Foundamentals of Information Technology Law

Lesson 1 – Law and legal categories: introduction to legal orders.

"It's a law of thermodynamics, and no one has ever witnessed a sustained violation of it."
A scientific law is a statement of fact, deduced from observation, to the effect that a particular natural or scientific phenomenon always occurs if certain conditions are present. **If the law is violated, it ceases to be a law.**

"A referee is appointed to a football game in order to apply the laws of the game".
It is a rule defining correct procedure or behavior in a sport. **If the law is violated the consequence is losing the game or being expelled.**

"All our life we live knowing that God's justice demands satisfaction for our transgression of God's law. The body of divine commandments as expressed in any religious text. **The consequence of a violation of the law is sin**.

"Shooting the birds is against the law. They were taken to court for breaking the law. **The system of rules which a particular community recognizes as regulating the actions of its members. The consequence of the violation of the law is the imposition of penalties**.

Legal norms may serve different purposes:
- Allocating goods or services.
- Prohibiting certain behaviors that are harmful to the society.
- Creating and attributing public powers among different bodies.

The relationships among members of the same social group are regulated by several norms, where norms are something that is typical, expected, standard.

The sources of norms are:
- **Social**, social behavior.
- **Moral**, subjective authority and personal beliefs.
- **Religious**, religious texts.
- **Legal**, legal system.

Legal norms are produced by the legal system (or rather from those sources that are given system internally recognizes) which have the power of producing binding effects on individuals subject to the system. Unlike other categories of norms, legal norms can be enforced y the state through the imposition of penalties.

The **characteristics of legal norms** are:
- **Effectiveness**, the ability of a legal system to impose binding rules on individuals; it is not affected per se by limited violations of single norms, provided that the authority (often the State) can impose its political power over individuals within the relevant territory. Effectiveness is also a property of those norms that are produced by a legal system that is able to impose binding rules on its participants.
- **Force of Law**, describes the ability of norms to innovate the legal systems. It depends on effectiveness, which refers to the ability of norms to produce effects and be imposed as legal duty on participants in the system.
- **Generality**, framed as applicable to an indefinite number of individuals.
  "**Everyone** who commits first degree murder or second murder is guilty of an indictable offense and shall be sentenced to imprisonment for life".
- **Abstractness**, framed as applicable to an indefinite number of situations.
  "Everyone who commits first degree **murder** or second degree **murder** is guilty of an indictable offense and shall be sentenced to imprisonment for life".

Identifying legal norms, each legal system has some golden norms which are established by the constitution, which is the institution that identify the different sources in the legal system.

- Made by a **competent authority** (recognized as source of law).
- **Nomen Iuris**, the name of the law, it identifies a specific legal source.
- **Legislative Procedures**.

Legal norms can be implemented by the state, which is the social institution entitled to use the force and penalties to assure that laws and rules are followed. Unless there is an entity such as the State, the laws and rules won't be binding on the individuals.

Legal system (**ubi societas** society, **ibi ius** laws) there is a strict relation between **Social Institutions** and the **Body of Legal Norms**.
Legal system as **social institution**, **constituent elements** are:

- A certain number of subjects, who make up a social group and are connected to each other.
- Common criteria of evaluation are applied to categorize individual behaviours as licit or illicit, mandatory or not…
- Relationship established between individuals are qualified by law as either favourable or unfavourable legal situations.
- Titular power and authority assigned within the group (Art.1 Italian Constitution, individuals are considered to be the original holder of the sovranity, which has gradually been transferred to the State) .
- Certain organs within the system are entitled to the legitimate use of force (Punishments to enforce the law).
- Authority has means of coercion to ensure the legitimate exercise of power.

Classification of legal system

Fluid and Widespread	Authoritarian or concentrated
Voluntary (ex. EU)	Necessary
Territorial (*If your sovereign power extends to a specific territory*, EU)	Non-territorial (*WTO*)
General (*goals, such as EU has a general legal system)*	Specialized (*EU initially started as specialized when trying to establish a unique market*)
Independent (*no superior authorities on which the state depends*)	Derived (*EU, some states decided to form that legal system*)
Sovereign (*generally State are usually sovereign*)	Non-sovereign (*WTO*)

There is a **pluralism of legal systems**, the State is only one among the existing legal systems

The **State** has a legal system meeting the following characteristics:

- Authoritarian or Concentrated
- Necessary
- Territorial
- General
- Independent
- Sovereign

"*A legal system having general ends which exercises sovereign powers over a specific territory, to which the subjects belonging to such system are necessarily subordinated* " – Costantino Mortati.

Three **characterising elements** of the State legal system are:

- **Territory**, the State owns a territory which can be:
  - **Dry land**.
  - **Continental shelf**.
  - **Waters included within the confines of the State**.
- **Sovereignty**, it can be limited by the existence of superior authorities, such as European countries and EU.
  The **impact of the Internet on sovereignty**,
  - **No more borders**, everywhere and nowhere
  - **Jurisdiction** to prescribe, to adjudicate, to enforce -> issues.
  - **Governance of crucial issues** (domain name assignments) **in the hand of a few agencies**.
  - Neutrality and freedom from governmental interferences.
- **People**, citizenship is a concept identifying the condition of being bound to a given State.
  The **concept of people is different from**:
  - **Population**, temporary sum of individuals living in the territory of the State
  - **Nation**, community or race of people with shared culture, traditions, history, and (usually) language.
  - **Voters**, individuals who have the legal right to vote in elections in a given State.

  Citizenship is a concept identifying the condition of being bound to a given State:
  - From which the individual receives certain rights.
  - To which he or she owes certain obligations.
  - Is forced to respect certain duties

  Two criteria are used as distinctive elements to differentiate citizens from aliens:
  - Ius Sanguinis
  - Ius Soli

Lesson 2 – Forms of State and forms of Government.

Forms of State: the relationship between the state that can legitimately exercise coercive power, on one hand, and its citizens, taken individually or as a community, on the other.
[to understand the shift of power from public authorities to platforms]
So it is a set of values and principles that are behind the relationship behind the State and citizens.
ex. Equality is a value that have changed over time, from slavery to inequality between men and women, but the set of values and principles have changed over time in order to achieve equality.
There are two different methods:

- **diachronic**: how forms of state evolve over time, from the basic structure of the state to the current one.
- **synchronic**: how today we can witness different organizations of the State which means different relationship between the State and the Citizens.

Diachronic Method

- **Feudal state**
  - 1648 Peace of Westphalia - it is the turning point which led to the first moment in which state recognized themselves as sovereignty entities and independent from each other.) The state began to be considered a social institution, it is the passage between the feudalism and medieval universalism, the Holy Roman Empire to modern state.

Each State is sovereign and has power over a permanent population which is established over a limited territory. Prior to the peace, the organization of the community was feudalism in which there was a total identification of the feudal lord with the possession of the land. The organization of the community was based on private agreements between individuals. And the sole aim was the protection of the lands and its related possessions from external attacks. The lord was giving protection of everyone under his sovereignty, in exchange of services on the land. It cannot considered a State because there is not a complete sovereignty, each feud is independent and there was not the concept of people. People were only workers for a specific purpose, they did not have rights expect from being compensated for the service on the land ⇛ no concept of citizenship. The State has general ends while feudalism didn't.

- **Absolute State**
  Shift of power from the feudal lords, to the kings (and thus the stabilization of monarchical authority). Land did not anymore imply power, but money was the actual form of power. The possession of power is proportional to the possession of money. And it has a sovereign power (legislative → make laws, executive → apply the law and make it effective, juridical → enforce the law and make sure it is not violated) resides in the King. In the absolute state the three components of the sovereign power were in the hand to the King. **Absolute power** means that it has no constraint, and all the powers were resigned in the King and nobody could oppose to it. The general goal was to have money, there is no more the idea of protection of the land. The king is considered the holder of the sovereign power.

- **Liberal State**
  It is characterized by the separation of powers based on fact that there is no more the same body holding the three powers but powers are allocated among different and separate authorities. There is a judiciary which exercise juridical power, Parliaments had legislative power most of the time in accordance with the king. There is a limitation of monarchical power. The concept of popular and national sovereignty: the power is under the control of the people which are part of the parliament and have relationship with King.

  The introduction of the rule of law is faced all the state activities are subject to law, and implies the separation of the three different power and therefore political power is subject to constraint too. The rule of law is introduced because constitution begin to being signed, which are placing boundaries over bodies which exercise political power. Another feature is the protection of first generation rights (Negative rights are those which do not require the state intervention to be protected but can be fulfilled when the state does not interfere with their enjoyment → ex. the freedom of expression: the state doesn't have to build anything ≠ the right of education: the state has to build schools.) The individual rights were the first right protected in the first liberal state and for this reason are defined first generation rights. Strong separation between State and society (limited intervention in the economy).

- **Democratic / Pluralistic State**
  A shift is faced (only upper classes had rights in the Liberal State) now everybody has rights and there are no more distinctions based on social status. There is the recreation of *mass parties*, which capture social instances and the political interest rises, therefore political rights are open to everyone. While previously the parties were reserved only to upper classes. There are also *social and economic rights* and not only first generation rights, which are second generation rights. The attention on social and economic rights led to *increase of social welfare* in fact Welfare States were born. The State reaches its highest point of sovereign power. Between the democratic and the welfare state some Nations went through a period

which is called the totalitarian state (for example Italy, Germany and Japan). Passage to a multiclass society and the creation of mass parties is faced which increase the participation in the political life of the Nation. Second generation rights are recognized such as education and health care.

Using the **synchronic** method state look at the current organization of the political power and how it is exercise on the citizens.

Unitary state: there is a central government which has a total legislative power (China).

Decentralized state: sub-state entities are present and exercise some part of the legislative power. For example the United States of America

- **Federal State**: (USA and Germany) some subject manners are reserved for the central state.
- **Regional state**: (Italy and Spain) the constitution states the subject manners reserved for the regional government.

The distinction is made on the basis of **five elements**:

- Extent of the legislative power is exercised by the sub-state entities.
- Existence of a separate branch of the judiciary at sub-state level.
- Presence of a second Chamber of the parliament that represents the sub-state entities - if there is no a Second Chamber then it is a regional state.
- Involvement of sub-state entities in constitutional amendment.
- Existence of sub-national constitutions, subnational entities have its own constitution: generally Federal States have a constitution for each state while regions do not have a constitution

Allocation of **Legislative Powers** in the **Italian Constitution**
Executive legislative power: **State**
Concurring legislation: **State** and **Regions**
Residual legislation: **Regions**.

Forms of government
Set of rules concerning the distribution of power among the branches of the government (bodies of the central government)
Four different forms:

- **Parliamentary Executive** (Italy)
- **Presidential Executive** (USA)
- **Semi-Presidential Executive** (France)
- **Directorial Executive** (Swiss)

The classification of forms of government is based on three methods:

- Whether there is both a head of state and a head of government
- Whether of the incumbents of these institutions are popularly elected
- Whether the incumbents serve for a fixed term

Parliament - Parliamentary executive
It is elected by the electoral body.
It has relationship:

- Elects the head of the state
- Grants and revokes confidence to the executive

The executive needs to have confidence otherwise elections will happen again in order to re-establish the confidence.
There is both a head of state and a head of government, there is no popular election of the head of state, so the elections are not direct. The head of state serve for 7 years while the head of government serve for fixed terms (2 normally) if he is able to get to the end.

Presidential executive

- Electoral body elects the congress
- Popular elections are held in order to elect the president
- No confidence relationship between congress and the president. There is no head of state and government because they are the same person which is the president.
- There are some mechanism that coordinates the president and the congress.

Congress has the power of impeachment only in certain circumstances.

The President creates a cabinet, with secretaries of states

Differences:

Parliamentary Executive	Presidential Executive
Head of state + Head of government	Head of State and Government are combined into one institution: the President
Neither the head of state nor the head of government is popularly elected	The president is popularly elected
Generally, the head of government does not serve for a fixed term	The president serves for a fixed term

Semi-Presidential Executive
Electoral body elects both the parliament and the president - which means that he is popularly elected. There is no confidence relationship between the parliament and the president. The parliament votes confidence to the government / cabinet which is appointed by the president.
The executive power is splitted between the president and the government (parliamentary executive the head of state has no political power). The majority in the parliament can shift in a short period of time so the executive power could potentially be exercised by two organs coming from different parties.

Cohabitation: the scenario in which two different parties share executive power. If the situation is not verified the president exercise the complete executive power, while if the political background (cohabitation scenario) is different also the prime minister will have some executive power. The president serves for a fixed term (5 years, it was reduced from 7 in France)

[read the Directorial Executive]

Lesson 3 – The Italian constitutional System and Sources of Law

- **1946** institutional referendum to determine whether Italy should have kept being a **Monarchy** or become a **Republic**

The people voted for the **Republic**. After a constituent Assembly was elected to draft and approve the Constitution of the Republic.

Italy lost the World War II and was completely destroyed by the Allied bombings and war. Constitution drafted with the aim to avoid the return of Fascism period. Need to restate rights and freedom after the dark Fascist age. Need to avoid risks of the Communism.

From the Albertine Statute to the Constitution
Which signed the passage from a flexible to a rigid constitution: the legal system should be in line with the supreme laws which are the one included in the constitution. The constitution cannot be changed, there are some exception but there is a precise procedure that must be followed over a precise period of time. The rigid constitution is important because it should be maintained and respected over time, and if a change is needed it should be really fundamental.
The **Albertine Statute** was a flexible constitution allowing the parliament changes just by passing a law.

Constitutions may be:

Codified - One single document (set of provisions in one single document)	**Uncodified** (UK, Israel)
Long containing the frame of government and the bill of rights (first, second and third rights*)	**Short** containing the frame of government (France)
Flexible formally equal to ordinary laws, therefore the Constitution may be modified with an ordinary law	**Rigid** at the top of the hierarchy of the legal sources therefore modifications require a special amendment procedure
Voted drafted and voted by a constituent assembly/ people	**Octroyée** granted by a monarch

* third generation rights = privacy, environment

Italian Constitution
It was made by a special organ that had the role of creating the Constitution.

The **Italian Constitution is**:
- **Codified**: written
- **Long**
- **Voted**
- **Rigid**, means that there is a special **Amendments Procedure:**
    - It requires a double vote of each chamber of the parliament.
    - There must be an interval between the votes of not less than three months for the vote of the constitution. Time is required to internalize the proposal of constitution. It shall be approved by a qualified majority - which is greater than the majority - of the government - of the members of each chamber in the second voting. A qualified majority means that the ⅔ must be in agreement. The constitution requires the highest approvation possible.

- There must be the possibility of recourse to the people through a popular referendum. The referendum is called only if the qualified majority is not reach in the second voting. There is a popular referendum for regaining the approbation.

Constitutional Organs

- **The Parliament**: it is made of two chambers which are voted by the citizens. **Chambers of Deputies**, made of 630 members and elected by the citizens above the age of 18. **Senate,** made of 315 members and elected by the citizens above the age of 18. The two chambers have the same functions and duration of 5 years. The chambers should draw confidence toward the government, if the confidence is withdrawing elections should be established.

- **The president of the republic***:* he is elected by the parliament, but he has no political/executive power. His charge lasts for 7 years and there is the opportunity of being reelected. He appoints the President of the Council of Ministers and upon the latter's proposal, the Minister. He promulgates the bills. He has the power to grant reprieves and pardons.

- **The government***:* which is the executive branch. Normally there is the president who is the President of the Council and the Council of Ministers. He can adopt legislative acts under specific circumstances and the legislative power is temporary. He directs the administration of the State. Ministers are on top of their Ministry and of the bureaucratic administrative offices.

Sources of Law in Italy
Super Primary Sources, have the highest rank in the constitution which is typical of rigid constitutions. **Constitutional Laws,** are the ones needed to change the Constitution.
Law, are **primary sources** and just they are just below the Constitution.
Local regulations, **secondary sources**.

Constitutional Justice (no study)
Constitutional court makes sure that the constitution is not violated or overruled by other law written for primary sources. Check that there are no conflicts between primary sources and constitution otherwise the supremacy of the constitution is violated.
The members are elected some by the Parliament (5 members) others are appointed by the president of the Republic (5) and the last from the supreme courts (5).
Justices are the members of the constitutional court and they are in charge for 9 years and cannot be re-elected.

Lawmaking process (Not Compulsory)
There is a proposal which can either come from the parliament, or the regions, or the citizens, or the CNEL. It is introduced in the chamber or the senate and then in the other organ, it must be approved by both and then the bill is turned in law. The promulgation of the law is the signing of the law by the president. Once the law is published on the **Italian Official Journal of Law**, it will become effective after 15 days.

Legislative decrees and Law Decrees
Legislative Decrees, law that grants to Government the power to issue decrees within specified limits. Such decrees have the same force as the law.
Law decrees, the act is different and approved when there are situations of emergencies. The government and the executive approve a law decrees to move the resources to the sector damaged.

Within 60 days Parliament shall convert into law, otherwise the cease to be effective. There is no time to wait for the double approvement of the chambers.

Conflicts of law
There is a **hierarchy of law** (Constitution - Super primary - Primary - Secondary). If there is a conflict, which means that the norm has a different meaning or there is contradiction between two rules.

- If the norms are from the same rank - chronological orders is watched, the latest law is derogating the previous one. ***(Lex posterior derogat priori)***.
- If norms have different ranks - the law with the highest rank prevale (***Lex superior derogat inferiori)***
- ***Lex specialis derogat generali*** - does not refer to the rank or the timing but only to the scope of application of the certain provision. The special norm prevails, and the general norm keeps prevailing in all the other cases.
- ***Competence*** - not refer to the rank or the scope of application, but to the appropriate legal order to produce the law so there is a delegation of law from the state (ex European Law).

Lesson 4 – The Characteristics of the European Union Legal Order. Sources of Law.

The European Union - The origins
After the World War II, 6 countries: Italy, Belgium, France, Western Germany, Netherlands and Luxembourg decided to realize an economic union, aimed at achieving peace after the War.

The European Union – Community Structure
Economic Union requires a Political Union in the long term.
This Union was established through three communities:

- **ECSC**, European Coal and Steel Community
- **EURATOM**, European Atomic Energy Community
- **EEC**, European Economic Community

The first two were established with the Treaty of Paris (1951), while the third with the Treat of Rome (1957), which is the one still active, representing the European Community right now.

The European Union – International Organization
From a legal perspective the two Treaties are international sources of law, creating obligations to the states, creating the environment for a deeper political integration.

The European Union – Treaties

- **1951 Paris Treaty**
- **1957 Rome Treaty**
- 1986 Single European Act
- **1992 Maastricht Treaty**
- 1997 Amsterdam Treaty
- 2001 Nice Treaty
- **2004 European Constitution Treaty**, attempt to define a Constitution for Europe, which was rejected by some States of the Union through internal referendums, making the Treaty a failure.
- 2007 Lisbon Treaty

The European Union – 1985 Schengen Agreement

In 1985 was established an agreement, with which more states took part to the European Union, and its purpose was to establish freedom of circulation of individuals, capitals, but the achievement of this economic freedom allowed to abolish border checks between signatory countries.

The European Union – 1992 Maastricht Treaty
It was an important treaty in the further economic integration of the states, with the first steps towards the definition of the **EURO**.

The Lisbon Treaty – Basic Structure of EU Treaties System
The Charter of Fundamental Rights of the European Union is based on two pillars that are:

- **Treaty on the European Union**, sets out principles of the EU (purpose and scopes) and the governance of EU's **central institutions**.
- **Treaty on the Function of the European Union**, sets out the basis of the **EU Law**, that is the scope of the EU's legislative authority and legal principles in the areas where the EU operates.

Charter of Fundamental Rights of the EU
The Charter consists of 54 articles divided into 7 titles:

- Dignity
- Freedoms
- Equality
- Solidarity
- Citizens' rights
- Justice
- General Provisions (e.g. Art. 52)

Equal importance of all rights, irrespective of categories

EU Institutions

- **European Council,** the European Council is **composed by head of states or governments of the EU**. It has no legislative authority, but it only sets the political agenda and objectives of the EU. The meetings of the Council are at least twice a year.
- **Council of the European Union**, the Council of the European Union is **composed by one representative (a Ministry) of Member states' governments**. Different compositions (depending on the subject matter to discuss). Together with the European Parliament exercises the **legislative authority**.
- **European Parliament**, the European Parliament is composed of **705 MEPs** (Members of European Parliament) elected by EU citizens every 5 years. MEPs are divided in 20 commissions on different topics. It has legislative functions together with the Council.
- **European Commission**, the European Commission (executive branch) is made of **27 components** (one for each Member State), in charge for 5 Years. It has the **legislative initiative**. Promotes the **general interest** of the EU. Oversight on the **application** of EU Law.
- **Court of Justice of the European Union**, the Court of Justice of the European Union is composed by **27 Justices** (one for each member state) and **11 Advocates general**. It oversees the uniform application and interpretation of the EU Law. It resolves disputes between Member states, the EU and Member states, EU institutions and between individuals and the EU.

