights. It is called a non-litigation case.

Here's a brief *overview*:

- *Initiative*
  - *Any jurisdiction* of a Member State (MS) can request a preliminary ruling, based on the nature and instance of the case, and also at the parties' request

- *Object*
  - The ECJ gives *interpretation* of EU law provisions and assesses the *validity* of acts from EU institutions

- *Development*
  - The process begins with national proceedings within a Member State
  - The national judge may refer the case to the ECJ for a preliminary ruling
  - Typically, this referral leads to a suspension of the national proceedings
  - The ECJ's decision is binding and *compulsory* for national judge handling initial case

14.2 BODIES OF THE EU

Here we descrive the **bodies** within the European Union focused on data protection and fundamental rights:

- European Data Protection Supervisor (EDPS) – here
    - Independent body monitoring and ensuring that EU institutions and bodies respect people's right to privacy when processing their personal data, intervening and cooperating when necessary

- European Data Protection Board (EDPB) – here
    - Independent body ensuring the consistent application of data protection rules throughout the EU (both GDPR and Data Protection Law Enforcement Directive), promoting cooperation between national data protection authorities in the EU

- Agencies of the European Commission – here
    - EU decentralized bodies distinct from the institutions
    - Specific tasks

- Fundamental Rights Agency
    - It focuses on the core rights and freedoms within the EU context

15 LECTURE 14 – PRIVACY AND RIGHTS (01 - 12)

15.1 PRIVACY – RIGHT TO BE LET ALONE & TO PERSONAL DATA

The concept of **privacy** encompasses various dimensions such as the right to reputation, honor, personal and family life, and the control over personal information, underpinning the legal distinction between private and public spheres.

Privacy and the Right to be Let Alone (1890), introduced by Warren and Brandeis, sees privacy as a pivotal human right, involving the protection of personal reputation, honor, image, and family life. It emphasizes personal autonomy, including the control of personal information, and underscores the legal need to distinguish private matters from public exposure. This concept has common law origins.

So, we start a distinction between what is private from what is public.

15.2 HUMAN RIGHTS – RIGHT TO PRIVACY AND PERSONAL DATA

There is a fundamental difference in how privacy is viewed within Common Law and Civil Law traditions.

Common Law tradition	Civil Law tradition
RIGHT TO LIBERTY	RIGHT TO DIGNITY

- In the Common Law system, privacy is primarily seen through the lens of liberty, emphasizing an *individual's right to be free from unwarranted intrusions*
    - Here there are stronger protections for personal freedoms and rights against government intrusion

- On the other hand, Civil Law tradition places a stronger emphasis on dignity, viewing *privacy as integral to the respect* and *inherent worth of individuals*
    - This might translate to laws that protect personal honor, privacy, or social welfare

Under Article 8(1) of the Charter of Fundamental Rights of the European Union (CFR),

«Everyone has the right to protect personal data concerning him or her»

Here is also given the precise definition of personal data:

«Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person» Art. 4(1)(1) GDPR

Basically, any information related to an identifiable living individual.

The *rights to privacy and personal data* are distinct but share significant overlaps. The protection of both is crucial in safeguarding individuals' autonomy across various identifiers such as race, nationality, or religion.

- These rights are instrumental in protecting individuals from invasive practices that could threaten personal integrity and autonomy
- In particular, these are rights belonging to individuals as human beings regardless of race, sex, nationality, ethnicity, language, religion or any other status

15.3 History – Right to Privacy

Here we give an *overview* about the history of privacy:

- UN Universal Declaration of Human Rights (1948)
    - *Article 12*
        - No one shall be subjected to *arbitrary interference* with his privacy, family, home or correspondence, nor to attacks upon his *honour and reputation*
        - Everyone has the right to the protection of the law against such interference or attacks

- International Covenant on Civil and Political Rights (1966)
    - *Article 17*
        - 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation
        - 2. Everyone has the right to the protection of the law against such interference or attacks

- UN Convention on the Rights of the Child (1989)
    - *Article 16*
        - *No child* shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation
        - *The child* has the right to the protection of the law against such interference or attacks

- European Convention of Human Rights (1950)
    - *Article 8 – Right to respect for private and family life*
        - 1. Everyone has the right to respect for his private and family private life, his home and his correspondence
        - 2. *There shall be no interference by a public authority* with the exercise of this right *except* such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

16 LECTURE 15 – RIGHT TO PRIVACY AND EU DIRECTIVES (06 - 12)

16.1 RIGHT TO PRIVACY

While originally not present in the 1948 Universal Declaration of Human Rights, we can quote from its article 12 the following statement on **privacy**: "No one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".

The **Nice Charter (2009)** and the **EU Charter of Fundamental Rights (2009)** are crucial because they provide a codified set of rights that are legally binding on the European Union (EU) and its member states. These documents consolidate and ensure a wide range of civil, political, economic, and social rights for EU citizens and residents – see for them here.

The transition from the Nice Charter to the EU Charter of Fundamental Rights marked a significant evolution in the EU's commitment to protecting fundamental human rights. These charters are instrumental in shaping EU laws and have a direct impact on the legislation of member countries, aligning them with shared European values and legal standards.

We quote different *articles* now from EU Charter of Fundamental Rights:

- Article 7 – Respect for private and family life
    - 1. Everyone has the right to respect for his or her private and family life, home and communications
    - 2. There shall be no interference by a *public authority* with the exercise of this right *except* such as is in accordance with the law and is *necessary* in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

- Article 8 – Protection of personal data
    - 1. Everyone has the right to the protection of personal data concerning him or her
    - 2. Such data must be processed fairly for *specified purposes* and on the basis of the consent of the person concerned or some *other legitimate basis* laid down by law
    - Everyone has the right of *access* to data which has been collected concerning him or her, and the right to have it *rectified*
    - 3. Compliance with these rules shall be subject to control by an *independent authority*

- Article 52 – Scope and interpretation
    - 1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others
    - 2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties

16.2 RIGHT TO PERSONAL DATA PROTECTION

The OECD Privacy Guidelines (with OECD standing for Organisation for Economic Co-operation and Development) established in 1980, represent a set of universal standards aimed at balancing the rights of data subjects with the needs of data controllers. These introduce *several key principles*:

