DYP NOTES

CHAPTER 2.-PROFESSIONALISM: BASIC CONCEPTS

1.- DEFINITIONS

Human beings have needs which must be covered to live comfortably, so they work in order to get what they want. For certain reasons, work tends to require more specialised skills:

- We are not able to produce everything we want.
- Specialisation often leads to greater productivity because of factors of scale.

Specialise: concentrate on and become expert in a particular subject or skill.

Theory: a supposition or a system of ideas intended to explain something, especially one based on general principles independent of the thing to be explained.

Practice: the actual application or use of an idea, belief, or method, as opposed to theories relating to it.

Praxis: practice, as distinguished from theory. Something practical that is used as it works well, but it is not based in any theory, only in previous experiences.

Best practice: commercial or professional procedures that are accepted or prescribed as being correct or most effective.

Technique: a way of carrying out a particular task, especially the execution or performance of an artistic work or a scientific procedure.

Amateur: a person who engages in a pursuit of an unpaid basis

Work: activity involving mental or physical effort done in order to achieve a result. Work as a means of earning income (employment).

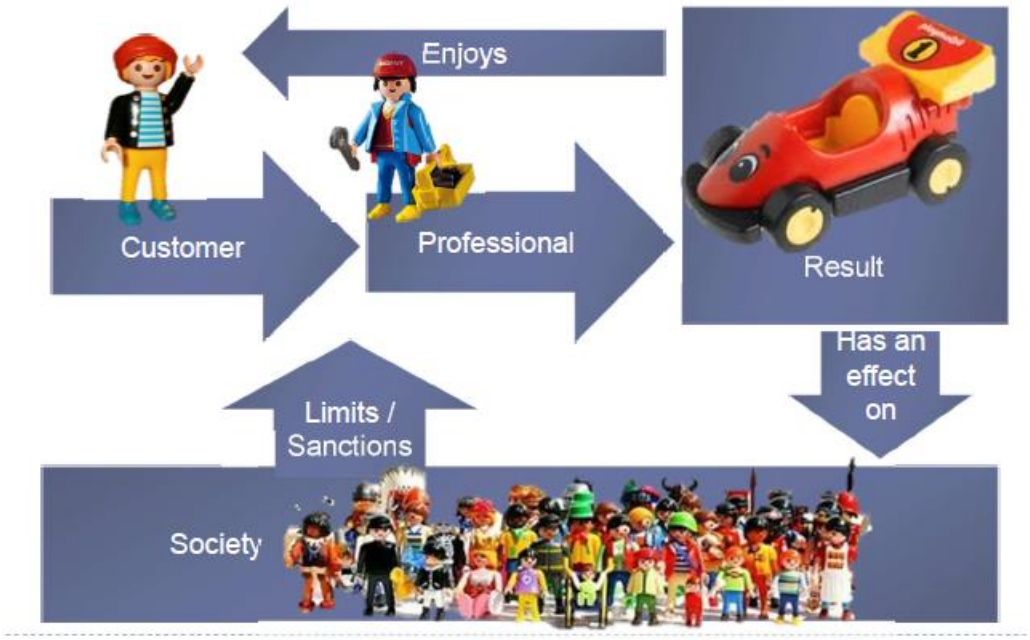
Job: a paid position of regular employment.

Profession: a paid occupation, especially one that involves prolonged training and a formal qualification.

Professional: a person engaged or qualified in a profession.

Professionalism: the competence or skill expected of a professional.

2.- GENERAL MODEL OF INTERACTIONS



3.- ACTORS TO BE CONSIDERED

Customer (one-time relation) / Client (recurring relation): person or entity requesting the services of a professional.

Professional: person who performs the necessary actions to satisfy the client request, within the limits that the society allows (ethical and legal).

Concerned society: a group of people who feel affected by the process, the result or its use. They have the capacity to influence any of those involved in the process and regulate it.

3.1.- CUSTOMER/CLIENT

The request made may be sanctioned by society (ethical and/or legal). The client seeks a professional based on:

- **The power of expert opinion**: based on the customer's perception of the experience, special skills or knowledge of the professional.
- **Reference power**: based on the behaviours or personal characteristics of a professional which are admired by the customer or other people who influence the customer.
- **Legitimate power**: comes from the authority of your rate and position in the chain of command.