EU Legislative Acts
In the European Legal System we can differentiate among:

- **Binding Sources**:

    - **EU Regulations**, complete **set of rules** applicable throughout the EU. Unless specifically required to do so, Member states have not to transfer the provision into State Law. Automatically supersede contrasting national provisions.
    - **EU Directives**, set a **goal** to be reach throughout the **EU**. Member states can achieve the objective set out in the directive using the most appropriate internal legislative instrument, within the deadline set. The **EU Commission** can open investigation and sanction Member states that fail to adopt the directive's provisions.
    - **EU Decisions**, binding only towards its **addressees**. **States** or **individuals** (natural or legal persons) clearly identified.
- **Non-Binding Sources**:
    - **EU Recommendations**, EU Institutions make use of these acts to externalize goals that they deem advisable, without imposing any legal obligation.
    - **EU Opinions**, allow the EU Institution to express its position in a non-binding way.

States have to comply with the binding sources and would occur in problems if they don't follow them.

European Legislative Process – Ordinary Legislative Procedure
The **legislative initiative** rest in the hands of the **EU Commission**, but **legislative power** is actually exercised by the **EU Parliament** and the **EU Council**, which act as **co-legislator**.

Council of Europe
The Council of Europe (COE) is an intergovernmental organization (47 Member States) devoted to promoting human rights, education and culture. One of its foundational documents is the *European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).*
Some 800 millions of people are actually living under the protection of the ECHR, as a "minimum rule" of human rights protection.

Europe as Country of Rights

Court of Justice of the European Union
The **Court of Justice of the European Union** has a crucial role in transforming a community based on economic purpose into a second European Human Rights protection system. Fundamental rights were originally meant as the grounds of possible limitations to the economic freedoms set forth in the Treaties (i.e. exceptions). Strong activism in ensuring the respect of fundamental rights both against EU Institutions and the Member States, the role of the Charter.

Council of Europe	European Union
International legal order having the **specific purpose** of protecting human rights	A system designed to ensure peace through economic integration: legal order having **general purposes**
47 contracting parties (27 of which are EU Member States)	27 Member States
European Convention on Human Rights ("ECHR")	Charter of Fundamental Rights of the European Union
European Court of Human Rights (based in Strasbourg) ensuring the respect of the rights and freedoms enshrined in the ECHR.	**Court of Justice of the European Union** (based in Luxembourg) ensuring the supremacy of the Treaties and the consistent application of EU law among Member States.

The Court of Justice of the European Union is composed by **27 Justices** (one for each member state) and **11 Advocates general**. Judges and Advocates General are appointed for a term of office six years (renewable).

The Court may sit as a **full court**, in a **Grand Chamber** of 15 judges or in **Chambers** of 3 or 5 judges.
The Court sits as a full court in the particular cases prescribed by the Statue of the Court and where the Court considers that a case is of exceptional importance.
The Court sits in a Grand Chamber when a Member State or an Institution which is a party to the proceedings so requests, and in particularly complex or important cases.

The **Court of Justice** and the **Protection of Fundamental Rights.** Primary objective of the Treaties was a union based on economic integration and there was no express provision on human rights. The main problem of the Court is the reconciliation with promotion of fundamental economic freedoms.

The **Preliminary Reference**, Art. 267 TFEU,
"The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning:

- The **interpretation** of the Treaties
- The **validity and interpretation** of acts of the institutions, bodies, offices or agencies of the Union"

The **Implications of the preliminary ruling mechanism** are:

- National proceedings is suspended until the Court of Justice has given its ruling.
- Court's decisions are binding on all of the national authorities of Member States.
- If the EU Law is declared invalid all of the instruments based on it are invalid as well.

The European Court of Human Rights
The main role of the ECHR is to receive applications from any person, non-governmental organization or group of individuals that claims to be victim of a violation of the rights set forth in the ECHR by one of the Contracting Parties.
The European Court of Human Rights is composed of 47 Judges, 1 from each of the Contracting States. Judges are elected for a 9 years non-renewable term. A 3-judges committee may rule on the admissibility of the case. Each Chamber is composed of the President of the relevant Section, the "national judge" and 5 other judges. There exist 5 sections in which Chambers are formed.

Differences between the two Courts – Judicial remedies before the European Courts

ECHR, application can be submitted by any citizen of a High Contracting Party […] only after all the national judicial remedies failed to address the violation Scope of the scrutiny: ruling on alleged violations of the ECHR.
Court of Justice of EU, Court of the complex EU system: many functions. Usually not triggered by individual citizens. Proceedings against a Member State for failure to fulfil an obligation. Annulment proceeding. Proceeding for failure to act. Preliminary ruling.

Lesson 5 – History of the Internet. The relationship between law and the Internet.

ARPANET - The Origins
Sputnik, the first USSR satellite. The US realized that the USSR was more technologically advanced. **ARPA** (Advanced Researches Projects Agency) was founded with the intent to do researches and find innovative solutions for military purposes, such as the development of a way to securely and immediately exchange information. ARPA created **ARPANET** in 1969, which principal am was to allow information exchange also in case of nuclear disaster, but also, enhance information exchanges for research purposes. Important role of universities.

ARPANET – The Importance of Nodes

The idea of ARPANET was to develop a network made of nodes (hosts) that would allow the communication among them even if one of the nodes would stop working. The development of nodes in the network was facilitated by a mixture between universities and military. However, the U.S. Government decided to split ARPANET in **MILNET** (to ensure secrecy in military communications) and **ARPANET** (used by universities to exchange information).

ARPANET – The Need to Have Uniformity
Scientists developed **Protocols**, which **sets of rules** aimed at allowing communication. The most important one is the **TCP/IP**.

From ARPANET to INTERNET
From the various networks of ARPANET we arrived to a network connecting hosts worldwide, the INTERNET. Each node in the Internet can be connected by different means of connection such as: optical fibres, satellite, radio, infrared, …

INTERNET – TCP/IP Protocol
The protocol used by Internet is the TCP/IP through which one single packet of information is divided in multiple smaller packages, travels singularly in the network towards the destination and the packages are recomposed when the final host is reached.

INTERNET – HTTP Protocol
In 1991, while woking at the CERN in Geneva, Tim Berners Lee developed the HTTP Protocol (Hyper Text Transfer Protocol). This protocol allows a **Client** (browser) to ask a **Server 1** an information which is hosted on a **Server 2**, and this transfer of information is made possible by an **hyperlink**.

INTERNET – Browser
The browser retrieves, presents and transfers information from the World Wide Web in a visible and user-friendly way.

INTERNET – IP Addresses and DNS
The IP Address means to clearly identify one computer (host) in the whole network, while the DNS (Domain Name System) is the tool that associates each IP Address with a user-friendly name, to reach that particular host. From which derived the creation of **associations/agencies** aimed at disciplining the assignment of IPs.

INTERNET – Domain Name System
We have a Net of Databases, hence a list of all IP addresses of servers in the network. DNS is useful to facilitate conversion between DNS and IP. Handle the domains which are structure among different levels in the URL address: .it, .com, .net (are first level domains).

INTERNET – Self-regulatory agencies
During time, Internet self-regulated itself via several agencies that emerged de facto, which are private entities that handle crucial functions. This brings to the surface a series of problems that are not easily solvable.

- **ICANN** (Internet Corporation for Assigned Name and Numbers), manages **Internet Protocol** numbers and **Domain Name System** root. It is under the control of the U.S. Department of Commerce until Oct. 1, 2016. Now is under the control of international stakeholders (internal committees).
- **IANA** (Internet Assigned Number Authority), founded in 1988, it is the department of ICANN that globally oversees assignation of **IP Addresses**.

- **ISOC** (Internet Society) is a no-profit organization founded in 1992 with offices all around the world. It provides standards for the management of Internet. *"... to promote the open development, evolution and use of the Internet for the benefit of all people throughout the world"*.

INTERNET – Problems with self-regulatory agencies

- They self-emerged and were self-regulated, but also were strictly connected with the United States, in particular with the Department of Commerce, without any other relation with other countries.
- The lack of accountability, there was no specific requirements for these agencies.
- In case of controversies, there was internal private justice instruments.

Internet Regulation – Declaration of the Independence

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" – John Perry Barlow (cyber-libertarian).

Internet Regulation – Sealand Principality

Copyright issues in Sweden with the host thepiratebay.org.
The website attempted to buy the micro-nation **Sealand**, in order to esape from prosecution (www.sealandgov.org").

Internet Regulation – Self–Regulation?

Often referred to as "cyberanarchy". Simpatized by David Johnson and David Post. They sustained that Cyberspace is a place where distinct laws apply. Necessary for the Internet to govern itself. "Internet Citizens" (users) will obey laws of electronic entities like service providers.

Internet Regulation – External/State–Regulation?

Jack Goldsmith and other academics were against the cyberanarchy, sustaining that the activity in cyberspace can be assimilated to transnational activity (Email, Telephone). Traditional legal tools and choice-of-law problems are applicable in the cyberspace. This theory sustains that the States is still the authority that has the jurisdiction, therefore illegal behaviours on the Internet have to be punished by the States.

Lesson 6 – Jurisdiction and the Internet.

The problem with the Internet is that it is not clear where the State can apply its Sovereign power. For example, gambling services, activities which have very strict regulations in some countries and less strict in others. Internet has allowed gambling services to expand their access beyond their base-country borders, maybe also in places where gambling is in some way prohibited. This generates a **Jurisdictional Issue**.

Jurisdiction

Three different concepts of "Jurisdiction":

- **Prescriptive Jurisdiction**, the State legislature's right to create, amend or repeal legislation (power to create legal norms).
- **Enforcement Jurisdiction**, the State's right to enforce the legislation (power to make sure that the law is applicable and applied)
- **Adjudicative Jurisdiction**, the ability of courts to hear and decide on matters.

When considering the Internet case, the problems concern mainly the second two types of jurisdiction.

The US Scenario

- **Pennoyer v. Neff (1878**)
  The defendant must be brought within a State's jurisdiction by service of process within the state of voluntary appearance: required physical presence. (Individual presence of the person on which you want to apply the law).
- **International Shoe (1945)**
  Washington State taxes on an Illinois shoe company? The defendant needs not be present so long as he has **certain minimum contacts** with the forum so that it does not offend traditional notions of fair play and substantial justice. (There is a reasonable expectation that defendant had a contact on that State, therefore the authorities of that State can claim to have jurisdiction).

How much extensive must a party's contact with a state be for the courts of that state to be able to exercise jurisdiction over that party?

- **Hanson v. Denckla (1945)**
  There be some acts by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws. (It means that there if you are getting the benefits of trading in one State, then you're subject also to "negatives", such as that State's jurisdiction).

Therefore the two "tests" defined for the relationships between States are:

- **Minimum Contact**
- **Purposeful Availment**

No physical presence but … damage
Calder v Jones (1984)
A professional entertainer who lived and worked in California and whose television career was centred there started a lawsuit in California, claiming that she had been libeled in an article written and edited by authors in Florida and published in a national magazine having its largest circulation in California. The authors, both residents of Florida, were served with process by mail in Florida, and claimed lack of personal jurisdiction.
The Court developed the "**Effects Test**". There is a reasonable expectation for the defendants to be sued in the forum State: jurisdiction in California is proper because the effects of the Florida conduct were felt there.

No physical presence but … contract
Burger King Corp. v Rudzwicz (1985)
Personal jurisdiction is proper even though defendants never went to the forum State because "it is an inescapable fact of modern commercia life that a substantial amount of business is transacted wholely by mail and wire communications across State lines". (Deny of Pennoyer 1878 decision).

The US Scenario – Zippo v Zippo Dot Com (1997)
On this occasion, the Court developed the "**Sliding Scale Test**", the Court tried to state in which situations a forum State can apply jurisdiction over a website.

- The first scenario is the one where the website is **actively operating** with the purpose of doing business, with objectives located in another State. If the website is doing so, the State where the website is doing business can claim the right to apply its jurisdiction.
- The second scenario is the one where the website is acting in a merely **passive way**. In this situation is difficult for another State to apply its jurisdiction.

- There exists also a big "grey" area called **Middle-ground**, which depends on the actual level of interactivity of the website. In this scenario might be up to the Court to decide whether the website was able to establish a contact with the different subjects involved creating a jurisdiction claim.

The problems in the Zippo case
Almost all disputed cases were left in the land of "interactivity", where courts were given no guidance except to analyse and weigh the levels of interactivity.
The Zippo test followed a one-size-fits-all approach, for all Internet disputes: but Internet disputes come in many different sizes and shapes. It may falsely describe the nature of Internet and computer-related communications: the World has changed!

Internet Regulation – The role of Courts as "substitute" regulators
Dow Jones & Company v. Gutnick (HCA)
- Defamation involving an online newspaper based in the U.S.
- "*The fact the publication might occur everywhere does not mean that it occurs nowhere"*: Gutnick had the right to sue for defamation at his primary residence and the place he was best known (Australia).
- If people wish to do business or to carry out any activities in different countries, they can hardly expect to be absolved from compliance with the laws of those countries.

Hold:
- Existing principles of defamation law are that legal proceedings should be undertaken in the place where the communication is received, not where the communication is sent from. This applies equally to internet communications, despite the new nature of the technology.
- In this case, involving information published on the Interne in the United States and read in the State of Victoria, Australia, the suitable jurisdiction for a court action is Victoria. (It is not important where an information is posted, but rather where that information is read).

Lewis v. King (EWCA) (2004)
The parties both were U.S. citizens and residents, and the offending statements were posted to websites located in the U.S.. Those statements were published in Great Britain, only in the sense that the website on which they appeared could be viewed by readers in Great Britain, and apparently were.

Forum shopping/regulatory arbitrage? Different burden of proof. **A publication occurs when a message is posted on a website and becomes accessible in the UK**: EWCA jurisdiction is proper.

There is an initial presumption that the natural or appropriate forum for the trial is the place where the tort is committed; in defamation that would be where the libel was published.
However, the more tenuous the Claimant's connection with this jurisdiction the weaker this consideration becomes; in Internet cases the court's discretion will be more "open-textured" so as to give effect to the publisher's choice of a global medium. (The fact that you used the Internet makes you subject to jurisdictions that are outside of the national borders).
The judge must consider what is the appropriate forum without any consideration of whether there is a "juridical advantage".

Google Spain – Jurisdiction
Mr. Costeja Gonzalez lodged with the Spanish Data Protection Authority a complaint against La Vanguardia, which publishes a daily newspaper with a large circulation and against Google Spain and Google Inc.

The complaint was based on the fact that, when an internet user entered Mr. Costeja name in the Google search engine, he would obtain **links to two pages of La Vanguardia**, of **19 January** and **9 March 1998** respectively, on which an announcement mentioning his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

Google defends himself saying that the data processing part of his work is only done in the U.S., while Google Spain is only interested in the advertising business part.

So, by the complaint Costeja Gonzalez, the Spain Court requested:

- **La Vanguardia** to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. La Vanguardia refused appealing to the Freedom of expression.

- **Google** to remove the personal data relating to him. He stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them now was entirely irrelevant. Google refused appealing to the fact that he doesn't control the content posted by third parties and furthermore he is not subject to EU Law.

The Court of Spain asked the European Court of Justice for a clarification of Article 4.
With regard to the territorial application of [the Directive]:
Must be considered that an "establishment", within the meaning of Article 4(1)(a) exists when any one or more of the following circumstances arise:

- When the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State.
- When the parent company designates a subsidiary located in that member state as its representative and controller for two specific filling systems which relate to the data of customers who have contracted for advertising with that undertaking.
- When the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities, with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?

In order to satisfy the criterion laid down in that provision, it is necessary that the processing of persona data by the controller be **"carried out in the context of the activities" of an establishment of the controller** on the territory of a Member State.

Google disputes that this is the case since the processing of personal data at issue in the main proceedings is carried out exclusively by Google Inc., which operates Google Search without any intervention on the part of Google Spain; the **latter's activity is limited to providing support to the Google group's advertising activity which is separate from its search engine service**.

In the light of the objective of preventing individuals from being deprived of the protection guaranteed by the Directive, it must be held that the **processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out "in the context of the activities" of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.** (Therefore EU Law is applicable).

In these circumstance, **the activities of the operator of the Search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable** and that engine is, at the same time, the means enabling those activities to be performed.

That being so, **it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46**, which would compromise the directive's effectiveness and the effective complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure.

Defamation
Shevill (1995)
Art. 5 of Brussels Convention (1968)
On jurisdiction and the enforcement of judgments in civil and commercial matters. A person domiciled in a Contracting State may, in another Contracting State, be sued:

- […]
- […]
- In matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred. (**Effects Test**).

… the victim of a libel by a newspaper article distributed in several Contracting States may bring an action for damages against the publisher either before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award damages for all the harm caused by the defamation, or before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm cause in the State of the court seized.

(a person libeled by a newspaper has then two options:

- Sue the newspaper in the Country where the publisher is based, and you can claim damages for all the harm caused by the defamatory act.
- Claim for damages in every State he suffered harm for his reputation. In this case you can claim from every Court damages for the part of harm caused in that particular State).

eDate Advertising (2011)
… in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of **all the damage caused**, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the centre of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage cause in the territory of the Member State of the court seized.

Lesson 7 – Freedom of Expression, a comparative overview.

Licra vs. Yahoo!

A website hosted auctions for the sale of Nazi memorabilia, prohibited under French criminal law. First Amendment, because the sale of Nazi memorabilia is covered by the First Amendment protection. TGI Paris ordered Yahoo! To prevent access to the website from the French territory. Yahoo! challenged the injunction before US courts: jurisdiction of the French court is appropriate (**purposeful availment**).
In addition to the first amendment there is no protection for expressions likely to pose a threat to other fundamental rights enshrined in Western constitutions.
Forum shopping and regulatory arbitrage, the problem is the enforcement. The saga before the US Courts: a right to regulate freedom of expression from outside the US?

What does "Freedom of Expression" mean?
The universalization of civil and political rights implies that the free expression rights formally cover **all communicative activities** by any single citizen.

The *"Declaration of the rights of man and of the Citizen"* - France (1789) stated:
"The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen ay, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of the freedom as shall be defined by law"

The Evolution of the Concept
States have assumed a more active role in the regulation of free expression (e.g. audiovisual, communication, protection of pluralism). These regulatory schemes go beyond the original liberal idea of lack of state interference, putting in the hands of public institutions the task to create and foster the conditions for a fair and equal access to information by any citizen (**pluralism**). The digital era and especially the Internet have introduced new kinds of communicative instruments that have continued to **change and decentralize** the structure of the public sphere as well as the communications market.

From State action to a Transnational/Global regulation?

From Atoms to Bits
Absence of explicit provisions concerning freedom of expression on the Internet. A matter of **balancing** fundamental rights. Courts as "**playmakers**".

Worldwide Differences

- **USA**, **Protective.**
  The *American Constitution – First Amendment* USA (1791). "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the **freedom of speech**, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances".*

  U.S. Supreme Court.
  Supreme Court, Police Dept. of Chicago vs. Mosley, 408 U.S. 92 (1972) – Justice Thurgood Marshall:
  "The First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content… our people are guaranteed the right to express any thought, free from government censorship. The essence of this forbidden censorship is content control".

  Freedom of speech is weighed with other interests such as public order and decency, national security, the rights to reputation, fair trial, …

Standard of Judicial review:

- **Intermediate Security** (e.g. commercial speech). Important Government interest or means related to that interest.
- **Strict Scrutiny** (e.g. political speech). Compelling governmental interest, law narrowly tailored, least restrictive means test.

Restriction to freedom of expression

- **Incitement**, limitation can apply in case of incitement of an "imminent lawless action" (SC Brandeburg vs Ohio, 1969).
- **False Statements**, not protected under the First Amendement (SC Gertz vs Robert Welch, Inc., 1974)
- **Obscenity**, not protected, "prurient interest" concept, "Miller test" (SC Miller vs California, 1973).

Hate Speech

Insults, slurs or epithets directed to someone within a certain group of people.
Supreme Court, **Beauharnais vs Illinois**, **1952**: libel and group libel are not covered under the First Amendment.
Supreme Court, Brandenburg vs Ohio, 1969: KKK case, freedom of hate speech unless it is directed to producing an "imminent lawless action".

Reno vs ACLU (1997)

The **Communication Decency Act** (1996) criminalized the online distribution of obscene or indecent materials to any person under 18. The Court ruled it **unconstitutional**. The restrictions were too vague and lacked the precision required to limit free speech: the concepts of "indecent" and "patently offensive" contents were not appropriately defined.

Ashcroft vs ACLU (2002)

Attempt to regulate minors protection online: **The Child Online Protection Act (1998). "Material harmful to minors"**, *"any obscene material that, based on community standards, an average person would consider to appeal to a prurient interest".* The Court ruled it **unconstitutional.** COPA failed to meet the standards required to circumscribe free speech limitations.

Ashcroft vs Free Speech Coalition (2002)

The **Child Pornography Prevention Act** (1996) prohibited the diffusion of images that appeared to be minors engaged in sexual activity and any form of speech conveying the impression that the images represented minors involved in sexual conduct. The Court ruled it **unconstitutional**. The restrictions to the freedom of expression were disproportionate and overbroad.

- **Europe**, **Restrictive**

Historically, nations on the continent of Europe had a low level of protection for freedom of expression. Ù
Different levels of protection nowadays:

- European Convention on Human Rights (ECHR)
- EU Charter of Fundamental Rights (Charter)
- National Constitutions (Art. 21 It. Constiution)

Art. 10 ECHR – Statement of principle

(1). Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and idea 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.