- Collection limitation
    - There should be *limits to the collection of personal data*, which must be obtained by *lawful and fair means*
- Data quality
    - Personal data should be *relevant to the purposes for which they are used*, and be accurate, complete, and up-to-date
- Purpose specification
    - The *purposes for which personal data are collected should be specified* at the time of data collection
- Use limitation
    - *Personal data should not be disclosed*, made available, or otherwise used *for purposes other than those specified* except with the consent of the subject or by the authority of law
- Security safeguards
    - *Personal data should be protected by reasonable security safeguards against risks* such as loss or unauthorized access, destruction, use, modification, or disclosure
- Openness
    - There should be a *general policy of openness about developments, practices, and policies* with respect to personal data
- Individual participation
    - An individual should have the *right to obtain data about themselves*, and to have data corrected or erased if it is inaccurate, incomplete, outdated, or processed unlawfully
- Accountability
    - *Data controllers should be accountable for complying with measures* that give effect to the principles stated above

The Council of Europe's (CoE) Convention 108, established on January 28, 1981, serves as the first *legally binding* international treaty concerning data protection, so to give *universal standards*.

- It was born as a convention for the protection of individuals with regard to automated processing of personal data
- It outlines standards for the protection of individuals with regard to the automated processing of personal data, aiming to secure the individual's right to privacy
- The Convention 108+ update, adopted on May 18, 2018, enhances these protections to address new challenges in data privacy and adapts to technological developments, reinforcing the universal standards initially set out in the original convention

CoE Convention *Main Principles* follow here:

- Protection of the individuals against Personal Data (PD) abuses
- Regulation of transborder data flows
- Fair and lawful collection
- Legitimate purposes
- Processing for the same purposes for which data were collected
- Storage duration (no longer than necessary)
- Quality of data: adequate, relevant not excessive (proportionality)
- Sensitive data (special categories of data)
- Right to know information stored and to have it rectified
- Possible overriding interests for different processing activities

The applicable EU legislation on the right to personal data protection follow here:

- Article 39
    - In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the *Council* shall adopt a *decision laying down the rules* relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which *fall within the scope of this Chapter*, and rules relating to *free movement* of such data
    - Compliance with these rules shall be subject to the control of independent authorities

- Article 16
    - 1. Everyone has the right to the protection of personal data concerning them
    - 2. *The European Parliament and the Council*, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free *movement of such data*. Compliance with these rules shall be subject to the control of *independent authorities*
    - 3. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union

EU Data Protection Directives are two:

- Directive 95/46/EC – Data Protection Directive on the pr*otection of individuals with regard to the processing of personal data* and on the *free movement of such data* – complete text here
    - Limited harmonization → GDPR

- Directive 2006/24/EC – Data Retention Directive on the *retention of data generated or processed in connection with the provision of publicly available electronic communications services* or of *public communications networks* and amending Directive 2002/58/EC – here
    - Repealed by ECJ in Digital Rights Ireland | C-293/12 + C-594/12

17 LECTURE 16 – EU DATA PROTECTION DIRECTIVES (13 - 12)

17.1 APPLICABLE EU DATA PROTECTION DIRECTIVES

The following **directives** are *integral components of EU's legal framework* aiming to pro*tect personal data and individual privacy across different contexts and sectors*, *enhancing security and trust* in digital services.

- 1. Directive 2002/58/EC – ePrivacy Directive
    - Focuses on the protection of privacy in electronic communications
    - It regulates processing of PD in the electronic communications sector and includes provisions on confidentiality of communications, cookies, unsolicited marketing

- 2. Directive 2016/680/EU – Law Enforcement Directive
    - Pertains to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offenses
    - It aims to ensure data protection within the law enforcement sector and facilitates the cross-border exchange of such data within the EU, replacing the older Framework Decision 2008/977/JHA (Justice and Home Affairs Council) to better align with modern standards and the General Data Protection Regulation (GDPR)

17.2 DIRECTIVE 2002/58/EC | E-PRIVACY DIRECTIVE

Going more specifically on this directive, we give the following **definitions**:

- User
    - Any *natural person* using a *publicly available electronic communications service*, for private or business purposes, without necessarily having subscribed to this service
    - This is also called subscriber

- Traffic data
    - Any data *processed* for the purpose of *the conveyance of a communication* on an electronic communications network or *for the billing* thereof

- Location data
    - *Any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user* of a publicly available electronic communications service

- Communication
    - *Any information exchanged or conveyed* between a *finite number of parties* by means of a *publicly available electronic communications service*
    - This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber/user receiving the information

As an overview of the directive:

- *Scope of application*
  - "Services concerned" processing of PD in connection with the provision of publicly available electronic communications services in communications networks within EU
- *Service provider*
  - Required to take appropriate technical and organizational measures to ensure security of its services
- *Objective*
  - Require MSs to ensure confidentiality of communications and related PD (i.e. traffic data) processed through public communication networks/publicly available electronic communications services

Other features:

- *Automatic call forwarding*
  - By third parties to the subscriber's terminal, unless stopped
- *Directories of subscribers*
  - Possible, but based on consent (express or implied)
- *Unsolicited communications*
  - Automated calling systems without human intervention / fax / e-mail / direct marketing possible, but with clear, distinct and prior consent possibility to object free of charge & easily

17.3 DIRECTIVE 2018/1972 EUROPEAN ELECTRONIC COMMUNICATIONS CODE (RECAST)

The **European Electronic Communications Code (Recast)** is outlined in **Directive 2018/1972**.

It sets an EU-level legal framework to coordinate national legislation on electronic communications networks and services, from the telephony services and the single European emergency number 112 to basic internet access that must now be considered as a universal service by EU countries, with an emphasis on not processing personal data – see here.

The directive has the following *goals*:

- Implement an *internal market* in electronic communications
- Promote *fair competition* between companies
- Ensure equal and fair access to these services
- Promote *connectivity* all across EU

18 LECTURE 17 – EU DATA PROTECTION DIRECTIVES (15 - 12)

18.1 DIRECTIVE 2016/680/EU | DP LAW ENFORCEMENT DIRECTIVE

Directive 2016/680/EU, also known as the **Data Protection Law Enforcement Directive**, addresses personal data protection in criminal matters within the EU – see here.

