Fundamentals of Information Technology Law

- **Legal Norms** and **Legal System**
  - Characteristics
    - Effectiveness
    - Force of Law
    - Generality
    - Abstractness
  - **Legal Norms** are produced by the legal system which have the power of producing binding effects on individuals subject to the system. Unlike other categories of norms, legal norms can be enforced by the State through the imposition of penalties.
  - **Legal System** is a strict relation between **Social Institution** ad the **Body of Legal Norms**, for example the **State**. The State is 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.
- **European Union Legal Order and Sources of Law**
  - **Fundamental Treaties**
    - **Treaties of Paris**
      - ECSC, European Coal and Steel Community
      - EURATOM, European Atomic Energy Community
    - **Treaty of Rome**
      - EEC, European Economic Community
    - **Schengen Agreement**
      - **Freedom of Circulation of Individuals**
    - **Treaty of Maastricht**
      - **Euro**
    - **Treaty of Lisbon**
      - **Charter of Fundamental Rights**
      - **Central Institutions**
        - **European Council**, composed by the **Head of State** or **Governments of the EU**
          - No legislative power, sets political agenda and objectives of EU.
        - **Council of the European Union**, composed by **one ministry of Member State's governments**
          - Legislative Power
        - **European Parliament**, composed by 705 members elected by EU citizens.
          - Legislative Power
        - **European Commission**, composed of 27 members one for each State.
          - Legislative Initiative and oversight the application of EU Law.
        - **Court of Justice of the European Union**, composed by 27 Justices and 11 advocate general.
          - Oversees the uniform application and interpretation of EU Law and resolves disputes.
  - **EU Legislative Acts**
    - **Binding Sources**
      - **EU Regulations**, complete set of rules applicable throughout the EU, not necessary to be transferred into State Law.
      - **EU Directives**, set a goal to be reach throughout the EU within a deadline.
      - **EU Decisions**
    - **Non-Binding Sources**
      - **EU Recommendations**
      - **EU Opinions**
  - **Council of Europe**
    - Intergovernmental Organisation devoted to promoting human rights, education and culture.
    - Fundamental Document **ECHR**, European Convention for the Protection of Human Rights and Fundamental Freedoms.
- **Italian Constitution and Source of Law**
  - **1946**, from **Monarchy** to **Republic**
  - From **Albertine Statute** to the **Constitution**
    - Codified (written)
    - Rigid
      - To change it requires a double vote of each chamber of the parliament.
    - Voted
    - Long
  - **Constitutional Organs**
    - **Parliament**
      - Chambers of Deputies
      - Senate
    - **President of the Republic**
    - **Government**
      - President of the Council
      - Council of Ministers
  - **Source of Law**
    - Constitutional Laws
    - Super-Primary Laws
    - Primary Laws (Law and Law Decrees)
    - Secondary Laws (Local Regulations)
  - **Conflicts of Laws**
    - At equal rank, the latest law is derogating the previous one.
    - The law with the highest rank prevale.
    - The special norm prevails.
- **Forms of State** and **Forms of Governments**
  - **Forms of State** is 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.
    - Feudal State
    - Absolute State
    - Liberal State
    - Totalitarian State
    - Democratic/Pluralistic State
  - **Forms of Government** is the set of rules concerning the distribution of power among the branches of the government.
    - Parliamentary Executive
      - Head of State
      - Head of Government
    - Presidential Executive
      - Head of State and Head of Government are the same person.
    - Semi-Presidential Executive
    - Directorial Executive
- **Privacy and Data Protection**
  - **Right to Privacy**
    - **USA**
      - Privacy is born in the U.S. with the Warren case.
      - Birth control was obtained through the enforcement of the fourth amendment and the reasoning that the use of contraceptives methods is a decision between wife and husband without the intervention of the State. And the same reasoning was applied for the sodomy.
    - **EU**
      - In Europe, the right to privacy is a super-right.
      - **Art.8 ECHR** provides a clear right to be free of unlawful searches with extreme exceptions.