Art. 10 ECHR – Limitation to the freedom
(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 con dence, or for maintaining the authority and impartiality of the judiciary.*

Interferences by public authorities are only allowed under the strict conditions that any restriction or sanction must:

- Be necessary in a democratic society
- Be prescribed by law
- Have a legitimate aim

No "Hate Speech" in ECHR
Although there is no "hate speech" definition, the **European Court of Human Rights** has established some parameters.
Two approaches to **ban hate speech**:

- By applying Art. 17 (prohibition of abuse of rights) if hate speech negates the fundamental values of the Convention;
- By applying the limitations provided for in Art. 10, II par. And Art. 11 (when the speech, although it is hate speech, is not apt to destroy the fundamental values of the Convention).

Art. 11 EU Charter of Fundamental Rights
Freedom of expression and information

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.*
2. *The freedom and pluralism of the media shall be respected.*

Freedom of Expression in the Italian Constitution
Art. 21 of the Italian Constitution
A new Constitutional right. Applicable to all forms of communication.
Only one express limit: **Public Morality**.

- First it meant the common sense morality
- Today intended as sexual modest and personal dignity.

Other implicit limits to protect a different set of rights (e.g. reputation).

ECTHR, Pravoye Delo and Shektel (2011)
"*The* ***risk*** *of harm posed by content and communications* ***on the Internet*** *to the exercise and enjoyment of human rights and freedoms* ***is certainly higher*** *than that posed by the press.*"
"*Therefore, the* ***policies*** *governing reproduction of material from the printed media and the Internet* ***may differ****: the latter undeniably have to be adjusted according to the* ***technology's***

specific features *to secure the* ***protection and promotion*** *of the* ***rights*** *and* ***freedoms*** *concerned.*"

ECTHR, Delfi vs Estonia (2015)
Imposing an online news portal to pay damages for having failed to promptly remove defamatory comments posted by anonymous users does not amount to a violation of right to freedom of expression entrusted to Art. 10 of the ECHR.
How would the CJEU have decided the case?

ECHTHR, MTE vs Hungary (2016)
A violation of Article 10 of the ECHR had occurred through the imposition of liability on the applicant providers: no clearly unlawful speech.
A **notice-and-take down system is sufficient** for balancing the rights and interests of all those involved in a given intermediary liability dispute: while in *Delfi* this rule was found to be inapplicable, as the contested comments constituted hate speech, thus allowing to impose liability on internet news portals when they fail to take measures to remove clearly unlawful comments without delay, no such utterances were found to be at issue in *MTE,* making the imposition of a stricter standard unjustifiable.

CJEU, Scarlet (2010) and Netlog (2012)
Protection of copyright must be **balanced** with:
- Users' right to data protection
- ISPs' freedom to carry out business
- Users' freedom of expression

Freedom of expression seems to play a **secondary role** compared to the right to data protection and the freedom to conduct business.

The European Approach
As opposed to the US view, European courts took a **restrictive approach.** Freedom of expression enjoys protection as fundamental right "among the others" (**non – absolute** right). A downgrading of the consideration attached to FoE in the non-digital environment.

Lesson 8 – ISP Liability provisions as Free Speech Rules.

ISP Liability – "Mere private law rules?"

The origins of ISP Liability in the US: Section 230 CDA: a free speech standpoint.
The DMCA and the influence on the European Union Legal Framework.
The evolution of Internet Services: a shifting paradigm of liability?
- The Attitude of the Court of Justice of the EU vis-à-vis ISP
- (passim) ISP liability in the ECHR view

Consequences on free speech: disinformation and hate speech as "stress test".

Service Providers are not delivering a content:
- **Access Providers**, Internet Connection
- **Caching Providers**
- **Hosting Providers**, they host the information, but they do not any control over the content, therefore they don't have any editorial responsibility.

Content Providers, are those providing the content and writing information in the web.

The origins of ISP Liability - Pre-Section 230 CDA decisions.

Cubby vs CompuServe
CompuServe was an Internet Service Provider, which hosted an online news forum. Cubby alleged that CompuServe was the publisher of third-parties defamatory statements, therefore it should have been held liable. CompuServe did not dispute the defamatory nature of the content. However, during the trial no evidence was presented showing that CompuServe either was aware or should have been aware of the existence of such defamatory content. The Court excluded CompuServe liability, stating that "CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so".
A computerized database is the **functional equivalent of a more traditional news vendor**, and the inconsistent application of a lower (i.e. stricter) standard of liability to an electronic news distributor than that which is applied to a public library, book store or newsstand **would impose an undue burden on the free flow of information**: the appropriate standard of liability to be applied is whether CompuServe **knew or had reason to know** of the allegedly defamatory statements.

Stratton Oakmont vs Prodigy Serv.
Stratton Oakmont argued that Prodigy should be considered a "publisher" of anonymous statements posted on its bulletin board.
Under the common law of defamation, if Prodigy were considered a publisher, it could be held liable for the statements of the unknown user. Conversely, if it were found to be merely a "distributor," it could not be held liable unless it knew or had reason to know about the allegedly defamatory statements.
The plaintiffs pointed to Prodigy's "content guidelines," which stated rules that users were expected to abide by, a software screening program which filtered out offensive language, and the employment of moderators for enforcing the content guidelines.
The Court found that such representations and policies were sufficient to treat Prodigy as a publisher
The Court distinguished the case from that involving CompuServe, which was found merely to be an "electronic for-profit library" or repository and thus a passive distributor.
In particular, the court pointed to **Prodigy's creation of an "editorial staff of Board Leaders who have the ability to continually monitor incoming transmissions**." The court noted, however, that bulletin boards should normally be considered distributors when they do not exercise significant editorial control, as Prodigy had done.

CDA 230 – The most important law protecting internet speech
Interactive Computer Service, any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.
Information Content Provider, any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

The origins of ISP Liability - The Communications Decency Act (1996)

“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”.
In passing the Communications Decency Act of 1996 the House explicitly stated its intent to overturn the result reached in the *Prodigy* case.
It precludes courts from claims that would place a computer service provider in a publisher's role. Lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions - such as deciding whether to publish, withdraw, postpone or alter content - are barred.
[…] No provider or user of an interactive computer service shall be held liable on account of
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)

The origins of ISP Liability – After the CDA

Zeran vs America Online, Inc.
Zeran brought an action against AOL, arguing that it unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter.
The district court granted judgment for AOL on the grounds that § 230 CDA bars Zeran's claims.
Zeran appealed, arguing that § 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. § 230, however, **plainly immunizes computer service providers** like AOL from liability for information that originates with third parties.
Congress' purpose in providing the § 230 immunity was evident: The amount of information communicated via interactive computer services is staggering. **The specter of tort liability in an area of such prolific speech would have an obvious chilling effect.** It would be impossible for service providers to screen each of their millions of postings for possible problems. **Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted**. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Reno vs American Civil Liberties Union
The CDA also criminalized the online distribution of «obscene» or «indecent» materials to any person under 18
Held: Unconstitutional.
The restrictions were too vague and lacked the precision required to limit free speech: the concepts of «indecent» and «patently offensive» content were not appropriately defined.
«The CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve».
«It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. But that interest does not justify an unnecessarily broad suppression of speech

addressed to adults. As we have explained, the Government may not reduc[e] the adult population to only what is fit for children».
«Radio and television, unlike the Internet, have received the most limited First Amendment protection because warnings could not adequately protect the listener from unexpected program content».
«On the Internet, the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material».

Copyright Enforcement and ISP Liability - The rise of the notice-and-take down regime

The Digital Millennium Copyright Act
A service provider shall not be liable for monetary relief, or for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider:

-
    - Does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
    - In the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
    - Upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

- Does not receive a financial benefit directly attributable to the infringing activity, in a case in which the servie provider has the right and ability to control such activity; and
- Upon notification of claimed infringement responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

ISP Liability in Europe – The E-Commerce Directive

Policy to enhance Freedom of Expression
- Art. 2(1)(b) of Directive 2000/31/EC: «any natural or legal person providing an information society service»
- Art. 1(1)(b) of EU Directive 2015/1535: «any service normally provided
    - for remuneration,
    - at a distance,
    - by electronic means and
    - at the individual request of a recipient of services».

Two pillars:
- **Liability Exemptions**
- **Absence of a General Obligation to Monitor**

Mere Conduit Providers (Art. 12)
The service provider consists of the mere transmission of information or the mere provision of access to a communications network.
The ISP is not liable for the information transmitted if it:
- Does not initiate the transmission,
- Does not select the receiver of the same and
- Does not select or modify the information contained in the transmission.

Caching Providers (Art. 13)
The service provided consists of the temporarily storage of information.
Liability Exemptions apply only if:

- The provider does not modify the information;
- The provider complies with conditions on access to the information;
- The provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- The provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- The provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Hosting Providers (Art. 14)
The service provided consists of the permanent storage of information
Liability Exemptions apply only if:

- The provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The Second Pillar, Absence of a General Obligation to Monitor (Art. 15)
Member States shall not impose a general obligation on providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

European and National Trends, the Evolving Liability Regime Applicable to ISP
Which assumptions behind the E-Commerce Directive (and Section 230 CDA)?
Recital 42: «The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored».

The View of the Eu Court of Justice – Active vs Passive Providers
Google France
In the event that the use of a keyword reproducing or imitating registered trademarks does not constitute a. use which may be prevented by the trade mark proprietor, may the provider of the paid referencing service be regarded as providing an information society service consisting of the storage

of information provided by the recipient of the service, within the meaning of Article 14 of Directive 2000/31, so that the provider cannot incur liability before it has been informed by the trade mark proprietor of the unlawful use of the sign by the advertiser?
The restriction on liability set out in Article 14(1) of Directive 2000/31 applies to cases '[w]here an information society service is provided that consists of the storage of information provided by a recipient of the service' and means that the provider of such a service cannot be held liable for the data which it has stored at the request of a recipient of that service unless that service provider, after having become aware, because of information supplied by an injured party or otherwise, of the unlawful nature of those data or of activities of that recipient, fails to act expeditiously to remove or to disable access to those data.
The legislature defined the concept of 'information society service' as covering services which are provided (i.) **at a distance**, (ii.) **by means of electronic equipment for the processing and storage of data**, (iii.) **at the individual request of a recipient of services**, and (iv.) **normally in return for remuneration**. Regard being had to the characteristics of the referencing service at issue in the cases in the main proceedings, the conclusion must be that that service features all of the elements of that definition.
In addition, a referencing service provider transmits information from the recipient of that service, namely the advertiser, over a communications network accessible to internet users and stores, that is to say, holds in memory on its server, certain data, such as the keywords selected by the advertiser, the advertising link and the accompanying commercial message, as well as the address of the advertiser's site. It is further necessary that the conduct of that service provider should be limited to that of an '**intermediary service provider**' within the meaning intended by the legislature; it follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is '**of a mere technical, automatic and passive nature**', which implies that that service provider '**has neither knowledge of nor control over the information which is transmitted or stored**'.
The mere facts that the referencing service is subject to payment, that Google sets the payment terms or that it provides general information to its clients cannot have the effect of depriving Google of the exemptions from liability.
Likewise, concordance between the keyword selected and the search term entered by an internet user is not sufficient of itself to justify the view that Google has knowledge of, or control over, the data entered into its system by advertisers and stored in memory on its server.
By contrast, the role played by Google in the drafting of the commercial message which accompanies the advertising link or in the establishment or selection of keywords is relevant.

L'Oreal vs eBay
Article 14(1) of Directive 2000/31/EC must be interpreted as applying to the operator of an online marketplace where that operator has not played **an active role** allowing it to have **knowledge or control** of the data stored.
The operator plays such a role when it provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them.
Where the operator of the online marketplace has not played an active role, it nonetheless cannot, in a case which may result in an order to pay damages, rely on the exemption from liability if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realized that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously.

The View of the EU Court of Justice – Ex Ante Monitoring Obligations
Scarlet vs SABAM

SABAM is the Belgian collecting society which had gone to court asking for the ISP, Scarlet, to monitor and block peer-to-peer transfers of music files which it represented.
In 2007, a Belgian court ordered Scarlet, an ISP, to bring to an end the copyright infringements of content of which the applicant was the rightholder, by making it impossible for its customers to send or receive in any way files containing a musical work in SABAM's repertoire by means of peer-to-peer software.
Does EU law permit a national court to issue an injunction against intermediaries whose services are used by a third party to infringe copyright, to order an ISP to install, **for all its customers, in abstracto (preventing measures)** and as **a preventive measure, exclusively at the cost of that ISP** and **for an unlimited period**, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files?
Such an injunction imposed on the ISP to install the contested filtering system would oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31.
In adopting such injunction, the national court would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.

Facebook Austria vs Eva Glawischnig-Piesczek
Ms. Eva Glawischnig-Piesczek, who was a member of the Austrian National Council, chair of the parliamentary party die Grünen (the Greens) and the party's federal spokesperson, applied to the Austrian courts for an injunction to be issued ordering Facebook to bring to an end the publication of a defamatory comment.
As Facebook did not react to her request for that comment to be deleted, Ms. Glawischnig-Piesczek sought an order requiring Facebook to cease publication and/or dissemination of photographs of Ms. Glawischnig-Piesczek if the accompanying message disseminated the same allegations as the comment in question and/or 'equivalent content'.
The Oberster Gerichtshof (Supreme Court of Austria), before which this case was ultimately brought, considered that the statements at issue were intended to damage the reputation of Ms. Glawischnig-Piesczek, to insult her and to defame her.
Having been called upon to adjudicate on the question whether the injunction can also be extended, worldwide, to statements with identical wording and/or having equivalent content of which Facebook is not aware, the Oberster Gerichtshof requested the Court of Justice to interpret the E-Commerce Directive in that context.
Ruling: a Member State is not precluded from stopping and preventing an illegal activity, which a Member State's court ruling has considered as such and the prohibition of monitoring obligations does not apply to a specific case.
Such a specific case may be found in a particular piece of information stored by a social network provider at the request of a certain user, the content of which was examined and assessed by a court having jurisdiction in the Member State, which, following its assessment, declared it to be illegal. Given that a social network facilitates the swift flow of information stored between its different users, there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network.
In those circumstances, it is legitimate for the court having jurisdiction to require a host provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information, irrespective of who requested the storage of that information. In particular, in view of the identical content of the information concerned, the

injunction granted for that purpose **cannot be regarded as imposing on the host provider an obligation to monitor generally the information which it stores**, or **a general obligation actively to seek facts or circumstances indicating illegal activity**, as provided for in Article 15(1) of Directive 2000/31.
In order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, to be capable of achieving those objectives effectively, that injunction must be able **to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently,** because of the words used or their combination, compared with the information whose content was declared to be illegal. Otherwise, the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he/she is a victim.
Article 15(1) of Directive 2000/31 implies that the objective of an injunction consisting, inter alia, of effectively protecting a person's reputation and honour, may not be pursued by imposing an excessive obligation on the host provider.
Therefore, it is important that the equivalent information contains **specific elements which are properly identified in the injunction**, **such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal. Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content.**
In the view of the CJEU, automated technologies could then seek this information, which *does not require further analysis* and falls within the specific characteristics of the injunction. Directive 2000/31 does not make provision for any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt in accordance with that directive: accordingly, it does not preclude those injunction measures from producing effects worldwide.
Directive 2000/31, in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

- ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;
- ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, or
- ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

The View of the European Court of Human Rights – A more human rights-based standpoint
Delfi vs Estonia (2015)

Imposing an online news portal to pay damages for having failed to promptly remove defamatory comments posted by anonymous users does not amount to a violation of right to freedom of expression entrusted to Art. 10 of the ECHR.

MTE/Index.hu vs Hungary (2016)

MTE and Index.hu Zrt: two Internet news portals in Hungary which published the same article, criticizing two real-estate websites managed by a unique company.

In both the news portals, users wrote offensive comments against the real-estate company, which sued MTE and Zrt.

Hungary's supreme court upheld the decisions of the lower courts, declaring MTE and Zrt liable for having permitted such offensive and unlawful comments to be published.

Ruling: the ECHR stated that Hungarian courts did not properly balance the right to good reputation and the protection of freedom of expression

It listed a series of criteria which made it come to that conclusion:

- The context of the comments.
- The efforts MTE and Index have made to remove them promptly.
- The consequences of the comments for the real-estate company.

Lesson 9 – Trends in ISP Liability.

Internet Service Providers – The Italian Legislation

In Italy there is a division of providers in three categories:

- **Mere Conduit**
- **Caching**
- **Hosting**

And no general obligation to monitor.

Internet Service Providers – Notice-and-takedown procedure in Italy

When on notice of illegal content or activities, including by receiving service of a take-down order properly issued by the competent Administrative or Judicial Authority…

… hosting providers shall promptly remove access to the relevant infringing content.

What does "being on notice" (having actual knowledge) of illegal conduct/content mean for an ISP?

- Being served with an order of the competent authority specifiying the URL of the content to be taken down?
- Being served with an ex parte notice and takedown request regarding specific content identified by the relevant URL?
- Being served with an ex parte notice and takedown request concerning allegedly illegal content uploaded by third parties on the relevant platform (with no mention of URLs or mention of an URL as example)?

According to certain courts, when it comes to an active service provider there is no need to mention specifically the URLs of every piece of illegal content/information. The assumption behind this reasoning is that being more "active", these providers have more control (then, knowledge).
Other courts, however, challenged this assumption and required specific indication of illegal content/information to consider the ISP "on notice".

In 2019, the Italian Supreme Court ruled that active providers cannot benefit from the liability exemptions. The Court referred to some signs suggesting that the hosting provider has an active role (not all of these must be present):

(i) filtering, (ii) selection, (iii) indexing, (iv) organization, (v) cataloging, (vi) aggregation, (vii) evaluation, (viii) use, (ix) modification, (x) extraction, or (xi) promotion of content.

If made in the context of a business-oriented management of the service.

The Supreme Court held that, for a provider to become aware, it is not required that the rightholder send a formal cease-and-desist letter: **a simple communication suffices**.
Also, it did not exclude that simple indication of the title of the work could be enough. A URL is required only when "indispensable" to identify the infringing content.
The Court also ruled that **a notice-and-takedown request imposes on the relevant provider an obligation of 'stay-down'**, ie to prevent the re-uploading of the same infringing content: it has nothing to do with imposing a general monitoring obligation.

The Google vs Vivi Down Case
Factual Background
On September 8, 2006 a video showing a disabled student being bullied by three of his schoolmates was posted on Google Video; The video was flagged by many users; Video top ranked within the "funny videos" category; Italian postal police sent a removal notice on November 7, 2006; Removal of the video occurred on the same day.
The Public Prosecutor of Milan started the investigations for two charges:

- Co-participation in aggravated **defamation**;
- Violations of **Data Protection Rules** (in particular, Section 167 of Privacy Code);

Google's management was placed under investigation.

First Instance Court of Milan
The judge acquitted all the four executives from the charge of defamation. They had **no legal obligation** to prevent the defamation by exercising a preventive control over content loaded on Google-video site.
The executives were found guilty for privacy violations, given 6-months jail terms. The judge suspended the sentences because they were first-time offenders who had committed a minor crime.

First Instance Court of Milan – Reactions
"[] *we are deeply troubled by this conviction for another equally important reason. It attacks the very principles of freedom on which the Internet is built. Common sense dictates that only the person who films and uploads a video to a hosting platform could take the steps necessary to protect the privacy and obtain the consent of the people they are filming. European Union law was drafted specifically to give hosting providers a safe harbor from liability so long as they remove illegal content once they are notified of its existence.*"

Court of Appeals of Milan
Two Issues at the Court of Appeals of Milan:

- **Data Protection Framework**, Who is the controller? Who is the processor?
  Three relevant relationship to take into account:
  - Between uploading user (**Data Controller**) and bullied boy (**Data Subject**)
  - Between Google (**Hosting – Data Controller**) and uploading user (**Data Subject**)
  - Between Google and the bullied boy, **No Relationship**, Google makes no autonomous determination with regard to the purpose of use and the related procedures of data subject's personal data.
    Therefore it followed the **acquittal** from data protection law infringement.

- **ISP Liability**, How "passive" should be an ISP to benefit from the liability exemption?

*"In today's world, the **services that an ISP offers** are **not limited to the technical process** that simply sets up and provides access to the network: as in the case of the content provider, they extend to make it possible for users to submit their own content and other people's content on the network. **They cannot**, therefore, **escape the duty to comply with the standard regulations governing liability for data processing**." "[] It follows that **all the elements considered in this case** (the possibility of filtering, of take-down, of identifying content by using key words, of indexing content and any use for advertising purposes) **lead to the view being formed** that **Google Video must be classified as active hosting** at the very least." "[] Given that it is able to organize and select the material sent by users, **any possibility of Google Video being in a position to continue to insist with its claim that it is neutral can in fact be ruled out**." "[] In order to establish liability on the grounds of an omission on the part of a host or content provider, it has to be established whether there is a duty provided by law on the part of that provider to prevent the event. So what has to be established on the one part is the existence of a duty of care and on the other, the possibility, in practice, of carrying out prior screening.*"

Therefore it followed the **acquittal** from the defamation charges.