- This directive replaced **Decision 2008/977/JHA** and aimed to cover areas previously governed by the *Data Retention Directive*, which had been voided
- It was part of a broader reform, introduced simultaneously with the General Data Protection Regulation (GDPR), together known as the "*PDP Package*"
- This package seeks to modernize and harmonize data protection frameworks across the EU, specifically focusing on processing personal data by police and judicial authorities for the purposes of preventing, investigating, detecting, and prosecuting criminal offenses

18.2 EU DATA PROTECTION REGULATIONS

Directive 2016/680/EU focuses on data protection within law enforcement activities. It emphasizes *principles* like data protection by design and by default, ensuring robust data security measures, and requiring data breach notifications. It reports the following *points*:

- Data protection by design / by default
- Data security
- Data breach notifications
- Appointment of Data Protection Officers (DPOs)
- Emerging tech challenges

Importantly, it restricts decisions based solely on automated processing, such as profiling, particularly those based on sensitive data, to prevent discrimination. These stipulations aim to balance effective law enforcement with the protection of individual privacy rights.

There are also other *regulations* to note:

- **Regulation 2016/679/EU General Data Protection Regulation (GDPR)** – here
    - GDPR sets a comprehensive framework for data protection across the EU, applying strict privacy and security standards to protect individual rights
- **Regulation 2018/1725/EU – Protection of natural persons on processing of PD** – here
    - It sets forth the rules applicable to the processing of personal data by European Union institutions, bodies, offices and agencies

The reference to the Digital Services Act (DSA) and Digital Markets Act (DMA) suggests a broader regulatory environment aimed at digital platforms, promoting fair competition and accountability.

These are two significant pieces of EU legislation aimed at regulating digital platforms to ensure a safer digital space and promote fair competition.

- DSA focuses on creating a safer digital space where users' fundamental rights are protected
- DMA targets large online platforms acting as "gatekeepers" to ensure that these platforms do not abuse their powerful market position

18.3 GDPR – Main Subjects & Data Subject

The **General Data Protection Regulation (GDPR)** is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in and outside of the European Union (EU).

We will now discuss it with the distinction of the following main *subjects*:

- Data subject
- Controller
- Processor
- Sub-processor
- Data protection officer (DPO)
- Supervisory authority

The term "**data subject**" in GDPR refers to any individual who can be identified, directly or indirectly, by information such as a name, an identification number, location data, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

In has the following *main rights*:

- Right to transparency of communication
- Right to be informed of purposes
- Right to access
- Right to rectification, erasure*, restriction
    - Right to be forgotten
- Right to data portability
- Right to object

19 LECTURE 18 – GDPR: PROCESSOR & CONTROLLER (20 - 12)

19.1 CONTROLLER: OBLIGATIONS AND DPMS

The General Data Protection Regulation (GDPR) defines a **controller** as:

- "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means *of the processing of personal data*"

When two or more entities jointly determine the purposes and means of processing, they are considered **joint controllers**. This designation carries specific responsibilities regarding the lawful handling of personal data, including ensuring transparency, data security, and adherence to data protection principles laid out by the GDPR.

Controllers have also **obligations**: as a general rule, *a controller is responsible and liable for any processing of personal data carried out by itself and on its behalf*. Specifically, here we list the *main obligations* of the Controller:

- Adoption of appropriate TOMs (Technical and Organizational Measures) for GPDR compliance
- Record of processing activities
- Cooperation with data subjects
- Cooperation with supervisory authorities

A Data Protection Management System (DPMS) is a *risk-based internal compliance framework* designed primarily to ensure GDPR compliance.

- It includes a robust IT security concept that manages and oversees the technical and organizational aspects of data processing activities
- By adopting and implementing appropriate Technical and Organizational Measures (TOMs), DPMS aims to document these activities comprehensively and enhance overall data protection compliance within an organization to GDPR
- The aim is to *achieve compliance with GDPR, by adopting appropriate TOMs*

19.2 PROCESSOR: OBLIGATIONS AND CONTENTS OF THE RECORD

The General Data Protection Regulation (GDPR) defines a **processor** as:

- "A natural or legal person, public authority, agency or other body which processes* personal data on behalf of the controller"

Let's specify what *processing of personal data means:

- *Any operation or set of operations which is performed on personal data or on sets of personal data*, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

We list here the main **obligations** of the processors:

- Act upon instructions of the Controller
- Implement TOMs
- Appoint a Representative within the EU
- Maintain a record of processing activities
- Cooperate with Supervisory Authorities
- Designate a DPO - Data Protection Officer (where required)

Here is outlined the record-keeping responsibilities under GDPR for both controllers and processors of personal data.

CONTROLLER	PROCESSOR
Name and contact details of the (joint) controller(s), the representative(s) and DPO(s)	Name and contact details of the processor(s) and (joint) controller(s), the representative(s) and DPO(s)
Purposes	Categories of processing
Description of the categories of data subjects and categories of personal data	--
Categories of recipients to whom personal data are or will be disclosed (including outside EU and/or international organisations)	--
Transfer to third countries/international organisation and documentation of suitable safeguards	Transfer to third countries/international organisation and documentation of suitable safeguards
Envisaged time-limits for erasure of the different categories of data	--
General description of TOSMs	General description of TOSMs

20 LECTURE 19 – GDPR: DPO, AUTHORITIES, MAIN NOTIONS (22 - 12)

20.1 DPO & SUPERVISORY AUTHORITIES

According to GDPR, the **data protection officer (DPO)** is:

- "A person *who advises on compliance with data protection rules in organisations* undertaking data processing"

Voluntarily appointed by controllers, unless:

- A public authority or body carries out the processing
- The controller's or processor's core activities consist of processing operations requiring the regular and systematic monitoring of data subjects on a large scale
- The core activities consist of categories large-scale processing of special categories of data or personal data relating to criminal convictions and offences"