        - Public Safety
        - National Security
        - Economic Well-Being
        - Prevention of Disorder or Crime
  - **Right to Data Protection**
    - **Definitions**
      - Based on the concept of personal data, requires that the use of the same by private and public bodies is made in accordance with specific legal standards.
      - **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.
      - **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.
      - **Data Processor**, a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
      - **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.
    - **Regulations**
      - **Data Protection Directive 95/46/EC**
        - The Data Protection Directive, officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union (EU).
        - 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.
          - The adequacy of the level of protection shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations.
          - **Safe Harbour** was introduced in 2000 to regulate the transfer of data to a third country (US) assuring an adequacy of protection. It was a self-certification mechanism which went out of date soon.
          - **Schrems Case**
            - The ability of Directive 95/46 in protecting the transfer of Data to third countries was questioned, and the Court found the Safe Harbour mechanism inadequate to efficiently protect the data.
            - No binding definition of "**Adequate**"
            - Third country must ensure an **essentially equivalent** level of protection
            - Periodic assessments of the adequacy of third countries procedures, and not interference from governments' on personal data must occur.
            - The Safe Harbour mechanism was indeed **declared invalid**, October **2015**
            - In **2016**, the **Privacy Shield** substituted the Safe Harbour mechanism.
        - **Principles**
          - **Transparency**, the data subject has the right to be informed when his personal data is being processed.
          - **Legitimate Purposes**
          - **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 kept up to date. 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.
      - **E-Privacy Directive 2002/58/EC**
        - 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. It applies to processing of personal data in connection with provision of publicly available electronic communications services in public communications networks.
        - **Digital Rights Ireland Case**
        - **Confidentiality of Communications**
          - Security in the processing of personal data
          - Ban unsolicited communications
        - **Prior User Consent** is required for **SPAM** and to store **Cookies**
        - It **complements** the Directive 95/46 before and **GDPR** now as a **lex specialis** for electronic Communications services in the privacy framework addressed by GDPR.
        - Limited in the scope of application to traditional telecoms providers, therefore a new e-privacy regulation is on the making. **E-Privacy Regulation**
          - Contrary to an EU Directive, an EU Regulation is a legal act of the European Union that becomes immediately effective as law in all member states simultaneously.
          - **Key Points**
            - **New Players**
            - **Cookie Law**
            - **Content and Metadata**
            - **Spam**
      - **Data Retention Directive 2006/24/EC**
        - Data Retention means the ways according to which the data is stocked and processed and for how long.
        - **Annulled because against the principle of Proportionality.**
          - Retention period between 6 months and 2 years (too long).
          - No clear definitions of serious crime.
          - No procedural rights.
        - Restrictions of Fundamental rights (Privacy) must comply with art.52 of the Charter and therefore they must not affect the DNA of the rights.
      - **General Data Protection Regulation GDPR**
        - It substituted the **Directive 95/46**.
        - **Material Scope**
          - Applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means which form part of a filing system or are intended to form part of a filing system.
        - **Territorial Scope**
          - 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.
          - Applies to the processing of data subjects located in the EU by a controller or processor not established in the EU.
        - The GDPR is applicable not only to information directly related to an identified person, but also to information that makes the person **identifiable**.
          - **Pseudonymisation**
            - 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. GDPR is still applicable.
          - **Anonymisation**
            - Processing of personal data in such a manner that the data subject is not or no longer identifiable. GDPR is not applicable.
        - **Principles**
          - **Lawfulness, Fairness and Transparency**
            - Mainly based on **Consent** of the Data Subject
            - Consent may not be required when:
              - **Performance of a Contract**
              - **Legal Obligation** of the Data Controller
              - **Vital Interest** of the Data Subject
              - **Public Interest**
          - **Purpose Limitation**
            - Limit to those necessary to the purpose
          - **Data Minimization**
            - Limit to those necessary to the purpose
          - **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
        - **Data Subject Rights**
          - 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.
          - Right to Rectification
            - Right to be Informed
            - 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.
          - 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.