The Supreme Court of Cassation
Supreme Court of Cassation entirely confirmed the Court of Appeals of Milan's decision.
Google as a **hosting provider**:

- Does not have to supervise data uploaded by a third party.
- Does not have to inform the third party about the personal data processing rules.

The Court declared that Google is merely an **Internet Host Provider**. It simply provides an **online platform where users can upload videos**, of which content the users are exclusively in charge (of privacy concerns). Nevertheless, it has to immediately remove unlawful contents in case the authority orders to do so.

Lesson 10 – Fake News, Disinformation and Hate Speech Online.
Most Important topics:

-
- **Self-regulation vs Public Regulation (advantages and drawbacks).**
- **Code of Practice of 2018, bad decisions of sounding board.**
- **Free marketplace of ideas (Justice Holmes), difference between US and EU, due to 1st amendment.**

The Post-truth Era
According to the Oxford Dictionary post-truth is an adjective defined as "**relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief**".

Post-truth was the "World of the Year" 2016.

New Phenomena?
Fake news and hate speech are not something new.
An old and a recent example of fake news:

- "**The Great Moon Hoax**" (1835)
- "**How Teens in the Balkans Are Duping Trump Supporters with Fake News**" (2016)

Characteristics of News online:

- Speedness
- No Point of Return
- Amount of Information
- 24 Hours
- Attention is a Limited Resource

The Digital Realm

- Even if fake news and hate speech contents are not new in the history, their renewed importance is related to the dissemination through a global means of communication: the Internet.
- No scarcity of resources on the Internet.
- But, scarcity of time for users to assess the quality of online contents?

The Role of Algorithms: the Filter Bubble Effect

Pariser, personalized searches and filter bubbles:

> Filter bubble is "a state of intellectual isolation that can result from personalized searches when a website algorithm selectively guesses what information a user would like to see based on information about the user, such as location, past click-behavior and search history".

Negative effect on the marketplace of ideas.
Sunstein, confirmation bias, polarization.

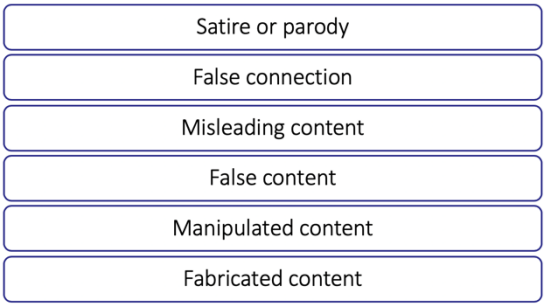
Fake News

There is no legal definition of fake news. According to the Cambridge Dictionary, the notion of fake news include "**false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke"**.

Fake News – Legal Challenges

Against this (uncertain) scenario, some claims emerge:

- Criminalizing the publication of fake news (user/publisher-side)
- Criminalizing the spread of fake news (ISP-side)
- Filtering the flow/circulation of fake news (ISP/Third parties-side)
- Criminalizing/Filtering hate speech (user/publisher/ISP-side).



Hate Speech, in search of definition and meaning

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Illegal hate speech is defined as: "**the public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin**".

Three main questions

- Is disinformation/misinformation *per se* a problem?
  What degree of tolerance is offered by the US and European constitutionalism respectively?
- How can fake news be defined?
  Where to draw the thin red line between fake news and truth?
- Who should be in charge of removing fake news from the Internet?

Whether disinformation is a problem

- The definition of truth is not always clear
- Some news can be only partially true (fake news?)
- Fake news is not illicit in itself
- Rather, fake news becomes problematic when affects constitutional interests.

Marketplace of ideas

The emergence of truth is the result of the public confrontation of **different points of view**, no matter how offensive, wrong or inadequate they may be *(Abrams v. United States,* 250 US, 616, 630, 1919*)*: "**the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out**".

The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a **clear and present danger** that they will bring about the substantive evils that the United States Congress has a right to prevent. It is a question of proximity and degree. When a nation is at war, many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight, and that no Court could regard them as protected by any constitutional right *(Schenck v. United States,* 249 U.S. 47, 1919).

Europe – ECHR

Two possible ground for limiting the spread of fake news:

- Article 10, para 1: "to **receive** and impart information and ideas" (right to be informed).
- Article 10, para. 2: three-step test.

Fake news and the Internet

How have courts reacted to the rise of the Internet while protecting freedom of expression?
Europe -> **Restrictive**
USA -> **Protective**

The Marketplace of Ideas

- **Milton**, truth as a streaming fountain
- **Mill**, truth as the result of the free market
- **Justice Holmes**, emergence of truth is the result of the public confrontation of different point of view, no matter how offensive, wrong or inadequate they may be
- **A new digital marketplace of ideas**,
    - **Yes**, the Internet offers an unrestricted and borderless space for opinions, ideas ad thoughts to flow.
    - **No**, the Internet is not a **free** marketplace.

Defining "Fake News"

- The definition of truth is not always clear
- Some news can be only partially true (fake news?)
- Fake news is not illicit in itself
- Rather, fake news should become relevant for the legal system when the protection of constitutional interests is affected.
- Among fake news, three clusters can be distinguished:
    - False information created ad hoc by actors with significant economic power with deceptive intent (politic propaganda, Trump and Russia).
      Remedy? Transparency

    - Information circulating in the Internet that becomes *vox populi* (the case of vaccines in Italy).
      Remedy? Education
    - False information which harms individual and collective interests (discriminator or defamatory statements).
      Remedy? Law
- Does the use of the Internet for circulating fake news trigger the adoption of a different approach and, accordingly, of ad-hoc legal measures?
- Is law the only remedy/ the last resort?

Fact Checking Algorithms and Digital Platforms
Is it possible to argue that the use of fact-checking algorithms, which rank content depending on accuracy or nature, makes digital platforms aware of the hosted content?
(Responsabilization of platforms does not mean editorial responsibility)

How to deal with fake news and hate speech online?
Three possible drawbacks to take into account:
- How to reconcile the regulatory measures against fake news and hate speech content with freedom of expression (collateral censorship).
- How to avoid concentration of power in the hands of (a few) specific authors (see *Google Spain*).
- How to ensure an effective legal enforcement of remedies online (privatization of the protection of rights).

Public vs Self-Regulatory Solutions

Public Regulation
- **Germany** – NetzDG or "Network Enforcement Act" – June 30, 2017.
  The **Goal** was holding social media networks responsible for hosting fake news and hate speech. Social media networks (with more than 2 million registered users in Germany) must remove hateful content or fake news within a 24 hour time frame (if the content is manifestly unlawful). Specifically cites "the experience in the US election campaign" as a reason for a crackdown on "punishable false reports ('fake news')." Punishments consisting in fines up to € 5,000,000 (monetary penalties).
- **Italy**, proposal for the introduction of criminal penalties through the draft "disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica" (Disegno di Legge Gambaro).
- **Czech Republic**, a Government task force called the "Centre Against Terrorism and Hybrid Threats" dedicated to counter "disinformation campaigns related to internet security."
- **Singapore**, new laws to tackle fake news will be introduced in the next future.

Self-Regulation
- **Facebook**, hiring 3,000 more moderators to monitor illicit content (private censorship?). Advertisements on how to spot fake news. Cooperation with Fact-Checking providers.
- **Twitter**, a tool to allow users to flag tweets containing fake news may be introduced

Co-Regulation
In 2016 the EU adopted the Code of Conduct on countering illegal online hate speech. The **Goal** was ensuring that requests to remove content are promptly handled. Participation of NGOs and public bodies from across the EU to provide data on how quickly such illegal content was removed.

2018: EU Code of Practice on Disinformation

It was called "the so called code of practice" because it was missing of the essential criteria.

A multi-dimensional approach to disinformation: the HLEG on fake news and online disinformation

- Enhance **transparency** of online news, involving an adequate and privacy-compliant sharing of data about the systems that enable their circulation online;
- Promote **media and information literacy** to counter disinformation and help users navigate the digital media environment;
- Develop tools for **empowering users and journalists** to tackle disinformation and foster a positive engagement with fast-evolving information technologies;
- Safeguard **the diversity and sustainability of the European news media ecosystem**.
- Promote **continue research** on the impact of disinformation in Europe to evaluate the measures taken by different actors and constantly adjust the necessary responses.

The threat is disinformation, not "Fake News"
"false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. The risk of **harm** includes threats to democratic political processes and values, which can specifically target a variety of sectors, such as health, science, education, finance and more".

Does not cover issues arising from the creation and dissemination online of illegal content (notably defamation, hate speech, incitement to violence), which are subject to regulatory remedies under EU or national laws. Nor does it cover other forms of deliberate but not misleading distortions of facts such a satire and parody.

Lesson 11 – The Origins of Privacy and Data Protection in the US and Europe.
Italy has some roots connected to ideas on which Europe is based, that makes impossible to private citizens of privacy in a permanent way.

The Origins of the Right to Privacy
Privacy is not born in Europe, but in U.S., even if it's taken very seriously in Europe.

1850-1890: The coming of the "sensationalistic press", favoured by the use of new technologies (handheld camera), increased the intrusions in individuals' private life.
1884: Eastman Kodak Company introduced the "snap camera", which allowed to "take candid photographs in public spaces".
Between 1850 and 1890, U.S. newspaper circulation grew by 1,000 percent—from 100 papers with 800,000 readers to 900 papers with more than 8 million readers.

Warren & Brandeis, "Right to Privacy", *Harvard Law Review*, 1890: From a personal experience (Warren) to a new fundamental right
The personal experience of S.D. Warren. The Boston gazette was commenting the nightlife of miss. Warren. Therefore the lawyer didn't want his reputation affected by the behavior of the wife. He wrote an article on Harvard Law Review, where he wrote the theorization of privacy. The idea was the "Right to be left alone" and to avoid intrusion in the personal life.

"The existing law affords a principle from which may be invoked to **protect the privacy** of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds"

Technology, such as Cameras at the time, is something that changes the rules of the game. A change in technology requires a change in the ruling system.

Right to Privacy and Data Protection
In relation to technology we can do a basic distinction between:

- **Right to privacy**: right to be let alone is conceived as the freedom from any unauthorized intrusion or interference by public and private bodies into private life. (At the times of Warren, was the "Right to be left alone").
- **Right to data protection**: based on the concept of personal data, requires that the (authorized) use of the same by private and public bodies is made in accordance with specific legal standards.

Nowadays it's a dynamic concept, since there is the possibility to store thousands and thousands of data. It's no more just a static "Don't be inside my house and my spaces", therefore there is no processing of the data, it's just static. In a dynamic approach there is a permanent control and the data it's not forgotten after the journal is throw away, but it's stocked in the databases.

Privacy Laws in the US
Fourth Amendment, US Constitution (1791)
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

The Supreme Court, one century later, changed the interpretation of this amendment, in order to include a privacy protection perspective.

Privacy in the US
"Shadow right, it's hidden behind"

- **Griswold vs. Connecticut, 381 U.S. 479 (1965)**
  The Supreme Court found a state law which prohibited the use of contraceptives to be in violation of **"right to marital privacy"** (it's not an issue of the State whether a family decides to use contraceptives) protected under the 4th Amendment.
  Griswold v. Connecticut, the Supreme Court decision that made legal access to birth control the law of the land. The ruling stated that **birth control is a matter of privacy**, and something to be decided between a woman and her doctor. (It is generally recognized as the predecessor to Roe v. Wade and Lawrence v. Texas). Estelle Griswold, the Executive Director of the Planned Parenthood League of Connecticut, and Dr. C. Lee Buxton had opened a birth control clinic in New Haven in order to test the law in Connecticut which had outlawed birth control, and were subsequently arrested. The case went to the Supreme Court, and it was found that the law violated the 14th amendment, which states, "no state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law…nor deny any person the equal protection of the laws."
- ***Roe v. Wade*, 410 U.S. 113 (1973)**

The right of a woman to have an abortion is covered by the right to privacy, even though this right must be balanced with the state's interests to protect prenatal life and women's health.

- ***Lawrence v. Texas*, 539 U.S. 558 (2003)**
  Based on the constitutional protection afforded to the right to sexual privacy, the Supreme Court struck down the laws of fourteen states that had imposed criminal penalties for the offense of sodomy.

From the US to Europe

Privacy and Data Protection in the European legal order

- While in U.S. the "Free Speech" is unattackable as stated by the First Amendment, in Europe, Privacy is its equivalent, privacy is a real super-right.
- Art. 8 ECHR: «**Everyone has the right to respect for his private and family**». Right to private life/privacy (right to be let alone).
- Convention of the Council of Europe No. 108/1981 **for the Protection of Individuals with regard to Automatic Processing of Personal Data.**
  "Processing of personal data": from the right to privacy to the right to data protection.

Right to Privacy in the ECHR

Article 8
"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."

This article clearly provides a right to be free of unlawful searches, but the Court has given the protection for "private and family life" that this article provides a broad interpretation, taking for instance that prohibition of private consensual homosexual acts violates this article. The protection afforded by Art. 8 ECHR is not without limits. The rights enshrined in paragraph 1 may be interfered with subject to the conditions laid down in paragraph 2. In accordance with this structure of Art.8, the following approach to scrutinizing cases, in which this article may have a bearing, may be taken:

- In a first step, it should be established whether there is an interference with the right to private life, family life, home or correspondence. To this end, it has to be established whether a certain measure, action or omission (see below) falls within the scope of one the interests, which Art.8 para 1 protects, and whether it has some impact on the way in which the rights can be exercised, whether it limits the extend to which the right can be enjoyed. The scope of private life, family life, home and corresponce are dealt with on the parts of this website dealing with the respective rights.
- Then it should be scrutinized whether this interference is justified pursuant to Art.8 para 2 ECHR.

Privacy and Data Protection in the EU

- Data Protection Directive 95/46/EC **GDPR**
  That it is the directive adopted in Internet times, during the transition in 1995, dynamic nature.
- E-privacy Directive 2002/58/EC **Still in force but…**

- Data Retention directive 2006/24/EC **Directive 2016/680**.

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
The notion processing means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

Treaty on the functioning of the EU (Art. 16)
Everyone has the right to the protection of personal data concerning them (Art. 16).

Charter of Fundamental Rights of the EU
Respect for private and family life /Art. 7).
Everyone has the right to respect for his or her private and family life, home and communications.

Protection of personal data (Art. 8).
- Everyone has the right to the protection of personal data concerning him or her.
- 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.
- Compliance with these rules shall be subject to control by an independent authority.

From a purely market-oriented perspective:
- Personal data as an asset, with economic value for business purposes, **free circulation of data**.

To a Human Rights Perspective:
- Protection of personal data, **fundamental rights of privacy and data protection**.

Privacy and Data Protection in the EU - Data Protection Directive 95/46/EC GDPR

Definitions:
- **Personal Data**, any information relating to an **identified** or **identifiable natural person** (Data subject, **e.g. Youtuber**).
- **Processing of Personal Data**, any operation performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage …
- **Data Controller**, the natural or legal person, public authority, agency or any other body which determines the purposes and means of the Processing of Personal Data. (**e.g. Youtube).**
- **Data Processor**, a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the controller.

Consent, Data Subject's consent. Any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. (**e.g. Lombardy tracing mobile phones**, temporary measures taken on reducing the privacy of individuals temporarily without their consent).

Principles:

- **Transparency**, the data subject has the right to be informed when his personal data is being processed. The controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. (art. 10 and 11). Data may be processed only under the following circumstances (art. 7):
    - When the data subject has given his consent.
    - When the processing is necessary for the performance of or the entering into a contract.
    - When processing is necessary for compliance with a legal obligation.
    - When processing is necessary in order to protect the vital interests of the data subject.
    - When processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.
    - When processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12).

- **Legitimate Purposes**, personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. (art. 6 b)

- **Proportionality**, personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. (art. 6). When sensitive personal data (can be: religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply. (art. 8). The data subject may object at any time to the processing of personal data for the purpose of direct marketing. (art. 14). A decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data. (art. 15) A form of appeal should be provided when automatic decision - making processes are used.

Data Protection Authorities
Transfer to third non-EU Countries
Member States shall provide that the transfer to a third country of personal data may take place only if the third country in question ensures an adequate level of protection.

Lesson 12 – The European Right to Digital Privacy: The Digital Rights Ireland case.
Steps Forward by the CJEU
- **Data Retention (Digital Rights Ireland)**
- **Google Spain**

- **Schrems**
- **Tele 2 Sverige**

The two cases were adopted by European Court of Justice, to define laws.

Data Retention Directive (2006)

Data retention means the ways according to which the data is stocked and processed and for how long. The duration of Data retention is important because Data could be very important to carry on investigations, institutions can arrive to the identification of the possible criminals. Also, to prevent terrorism attacks (London 2005).

- Created in reaction to the terrorism' attacks, then it can be shifted to Pandemic seasons
- It was not against the DNA of the rights, but against the principle of proportionality.
- The proportionality principle was broken for 3 reasons:
  - No definition of Serious Crime.
  - No Procedural Rights.
  - 2 Years was too long.
- The directive was annulled because was a piece of secondary legislation of European Union, which was against the Primary Legislation.

Mandatory retention of traffic and location data (Article 5) for ISP and ECS, identifying:

- Source and Destination
- Location
- Users' Device
- Date and Time
- Type of Communication
- Duration

Therefore, they can't retain the content of the conversation, so the essence of the right is not affected.

Retention period between 6 months and 2 years, it means that the Data could be retained from 6 months to 2 years, for specific reasons otherwise they should be deleted earlier. One of these reasons is the prevention of terrorism attacks, or:

"*for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law*" (Art. 1).

The Ruling

- **Art. 52 Charter (of fundamentals right of EU)**
  Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the **essence** of those rights *(DNA of the 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 recognized by the Union or the need to protect the rights and freedoms of others.

Guideline for dealing with crimes, but also for modern problems like Pandemics. If the Member States want to restrict one of the rights provided by the Charter, for example privacy, they should respect such conditions: not affecting the DNA of the rights and should be proportionate, it means that has to be necessary and should not restrict more than the necessary.

- **The Essence of the Rights**

"[I]*t must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such*".
"[T]*he use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organized crime*."
Data retention "*genuinely satisfies an objective of general interest*."

- **Principle of Proportionality**
  - The Directive has exceeded the limits imposed by compliance with the **principle of proportionality**. *(According to the Court of Justice this directive of 2006 affects the principle of proportionality, because…)*
  - There is no definition of "**serious crime**" and "**competent authorities**". *(During emergencies, Governments have more power to restrict rights, in authoritarian countries they will far more than the necessary to strength the regime, so the interpretation of "serious crime" cannot be left to the single state , because then it will change by state and state according to the ideas of the governments)*
    There are no objective and procedural criteria to establish limits of access to the metadata by the authorities. *(According to the Court of Justice there aren't clear procedures, how are they treated, to establish the limits of access to the metadata)*
    Excessive length of the retention period.
    (The time is too long, two years, even if the goal to prevents crime is reasonable, it's not proportionated).
  - The Court refuses the idea of **mass surveillance** of "*the entire European population*". *(Freedom and privacy are fundamental rights)*
    The metadata (Art. 5), taken as a whole, allow specific and precise deductions concerning private lives, habits, relationships, movements of the users.
    Absence of any relationship between the retained data and the serious crimes.
  - The Directive does not ensure a high level of protection since it does not guarantee the "*destruction of the data at the end of the data retention period*". *(It's important because the Data that it isn't destructed can be aggregated, anonymized and used to do Big Data previsions)*
    The Directive does not require that the data in question is to be retained within the European Union.
    On those grounds, the Court rules that the Directive 2006/24/EC is invalid.

Data Retention Saga Continues

- **Principle of Proportionality**
- Importance of Security Measures
- Role of the **Nizza Charter** to interpret EU Law, *the role of the Nizza Charter is a sort of "bill of rights" of the European Institutions, but it binds also the institutions of the Member States.*
- Data shall be retained within the EU.

Over every institution in EU Area there is the ECHR, but, for example, Russia is neglecting the obligations dictated. *Quoted the Article 8.*

Lesson 13 – The European Right to Digital Privacy: The Google Spain case, "Right to Be Forgotten".

Right to Be Forgotten,
CJUE, Google Spain (2014)
Mr. Costeja Gonzalez (Lawyer practitioner in a law firm) lodged with the Spanish Data Protection Authority a complaint against *"La Vanguardia"*, which publishes a daily newspaper with a large circulation and **Google Spain** and **Google Inc**.

The complaint was based on the fact that, when an internet user entered Mr Costeja name in the Google search engine, he would obtain links to two pages of La Vanguardia, of 19 January and 9 March 1998 respectively, on which an announcement mentioning his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

By the complaint Costeja Gonzalez requested:

- **La Vanguardia**, to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. (*The publication of La Vanguardia was a* ***mandatory publication****, therefore the Spanish authority had to reject the request to remove the article from "La Vanguardia"*).
- **Google**, to **remove** the **personal data relating to him**. He stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant. (*The Spanish authority accepted this request, Google challenged this decision in front of a judge in Madrid, however in Madrid didn't know if the request to remove from Google was in compliance or not with the European Directive 95/46, so he asked for clearance from the Court of Justice (preliminary reference procedure), the question asked are the one that follow).*

The complaint was upheld in so far as it was directed against **Google Spain** and **Google Inc.**
The Authority (Agencia Espanola de Proteccion de Datos) considered that operators of search engines are **subject to data protection legislation** given that they carry out data processing for which they are responsible and act as intermediaries in the information society.