Instead, the **supervisory authorities** are defined as:

- "Independent public authority established by each Member State pursuant to Article 51 – the article is Control Authority in GDPR"

They have various responsibilities:

- Data subjects' complaints
- Be responsible for monitoring the application of the GDPR, in order to protect fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union
- Contribute to the consistent application of the GDPR throughout the Union and collaboration with the EU Commission

20.2 MAIN NOTIONS

From here, some *main notions* about GDPR will be delighted:

- **Personal data**
  - *Any information relating to an identified/identifiable natural person* ("data subject")
    - An identifiable natural person is one who can be identified, directly or indirectly
    - In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic identity of that person

- **Sensitive data**
  - *Special categories of personal data*
  - Personal data revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs*, or *trade union membership*, and the processing of g*enetic data, biometric data* for the purpose of uniquely identifying a natural person, data concerning *health* or data concerning a natural person's *sex life or sexual orientation*

Written by Gabriel R.

In principle, the processing of sensitive data is considered prohibited.

There are a few *exceptions* however:

- Explicit consent (specified purposes)
- Employment law / social security and social protection law
- Protection of vital interest
- Legitimate activities of foundations, associations, non-profit bodies – members or former members
- Manifestly made public by DSs (Data Subjects)
- Legal claims
- Substantial public interest
- Preventive / occupational medicine
- Health - public interest
- Scientific and historical research – public interest

GDPR does not define explicitly the **purposes**, but they can be generally described as:

- "Aims for which data are collected and processed"

Instead, GDPR defines the **consent** (of the data subject) as:

- "*Any freely given, specific*, informed and *unambiguous indication* of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Moving on, GDPR defines the **processing** as:

- *"Any operation or set of operations which is performed on personal data or on sets of personal data,* whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

Also, GDPR defines a **DPIA – Data Protection Impact Assessment**, as:

- Assessment of the impact of the envisaged processing operations on the protection of personal data helping identify/minimize data protection risks of a project (particularly, determining "whether processing likely result in high risk")
- These is mapping $Controller \longleftrightarrow DPO$, since one determines how data will be handled while the other one guarantees rules are respected according to Controller dispositions

The DPIA contents follow here:

- Systematic description of the envisaged processing operations + purposes + legitimate interest of the Controller (if any)
- Assessment of the necessity and proportionality of the processing operations *in relation to the purposes*
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance

Written by Gabriel R.

21 LECTURE 20 – GDPR: MAIN PRINCIPLES FOR PD PROCESSING (10 - 01)

21.1 MAIN PRINCIPLES FOR PERSONAL DATA PROCESSING

In this lecture, we start considering all of the **main principles for data processing** (such are listed):

- Lawfulness
- Fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

21.2 LAWFULNESS, TRANSPARENCY, PURPOSE LIMITATION

Lawfulness and fairness are based on legal permission given from the DS consent. Legal permission is necessary for:

- Performing a contract
- Complying with a legal obligation
- Protecting vital interests
- Performance of a task of public interest
- Legitimate interests of the controller/third party

Transparency describes *how PD are used, consulted or otherwise disclosed*. The *information* which should be note is the following:

- On the identity of the controller
- On the purposes of the processing
- On the DS rights / to obtain confirmation and communication of processing activities
- On risks, rules, safeguards and rights in relation to processing activities

Purpose limitation principle requires that personal data be processed only for *specified, explicit, and legitimate purposes*. The key aspects are the following:

- *Legitimacy*
    - The purposes for processing must be in accordance with existing applicable laws
    - This ensures that data processing is lawful and compliant with relevant regulations
- *Detail of the purpose*
    - The purpose must be clearly defined and communicated
    - Any further processing operations need to be verified to ensure they are compatible with the initial purposes for which the data was collected

21.3 Data Minimisation, Accuracy, Storage Limitation

The **data minimization** principle ensures personal data shall be *adequate, relevant and limited* to what is necessary in relation to the purposes for which they are processed. Here:

- An assessment of proportionality should be made
- Accurate technical and organisational measures

The principle of **accuracy** ensures personal data should be *accurate and kept up to date*.

- If data is inaccurate, erasure or rectification must be done
- Personal data shall reflect the reality of any given situation
- Inaccuracy may imply legal consequences even for the subjects involved

Storage limitation principle says personal data shall be kept in a form that permits identification of data subjects for no longer than necessary for the processing purposes, basically the *bare/strict minimum*.

21.4 Integrity and Confidentiality, Accountability & Privacy Policy

Integrity and confidentiality principles *ensure personal data shall be processed in a manner that ensures their appropriate security*. This is necessary to avoid:

- Unauthorised/unlawful processing
- Unauthorised/unlawful access
- Accidental loss, destruction, damage

The principle of **accountability** focuses on focusing on two key roles:

1. *Controller*: This is typically the entity (organization or individual) that determines the purposes and means of processing personal data, ensuring compliance with data protection laws
2. *Processor*: This is the entity that processes personal data on behalf of the controller

Both controllers and processors must take responsibility for their handling of personal data.

A **privacy policy** is a crucial document for any organization handling personal data and some templates on how to write a policy is here. The topics asked are the following:

- What data do we collect?
- How do we collect your data?
- How will we use your data?
- How do we store your data?
- Marketing
- What are you data protection rights?
- How to contact us
- How to contact the appropriate authorities

Inside of websites, some questions can be asked on this:

- How do we use cookies and what types of cookies do we use?
- How to manage your cookies
- Privacy policies of other websites
- Changes to our privacy policy

22 LECTURE 21 – EU DATA AND REGULATIONS (12 - 01)

22.1 EU DATA STRATEGY

The **European Data Strategy** is a comprehensive plan initiated by the European Union (EU) to create a single market for data. This strategy is aimed at making the EU a leader in the data-driven economy, ensuring that data flows freely across the Union and is utilized to its full potential for the benefit of society and businesses alike. Its main principles are:

- *Free flow of personal data*
    - Guaranteeing protection, privacy, portability, cross-border data flow, ensuring respect of rules according to regulatory frameworks
- *Free flow of non-personal data*
    - Ensure improvement over data localization restrictions, data availability for regulatory controls, portability/interoperability
- *Single market for data*
    - Data sharing among sectors, aiming to clarify with acts data and its usage, between sectors and infrastructure

The EU Data Strategy, initiated in 2020, is a comprehensive framework aimed at making the European Union a global leader in the data-driven economy. It encompasses various regulations and acts designed to ensure a balanced, fair, and innovative digital environment.