            - According to specific grounds
              - Provided that it is not excluded in some cases (Freedom of Expression)
          - Right to Restrict the Processing
            - The data subject shall have the right to obtain from the controller the restriction of information
            - Accuracy of personal data is contested
            - Unlawful processing
            - Controller no longer needs personal data
          - Right to Object
            - The data subject shall have the right to object on the basis that consent has never been given
          - Right to Data Portability
            - 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.
            - Not applicable when performing a Contract
            - Not applicable with data subject's explicit consent
            - Not applicable if authorised by Union or Member State Law to which the controller is subject
          - Right to not be subject to automated decision-making
        - **Data Controller Obligations**
          - **Data Breach Notification**
            - When aware of a data breach, the controller shall notify the competent authority within 72 hours.
          - Record of Processing Activities
          - **Data Breach Communication**
            - When aware of a data breach, the controller shall notify the competent authority within 72 hours and if the risk is high for the rights and freedoms of natural persons, it should also communicate the data breach to the data subject without undue delay.
          - Prior Consulting
          - **DPIA**
            - **Data Protection Impact Assessment**, important tools for accountability, as they help controllers to comply with GDPR requirements and to demonstrate that appropriate measures have been taken to ensure compliance. An assessment is conducted to define which is the risk, if you realise that the specific data processing has high risk, you have to ask to the supervisory authority consultation on the process of data.
          - **DPO**
            - **Data Protection Officer**: the controller and the processor shall designate a data protection officer. He's the contact point between data controllers/processors and supervisory authorities).
          - **Risk-Based Approach**
            - The GDPR encourages 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.
        - **Transfer of Data to Third Countries**
          - Nothing has changed from Directive 95/46

- **Right to Internet Access**
  - **Freedom of technical access to the Internet**
    - **Human Right**
      - It hasn't been defined as a Human right, but rather as mean to enjoy other human fundamental rights such as the freedom of expression.
    - **Fundamental Right**
      - Affected by different constitutional decisions in every country.
      - Costa Rica — Fundamental Right
      - Honduras
      - Greece
      - USA
      - Venezuela
      - Ecuador
      - France — Freedom of Internet Access rather than right to Internet Access
      - UK
      - Finland
      - Estonia — Universal Right
      - Italy — First country to introduce a "Bill of Rights" of the Internet, where "liberty, equality, dignity and unique diversity of each individual" are protected
      - Spain
    - **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.
    - **Freedom of Expression**
      - 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.
    - **Constitutional Rank**
    - **Primary Law Rank**
  - **Freedom on the Internet**
- **CyberSecurity Framework**
  - 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.
    - **Strategic Priorities**
      - **Cyber Resilience**
        - Economic Logic, develop a secure information society for all
        - Security Logic, protecting critical infrastructure agains terrorist attacks
      - **Cyber Crime**
        - Fast growing, high-profitable and low-risks
      - **Cyber Defense**
        - CSDP, Common Security and Defence Policy
      - **Develop the industrial and technological resources for cyber security**
      - **Establish a coherent international cyberspace policy**
    - **ENISA** EU Agency for Network and Information Security
      - Provides practical advice for the public and private sector in EU countries and for the EU institutions.
      - Supports drafting of EU policy and law on network and information security.
    - **NIS Directive**
      - EU tried to create a cooperation among European countries in facing cybersecurity attacks and emergencies.
      - 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:
        - Designation of competent authorities — One per State (Point of Contact)
        - **CSIRTs**, Computer Security Incident Response Teams
        - Adoptation of National cybersecurity strategies
          - Roles, responsibilities, cooperation of governments and other parties
          - Education, awareness-raising and training programs
          - Plan to identify risks
          - Preparedness to handle and respond to cyberattacks
          - Research and development planning
    - **Cybersecurity Act 2017**
      - Introduces a new approach mainly focused on the certification sector, with a certification framework comprehensive of set of rules, technical requirements, standards and procedures.
- **Internet and Law**
  - From **ARPANET** to **INTERNET**
    - TCP/IP
    - HTTP
  - **IP Addresses** and **DNS**
  - **Self-Regulatory Agencies**
    - **ICANN**
    - **ISOC**
    - Problem of Private Entities and strict connection with U.S. Department of Commerce.