Google Spain/Google, Inc. appealed to the Audiencia Nacional de Madrid. The latter issued an **order for reference to the CJEU** with the following questions:

- **Does the activity carried out by Google as search engine amount to a processing of personal data?** *(Is what google is doing covered by the Directive, are we dealing with data processing or not?)*
- **If so, does Google qualify as data controller?** *(Is Google a Data Controller or a Data Processor? Only if google is a data controller is obliged to remove information, otherwise the only responsible is the newspaper)*
- If so, **may a national data protection authority order Google to remove links to indexed information without prior consulting the owner of the web page?**
- If so, is such an obligation excluded when the information contains personal data lawfully published by third parties?

Advocate General JAASKINEN *(suggesting body that suggest which could be the solution, colored answers show the relation between the advocate general and the court of justice answers.).*
"*The particularly complex and difficult constellation of fundamental rights that this case presents prevents justification for reinforcing the data subjects' legal position under the Directive, and*

imbuing it with a right to be forgotten. This would entail sacrificing pivotal rights such as freedom of expression and information.

*I would also **discourage** the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the internet search engine service provider.*"

- **Does the activity carried out by Google as search engine amount to a processing of personal data? Yes**
  Agree
  Application of EU law, broad interpretation of the notion of 'establishment' and of the words 'in the context of the activities'.
  'in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively'.

- **Does Google qualify as data controller? Yes *Disagree***
  It has **no relevance whether the search engine has actually knowledge of the fact the personal data are contained in the websites subject to indexing**. *(The Court said that google is responsible since it's responsible of the indexing and the amplification of the search engine, the Court is manipulating the interpretation of the Directive 95/46 to apply).*
  Therefore, it amounts to a **data controller** and as such bears the obligations provided by the Directive 95/46.
  Search engine provider as "controller", this finding is not supported by empirical evidence but rather relies on the goal of affording individuals' data privacy broad protection.
  'it would be contrary not only to the clear wording of the Directive but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties'.

- **Does a "right to be forgotten" have any legal grounds? Yes** *Disagree*
  (Literally speaking no, because these aren't information false or incomplete, these are simply old).
  Art. 12 and 14 of the Directive 95/46 provide data subjects with the right to objection and to request the erasure or blocking of personal data in case of unlawful processing of the same.
  In the Court's view, **since not up-to-date news amounts to not correct information, an unlawful processing of personal data is at stake** and, accordingly, the rights under Art. 12 and 14 are **enforceable against the search engine** provider.
  Broad interpretation of "unlawful processing".

  Art. 12, lit. b of the Directive as legal ground for the RTBF, Extensive interpretation of this provision: the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular **because of the incomplete or inaccurate nature of the data.**
  Not a *numerus clausus* of conditions: Art. 12, lit. b only mentions some examples of the conditions authorizing data subject to enforce their rights.

- **May a national data protection authority order Google to remove links to indexed information? Yes *Disagree***

It is **first for the search engine provider**, in its capacity as data controller, to receive the requests of data subjects under Art. 12 and 14 and, if the case, to remove from the search results links to contents considered to be in breach of the right to be forgotten.
No prior consultation of the web site owner is necessary (freedom of expression at risk?) *(A private company such Google is now deciding the balance between privacy and access to information, freedom of speech, it is the privatization of some fundamental rights, however it).* However, data subjects may go before the **competent DPA or judicial authority** and ask for the removal of undesired contents.
Processing of personal data and freedom of expression. Article 9 of the Directive does not apply to the processing of personal data carried out by search engine providers. The Court has revisited the broad interpretation of the scope of this exception provided in *Satamedia* with respect to the relationship between data protection and freedom of information.

An Internet search engine provider may, upon certain conditions, **remove from the search results certain links to undesirable contents**. Removal of search results is **upon request of the concerned natural/legal person**. No guarantees for users' **freedom of information** and the dawn of the so-called "*right to be forgotten*."

Why Google wanted to have U.S. Law applicable rather than the Spanish/European Law? In Europe there is a different consideration of the freedom of expression, especially when it is compared to other rights. Now, the Court of Justice declared that the freedom of expression shall be balanced with the right of an individual to be "forgotten." Who carries out this balance? On which basis? *(Huge Conflict of Interest, due to a lack of public informatic structure).*

Article 17 – GDPR (2018) *(Ultimate decisions in Europe, still active nowadays).*

Lesson 14 – The European Right to Digital Privacy: The Schrems Case.

Art. 25, Directive 95/46/EC
(What happens when data is transferred to a country which is not member of the European Union, in order to regulate these differences, the EU Directive introduced some mechanisms allowing the transfer of the Data, the most important option is to rely on the Adequacy decision, a decision approved by the European Commission, by which the competent body afford adequate level of protection, which vary on the nature of the data. The Directive introduced some criterion to evaluate the adequacy of the level of protection).

- The transfer to **a third country** of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures **an adequate level of protection**. *(Adequacy-decision is the more general).*
- The adequacy of the level of protection afforded by a third country shall be **assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations**; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
- The Commission may find that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into…for the protection of the private lives and basic freedoms and rights of individuals.

(In the U.S. there is no federal legislation regarding data-trasnfer, there was only a registry in which companies transferring data had to self-certificate the conditions they were using. In 2000 EU needed something more specific than Directive of 95, due to a huge increase of data transportation. The EU Commission adopted the "Safe Harbour" decision, which was a validation of the self-certification mechanism in use in the U.S.)

Safe Harbour
2000/520/EC: Commission Decision on the adequacy of the protection provided by the safe harbor privacy principles.
Safe Harbour: mechanism of self-certification.
Intended for U.S. organizations that process personal data collected in the EU, the Safe Harbor Principles are designed to assist eligible organizations to comply with the EU Data Protection Directive and maintain the privacy and integrity of that data. U.S. companies can opt into the program (I.e. self-certify) as long as they adhere to the 7 principles and 15 frequently asked questions.

(The growing complexity of digital companies in 15 years, made the self-certification method obsolete.
During NSA scandal, a student questioned the security of personal data transferred to the U.S. according to the "Safe Harbour". Data Protection authority said that the mechanism was enough but, the High Court of Ireland started doubting too, therefore it asked to clarification to the Court of Justice and the invalidation of the mechanism on the basis of a violation of Art. 7 and 8 of the Charter, the decision and reasoning of the Court of Justice follows…)

Schrems Case (2015)
Schrems asked the DPC to prohibit Facebook Ireland from transferring his personal data to the US. He contended that the law and practice in force in the US did not ensure adequate protection of the personal data against the surveillance activities that were engaged in there by the public authorities. The DPC rejected the complaint. The High Court held that the mass and undifferentiated accessing of personal data is contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution.
However, the case concerns the implementation of EU law as referred to in Article 51 of the Charter and that the legality of the decision at issue in the main proceedings must therefore be assessed in the light of EU law. According to the High Court, Decision 2000/520 does not satisfy the requirements flowing both from Articles 7 and 8 of the Charter.

Advocate General Bot
"Article 28 of Directive 95/46/EC, read in light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that **the existence of a decision adopted by the European Commission on the basis of Article 25(6) does not have the effect of preventing a national supervisory authority from investigating a complaint alleging that a third country does not ensure an adequate level of protection of the personal data transferred** and, where appropriate, from suspending the transfer of that data".
"Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the Department of Commerce of the United States of America is **invalid**".

Court of Justice

“Until the Commission decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, admittedly cannot adopt measures contrary to that decision.
Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.
However, a Commission decision adopted pursuant to Article 25(6) of Directive 95/46, such as Decision 2000/520, **cannot prevent persons whose personal data have been or could be transferred to a third country from lodging with the national supervisory authorities a claim** concerning the protection of their rights and freedoms in regard to the processing of that data.
A decision of that nature **cannot eliminate or reduce** the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of the directive”.

“Neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an **adequate level of protection**. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country ‘**shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations**’ and lists, **on a non-exhaustive basis**, the circumstances to which consideration must be given carrying out such an assessment”

(No binding definition of “adequate”, is a flexible definition on purpose. The general purpose of Directive is to ensure a high level of protection of data. Then the Court starts making some reasonings regarding the level of protection of data abroad, and agree on the fact that data cannot be protected as in Europe, but can be meant as requiring an essentially equivalent level of protection)(Adequacy doesn’t mean identity, but an essentially equal level of protection, therefore there is a sort of manipulation and interpretation of the word adequacy from the Court).

“Article 25(6) of Directive 95/46 **implements** the express obligation laid down in Article 8(1) of the Charter to protect personal data and is intended to ensure that the high level of that protection continues where personal data is transferred to a third country …
The word ‘adequate’ in Article 25(6) of Directive 95/46 admittedly signifies that a third country **cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order**. However, as the Advocate General has observed in point 141 of his Opinion, the term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is **essentially equivalent to that guaranteed within the European Union** by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded”.

(Even if the legal norms applicable in the third country are different from EU, those norms must prove, in practice an essentially equivalent level of protection to that guaranteed within the European Union).

“Even though the means to which the third country has recourse for the purpose of ensuring a level of protection may differ from those employed within the European Union those means must nevertheless prove, in practice, effective in order to ensure protection **essentially equivalent** to that guaranteed within the European Union.
Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision **to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third**

country is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard".

(Since the technology is changing, the Court said that there must be a regular check from the European Commission whether the finding relating to the adequacy of the level of protection ensured by the third country is still factually and legally justified. On both sides, if EU Law changes either third countries' law changes).

"Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' **have primacy over the safe harbour principles**, primacy pursuant to which self-certified US organisations receiving personal data from the EU **are bound to disregard those principles without limitation where they conflict with those requirements** and therefore prove incompatible with them.
In addition, it does not contain any finding regarding the existence, in the US, of **rules intended to limit any interference with the fundamental rights of the persons whose data is transferred from the EU**, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security. Nor does Decision 2000/520 refer to the existence of **effective legal protection against interference** of that kind".

(The EU Court wanted the data to be safe also from the government's interference).

"Legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as **compromising the essence** of the fundamental right to respect for private life, as guaranteed by **Article 7** of the Charter. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, **does not respect the essence** of the fundamental right to effective judicial protection, as enshrined in **Article 47** of the Charter".

Therefore Decision 2000/520 is invalid. (October 2015)
(What happened the day after?)
Transfer of Personal Data to Third Countries

- **Adequacy Decision ->** No longer working if transferring data from EU to U.S.

The following are alternatives

- **Binding Corporate Rules** are rules that can be equalized internal policies adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. *(They require a long time to be approved and enter in function).* Furthermore, no transfer can be made on this basis outside the group.
- **Standard Contractual Clauses** are set of clauses (approved by the EU Commission) that can be adopted in the agreements between different subjects, however they are quite rigid.
- **Data Subject Consent**

The aftermath of the Schrems Judgment
The **Judicial Redress Act** affords persons whose data are shared by EU and other countries with US law enforcement agencies for the purpose of investigating, detecting, or prosecuting criminal offenses - including citizens of EU Member States – access to civil remedies for certain violations of those protections, and access to court proceedings in which those remedies can be pursued.

Privacy Shield
In 2016, the **Privacy Shield** substituted the Safe Harbour mechanism. "While the US and the EU share the goal of enhancing privacy protection, the US takes a different approach to privacy from that taken by the EU. The US uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. **Given those differences and to provide organizations in the US with a reliable mechanism for personal data transfers to the US from the EU while ensuring that EU data subjects continue to benefit from effective safeguards and protection** as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries, the Department of Commerce is issuing these Privacy Shield Principles".

Lesson 15 – The General Data Protection Regulation: general principles.

EU GDPR – Timeline
- January 2012, Commission Proposals
- March 2014, EU Parliament, First Reading
- June 2015, Council released its general approach
- December 2015, EU General Data Protection Regulation was agreed
- 2018 General Data Protection Regulation came into force.

An Overview
- Directly applicable in all the Member States
- Replaces the 1955 Data Protection Directive
- Replaces, to the relevant extent, the national laws transposing the 1995 Directive
- National laws applied until 25 May 2018; later, kept in force only in the provisions not covered nor replaced by the GDPR.

From a Directive to a Regulation?
- From Harmonization there was a shift to uniformity.
- **Broad margins of maneuver for Member States**.
  (There are some specific areas of GDPR where States have margin to adopt some more specific provisions.) **Lawfulness of processing – Article 6(2) GDPR**
  Member States may ***maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e)*** [see below] *by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations.*
  (c) processing is **necessary for compliance with a legal obligation** to which the controller is subject;
  (e) processing is **necessary for the performance of a task carried out in the public interest or in the exercise of official authority** vested in the controller;
- **Conditions applicable to child's consent in relation to information society services** (Art. 8 GDPR).
  Member States may provide by law for a lower age for those purposes (16) provided that such lower age is not below 13 years. *(Member States can lower the age of 16, but they can't go under 13).*
- **Processing of special categories of personal data** (Art. 9(2)(g) GDPR).
  Processing of ***personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership****, and the processing of* ***genetic 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 shall be prohibited.
Paragraph 1 shall not apply if one of the following applies: processing is necessary for ***reasons of substantial public interest****, on the basis of Union or* ***Member State law*** *which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*

Scope of Application

- **Material Scope (Art. 2 GDPR)**
  - The GDPR applies to the **processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system**.
  - There are some exceptions, from which the most important: *by a natural person in the course of a purely personal or household activity*. *(The GDPR doesn't cover a situation like the citated).*
- **Territorial Scope (Art. 3 GDPR)**
  The GDPR applies:
  - **to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not [*Google Spain*].**
  - to the processing of data of data subjects located in the EU by a controller or processor not established in the EU, where the processing activities are related to:
    - **the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or**
    - **the monitoring of their behaviour as far as their behaviour takes place within the Union.**
  - by a controller not established in the Union, but in a place where Member States' national law **applies by virtue of public international law.**

Personal and Non-Personal Data
Personal Data: any information relating to an **identified or identifiable natural person** (**Data Subject**).
Processing of Personal Data: any operation performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, … .
The principles of data protection should apply to **any information concerning an identified or identifiable natural person**. *(The GDPR is applicable not only to information directly related to an identified person, but also to information that makes the person identifiable, such as IP Address).*
Personal data which have undergone **pseudonymisation**, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.
To determine whether a natural person is identifiable, **account should be taken of all the means reasonably likely to be used** either by the controller or by another person to identify the natural person directly or indirectly.
To ascertain whether means are reasonably likely to be used to identify the natural person, **account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments**.

Pseudonymisation
(Even with pseudonymization the GDPR is still applicable)

- '**Pseudonymisation**' means the processing of personal data in such a manner that the personal data **can no longer be attributed to a specific data subject without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- WP29: Pseudonymisation consists of replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymisation when used alone will not result in an anonymous dataset.

Anonymization
(GDPR is not applicable)

- The principles of data protection should therefore not apply to **anonymous** information, namely information **which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.**
- The GDPR does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Controller: the natural or legal person, public authority, agency or any other body which determines the **purposes and means** of the processing of personal data.
Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. *(Processor is not acting by himself, but he is following the decisions of the controllers).*

Principles

- **Lawfulness, fairness and transparency**
- **Purpose limitation** *(limit to those necessary to the purposes).*
- **Data minimization** *(limit to those necessary to the purposes).*
- **Accuracy** *(Accurate data, up to date).*
- **Storage limitation** *(data to be kept permitting identification of data subject no longer that the time needed for the purpose agreed).*
- **Integrity and confidentiality**
- **Accountability** *(Data Controller should be accountable and responsible, being able to show that treated data in compliance with the GDPR principles).*

Lawfulness of Processing
Main legal basis to process personal data is the **Consent**, which consists of:

- Freely given
- Specific and Informed
- Unambiguous
- Revocable
- Provable

Consent is not required when the processing is necessary to:

- The **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Comply with a **legal obligation** to which the controller is subject.
- The **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

- **Protect the vital interests of the data subject** or of another natural person.
- For the purposes of the **legitimate interests pursued by the controller** or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Lesson 16 – The General Data Protection Regulation: Rights and Obligations.
(Risk base approach, depending on the entity processing data (Hospitals, social networks, small online shops, the control has to be different according to the quantity and risk assessed).
Processing of Personal Data

- **Data Subject - Rights**
  - **Right of Access**
  - Right to be Informed
  - Right to Rectification
  - Right to Erasure
  - Right to Restrict the Processing
  - Right to Object
  - **Right to Data Protability**
  - **Right to not be subject to automated decision-making**

- **Data Controller/Processor – Obligations**
  - Data Breach Notification
  - DPO
  - Record of Processing Activities
  - **Data Breach Communication**
  - **DPIA**
  - **Prior Consultation**

Right to Access

- The data subject has the **right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed**, and access to the personal data.
- The **controller shall provide a copy of the personal data** undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.
- Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the **information shall be provided in a commonly used electronic form**.
- **The right to obtain a copy of data shall not adversely affect the rights and freedoms of other parties.**
- The **Information to be provided:**
  - The **purposes of the processing**
  - The **categories of personal data** concerned
  - The **recipient to whom the personal data have been or will be disclosed**
  - Where possible, the envisaged **period for which the personal will be stored**, or, if not possible, the criteria used to determine that period
  - the existence of the **right to request from the controller rectification or erasure or restriction of processing** of personal data;
  - the **right to lodge a complaint with a supervisory authority**;
  - where the personal data are not collected from the data subject, any available information as to their source;

- the **existence of automated decision-making, including profiling**, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right to Rectification (and Integration)

- The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her.
- Taking into account the purposes of processing, the data subject shall have the right to **have incomplete personal data completed**, including by means of providing a supplementary statement.

Right to Erasure

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**.

- According to specific grounds (consent withdrawal, objection, unlawful processing)
- Provided that it is not excluded in some cases (freedom of expression, legal obligation, public interest) *(There might be circumstances where the erasure is not possible, because there are reasons like protection freedom of expression).*

Right to Restriction of Processing

(You're not interested in the erasure of information, but you are asking for a restriction of information)

The data subject shall have the right to obtain from the controller **restriction of processing** where:

- The **accuracy of the personal data is contested** by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- The **processing is unlawful and the data subject opposes the erasure** of the personal data and requests the restriction of their use instead
- The **controller no longer needs the personal data** for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- The **data subject has objected to processing pending the verification whether the legitimate grounds** of the controller override those of the data subject.

But: with the exception of storage, personal data shall only be processed with the data subject's consent or **for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest**.

Right to Object

(Similar to the right to erasure, you object that there has never been the consent to process data).

The data subject shall have the **right to object**, on ground relating to his or her particular situation, at any time to the processing of personal data concerning him or her where processing is necessary for:

- The **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.
- The purposes of the **legitimate interests** pursued by the controller or by a third party.

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Right to Object, the case of direct marketing

Where personal data are processed for **direct marketing purposes**, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, **which includes profiling to the extent that it is related to such direct marketing.**

- **The personal data shall no longer be processed for such purposes**.

Right to Data Portability (Important)

The data subject shall have the **right to receive** the personal data concerning him or her, **in a structured, commonly used and machine-readable format** and have the **right to transmit** those **data from the controller to a new controller, without hindrance** *(Without suffering any negative effect/obstacle),* where:

- **The processing is based on a contract or consent**
- **The processing is automated**

The right to data portability shall not adversely affect the rights and freedoms of others.

Automated Individual Decision-Making, including Profiling

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.

The right does not apply where the processing:

- Is necessary **for entering into, or performance of, a contract** between the data subject and a data controller
- Is **authorized 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
- Is based on the **data subject's explicit consent**.

Risk-Based Approach

- The GDPR encourages controllers to engage in risk analysis and to adopt **risk-measured responses**. It imposes **additional obligations** for data processing activities that pose a **high risk** to individuals, while **requiring controllers to account for risk in complying** with many provisions of the GDPR.
- Controllers that engage in **low-risk** processing activities, or that **adequately address risk**, may avoid specific requirements (e.g. to notify a data protection authority of a data breach, to appoint a representative in the EU). The GDPR also requires the supervisory authorities to consider the risk level of the activity when deciding whether to impose fines for a violation.

Data Protection by Design and by Default – Art. 25 GDPR

Controllers must ensure that, both in the planning phase of processing activities and the implementation phase of any new product or service, data protection principles, and appropriate safeguards, are addressed and implemented.

- For example, the controller must implement measures that provide for the security of any data processed, and give effect to the rights of data subjects.

Compliance with data protection law should not be an after-thought, but should be treated as a key issue in the planning and implementation of any new product or service that affects personal data.