- **Regulation 2018/1807 (Free Flow of Non-Personal Data)**: *Eliminates data localization restrictions within the EU* and promotes *data portability* and *interoperability*
- **Data Governance Act (DGA) (2022)**: Establishes a *framework for the ethical and transparent reuse of public sector data*, *data altruism, and data-sharing intermediaries*
- **Digital Services Act (DSA) (2022)**: Imposes *obligations on online platforms to enhance user safety, transparency* in advertising, and *consumer protection*
- **Digital Markets Act (DMA) (2022)**: Regulates *large digital platforms (gatekeepers) to ensure fair competition* and *prevent market abuses*
- **AI Act (Expected 2024)**: Creates a *legal framework for AI systems based on their risk level*, ensuring *safety*, *transparency*, and *fundamental rights*
- **Data Act (Expected 2024)**: *Regulates IoT-generated data access and sharing*, enhancing data *portability* and *fairness* in data-related contracts.

22.2 REGULATION 2018/1807

Regulation 2018/1807 has the purpose of *ensuring free flow of data other than personal data* laying down rules relating to data localization requirements. *Scope of the application* is the following:

- Applies to the *processing of electronic data* other than personal data
- Includes data processing provided as a service to users within the EU or carried out by a person within the EU
- Limited application to *sets of data* that contain both personal and non-personal data, where non-personal data provisions apply to the non-personal data part

Written by Gabriel R.

The data localisation requirements are the following:

- Obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law

In principle, data localization requirements are *prohibited*.

- This means that MSs cannot enforce rules that require data to be processed or stored within their territory, nor can they hinder the processing of data in another member state.

There are *obligations* upon the Member States to repeal any legal provision setting out data localisation requirements. The goals are the following:

- Encouraging the development and adoption of self-regulatory codes of conduct
- To contribute to a competitive data economy

22.3 Acts: DGA, DSA, DMA, AI & Big Data

The **Data Governance Act (DGA)** is a key component of the EU's data strategy, aiming to establish a robust framework for facilitating a safe data-sharing setting out conditions for their *re-use* and *intermediation services*. It covers data held by:

- Public bodies
- Private entities
- Citizens

Data = any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording.

The **EU Digital Services Act (DSA)** and the **EU Digital Markets Act (DMA)** are complementary legislative measures under the EU's digital strategy aimed at regulating the digital space. Their primary aims are to create a safer online environment and to ensure fair competition in digital markets.

In specific:

- DSA ensures the creation of a safer digital space, accounting for user protection and ensuring transparency and accountability
- DMA ensures fair competition while fostering innovation and growth, so to prohibit practices and enforce obligations and penalties in case of non-compliance

As general aims, we can report:

- 1. *Creating a safer digital space* where users' fundamental rights are protected
- 2. Establishing a *level playing field to foster innovation*, *growth* and *competitiveness*

The **Artificial Intelligence Act (AI Act)** is a landmark legislative proposal by the European Union which has the aim at establishing a harmonized legal framework for artificial intelligence.

The Act seeks to ensure that AI systems are used in a way that respects fundamental rights, promotes safety and transparency, and supports innovation and economic growth. Particularly, it enhances the capabilities of AI systems improving predictions, optimizing operations and personalizing service delivery.

It also gives the following *advantages*:

- Support socially and environmentally beneficial outcomes
- Key competitive advantages to companies and the EU economy

In the end, we define **big data** as "great volume, velocity and variety of (personal and non-personal) data and technological ability to collect, process and extract new and *predictive knowledge*".

23 EXAMS

(This section is dedicated to the material present between the Telegram group and what I archived in MEGA regarding the course, the material and exams + mock test present)

General rules – Instructions

You will have 75 minutes to conclude your test, which is divided into two sections and totally counts 8 questions.

The first part includes multiple-choice questions. Please, consider that some of them may have more than one correct answer.

The second part is made up of open questions. You are warmly invited to answer using the maximum recommended number of words.

Every question specifies the maximum number of points recognized for each correct answer in the overall assessment of your exam.

23.1 MOCK TEST – 17 JANUARY 2024

23.1.1 Multiple choice questions (MCQ)

1. The main difference between the EU and the US approaches to the legal regime of personal data is (1 pt)
    a. That the EU treats personal data as as an aspect of individual personality, whereas the US treats data as a market
    b. That only EU protects privacy
    c. That only the US protect privacy
    d. That only the US approach leverages individual consent to protect privacy

2. Correcting illegal bias in AI (2 pts – more answers)
    a. Is always legitimate
    b. Must be done in a way that does not violate basic legal principles such as equality
    c. Is legally impossible
    d. Can be done only by amending the algorithm or the dataset for the training

3. The processing of personal data pursuant to the GDPR may be lawfully carried out (2 pts)
    a. When data subjects expressed their own consent
    b. Based on the controller's free choice
    c. When there is no consent by data subjects, but the processing is needed for protecting the data subjects' or other individuals' vital interests
    d. When there is no consent, but the processing must take place to perform a contract between the controller and any third party

4. Which of the following are legislative instruments belonging to EU primary law? (1 pt)
    a. Treaty of the European Union, Treaty on the functioning of the European Union, Case law of the European Court of Justice
    b. Treaty of the European Union, Treaty on the functioning of the European Union, Charter of fundamental rights of the European Union
    c. Charter of fundamental rights of the European Union, Regulations, Case-law of the European Court of Justice

5. Which of the following answers is correct? (1 pt) The hierarchical system of EU law is structured as such:
    a. (1) Primary Law, (2) Secondary Law, (3) International Agreements
    b. (1) Founding treaties, (2) International Agreements, (3) Secondary Law
    c. (1) Primary Law, (3) Secondary Law, (3) Member States law

23.1.2 Open questions

6. *Please identify and illustrate three legal problems posed by social credit systems in no more than 150 words. (up to 6 pts)* – 139 words below

Social Credit Systems are national credit ratings and blacklists, mainly developed by the government of China and allow for easy yet for monitoring purposes, with governments defining good/bad actions according to their citizens behaviour. Given its context, it enables widespread/effective monitoring, not based on simple data but multiple channels of information, often collecting vast amounts of personal data without proper consent, potentially infringing individuals rights of privacy.