- **Internet Jurisdiction**
  - The problem with the Internet is that it is not clear where the State can apply its Sovereign power.
  - **3 Jurisdiction forms**
    - **Prescriptive Jurisdiction**, State power to create legal norms.
    - **Enforcement Jurisdiction**, State power to enforce the legislation.
      - When considering the Internet case, the problem concern mainly this type of jurisdiction.
    - **Adjudicative Jurisdiction**, ability of courts to hear and decide on matters.
  - **Shift**
    - **1878**, physical presence of the individual in the State to apply jurisdiction.
    - **1945**, minimum contact on that State allows the authorities of that State to have jurisdiction. **Purposeful Availment** of the benefits of trading in one State.
      - **Minimum Contact Test**
      - **Purposeful Availment**
    - **1984**, Jurisdiction can be applied in the States were the effect is perceived. Physical presence is no more a requirement, but **Damage** or **Contract** it is.
      - **Effects Test**
    - **1997**, application of Jurisdiction over websites if the **actively operate** with the purpose of doing business, with objectives located in another State.
      - **Sliding-Scale Test**
    - In cases of online defamation: it is no more important where an information is posted, but rather where the information is read. Using Internet makes you subject to jurisdictions that are outside of the national borders.
      - Sue the defendant in the Country where it is based for all the arm 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.
    - **Google Spain Case**
      - The jurisdiction can be applied to Google from the moment that its Spanish branch is doing business on advertising that it is unequivocally linked to the Google Search Engine and therefore, even if the data is processed in the U.S., the Directive 95/46 is applicable.
      - Google was defined by the European Court of Justice as a Data Controller and therefore responsible for the removal presenting information which were considered to be in breach of the right to be forgotten, even without prior consultation with the owner of the website.
- **Freedom of Expression**
  - **USA, Protective Approach**
    - Freedom of expression as intended in the **First Amendment** can be restricted only few situations.
      - **False Statements**
      - **Obscenity**
        - Communication Decency Act, distribution of obscene materials to any person under 18 is unconstitutional.
      - **Hate Speech**, only when it is directed to producing an "imminent lawless action".
        - KKK Case
  - **Europe, Restrictive Approach**
    - **Incitement**, limitation can apply in case of incitement of an "imminent lawless action".
    - In Europe we see 3 different level of protection of the Freedom of Expression
      - **ECHR**
        - Freedom of expression can be restricted.
          - When necessary in a **democratic society**.
          - When **prescribed by law**.
          - Have a **legitimate aim**.
          - **Hate Speech** can be banned when negates the fundamental rights of the convention.
      - **EU Charter**
        - A distinguish between **Press** and communication on the **Internet** must be taken into consideration. And according to these the policies may differ to secure the protection and promotion of the rights and freedoms concerned.
      - **National Constitutions**
        - Art. 21 of Italian Constitution limits Freedom of Expression on the base of **Public Morality**.
          - Initially intended as common sense morality.
          - Today is intended as **Sexual Modest** and **Personal Dignity**.
    - The **restrictive approach** followed by EU is expressed in the fact that freedom of expression enjoys protection as fundamental rights "among the others", it isn't an **absolute right** such as in USA. It has to be balanced with:
      - User's right to data protection
      - ISP's freedom to carry out business
      - Users' freedom of expression
- **ISP Liabilities Provisions as Free Speech Rules**
  - **Content Providers**, providing the content and writing information on the web.
  - **Service Providers**, not delivering any content.
    - Access Providers — The service provided consists of the mere transmission of information or the mere provision of access to a communications network.
    - Caching Providers — The service provided consists of the temporarily storage of information.
    - Hosting Providers — The service provided consists of the permanent storage of information.
  - **USA**
    - Internet Service Providers are liable for the content published only if they have editorial control over it. — **Prodigy**
    - **CDA 230**
      - 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.