Security of Processing
Must be taken into account:

- The State of Art
- The Nature, Scope, Context and Purposes of Processing
- The Costs of Implementation
- The Risk of varying likelihood and severity for the rights and freedoms of natural persons

The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia:

- The pseudonymization and encryption of personal data

Processing with High Risk

Activities	Additional Obligations	Exemptions
• Systematic and extensive automated profiling • Large-scale processing of special categories of data • Large-scale, systematic monitoring of a publicly accessible area • Other activities that are "likely to result in a high risk for the rights and freedoms of individuals" • Member state law	Privacy impact assessments	Member state law exempts specific activities
	Prior consultation with DPA	Controller implements appropriate technical and organizational measures to mitigate the risk
	Notification of data breach to individuals	• Controller implements appropriate technical and organizational measures (e.g. encryption) • The high risk is no longer likely to materialize • Notifying affected individuals would involve disproportionate effort

Processing with Risk

Activities	Additional Obligations	Exemptions
Examples • Data subjects deprived of control • Processing sensitive data • Profiling • Vulnerable individuals • Large-scale processing Potential Harms • Discrimination • Identity theft or fraud • Financial loss • Damage to the reputation • Loss of confidentiality • Reversal of pseudonymization • Significant economic or social disadvantage	Notification of data breach to DPA	Data breach is "unlikely to result in a risk for the rights and freedoms of individuals"
	Foreign controllers appoint EU representative	Processing is occasional, does not include large-scale processing of sensitive data, *and* is "unlikely to result in a risk for the rights and freedoms of individuals."
	Data security: Controllers must implement (and choose processors that implement) "technical and organizational measures" appropriate to the risk of a data breach	Controller processes only "anonymous data" not subject to regulation
	Risk-based compliance with GDPR's "general obligations"	Controller processes only "anonymous data" not subject to regulation

- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful:

Data Breach

- Destruction
- Loss
- Alteration
- Unauthorised disclosure of/access to

Of personal data transmitted, stored or otherwise processed.

Data Breach Notification

In the case of a personal **data breach without undue delay** and, where feasible, not later **than 72 hours** after becoming aware of it the controller shall **notify** the personal data breach to the **competent supervisory authority.**

Unless the personal **data breach is unlikely to result in a risk** to the rights and freedoms of natural persons.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Data Breach Communication

In the case of a **personal data breach without undue delay** and, where feasible**, not later than 72 hours** after becoming aware of it the controller shall **notify** the personal data breach to the **competent supervisory authority and**, when the personal data **breach is likely to result in a high risk** to the rights and freedoms of natural persons. **The controller shall communicate the personal data breach to the data subject without undue delay.**

Records of Processing Activities

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller.

Exemptions from the obligation to keep record of processing activities

The obligation does not apply to an enterprise or an organization employing fewer than 250 persons, unless:

- The processing it carries out is likely to result in a risk to the rights and freedoms of data subjects
- The processing is not occasional
- The processing includes special categories of data or personal data relating to criminal convictions and offences.

DPIA (Data Protection Impact Assessment)

A DPIA is a process designed to:

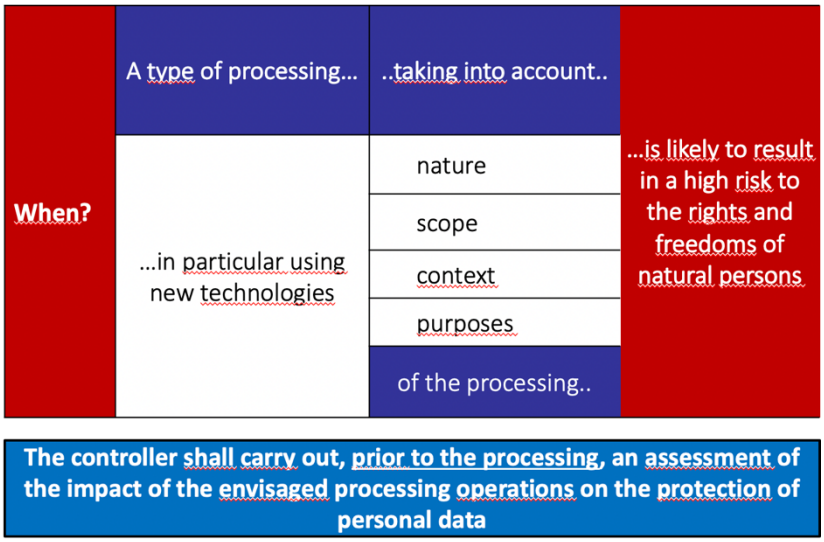
- Describe the processing
- Assess the necessity and proportionality of a processing
- Help manage the risks to the right and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).

DPIAs are important tools for **accountability**, as they help controllers to **comply with GDPR requirments** and to **demonstrate that appropriate measures have been taken to ensure compliance** (a process for building and demonstrating compliance).

(You conduct an assessment to define which is the risk, if you realize that the specific data processing has high risk, you have to ask to the supervisory authority consultation on the process of data processing).

Supervisory authorities shall establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA and of the kind of processing operations for which no DPIA is required.

Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority prior to processing.
If the supervisory authority finds that the intended processing would infringe the GDPR, in particular where the controller has insufficiently identified or mitigated the risk, it shall, **within up to eight weeks of receipt of the request for consultation** (extended by six weeks, taking into account the complexity of the intended processing), provide written advice to the controller and, where applicable, to the processor.
Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation. Member State may in any case require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.



Designation of the DPO (Data Protection Officer)
The controller and the processor shall designate a data protection officer in any case where:

- The processing is carried out by a **public authority or body**, except for courts acting in their judicial capacity.
- The **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring** of data subjects on a **large scale**.
- The core activities of the controller or the processor consist of processing **on a large scale** of **special categories of data** and personal data relating to **criminal convictions and offences**.

In cases other than those where the designation is mandatory, the controller or processor or associations and bodies representing categories of controllers and processors **may** or, when required by EU or national law, **shall** designate a DPO.
The DPO may act for such associations and other bodies representing controllers or processors.

Who is the DPO?

The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks provided by Article 39 GDPR.
The DPO may be a staff member of the controller or processor, or fulfill the tasks on the basis of a service contract.
The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

(Contact point between data controllers/processors and supervisory authorities)

Position of the DPO

- The controller and the processor shall ensure that the DPO is **involved, properly and in a timely manner**, in all issues which relate to the protection of personal data.
- The controller and processor shall support the DPO in performing the relevant tasks by **providing resources** necessary to carry out the same and **access to personal data and processing operations**, and to **maintain** his or her expert knowledge.
- The controller and processor shall ensure that the DPO **does not receive any instructions regarding the exercise of those tasks**. The DPO shall **not be dismissed or penalised** by the controller or the processor for performing his tasks. The DPO shall **directly report to the highest management level** of the controller or the processor.
- **Data subjects may contact** the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.
- The DPO shall be **bound by secrecy or confidentiality** concerning the performance of his or her tasks.
- The DPO may **fulfil other tasks and duties**. The controller or processor shall ensure that any such tasks and duties do not result in a **conflict of interests.**

Transfer of Personal Data to Third Countries
(Nothing changed from the Directive 95/46 to the GDPR)

- **Adequacy Decision**
- **Appropriate Safeguards**
    - **Standard Contractual Clauses**, the Commission has the power to decide that certain standard contractual clauses offer sufficient safeguards as required by the GDPR
    - **Binding Corporate Rules**, rules adopted by the competent supervisory authority as internal rules for data transfers within multinational companies. Binding corporate rules are like a code of conduct. They allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide an adequate level of protection.
- **Derogations for Specific Situations**, in the absence of an adequacy decision, or of appropriate safeguards, a transfer or a set of transfer of personal data to a third country or an international organization shall take place only on the specific conditions provided by Article 49 (e.g. Explicit consent of the Data Subject).

Penalties
"In order to strengthen the enforcement of the rules of this Regulation, penalties including **administrative fines** should be imposed for any infringement of this Regulation, **in addition to, or instead of appropriate measures** imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a **reprimand** may be issued instead of a fine".

"Member States should be able to lay down the rules on **criminal penalties** for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice".

Three possible "layers"

- **Criminal Penalties**
- **Administrative fines**
- **Appropriate measures, reprimand**

There exist two types of **administrative fines**:

- Administrative fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Lesson 17 – The e-Privacy Framework Cybersecurity: legal issues.

What is e-Privacy?

The exchange of information through public electronic communication services, such as the internet and mobile and landline telephony and via their accompanying networks, requires specific rules and safeguards to ensure the service and that network users' right to privacy and confidentiality are respected.

The e-Privacy Directive

The Electronic Privacy Directive (2002/58) was drafted specifically to address the **requirements of new digital technologies**, ease the **advance of electronic communications** services and **create favourable market conditions for the digital economy**. The subject of the directive is the «right to privacy in the electronic communications sector» and «free movement of data, communication equipment and services». It was designed to complement the data protection rules and other rules on telecoms.

Scope of application of the e-Privacy Directive

- Unlike the GDPR, the e-privacy Directive also protects the interests of legal persons.
- It applies to processing of personal data in connection with provision of publicly available electronic communications services in public communications networks.
- Does not apply to activities outside the scope of EU law, or concerning public security, defense and State security and the areas of the State in criminal law.

Note: e-privacy rules under the Directive only cover traditional telecoms providers; not other services such as Skype, WhatsApp, Facebook Messenger, Gmail, iMessage, Viber, etc.
There is a **convergence** due to the variety of usage of the new technologies, new services competing with the traditional operators, and the rules were crafted having in mind the traditional operators.

The e-Privacy Directive

The Directive sets out rules to:

- Ensure **security in the processing of personal data** (including the notice for data breaches).

- Ensure **confidentiality of communications**.
- Introducing safeguards in the **processing of traffic data**.
- **Ban unsolicited communications** where the user has not given consent.

Key Provisions of the e-Privacy Directive
Providers of electronic communication services must secure their services by at least:
- Ensuring personal data are accessed only by authorized persons;
- Protecting personal data from being destroyed, lost or accidentally altered and from other unlawful or unauthorized forms of processing;
- Ensuring the implementation of security policy on the processing of personal data.

The service provider must inform the national authority of any personal data breach within 24 hours. Individual users must also be informed if the personal data is likely to harm their privacy, unless specifically identified technological measures have been taken to protect the data.

EU Member States must ensure the **confidentiality of communications** made over public networks, in particular they must:
- **Prohibit the listening, tapping, storage or any type f surveillance or interception of communications and traffic data without the consent of users**, except where there is a legal authorization and in compliance with specific requirements;
- **Guarantee that the storing of information or the access to stored information on users' personal equipment is permitted only if the user has been clearly and fully informed**, *inter alia,* of the purpose of that access and has been given the right of refusal:
- When traffic data are no longer required for communication or billing, they must be erased or anonymized.
    - Service providers may process these data form marketing purposes for as long as the user gives his or her consent (consent may be withdrawn at any time).

Prior User Consent is required in a number of situations, including:
- To send unsolicited communications (SPAM). This also applies to short message services (SMSs) and other electronic messaging systems;
- To store information (Cookies) on users' computers or devices or to obtain access to that information.
    - The user must be given **clear and full information**, among others, on the purpose of the storage or access;
- For the appereance of telephone numbers, e-mail addresses or postal addresses in public directories.

EU Member States are required to have a system of penalties including legal sanctions for infringements of the Directive.

The scope of the rights and obligations can only be restricted by national legislative measures when such restrictions are necessary and proportionate to safeguard specific public interests, such as to allow **criminal investigations** or to **safeguard national security**, defense or public security.

Relationship with GDPR
GDPR gives effect to art. 8 of the EU Charter (right to data protection) v. e-Privacy Regulation gives effect to art. 7 of the Charter (right to privacy and respect of private life).
E-Privacy Regulation is intended to complement and enhance the GDPR rules.
E-Privacy constitutes *lex specialis* to GDPR. *(meaning that this is a law which regulates a specific domain, electronic communication service, while the GDPR is still applicable, however the privacy*

framework will contain some more specific rules to apply in these situations), (lex specialis derogate generali).

Recital 175: This regulation should apply to all matters […] which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC […] In order to clarify the relationship between this regulation and Directive 2002/58/EC, **that Directive should be amended accordingly. Once this regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this regulation.**

Art. 95: This regulation **shall not impose additional obligations** on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union **in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.**

Proposed e-Privacy Regulation: where are we?

- 10 Jan 2017, proposal for a regulation on the respect for private life and the protection of personal data in electronic communications.
- 19 Oct 2017, Adoption of the draft in EU Parliament
- 2018, Trilogue negotiations.
- 2019, Romanian Presidency did not adopt a Common Council Position.
- End of 2019, Finnsih Presidency + new EU Parliament: negotiations are likely to start and adopt "general approach".

Proposed e-Privacy Regulation: key provisions

- Set out to **replace the e-Privacy Directive** and **specify GDPR.**
- "New" providers are covered to ensure they guarantee the same level of confidentiality of communications as traditional telecoms operators → Over-the-Top communications services ("OTTs").
- The same rules and level of protection will directly apply across the EU (Regulation v. Directive).

Applies to communication content and metadata (e.g. time of a call, location), which have a high privacy component and must be anonymized or deleted if users did not give their consent, unless the data is needed for billing.

Main contentious issues:

- Location tracking.
- Browser and defaults settings.
- Tracking walls *(something that tracks usage of websites).*
- Confidentiality of communications.

Cookie Law

- Prior Consent
- Clear and Simple language
- Browser fingerprinting techniques should be subject to requirements.
- Cookies for purely analytical purposes should be exempted from the rule.
- New requirements for browsers: browsers must contain controls on cookies and users must choose these settings as part of the installation process.
- Settings must provide easy ways to allow or refuse cookies.

- Default settings for cookies are set in most current browsers to "accept all cookies" are not acceptable -> more intermediate solutions are needed (provide different degrees of acceptance, e.g., "refuse all", "reject third party cookies", "accept all").
- No consent is needed for no-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history) or cookies used by a website to count the number of visitors.

Rules guaranteeing privacy for content and metadata on electronic communications
- Prohibition to interfere with electronic communications (listen to, store, monitor, scan, etc.)
- Obligation to delete or anonymize content and metadata after the transmission
- Permitted uses:
    - Users' consent
    - Processing of the data is required for billing or security purposes.

Rules Protecting against SPAM
- Unsolicited electronic communications by emails, SMS and automated calling machines are banned.
- Direct marketing allowed where users give their consent.
- For voice-to-voice marketing calls, individuals may be protected "by default" or can be included in a "do-not-call" list → depends on national law implementation (*opt in/out*).
- Marketing callers will need to display their telephone number or use a special prefix.

Stronger and more effective enforcement
- Responsibility to monitor and enforce e-privacy rules is shifted to national data protection authorities.
- Competence to ensure the consistent application of the e-privacy regulation is awarded to the European Data Protection Board (i.e. GDPR body).

The European Electronic Communications Code
- Established by Directive (EU) 2018/1972
- Provides a set of rules to regulate electronic communications (telecoms) networks, telecoms services, and associated facilities and services;
- Sets out tasks for national regulatory authorities and establishes a set of procedures to ensure that the regulatory framework is harmonized throughout the EU;
- Aims to stimulate competition and increased investment in 5G and very high capacity networks, to achieve high quality connectivity, a high level of consumer protection and an increased choice of innovative digital services.

Focus: Cookies
Planet49 case: ECJ Judgment of 1 October 2019.
Case concerned the placing of cookies with the purpose of online tracking for behavioral advertising as a condition to access an online service (online lottery). The Directive has led to disparate approaches from national transposition laws and supervisory authorities.
- Pre-ticked boxes do not amount to valid consent.
- Expiration date of cookies and third-party sharing should be disclosed to users when obtaining consent.
- Different purposes should not be bundled under the same consent ask.
- In order for consent to be valid *"an active behaviour with a clear view"* ('intention') of consenting should be obtained.
- These rules apply to cookies regardless of whether the data accessed is personal or not.
- Still open question: what does "freely given" consent mean?

The Cybersecurity Framework
Cybersecurity ensures the security of network and information systems. It consists of the protection of internet-connected systems, including hardware, software and data, from different types of cyberattacks.

The challenges of cybersecurity
- Fundamental rights and freedoms
- Internet and Network Integrity
- Control by multiple entities
- Shared responsibility

EU's strategic priorities on cybersecurity
- Cyber Resilience
- Drastic reduction of cybercrime
- Develop cyber defense policy and capabilities
- Develop the industrial and technological resources for cyber security
- Establish a coherent international cyberspace policy.

Cyber Resilience
EU's approach:
- Economic logic, develop a secure information society for all.
- Security logic, protecting **critical infrastructure** against terrorist attacks.

Note: the e-Privacy and data protection frameworks provide relevant requirements to manage risks, security requirements, reporting obligations for security or data breaches.

Cyber Crime
Cybercrime is one of the fastest growing types of crime: it is high-profit and low-risk. Criminals often exploit anonymity of website domains. It can severely hamper the economy and national/regional plans of economic growth.

Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Cyber Defense Policy and Capabilities
Related to the Common Security and Defense Policy (CSDP).

EU Agency for Network and Information Security (ENISA)
- Established by EU regulations 460/2004 and 526/2013, repealed by the Cybersecurity Act.
- Provides practical advice for the public and private sector in EU countries and for the EU institutions, including:
  - Organizing cross-Europe cyber crisis exercises
  - Assist in the development of National Cyber Security Strategies.
  - Promoting cooperation between computer emergency response teams and capacity building.
- Supports drafting of EU policy and law on network and information security.

- Maintains a network of private and public stakeholders, works closely on joint research and communication activities, supports other EU Agencies

The NIS Directive
In this directive, the EU, for the first time, tried to create a cooperation among European countries in facing cybersecurity attacks and emergencies.
Key Definitions:

- **Cybersecurity**, the ability of network and information systems to resist action that compromises the availability, authenticity, integrity or confidentiality of digital data or the services those systems provide.
- **Network and Information System**, an electronic communications network, or any device or group of interconnected devices which process digital data, the digital data stored, processed, retrieved or transmitted.
- **Essential Services**, private or public entities with an important role for the society and economy, e.g. water supply, electricity services, etc.

Broad set of measures to boost the **level of security of network and information systems** to secure services vital to the EU economy and society.

Aims to ensure that EU Member States are well prepared and ready to handle and respond to cyberattacks through:

- The designation of competent authorities,
- The set-up of computer-security incident response teams (CSIRTs),
- The adoption of national cybersecurity strategies.

Establish EU-level cooperation at strategic and technical level.
Introduces the obligation on essential service providers and digital providers to take **appropriate security measures** and to **notify the relevant national authorities about serious incidents**.
Improve National Cybersecurity Capabilities
EU Member States must:

- **Designate 1+ national competent authorities** and CSIRT and identify a single point of contact *(The point of contact is the authority which will cooperate with the point of contact of other states in order to develop a strategy and advise other countries of a possible threat).*
- **Identify providers of essential services in critical sectors** and digital infrastructure where a cyberattack could disrupt an essential service.
- Put in place a **national cybersecurity strategy for network and information systems**, covering:
    - Preparedness to handle and respond to cyberattacks.
    - Roles, responsibilities, cooperation of governments and other parties.
    - Education, awareness-raising and training programs.
    - Research and development planning.
    - Plan to identify risks.

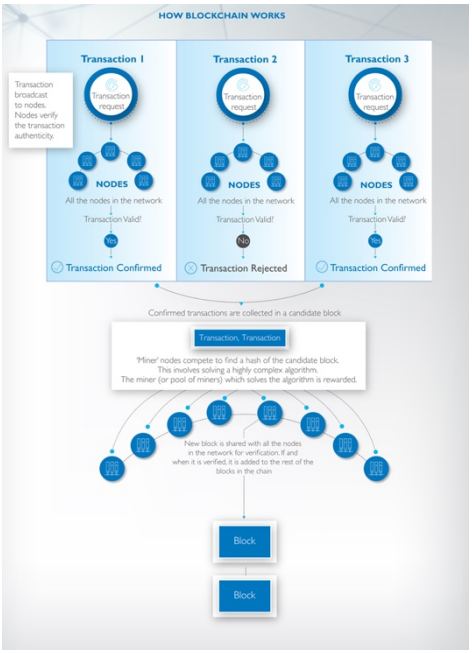
National competent authorities monitoring obligations

- **Assess the cybersecurity and security policies** of providers of essential services;
- **Supervise digital service providers**;
- Participate in the work of the cooperation group (formed by national NIS competent authorities + EU Commission + ENISA);
- **Inform the public where necessary to prevent an incident or to deal with an ongoing incident**, while respecting confidentiality;

- Issuing **binding instructions** to remedy cybersecurity deficiencies

Computer-security incident response teams (CSIRTs)
Responsibilities:

- Monitor and respond to cybersecurity incidents;
- Provide risk analysis and incident analysis and situational awareness;
- Participate in the CSIRTs network;
- Cooperate with the private sector;
- Promote the use of standardized practices for incident and risk-handling and information classification.



Security and Notification Requirements

- Promote a **culture of risk management** → businesses operating in key sectors must evaluate the risks they run and adopt relevant measures.
- These companies **must notify the competent authorities or CSIRTs of any relevant incident** (e.g. hacking, theft of data) that **seriously compromises cybersecurity** and has a **significant disruptive effect on the continuity of critical services and supply of goods.**
- Take into account an incident's duration and geographical spread and other factors (e.g. number of users).
- Key digital service providers will also have to comply with the security and notification requirements.