Lack of due process is another issue. Decisions made by social credit systems can significantly impact people's lives, yet often lack transparency or mechanisms for appeal. This violates fundamental principles of due process and fairness in legal systems.

Discrimination is a third problem. The algorithms underlying social credit systems may perpetuate or exacerbate existing societal biases, leading to unfair treatment of certain groups based on characteristics like race, gender, or socioeconomic status.

7. *Please, explain the main principles for personal data processing in no more than 200 words. (up to 6 pts)* – 189 words below

The main principles for personal data processing are fundamental guidelines that ensure the ethical and lawful handling of individuals' personal information. These principles include:

- Lawfulness, fairness, and transparency: Data must be processed legally, fairly, and in a transparent manner that individuals can understand.
- Purpose limitation: Data should be collected for specified, explicit, and legitimate purposes and not further processed in incompatible ways.
- Data minimization: Only necessary data should be collected, adequate and relevant to the specified purpose.
- Accuracy: Personal data must be kept accurate and up-to-date, with inaccurate data promptly corrected or erased.
- Storage limitation: Data should be kept in a form that permits identification of individuals for no longer than necessary for the processing purposes.

Written by Gabriel R.

- Integrity and confidentiality: Appropriate security measures must be implemented to protect personal data against unauthorized access, loss, or damage.
- Accountability: The data controller is responsible for demonstrating compliance with these principles.
- Data subject rights: Individuals have rights regarding their personal data, including access, rectification, erasure, and objection to processing.

These principles aim to balance the interests of organizations processing data with the privacy rights of individuals, fostering trust and responsible data handling practices.

8. *Please, illustrate in no more than 100 words the EU personal data protection package adopted since 2016. (up to 6 pts) – 100 words exactly below*

The EU package adopted since 2016 centers on the General Data Protection Regulation (GDPR), used since 2018. This law strengthens individuals' rights and imposes obligations on organizations processing personal data.

Key elements include:

- Enhanced user rights (access, erasure, portability)
- Stricter consent requirements
- Data breach notification within 72 hours
- Appointment of Data Protection Officers
- Privacy by design and default
- Hefty fines for non-compliance (up to 4% of global turnover)

The package also includes the Law Enforcement Directive for data processing in criminal matters and the ePrivacy Regulation (still in draft) to address electronic communications privacy.

23.2 First Exam – 8 February 2024

23.2.1 Multiple choice questions (MCQ)

1. Which of the following statements is correct (2 pts)
    a. Synthetic data is protected by GDPR
    b. The GDPR does not cover the protection of synthetic data
    c. The GDPR prohibits the creation and the dissemination of synthetic data
    d. Synthetic data and anonymized data are the same notion

2. The European Data Protection Board is (1 pt):
    a. An agency of the European Commission with the aim of protecting the fundamental right to data protection
    b. An independent body gathering the national supervisory authorities of each EU Member State
    c. An institution provided for by the Treaty on the European Union

3. Which of the following statements is correct?
    a. Freedom of thought cannot be affected by AI technologies
    b. Freedom of thought is not considered as a human right in most jurisdictions
    c. Freedom of thought deserves protection only once the individual shares his thoughts with others
    d. Freedom of thought is considered as a human right in most jurisdictions but hardly protected in itself

4. The charter of fundamental rights recognizes the right to privacy and the right to data protection to:
    a. Only to individuals with EU citizenship
    b. All individuals provided that they are in the EU
    c. Only to EU companies

5. Which of the following statements is correct?
    a. EU regulations and directives must be directly applied in any of their provision in all Member States
    b. Regulations are directly applicable in all Member States as such, whereas directives need to be implemented by every Member State
    c. Directives are directly applicable in all Member States as such, whereas regulations need to be implemented by every Member State

23.2.2 Open questions

1. Please describe in no more than 250 words the 2020 european data strategy conceive by the european union (up to 6 pts) – 224 words

Skeleton of answer provided by professors in Moodle:

- *The GDPR that paved the way to the 2020 European Data Strategy*
- *Aims of the EU Data Strategy: free flow of personal data, free flow of non-personal data, single market for data*
- *EU Data Strategy Package: Data Governance Act, Digital Services Act, Digital Markets Act, Artificial Intelligence Act, Data Act (a summarized description of their contents)*

My answer/take:

The European Union's 2020 Data Strategy builds upon the foundation laid by the GDPR, aiming to create a single European data space. This strategy focuses on enabling the free flow of personal and non-personal data across the EU, fostering a single market for data respecting personal data.

Key aims include:

1. Ensuring data can move freely within the EU
2. Respecting European rules and values
3. Making high-quality data available for innovation

To achieve these goals, the EU introduced a comprehensive package of legislative initiatives:

1. Data Governance Act: Facilitates data sharing across sectors and borders, establishing data intermediaries.
2. Digital Services Act: Regulates online platforms, ensuring user safety and protecting fundamental rights.
3. Digital Markets Act: Addresses market imbalances in the digital sector, promoting fair competition.
4. Artificial Intelligence Act: Proposes rules for the development and use of AI systems, ensuring they are safe and respect EU values.
5. Data Act: Aims to make more data available for use, clarifying rules on data access and use in business-to-business and business-to-government contexts.

This strategy package seeks to position the EU as a leader in the data-driven economy while maintaining high standards of data protection and digital rights. By creating a harmonized approach to data governance and digital markets, the EU aims to foster innovation, economic growth, and societal benefits while upholding its core values.