      - **Overturn Prodigy's decision.**
    - **Digital Millennium Copyright Act**
      - A service provider is not liable for […] if:
        - Does not have actual knowledge
        - Does not receive a financial benefit directly attributable to the infringing activity.
        - When obtains the knowledge of misconduct acts expeditiously to remove or to disable access to the material.
  - **Europe**
    - **E-Commerce Directive**
      - The e-Commerce Directive, adopted in 2000, sets up an Internal Market framework for online services, its aim is to remove obstacles to cross-border online services in the EU internal market and provide legal certainty for businesses and consumers. It establishes harmonized rules on issues such as the transparency and information requirements for online service providers, commercial communications; and electronic contracts and limitations of liability of intermediary service providers.
        - **Liability Exemptions**
          - Different between **Mere Conduit Providers**, **Caching Providers**, **Hosting Providers**.
          - Exemptions are applicable only if the activity is 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.
        - **Absence of a General Obligation to Monitor**
          - 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.
        - **Notice and Take Down** — **Google vs ViviDown**
          - **SABAM vs Scarlet**
          - **Facebook Austria**
            - Automated technologies could seek information, which does not require further analysis and falls within the specific characteristics of a previous injunction.
- **Trends in ISP Liability**
  - **No general obligation to monitor**
  - **Notice and Take Down** — A simple communication is sufficient and the URL is required only if indispensable to identify the infringing content.
  - **Italy**
    - Division of Providers in 3 Categories
      - Mere Conduit Providers
      - Caching Providers
      - Hosting Providers
    - **Active Providers** cannot benefit from the **Liability Exemptions**.
- **Fake News**
  - **Different Approaches**
    - **USA**
      - The rule to restrict the Freedom of Expression is again the First Amendment and, therefore, in case of creation of clear and present danger.
    - **EU**
      - Fake news become relevant for the legal system when the protection of constitutional interests is affected.
  - **Regulation**
    - **Public Regulation**
      - Both Germany and Italy pursued the goal of holding social media networks responsible for hosting fake news and hate speech.
      - Possible drawback in a too strict censorship of the freedom of expression.
    - **Self-Regulation**
      - More moderators and higher frequency of Notice and Takedown procedure
      - Associated with the Self-Regulation there is the risk of the **privatisation of the protection of rights**.
    - **Co-Regulation**
      - **2016, Code of Conduct** for Hate Speech.
      - **2019, Code of Practice** on Disinformation.
      - In both the Agreements, Tech Giants agreed in pursuing a war against hate speech and fake news, trying to recognise and take down with higher frequency notifications of misconduct.
- **Blockchain**
  - Blockchain is a technology involving a huge number of nodes (computers) how can either be memory for a fully or partial storage of the ledger of transaction, but also miners as computers able to run an algorithm to encrypt through hashing tables the data to be included in a block of the chain.
  - The problems associated with the regulation of data protection related to this new technology are many, on top of them:
    - **Data Minimization** and **Right to be Forgotten**
      - It's not built to minimise the usage of data and eliminate it after a certain time, rather, the blockchain is an "ever-growing" creature that is thought in such a way that would store for ever the encrypted information.
    - **Pseudonymization**
      - On the other hand, since data are encrypted, not fully anonymised they are still condition to GDPR application.
    - **Data controller**
      - Considering every node as a data controller would inappropriate since they aren't able to modify the data, neither give the data subject access to them.
- **Digital Single Market, 2017**
  - Is a policy belonging to the European Single Market that covers digital marketing, E-commerce and telecommunications.
    - Geo-blocking barriers were disrupted.
  - It substituted the e-commerce Directive of 2000.
  - This policy was intended to face the big changes in the online digital environment. Indeed the ECJ took into consideration both **economic purposes** and the **protection of fundamental rights** in its redaction. Shift from the e-commerce directive.
    - **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.
  - A new framework where platforms were more responsible, fair and transparent in protecting the core value was needed.
  - The **Online Sharing Provider** figure was defined and with it its duties in relation to copyright protected content.
    - **Video Sharing Platforms** (Youtube)
    - **Content Providers** (Netflix)