Improving EU-level Cooperation

- Cooperation group between national authorities
- CSIRT network comprising representatives of Member States' CSIRTS + Computer Emergency Response Team (CERT-EU)

Penalties

- EU Member States must apply effective, proportionate and dissuasive penalties to ensure that the terms of the NIS Directive are applied

The main question is that the Directive does not include public administration but rather only the private sector.

The Cybersecurity Act (2017)
It introduces a new approach mainly focused on the certification sector.
European cybersecurity certification framework:

- **EU certification framework for ICT digital products, services and processes** → comprehensive set of rules, technical requirements, standards and procedures.

Lesson 18 – Blockchain and AI - legal issues.

Blockchain and the law
What is blockchain?

- An append-only decentralized database
- Maintained by a consensus algorithm

- Stored on multiple nodes (computers)

It has the ability to decentralize business models, forms of human interaction and markets.
It can be used for record keeping, transferring value and smart contracts to automatically execute transactions: **#trust.**

The legal standpoint and disruptive technologies.
Two normative objectives: fundamental right protection vis-à-vis promotion of innovation.

Blockchain(s)

- On a blockchain, data is usually grouped into blocks that, upon reaching a certain size, are chained to the existing ledger through a hashing process.
- Data is thus chronologically ordered in a manner making it difficult to tamper with information without altering subsequent blocks.
- Hence, immutability of blockchains (at least it is very difficult): then, trust.
- However, it implies that the piece of information was included at some verifiable point in the past, not that the same is correct!
- DLTs (Distributed Ledger Technology) rely on a two-step verification process with asymmetric encryption.
- Every user has a public key (string of letters, username) and a private key (password): the private key can decrypt data that is encrypted through the public key. Public keys hide the identity of the individual unless they are linked to additional identifiers.

Nodes

- The nodes are the computers on which the ledger is stored.
- Some DLTs operate a distinction between "full" and "lightweight" nodes whereby only full nodes store an integral copy of the ledger from the genesis block whereas lightweight nodes only store those parts of the ledger of relevance to them.
- In **public and permissionless blockchains**, anyone can entertain a node by downloading and running the relevant software. Some (but not all!) nodes also function as "miners", which aggregate transactions into candidate blocks and hash a new block to the chain on the basis of a predetermined consensus protocol. *(Bitcoin for example).*
- Blockchains can also be **private and permissioned**, which means that they can run on a private network such as intranet or a VPN (as opposed to the internet) and an administrator needs to grant permission to individuals wanting to maintain a node. *(Notarchain for example).*

Blockchain(s)

- **Public and permissionless blockchain**: anyone can participate in the blockchain and become validator.
- **Public and permissioned blockchain**: everyone can participate in the chain as node and access data, but only some pre-authorized of the participants may act as miners and add data to the ledger.
- **Private and permissioned blockchain**: both validators and nodes that are merely participants have to be authorized by a set of actors (public and private governance).

GDPR vs Blockchains

- Blockchains offer a record-keeping function that dispenses from the need for third party intermediation *(middleman)* and by analogy can decentralize the collection, storage and processing of data. This stands in sharp contrast with the current data economy, characterized by economic centralization in the form of 'platform power'.

- Blockchains offer the promise of the decentralized handling of data and data sovereignty, a concept that focuses on giving individuals control over their personal data and allowing them to share such information only with trusted parties.
- GDPR shares the data sovereignty objective as it aims to give natural persons 'control over their own personal data'.
- For examples, the right to data portability *(right to receive the data regarding me, and to transfer them to another controller)* (Art. 20) enshrines this objective in allowing a data subject to receive data from a controller in order to give it to another controller.
- Blockchains do not, *per se*, provide any privacy guarantees so that for data sovereignty objectives to be achieved, they must be combined with additional mechanisms. Indeed, despite the technology's promises for data sovereignty, there are also perils for if the necessary safeguards are not implemented; blockchains can reveal any and all data stored on them.

Blockchain does not provide any privacy and guarantee regarding the data, therefore some measures have to be implemented.

- GDPR only applies to 'personal data', defined as 'any information relating to an identified or identifiable natural person' (the 'data subject').
- Where data is rendered **completely anonymous**, it no longer amounts to personal data and thus falls outside the scope of the legal framework.
- Where data is rendered **pseudonymous**, however, it continues to qualify as personal data as the indirect identification of a natural personal by an identifier remains possible.
- Two sets of data stored on blockchains can potentially be defined as personal data for the purposes of the GDPR: **transactional data stored in the blocks** as well as **public keys**.

Personal Data and Blockchain

- **Information stored on blocks** may be data related to an identified or identifiable natural person and therefore amount to personal data.
- Data can be stored on a blockchain in three alternative fashions: in plain text, in encrypted form, or by hashing it to the chain.
- Can these processes sufficiently anonymize personal data to allow it to evade the GDPR's scope of application? High threshold for anonymization: the processing must '*irreversibly prevent identification*'.
- Personal data stored on a blockchain in **plain text** clearly remains personal data for the purposes of the GDPR.
- According to the WP29, where data is **encrypted** it can still be accessed with the correct keys, meaning that it is not irreversibly anonymized (encrypted data can for example be connected to the data subject where transactions are effected for off-chain goods or where crypto-assets are converted into fiat currency).
- Encryption is considered a pseudonymization under the EU data protection regime given that the data subject can still be indirectly identified: so, it is not considered as an anonymization technique.
- Accordingly, transactional data that has been encrypted remains personal data for the purposes of the GDPR.
- The same applies (so far) to hashing.
- Transactional data can therefore be moved off chain to escape from the application of the GDPR
- **Public keys?** They are pseudonymous data (thus subject to the GDPR) and cannot be moved off chain as quintessential component of the technology.

(GDPR is still applicable on pseudo-anonymized data because even if the data is encrypted through hash, it isn't an irreversible process, there is still the possibility to go back to decrypted data). The only way to escape GDPR is to move data off chain.

Data Controller

- When it comes to **private blockchains**, it might still be possible to identify a central intermediary that can qualify as the data controller such as the systems operator that will be the addressee of the data subject's claims.
- For other DLTs, there is no central point of control as the network is operated by all nodes in a decentralized fashion.
- **Permissionless blockchains** are distributed and decentralized peer-to-peer networks that everyone can participate in to interact with unknown or untrusted counterparties. In such a setting either no node qualifies as the data controller in the absence of independent determination of the means and purposes of processing, or, more likely, every node qualifies as a data controller.
- Nodes are indeed not subject to external instructions, autonomously decide whether to join the chain, and pursue their own objectives.
- Determining that each node is a data controller raises considerable complications. The exact number, location and identity of nodes on a chain cannot be established without difficulty.
- Nodes are furthermore passive entities subject to the directions of software designed by developers. They (i) only see the encrypted or hashed version of the data; and (ii) are unable to make any changes thereto. Nodes are thus decentralized entities that cannot respond to the tasks the GDPR requires of centralized agents.
- The enforcement of obligations resting on nodes is thus burdened by significant difficulty.
- For the Bitcoin blockchain, there are currently approximately 11,000 nodes around the planet, of which about 1800 are in Germany and 800 in France.
- If one were to address each of these nodes, some of which may not be found in a single jurisdiction this would create two sets of problems.
    - **First**, a large amount of nodes would need to be contacted and compelled to comply, as opposed to a single controller in a data silo scenario.
    - **Second**, this may lead to forcing all nodes to stop running the blockchain software where GDPR rights cannot be achieved through alternative means.
- This would result in a situation where an entire blockchain would be taken down in one jurisdiction for noncompliance with a single data subject's rights, which may be considered disproportionate.
- It is moreover unclear how fines will be calculated where a data controller on an unpermissioned blockchain has failed to comply with data protection requirements given that Article 83 GDPR calculates them on the basis of annual worldwide turnover.
- French CNIL (Commission Nationale Informatique & Libertès): participants who have the right to write on the chain and who decide to send data for validation by the miners can be considered as data controllers. In fact, blockchain participants define the purposes and means of the processing. (**e.g., if a notary records his/her client's property deed on a blockchain, he/she is a data controller. If a bank enters its clients' data onto a blockchian as part of its client management processing, it is a data controller).**

Territorial Scope of Application

- Unpermissioned blockchains usually run on nodes located in various jurisdictions across the globe, leaving creators with no control over the geographic spread of the network. This makes DLTs inherently transnational in nature, triggering a range of jurisdictional issues.

- GDPR applies ‘to the processing of personal data in the context of the activities of an establishment of a controller or processor in the European Union, regardless of whether the processing takes place in the Union or not’.
- The GDPR’s broad territorial scope accordingly likely entails that its obligations bind many blockchain-based applications with only an indirect link to the EU.
- A further jurisdictional question relates to the application of European data protection requirements to the transfer of data to third countries.
- On permissionless ledgers we can presume that there is always an element of cross-border data processing: the data stored in blocks is hashed to the chain by a randomly selected miner that can be based anywhere. The ledger is subsequently updated on each node to reflect the addition of the new block.
- Transfer to third countries is possible under certain conditions (possibility of a data subject providing explicit consent for such a transfer, subject to being informed about possible risks). This could be easily implemented on a private blockchain where access is controlled and can be subjected to terms and conditions but it is not obvious how such consent could be acquired in respect of a permissionless chain.

Enforcement of the GDPR rights

- While from a legal perspective a data subject can invoke her rights vis-à-vis every single node, it is far from obvious how, from a technical perspective, nodes could implement related requests to correct, erase or restrict data.
- How a data subject can consent to the processing of his/her personal data on a blockchain indeed remains an as of yet unresolved question.
- **Data Minimization**
    - The GDPR mandates that personal data be ‘collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes’.
    - Conversely, once added to a blockchain, data will perpetually remain part of the chain, given that it is an append-only database that continuously expands. Distributed ledgers are by definition ever-growing creatures, which augment and accumulate further data with each additional block.
    - Integral copies of the chain are stored on each full node, quite the opposite of the data minimization spirit. Once data has been added to the chain, it can in principle no longer be amended or deleted, which makes it difficult not to say impossible to implement the minimization principle and storage limitation requirements.
- **Right to amendment/rectification**
    - The GDPR requires that personal data be accurate and up to date. Where this is not the case, ‘every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay’.
    - Two practical impasses:
        - A data subject cannot possibly identify any or all of a blockchain’s full nodes.
        - Second, even if the data subject succeeds in addressing a claim under the GDPR, nodes are simply unable to change any of the encrypted data stored in a block (immutability of ledgers).
    - Personal data can also be rectified ‘by means of providing a supplementary statement’.
    - Could the addition of new data to the chain of blocks, which rectifies data previously added (without however deleting the original entry), be considered to comply with the requirements set by the GDPR?

    - The GDPR also requires that the controller communicate any rectification or erasure of personal data to 'each recipient to whom the personal data have been disclosed'. This, can however be presumed to not apply to nodes as the same provision clarifies that controllers are dispensed from said obligation where 'this provides impossible or involves disproportionate effort'.
- **Right to access**
    - A data subject has the right to obtain confirmation from the controller whether or not her personal data is being processed. Data subjects are moreover entitled to be informed about safeguards that apply where data is transferred to third countries (relevant for blockchain, as a node validating a block in the EU will thereafter share that information with all nodes of the blockchain, irrespective of their geographical location).
    - Controllers don't know which data is stored on the blockchain as they often only handle the encrypted or hashed version thereof. Even if a data subject were successful in contacting a node, the latter would be incapable of verifying whether a data subject's personal data is being processed. The data subject could of course join an unpermissioned network and obtain a copy of all data, but it is questionable whether this would be regarded as a satisfactory solution in the eyes of the GDPR.
    - Article 15(3) GDPR moreover entitles data subjects to obtain a copy of their personal data undergoing processing from controllers, which would be equally impossible where its has been cryptographically pseudonymized.
    - Storing personal data off-chain is to be preferred for transactional data but remains unfeasible for public keys.
- **Right to be forgotten**
    - Immutability is one of blockchains' most heralded features. They are, by definition, unable to forget as they were specifically designed to be censorship-resistant. A straightforward application of the right to be forgotten to DLTs can be excluded.
    - However, the notion of 'deletion' may refer to a variety of options so that requests of erasure may be fullfilled in different manners.
    - It is worth distinguishing between transactional data and public keys.
    - Different solutions may apply to transactional data. Where personal data is recorded in a referenced encrypted and modifiable database as opposed to the blockchain itself, it can be deleted in line with data protection requirements without the need to touch the blockchain.
    - With regard to public keys compliance is again more burdensome. It must be recalled that the right to be forgotten is not an absolute right. Article 17(2) GDPR rather provides that the controller shall take 'account of available technology and the cost of implementation'. Could the reference to 'available technology' lead to an interpretation of the GDPR that dispenses from outright erasure in light of blockchains' technical limitations in favour of an alternative solution?

Blockchain and the GDPR

- Whereas the GDPR was fashioned for an age of centralized data silos, blockchains promise a future of decentralized data management.
- The new supranational data protection framework is already partly outdated in respect of its application to distributed ledgers for it simply cannot account for the technology's characterizing features.
- The same conclusion has been reached in respect of big data and artificial intelligence, indicating considerable challenges ahead.

- However, blockchains, if adequately designed, and the GDPR can share a common objective: giving a data subject more control over his/her data. This is of course only the case where blockchains are specifically fashioned to achieve that objective.

Artificial Intelligence

There are many issues related to AI and which are similar to the one relative to blockchain. Those are not only related to the GDPR even though the processing of personal data in artificial intelligence systems is a very debated issue. There are many opinions of this since the automated decision-making processing is something which is developing rapidly, and for this reason in Europe there is a specific provision preventing entirely automated decision systems to affect human rights. (art. 32 of the GDPR). Therefore, algorithms and AI might entail the processing of data and create some challenges. However, the most debate issue regard civil liabilities connected to the damages caused by the usage of AI systems. But there is not a provision giving specific rules.
Even if more and more machines will learn how to carry out different activities risks are always involved not only on the instruction received but also regarding the inputs that the machines receive. The challenge is to make sure that AI systems are working more like men rather than "animals"/resilient machines, they should develop skills and new functions.

The problems arise when the source of the input of the machine is not known or if the input is based on the experience of the AI machine.

Then, who is responsible of the harm in front of the law for an AI system?

- **The manufacturer** (the programmer): he is including some inputs but the harm might occurs not because of those inputs. Maybe from the inputs received during the activity
- **The user:** difficult to accuse a user
- **The insurance company**

It depends also which tradeoff between **human right protection and innovation** we want to follow:

- protection of human → strict rules and discouraging innovation
- soft rules → no incentives for the manufacturers to comply with very high standard

In general, there are **two possible options**:

- Attaching "electronic personality" to AI systems requiring the owner entering into insurance contract (like in the Ancient Rome for slaves, to whom a peculium was attached). Therefore the owner (which might not be the user) is liable. And he normally buys an insurance to cover the possible danger carried out by the AI system.
- Regulating "ex novo" liability of AI systems: creating new rules. The possible new rules are product liability.

Product liability might be based on

- Negligence: focusing on the conduct of the manufacturer; liability occurs in case of violation of a duty of care which actually caused a harm. You are seeking for an element in the conduct of the manufacturer which justices the fact that the cost of the harm is charged to him.
- Strict liability: strict liability claims focus on the product itself rather than on the conduct of the manufacturer; the manufacturer is liable if the product is defective, even if the manufacturer was not negligent in making that product defective.

Both options can be considered controversial. With the negligence option you are discouraging those who wants to use and implement AI systems since you are liable only if you violate a duty of care and you undermine the protection of the possible victims. In the other case you are providing the strongest protection to victims, so the manufacturer has no incentives to implement a AI system since he is always liable even if it is not his fault.

another problem: Machine Learning

It is not easy to allocate liabilities when you do not have something which is not executed as a result of an input given the manufacture. There is a divergence between the preconstructed behaviour and the behaviour experience, it can create harm.

The users should have the responsibility of making sure that the machine is learning in a proper way.

But there are also some liability regimes proposed by experts/commentators :

- Strict product liability (Directive 374/85/CEE)
- Tort liability (based on negligence/intention)
- Parental liability (objective liability since you are supposed to look after the action of the system)
- Liability for dangerous activities (burden of proof is reversed), or liability for animals
- Legal subjectivity (criminal law)

Those are all possible options, all with some pros and cons.

Lesson 19 – Digital Single Market and Online Platforms.

From Napster to Tech Giants
From an environment where providers were passive, to an active position.

As from the e-Commerce Directive to the Digital Single Market Strategy.
We are moving from a Directive centered principally on the economical aspect, to a fundamental rights dimension.

The Digital Single Market
This strategy was based in the need of ruling platforms.
There are 3 **pillars** of **Digital Single Market Strategy**:

- **Access**, better access for consumers and businesses to digital goods and services across Europe.
- **Environment**, creating the right conditions and a level playing field for digital networks and innovative services to flourish.
- **Economy & Society**, maximizing the growth potential of the digital economy.

The **DSM** is important because the digital environment is pervading our society.
It's not just an **economic reason**, the **role of fundamental rights** and the ECJ in shaping platforms responsibilities (e.g. Delfi case, Scarlet case). (shift of paradigm).

The Digital Single Market: the future of ISP in Europe
This 3 **documents** are not binding, are more intended to make clear the goals of DSM:

- Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe – COM 2016 (288).
    - A level playing field for comparable digital services.

- Responsible behavior of online platforms to protect core values.
- Transparency and fairness for maintaining user trust and safeguarding innovation.
- Open and Non-Discriminatory markets in a data-driven economy.

(*We need a new framework in which platforms are more responsible, protecting core values; to achieve this purpose they will follow a transparent and fair approach).*

- Commission Reccomendation of 1.3.2018 on measures to effectively tackle illegal content online – C(2018) 1177.
  - Submitting and processing notices.
  - Informing content providers and counter-notices.
  - Out-of-court dispute settlement.
  - Transparency.
  - Proactive measures.

- Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms - COM 2017 (555)

Internet Service Providers

- **The European Perspective (Art. 15 of E-Commerce Directive)**
  General rule: liability exception for ISPs as far as they act as **intermediaries** (service providers) and not as content providers.
  (Platforms take editorial decision on content that does not create but manages).

- **Hosting Providers (Art. 14)**
  - The service provided consists of the **permanent storage** of information (YouTube, Google Video, Facebook, …)
  - The host provider is not liable for the information stored on request of the content provider.
  - Liability exceptions do not apply if the author of the content is acting under the authority or the control of the *hosting* provider.

(We are not dealing with personal data processing (GDPR), but we are dealing with content, there are some intersections between the two of course).

Reforms of ISP Liability

The system of the e-Commerce Directive has not been repealed.

- Directive 2019/790 – **Copyright Directive** (Applied)
  A new role for online platforms? (or content sharing providers)
  - **Recital 61**, "*In recent years, the functioning of the online content market has gained in complexity. Online content-sharing services providing access to a large amount of copyright-protected content uploaded by their users have become a main source of access to content online. […] However, although they enable diversity and ease of access to content, they also generate challenges when copyright-protected content is uploaded without prior authorisation from rightholders. Legal uncertainty exists as to whether the providers of such services engage in copyright-relevant acts. […] That uncertainty affects the ability of rightholders to determine whether, and under which conditions, their works and other subject matter are used, as well as their ability to obtain appropriate remuneration for such use*." – Definition of Online Content Sharing Providers.

- **Recital 62**, *"Certain information society services, as part of their normal use, are designed to give access to the public to copyright-protected content or other subject matter uploaded by their users. […] The services covered by this Directive are services, the main or one of the main purposes of which is to store and enable users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit therefrom, either directly or indirectly, by organizing it and promoting it in order to attract a larger audience, including by categorizing it and using targeted promotion within it. Such services should not include services that have a main purpose other than that of enabling users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit from that activity."*

Use of protected content by online content-sharing service providers

- **Art. 17 (1)**, *"Member States shall provide that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users.*
  An online content-sharing service provider shall therefore ***obtain an authorisation from the rightholders*** *referred to in Article 3(1) and (2) of Directive 2001/29/EC, for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter."*

- **Art. 17 (3)**, "*When an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in this Directive,* ***the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article.***
  The first subparagraph of this paragraph shall not affect the possible application of Article 14(1) of Directive 2000/31/EC to those service providers for purposes falling outside the scope of this Directive".