2. *Please explain the so-called "Barbara Streisand Effect" in no more than 100 words (up to 6 pts)*

Skeleton of answer provided by professors in Moodle:

- *A brief summary of the facts of the case*
- *Description of the Effect: The protection of privacy through legal means can backfire and worsen the situation of the individual*
- *Takeaways:*
    - *The Legal protection of privacy can consist in avoiding seeking legal protection;*
    - *The legal vindication of privacy is different—and sometimes opposite—from the social enjoyment of privacy*

My answer/take:

3. *Please describe any legal provision included in EU primary law sources setting out the right to personal data protection in max 250 words – 230 words below*

Skeleton of answer provided by professors in Moodle:

- *Personal data protection in the TEU, starting from the values of the EU as protected by article 2 TEU and the protection thereof set out in article 3 TEU*
- *Personal data protection as set forth by article 16 TFEU*
- *The fundamental right to data protection in the Charter of Fundamental Rights (article 8 CFR) and possible reference to article 7 CFR on the right to privacy (and their differences)*
- *Possible limitations of fundamental rights and, specifically, of the right to data protection in light of the safeguard clause (article 52 CFR) – the balancing of conflicting rights*

My answer/take:

The right to personal data protection is enshrined in EU primary law through several key provisions (according to Article 8 CFR and part of the Nice Charter/EU Charter of Fundamental Rights in 2009):

- In the Treaty on European Union (TEU), Article 2 establishes respect for human rights as a core EU value. Article 3 further commits the EU to protect its citizens, which implicitly includes safeguarding their personal data.
- The Treaty on the Functioning of the European Union (TFEU) explicitly addresses data protection in Article 16. This article grants everyone the right to protection of their personal data and empowers the European Parliament and Council to establish rules on data processing.
- The Charter of Fundamental Rights (CFR) elevates data protection to a fundamental right in Article 8. This article guarantees the right to protection of personal data, requires fair data processing for specified purposes, and grants individuals rights to access and rectify their data. It's distinct from, yet complementary to, Article 7 CFR, which protects the right to privacy.
- Article 52 CFR allows for limitations on these rights, provided they are necessary, proportionate, and respect the essence of the rights. This enables balancing data protection with other rights or public interests when conflicts arise.

Written by Gabriel R.

Together, these provisions create a robust legal framework for personal data protection in EU primary law, reflecting its importance in the Union's legal order and values.

23.3 Second Exam – 22 February 2024

23.3.1 Multiple choice questions (MCQ)

6. Which of the following statements is correct (2 pts)
    a. Synthetic data is protected by GDPR
    b. The GDPR does not cover the protection of synthetic data
    c. The GDPR prohibits the creation and the dissemination of synthetic data
    d. Synthetic data and anonymized data are the same notion

7. The processing of personal data pursuant to the GDPR may be lawfully carried out (2 pts):
    a. When data subjects expressed their own consent
    b. Based on the controller's free choice
    c. When there is no consent by data subjects, but the processing is needed for protecting the data subjects' or other individuals' vital interests
    d. When there is no consent, but the processing must take place to perform a contract between the controller and any third party

8. The Charter of fundamental rights recognizes the right to privacy and the right to data protection to (1 pt):
    a. only to individuals with EU citizenship
    b. all individuals in the EU
    c. only to EU companies

9. When the European Court of Human Rights rules that a State has failed to protect a right of an individual (2 pts.):
    a. The Court's ruling replaces the domestic rule that is incompatible with the European Convention of Human Rights
    b. It is up to the State to remove the violation of the European Convention
    c. The individual can sue the State in the European Court of Human Rights

10. The European Data Protection Supervisor is (1 pt)
    a. A national authority supervising on data protection
    b. A supranational authority supervising on the activity of national supervisory authorities
    c. A supranational supervisor on any processing of personal data Member States citizens
    d. An independent body at the European level supervising on processing carried out by EU Institutions

23.3.2 Open questions

11. Please describe the structure of the "proportionality scrutiny" in no more than 200 words. (up to 6 pts) – *198 words below*

Skeleton of answer provided by professors in Moodle:

> *The answer should describe the three-steps or four-steps proportionality scrutiny that courts often employ to balance competing rights and interests. The sequence is extremely relevant because the scrutiny is a test: if a measure fails to pass one step, the measure is unlawful, and the scrutiny is over.*
>
> *The steps are the following:*
>
> a. *Does the measure under scrutiny pursue a legitimate goal?*
> b. *Is the measure concretely connected with the purported goal (this is the "rational connection" step—some courts omit it)?*
> c. *Is the measure necessary to pursue that goal? (This is the "least restrictive means" step)*
> d. *Are the benefits more than the sacrifices that the measure causes to the interests and rights that are involved?*

My answer/take:

The proportionality measurement has been a core problem when it comes to law because it is unknown how the scrutiny assessment can be implemented. This involves mainly four questions.

1. *Legitimate goal*: Does the measure pursue a legitimate aim? The court assesses if the purpose for limiting the right is valid and important enough to potentially justify the restriction.
2. *Lawful measure*: Is the measure compliant with privacy laws and frameworks? The court assesses if the purpose can be considered legitimate from a legal point of view and then accordingly remeasured when necessary
3. *Necessity* (least restrictive means): Is the measure necessary to achieve the goal, or are there less restrictive alternatives available? The court examines if the limitation on rights goes further than needed.
4. *Proportionality stricto sensu*: Do the benefits of the measure outweigh the costs to the affected rights and interests? This final balancing step weighs the positive outcomes against the negative impacts on fundamental rights.

This structured analysis helps ensure that any limitations on fundamental rights like data protection are justified, narrowly tailored, and balanced against other important interests or rights. It provides a framework for courts to systematically evaluate the lawfulness of measures

12. Please, explain what ‘personal data’ means according to the EU personal data protection legislation and the difference with sensitive personal data in no more than 200 words (up to 8 pts)

Skeleton of answer provided by professors in Moodle:

a. *definition of personal data according to article 4(1) of the GDPR*
b. *definition of sensitive data, even involving article 9 GDPR*
c. *differences in the processing of personal data and sensitive personal data*
d. *lawful reasons for processing personal data and sensitive personal data with or without data subjects’ consent*
e. *possible references to the origins of the definition of personal data and sensitive personal data (Convention 108, OECD Guidelines)*

My answer/take:

According to the EU's General Data Protection Regulation (GDPR), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). This includes identifiers such as names, identification numbers, location data, online identifiers, or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

'Sensitive personal data', referred to as 'special categories of personal data' in the GDPR, includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for unique identification, health data, and data concerning a person's sex life or sexual orientation.

The key difference lies in their processing requirements. While personal data can be processed under various lawful bases (consent, contract, legal obligation, vital interests, public task, legitimate interests), sensitive data has stricter processing conditions. Processing sensitive data is generally prohibited unless specific conditions are met, such as explicit consent or necessity for certain legal, medical, or public interest reasons.

These definitions have roots in earlier data protection frameworks like the Council of Europe's Convention 108 and the OECD Guidelines, which recognized the need for special protection of sensitive data.

13. Please, describe which are the main rights recognized to a data subject by the GDPR in max 250 words. (up to 8 pts) – *249 words below*

Skeleton of answer provided by professors in Moodle:

a. *Right to access*
b. *Right to data rectification*
c. *Right to data erasure – right to be forgotten*
d. *Right to processing restriction*
e. *Right to data portability*
f. *Right to limit the processing*
g. *Right to object to data processing*
h. *Right to lodge a complaint before the NSA*

My answer/take:

The General Data Protection Regulation (GDPR) recognizes several key rights for data subjects:

1. Right to access: Data subjects can request information about whether their personal data is being processed, where, and for what purpose. They are entitled to receive a copy of their data free of charge.

2. Right to data rectification: Individuals have the right to have inaccurate personal data corrected/completed if it is incomplete.

3. Right to erasure (Right to be forgotten): Data subjects can request the deletion of their personal data under certain circumstances, such as when data is no longer necessary for the original purpose.

4. Right to restrict processing: In certain situations, individuals can request the restriction of their personal data processing.

5. Right to data portability: Data subjects can request to receive their personal data in a machine-readable format and have the right to transmit it to another controller.

6. Right to object: Individuals can object to the processing of their personal data in certain circumstances, including for direct marketing purposes.

7. Rights related to automated decision making and profiling: Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

8. Right to lodge a complaint: Data subjects can file a complaint with a supervisory authority if they believe their rights under the GDPR have been infringed.

These rights empower individuals with greater control over their personal data and how it is used by organizations.

23.4 SECOND EXAM – 22 FEBRUARY 2024

23.4.1 Multiple choice questions (MCQ)

14. What is the difference between regulations and directives in EU law? (2 pts)
    a. Regulations are immediately enforceable, while directives need domestic execution
    b. Regulations are binding, while directives are only exhortations
    c. Regulations establish rules, whereas directives introduce principles
    d. There is no difference between the two notions

15. Social Credit Systems are (1pt):
    a. Intrinsically incompatible with basic legal principles
    b. Problematic insofar as they are opaque and have wide ramifications for the legal, economic, and social life of a subject
    c. Forbidden under Chinese law
    d. Forbidden under U.S. Law

16. The European Data Protection Board is (2 pts):
    a. An institution provided for by the Treaty on the European Union
    b. An agency of the European Commission with the aim of protecting the fundamental right to data protection
    c. An independent body gathering the national supervisory authorities of each EU Member State

17. The EU Charter of fundamental rights expressly safeguards (up to 2 pts):
    a. The right of data controllers and processors to process anyone's personal data
    b. The right of individuals to personal data protection
    c. The right of individuals to private and family life
    d. The right of individuals to process any other individuals' personal data

18. Should data controllers and data processors be separate entities, the GDPR sets out that (up to 2 pts):
    a. Data controllers are totally free to indicate one or more data processors, the latter not being bound by any obligation towards data controllers
    b. Their relationships need to be regulated by specific contractual agreements or by different acts provided for by law
    c. Their mutual relationships need to be regulated only by an order of any competent National Supervisory Authority

23.4.2 Open questions

19. *Why is the notion of synthetic data relevant in the field of privacy protection? How would you define synthetic data? (up to 6 pts)*

Synthetic data is relevant in the field of privacy protection because it offers a way to maintain data utility while significantly reducing privacy risks associated with using real personal data.

It is artificially generated information that mimics the statistical properties and patterns of real data without containing any actual personal information from real individuals.

It's relevant for privacy because of many reasons:

- Data anonymization: Synthetic data provides a more robust form of anonymization compared to traditional methods, as it doesn't contain any real personal identifiers.
- Reduced re-identification risk: Since synthetic data is artificially created, it dramatically lowers the risk of re-identifying individuals, a common concern with anonymized real data.
- Compliance facilitation: Using synthetic data can help organizations comply with data protection regulations like GDPR while still enabling data-driven innovation and research.
- Data sharing and collaboration: Synthetic data allows for safer sharing of data between organizations or researchers without risking exposure of sensitive personal information.
- Testing and development: It provides a privacy-safe alternative for software testing, machine learning model development, and other data-intensive processes.
- Overcoming data scarcity: In fields where personal data is limited or highly sensitive, synthetic data can provide a viable alternative for analysis and model training.

20. *Please describe how the right to privacy evolved into the right to personal data protection in no more than 150 words (up to 6 pts.)*

The evolution from privacy to personal data protection reflects the changing nature of information in the digital age:

- Initially, privacy focused on the "right to be let alone," protecting individuals from intrusion into their personal lives. This concept, rooted in common law traditions, emphasized physical privacy and protection of reputation

- As technology advanced, the focus shifted to informational privacy. The proliferation of digital data collection and processing raised new concerns about how personal information was used and shared.

- In response, the right to personal data protection emerged, particularly in Europe. This right, enshrined in the EU Charter of Fundamental Rights (Article 8) and the GDPR, goes beyond traditional privacy. It provides individuals with specific rights over their data, such as access, rectification, and erasure.

Unlike privacy, data protection is more proactive, imposing obligations on data controllers and processors. It addresses not just confidentiality, but also fairness, transparency, and accountability in data processing. This evolution reflects the need for more comprehensive protection in our data-driven society.

Written by Gabriel R.