- **Art. 17 (4)**, *"****If no authorisation is granted****, online content-sharing service providers shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter,* ***unless the service providers demonstrate that they have****:*
  - *Made best efforts to obtain an authorisations, and*
  - *Made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event*
  - *Acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b)."*

- **Art. 17 (5)**, *"In determining whether the service provider has complied with its obligations under paragraph 4, and* ***in light of the principle of proportionality****, the following elements, among others, shall be taken into account:*
  - *the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and*

- *the availability of suitable and effective means and their cost for service providers."*

*(The Directive here is taking into consideration the **Proportionality**).*

- **Art. 17 (6)**, *"Member States shall provide that, in respect of new online content-sharing service providers the services of which have been available to the public in the Union **for less than three years and which have an annual turnover below EUR 10 million**, calculated in accordance with Commission Recommendation 2003/361/EC, the conditions under the liability regime set out in paragraph 4 are limited to compliance with point (a) of paragraph 4 and to acting expeditiously, upon receiving a sufficiently substantiated notice, to disable access to the notified works or other subject matter or to remove those works or other subject matter from their websites. Where the average number of monthly unique visitors of such service providers **exceeds 5 million**, calculated on the basis of the previous calendar year, they shall also demonstrate that **they have made best efforts to prevent further uploads of the notified works** and other subject matter for which the rightsholders have provided relevant and necessary information."*

- Directive 2018/108 – **Audiovisual Media Service Directive** (Applied)
A new legal framework?
  - **Recital 1**, *"New types of content, such as video clips or user-generated content, have gained an increasing importance and new players, including providers of video-on-demand services and video-sharing platforms, are now well-established. This convergence of media requires an updated legal framework in order to reflect developments in the market and to achieve a balance between access to online content services, consumer protection and competitiveness."*

  - **Art. 1 (1) (aa)**, *"**Video-sharing platform service**" means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing."*

    (*A video sharing platform has not editorial responsibility, YouTube is mainly a video-sharing platform, while Netflix is a content provider and has editorial responsibility).*

  - **Applicable Provisions, Art. 28 (b) (1)**, ***Without prejudice to Articles 12 to 15 of Directive 2000/31/EC**, Member States shall ensure that video-sharing platform providers under their jurisdiction take **appropriate measures** to protect:*
    - *Minors from programmes […] which may **impair their physical, mental or moral development** in accordance with Article 6a(1);*
    - *The general public from programmes […]containing **incitement to violence or hatred directed against a group of persons** or a member of a group based on any of the grounds referred to in Article 21 of the Charter;*

- *The general public from programmes […] containing content the dissemination of which constitutes an **activity which is a criminal offence under Union law** (e.g. Article 5 of Directive (EU) 2017/541).*

- **Applicable Provisions, Art. 28 (b) (3)**, "*For the purposes of paragraphs 1 and 2, the appropriate measures shall be determined in light of the nature of the content in question, the harm it may cause, the **characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake, including those of the video-sharing platform providers and the users having created or uploaded the content as well as the general public interest**.*
  *Those measures shall be practicable and proportionate, taking into account **the size of the video-sharing platform service and the nature of the service that is provided**. Those measures **shall not lead to any ex-ante control measures or upload-filtering of content which do not comply with Article 15 of Directive 2000/31/EC.**"*

- **Regulation on Terrorism** (Proposal)
  - **Aim of the Regulation, Recital 1**, *"The Regulation aims at ensuring the smooth functioning of the digital single market in an open and democratic society, by tackling the misuse of hosting services for terrorist purposes and contributing to public security in European societies. The functioning of the digital single market should be improved by reinforcing legal certainty for hosting service providers, reinforcing users' trust in the online environment, and by strengthening safeguards to the freedom of expression, the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media".*

  - **Scope of Regulation, Art. 2**, *"The Regulation shall apply to hosting service providers offering services in the Union to the public, **irrespective of their place of main establishment.** This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles as referred to in **Article 6** of the Treaty on the European Union, and **shall apply without prejudice to fundamental principles in Union and national law relating to freedom of speech, freedom of the press and the freedom and pluralism of the media.***
    ***This Regulation is without prejudice to Directive 2000/31/EC. (Important)**"*

    (The directive still applies, but we still consider also Directive 2000/31/EC, that is e-Commerce Directive still applies).

  - **Hosting Providers and Terrorist Content,**
    - **Art. 3**, *Hosting service providers **shall act i**n accordance with this Regulation to protect users from terrorist content. They shall do so in **a diligent, proportionate and non-discriminatory manner**, and with due regard in all circumstances to the fundamental rights of the users and **take into account the fundamental importance of the freedom of expression, the freedom to receive and impart information and ideas in an open and democratic society** and with a view to avoiding removal of content which is not terrorist. These duties of care **shall not amount to a general obligation on hosting service providers to monitor the information they transmit or store, nor to a general duty to actively seek facts or circumstances indicating illegal activity.** Where hosting service providers obtain knowledge*

or awareness of terrorist content on their services, they shall inform the competent authorities of such content and remove it expeditiously.

(This is a clear example of the shift from an economic based regulation, to a fundamental rights one, where the rights play a big role in the decision of content regulation).

- **Art. 4 (2)**, Hosting service providers shall remove terrorist content or disable access to **it as soon as possible and within one hour from receipt of the removal order**.
- **Art. 6**, Without prejudice to Directive (EU) 2018/1808 and Directive 2000/31/EC hosting service providers may take **specific measures to protect their services against the public dissemination of terrorist content.** The measures shall be effective, targeted and proportionate, paying particular attention to the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the right to freedom of expression and the freedom to receive and impart information and ideas in an open and democratic society.

- **Transparency Obligations**, **Art. 9**,
  - Where hosting service providers use automated tools in respect of content that they store, they shall provide effective and appropriate safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable access to content considered to be terrorist content, are accurate and well-founded.
  - Safeguards shall consist, in particular, of human oversight and verifications, of the appropriateness of the decision to remove or deny access to content, in particular with regard to the right to freedom of expression and freedom to receive and impart information and ideas in an open and democratic society.

- **Effective Remedy, Art. 10**,
  - Hosting service providers shall establish an effective and accessible mechanism allowing content providers whose content has been removed or access to it disabled as a result of specific measures pursuant to Article 6, to submit a complaint against the action of the hosting service provider requesting reinstatement of the content.
  - Hosting service providers shall promptly examine every complaint that they receive and reinstate the content without undue delay where the removal or disabling of access was unjustified. They shall inform the complainant about the outcome of the examination within two weeks of the receipt of the complaint with an explanation in cases where the hosting service provider decides not to reinstate the content. […]

- **Regulation on e-Evidence** (Proposal)
  - **Aim and Scope**
    This Regulation lays down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data.
    "Electronic evidence" means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data.

The Regulation also applies to information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council 44 for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers.

Lesson 20 – Privacy in the Age of COVID-19.

Two models to be compared

«In the vocabulary of the Chinese», says the philosopher Byung chul Han, «the term "private sphere" does not appear, which has facilitated the construction of a whole infrastructure for surveillance that is highly effective in containing an epidemic».

«Digitalization is a collective thrill beyond individualism. In Europe the systemic use of big data would be, as it happens in Asia, much efficient than to rise again borders and walls. But such systemic use is not possible for the legal regime of protection of fundamental rights in Europe».

Is there a real trade-off between using new technologies to contain the spread of Covid-19 and protecting human rights?

- Which remedies are we considering? *i.e*., what do we mean by 'contact tracing'?
  - **Enforcement measures?**
  - **Tracking measures?**

- How to design such technological solutions?

China: Massive Surveillance

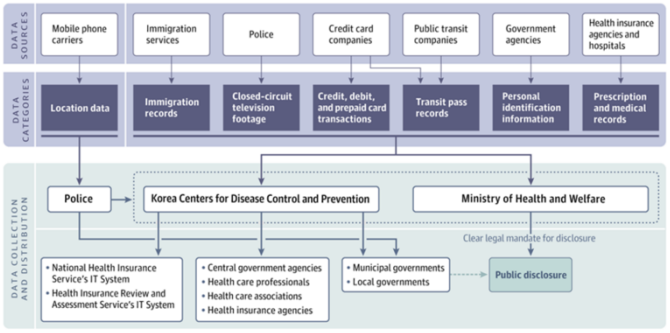
- Before people can do things like ride the subway or enter a crowded shopping mall, they have to prove they are at low risk of having Covid-19, by scanning a government-mandated QR "health code" on their cellphone that's either green (likely Covid-19 free), yellow (at risk of Covid-19), or red (likely Covid-19 positive); the code is based on information like a user's location and their medical and travel history, which is informed in part by a government questionnaire.
- Individuals generate these codes through a governmental tool named 'Health Code' in Alipay and WeChat, that nearly every citizen has installed on their phones and that they use to do everything from chatting to buying basic goods to hailing rides.
- Large resort to facial recognition techniques to control the activity of citizens. *(Not only to preventing the outbreak of the virus, but also to improve a gradually lifting of the lockdown).*
- In mid-February, local governments began lifting strict lockdown orders and private companies began rolling out app add-ons that help the government determine who can start safely leaving their house again without infecting others.
- General monitoring is made possible because of the use of app such as Alipay and WeChat in conjunction with other techniques (surveillance in public places, smart cities data..).

(China imposed the more restrictive measures, which proved to be among the more effective).

South Korea: COVID-19 Smart Management System (SMS)

(South Korea was almost ready and had an already organized system to deal with the pandemic, in addition to the fact, that Korea, is the "most connected" country in the world, which allowed the government to strictly control the citizens.)

Figure. Coronavirus Disease 2019 Contact Tracing in Korea: Sources, Categories, Collection, and Distribution of Data



South Korea: Corona 100

- South Korea's Centers for Disease Control and Prevention (KCDC) runs the contact tracing system that collects data from 28 organizations (the Police Agency, the Credit Finance Association, three smartphone companies, and 22 credit card companies)
- This system takes 10 minutes to analyze the movement of the infected individuals:
  - For people who come in contact with an infected person, the KCDC informs the local public health center near the infected citizen's residence and the health center sends the notification to them.
  - If they test positive, they are hospitalized at the COVID-19 special facilities. Those without symptoms are asked to remain self-quarantined for 14 days.
- Only epidemic investigators at KCDC can access the location information and once the COVID-19 outbreak is over, the personal information used for the contact tracing will be canceled.

Singapore

- **Enforcement Measures**

- **TraceTogether**
  "Instead of attempting to tackle the issue of contact tracing by answering the question of 'where,' we address contact tracing by answering the question of 'who', […] the virus doesn't care where transmission happens; it's only interested in whether there is a hospitable host in close contact" (Jason Bay, Senior Director of Government Digital Services at GovTech).
  - On a voluntary basis
  - Using Bluetooth
  - Data regarding interactions are stored locally, subject to encryption and then sent to the Ministry of Health in case the user is infected.

Israel: HaMagen (The Shield)

- Downloaded on a voluntary basis (by 1.5. milion Israelis) it alerts users who have crossed paths with a coronavirus patient.
- Users' personal and location data remain on their phones and are not available to others
- Possibility for users to cancel data.
- It allows users to decide whether to report their exposure to the coronavirus to the Ministry of Health.
- Open source.
- Limited duration (April 30).
- Problem: which legal basis for the tracking tool?
- First, emergency legislation (no legal scrutiny).
- Then, order of the Government based on emergency legislation and review by Knesset: order with limited duration, expired on April 30.
- Supreme Court: emergency legislation does not constitute the proper legal ground, as contrast to Covid-19 does not stand as a matter of national security.
- Parallely, Knesset had already suspended police use of cellphone data to enforce coronavirus quarantines adopted on the same legal basis.

Europe, EU law:

- **Art. 6 GDPR**
  Processing shall be lawful only if and to the extent that at least one of the following applies:
  - the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes […].
  - processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.
- **Art. 9 GDPR**
  Regulates the processing of particular categories of personal data (e.g., data concerning health): «personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic 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 **shall be prohibited»**.
  Paragraph 1 shall not apply if one of the following applies: […] processing is necessary for re**asons of public interest in the area of public health, such as protecting against serious cross-border threats to health** or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, **on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject.**

The Debate on Contact Tracing in Europe
What do we mean by contact tracing? A variety of options:

- Use of statistical data generated on anonymous basis to measure the degree of crowdedness of public places (e.g. Municipality of Milan / Lombardy region): use of mobile phone towers.
- Use of traffic and location data to monitor compliance with stay-at-home orders/obligations (e.g. for those tested positive to Covid-19).
- **Tracing and alerting contacts which crossed the path of patients tested positive within a given timeframe (e.g. 14 days) with a significant risk exposure (via BT or GPS signals)**. *(In Italy only the Bluetooth will be used).*

The **Italian way** (modeled on the Singaporean and Israeli paradigms):

- **Alerting contacts which crossed the path of patients tested positive within a given timeframe with a significant risk exposure (via Bluetooth signals)**.
- Tracing may therefore sound inaccurate, as no monitoring activity is implied.

EDPB (European Data Protection Board) guidelines

- **Voluntary Adoption.**
  The systematic and large-scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy.
  It can only be legitimized by relying on a **voluntary adoption** by the users for each of the respective purposes. This would imply, in particular, that **individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all**.

- **Public Nature**
  To ensure accountability, the controller of any contact tracing application should be clearly defined. The EDPB considers that the **national health authorities could be the controllers for such application**; other controllers may also be envisaged.
  In any cases, if the deployment of contact tracing apps involves different actors their **roles and responsibilities must be clearly established from the outset** and be **explained to the users**.

- **Purpose Limitation**
  In addition, with regard to the principle of purpose limitation, the purposes **must be specific enough to exclude further processing for purposes unrelated to the management of the COVID- 19 health crisis** (e.g., commercial or law enforcement purposes).
  Once the objective has been clearly defined, it will be necessary to ensure that the use of personal data is **adequate, necessary and proportionate**.

- **Principles**
  In the context of a contact tracing application, careful consideration should be given to the **principle of data minimisation and data protection by design and by default**:
  - Contact tracing apps do not require tracking the location of individual users. Instead, **proximity data should be used**;
  - As contact tracing applications can function without direct identification of individuals, **appropriate measures should be put in place to prevent re-identification**;
  - The collected information should **reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.**

- **Legal Basis**
  Furthermore […] the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears **that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest**, i.e. Art. 6(1)(e) GDPR.
  The basis for the processing referred to in article 6(1)(e) shall be laid down by Union or Members State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- **Safeguards**
  The legal basis or legislative measure that provides the lawful basis for the use of contact tracing applications should, however, incorporate meaningful safeguards including a reference to the voluntary nature of the application. A **clear specification of purpose** and **explicit limitations concerning the further use** of personal data should be included, as well as a **clear identification of the controller(s)** involved.
  The **categories of data** as well as the entities to (and purposes for) which, the personal data may be disclosed should also be identified. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing.
  Finally, the EDPB also recommends including, as soon as practicable, the **criteria to determine when the application shall be dismantled,** and which entity shall be responsible and accountable for making that determination.

The Italian Way: Immuni
- Voluntary Basis
- No prejudice affecting those who do not download the app
- Anonymous / Pseudonymous ID
- Alerting rather than tracking
- Controller: Ministry of Health
- Predominantly decentralized model
- Open-source app: "verifiable" code/functioning
- Adequate information notice prior to the download
- Data minimization: personal data collected are only those necessary for alerting users
- Anonymization, if possible; in any case, pseudonymization
- No user geolocalization (LE BT only)
- Automatic deletion of data at the end of the emergency.

Lesson 21 – The Right to Internet Access.
Do digital rights exist?
- *First layer: freedom of technical access to the internet*
- *Second layer: freedom on the internet itself.*

The … right to Internet Access?
- Neither the relevant provisions nor courts' decisions clarify whether the right to Internet Access does amount to a human or constitutional right.
- Difference between freedom to Internet access and freedom on the Internet.

Is the right to Internet Access an autonomous right?
- Right to Internet Access as an autonomous right?
  - Constitutional rank
  - Primary Law rank

(As a constitutional rank it's very difficult to restrict, while being a primary law, gives less guarantees, because another law could reduce its validity).

- Right to Internet Access as a medium for the enjoyment of other constitutional rights?
  - **Freedom of Expression** *(It exist, and can be restricted by the State in some cases, however it's not perceived as a positive obligation, which means that the State has not to provide you what's needed to have freedom of speech).*

- **Education** *(social-Welfare right, perceived as a positive obligation by the State, therefore bounding the right to Internet Access to the Education means that the State has to provide what's needed).*

(There is a tendency of connecting the Right to Internet Access to the freedom of expression, and the step forward that the European framework has made is not only to consider the means to access internet, but also the quality to enjoy the Internet (such as speed of the connection)).

Problems Connected to Internet Access

- Digital Divide
  - Italian Constitutional Court, No. 307/2004
  - Internet Access as a social right?
  - Internet Access as a medium to meet essential service levels

- Guaranteeing Internet Access requires investments in infrastructures
  - Governance of the network.

Does the Internet need a Bill of Rights?

Internet Governance Forum (IGF) purpose is to support the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new forum for multi-stakeholder policy dialogue. (http://www.intgovforum.org)

A Way to Reconcile Natural Freedoms and Regulatory Needs?

- 2007: Rio Conference – **Internet Bill of Rights**
- 2009: **Internet Rights & Principles Coalition**

An Internet Bill of Rights

- Italy: First European country to introduce an Internet Bill of Rights
- IGF (Internet Governance Forum) Italy. October 12, 2014
- http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf
- Pros and Cons of the Italian Way

UN Report – 2011

- F. La Rue (UN Special Rapporteur), *Report on the promotion and protection of the right to freedom of opinion and expression*.
- Internet access as a medium for users to exercise their freedom of expression and information.
- Is Internet access itself a fundamental right?

(There is a big difference between looking at the Right to Internet Access as a Human Right or as a Fundamental Right, because when dealing with it as a fundamental right, we have to take into consideration the specific constitutions of the States which will of course behave differently).

Internet Access: A Fundamental Right?

- "States should adopt effective and concrete policies and strategies … to make the Internet widely available, accessible and affordable to all".
- Despite these provisions, the Report does not expressly qualify Internet Access as a human right per se. Rather, it stresses the idea that Internet Access allows citizens to enjoy other human rights via the Internet.
- Different approaches among states to eliminate the "digital divide".

Internet and Constitutional Provisions

Only few (recent) Constitutions have specific provisions concerning the Internet and/or the freedom on the Internet and/or the free access to the Web.

- **Greece**, art. 5A, introduced in 2001
- **Honduras**, art. 182, introduced in 2003 – *habeas data*
- **Venezuela**, art. 28, introduced in 1999
- **Ecuador**, art. 16, introduced in 2008.

Estonia,

- Article 5 of Telecommunications Act (2000)
  Internet must be universally available to all registered users, regardless of their localization, at a uniform cost.
  - Internet Access is conceived as "universal right"
  - No discrimination based on territory
  - No price-discrimination
  - Requires private operators (ISP) to guarantee Internet access to all citizens

- ***UNIVERSAL SERVICE*** doctrine (access to a reasonable quality)

Finland

- **Finland, Article 60 of Communications Market Act (2009):**
  - Providers must guarantee users an appropriate Internet connection (broadband) at their domicile at reasonable costs and without any discrimination based on users localisation.
  - The Finnish Communications Regulatory Authority (FICORA) is tasked with verifying the costs applied by providers.

Spain

- **Spain, Article 52 of Law No. 2 of 2011**:
  Internet access is part of the telecommunications universal service and must be provided with a broadband at a downstream of at least 1 Mbit/second.
  Internet access must be guaranteed regardless of the specific devices or technologies (access is not limited to fixed infrastructures).
  It is for the Government to establish the conditions for accessing the public network and to modify the connection speed in accordance to the technological advancements.

US Supreme Court

- US Supreme Court, *Reno v. American Civil Liberties Union,* 26-6-1997
- The Supreme Court found that the Communications Decency Act (1996), by restricting the broadcasting of adult materials via the Internet, was against the First Amendment to US Constitution: "*Although the Government has an interest in protecting children from potentially harmful materials* […] *the CDA pursues that interest by suppressing a large amount of speech that adults have a constitutional right to send and receive*."

UK Courts

- **High Court of Justice – Court of Appeal, *The Queen v. Smith and Other,*** 19-7-2011
- "*A blanket prohibition on computer use or Internet access is impermissible. It is disproportionate because it restricts the defendant in the use of what is nowadays an essential part of everyday living for a large proportion of the public, as well as a requirement of much employment".*

- Restrictions on Internet connection must be **proportionate, reasonable** and in accordance with the **purposes** they are aimed to.

French Conseil Constitutionnel

- **Conseil Constitutionnel, *Hadopi*** (2009-580), 10-6-2009
- **HADOPI**: an administrative authority in charge of the control and sanctioning of copyright infringements via peer-to-peer networks. It had originally the power to disconnect users from the Internet in case of repeated breach of copyright.
- Freedom of Internet access and not right to Internet access.
- The Conseil did not qualify the Internet access as a fundamental right *per se,* but only as a condition for the enjoyment of the **freedom of communication** protected by Article 11 of the Declaration of the Rights of Man and of the Citizens (1789).

Costa Rica's Constitutional Court

- **Costa Rica - Sala Constitucional, 2010-12790**
- The advancements in technology have impacted on the way individuals communicate and develop social relationships.
- Therefore, nowadays access to technology qualifies as a basic instrument to enjoy fundamental rights such as democratic participation, freedom of expression, freedom of information.
- In particular, **Internet access amounts to a fundamental right**: reference is expressly made to the decision of the Conseil Constitutionnel which evoked Article 11 of the the Declaration of the Rights of Man and of the Citizens (1789).

Conclusions

- There are **no legal grounds at international level** to qualify Internet access as a fundamental right.
- Lack of **enforceability**: no judicial remedy.
- Is extending constitutional protection of other fundamental freedoms (arts. 15 and 21 of the Italian Constitution) enough?
- Internet Access as a social right, i.e. right to a positive action from a state for individuals to enjoy other fundamental rights.