3.2.- PROFESSIONAL

They are in charge of the work and require certain skills to enable them to carry out their work:

- **Technical skills**: they may need specific knowledge, skills or experience.
- **Social skills**: communication and interpersonal abilities.
- **Decision-making**: they manage conceptual models, create and design feasible solutions, choosing the one that maximizes customer satisfaction.
- **Independence**: they act with freedom, otherwise there is no responsibility.

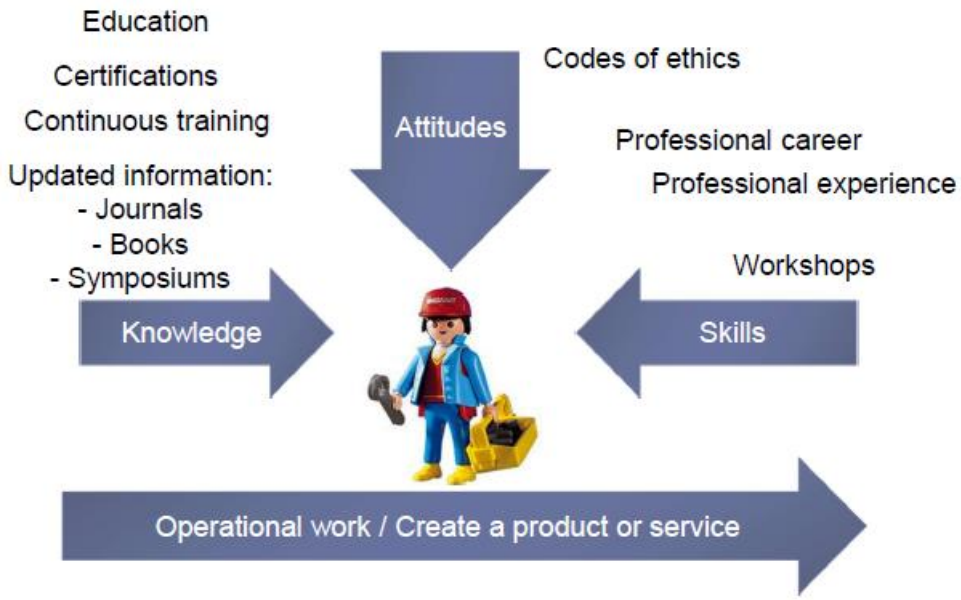
They have acquired these skills by:

- A training process.
- Self-learning.
- While working with colleagues.
- Their career.

These skills can be socially reinforced by:

- Regulated studies.
- State or associations accreditations.

Finally, practicing a profession is not a guarantee of professionalism.



3.3.- SOCIETY

Society ensures welfare by meeting the requirements of members and regulating the actions taken by clients and professionals.

The **State** protects the public interests, legislates and enforces laws.

There are different types of associations:

- **Professional associations**: ensure good practices, training, upgrading and certification of its partners.
- **Business associations**: protect companies involved in the provision of certain goods or services.
- **User associations**: ensure customer and stakeholder satisfaction.

Some professions are regulated because of their societal impact, and you can't practice them without a license. They are regulated by law, which now clearly defines the following:

- The accreditation process.
- When acting illegally, negligently, etc.

Professional associations represent the professional interests of their members. They watch over their training:

- They guarantee knowledge.
- Levels of certification and specific skills.
- Support for continuous training.
- Encourage interactions between professionals.

They lend support to the social vision of the profession:

- Collaboration in social events.
- Promotion and enforcement of their "codes of ethic".
- Punishment and expulsion of members who do not act professionally.

Business associations provide a particular good or service to society.

Advantages for society:

- Promoting the use of their products.
- Conducting training activities.
- Demonstrating the benefits of their products.

Disadvantages for society:

- Minimizing any information on disappointing cases.
- Lobbying: act of attempting to influence decisions made by officials in the government.
- Promoting an organized oligopoly market.

Users associations or **stakeholders** are sometimes non-profit. They promote the use and enjoyment of specific products or services. They defend user rights.

4.- PROFESSIONALISATION

Professionalisation is a social process by which any occupation transforms itself into a true "profession of the highest integrity and competence".

This process tends to involve establishing:

- Acceptable qualifications and a professional body.
- Some degree of demarcation between qualified and unqualified amateurs.

At some point individuals have demanded recognition and social status according to their activities. The state has regulated licenses and responsibilities to be assumed by those performing these activities. This had led to the professionalisation of the activity.

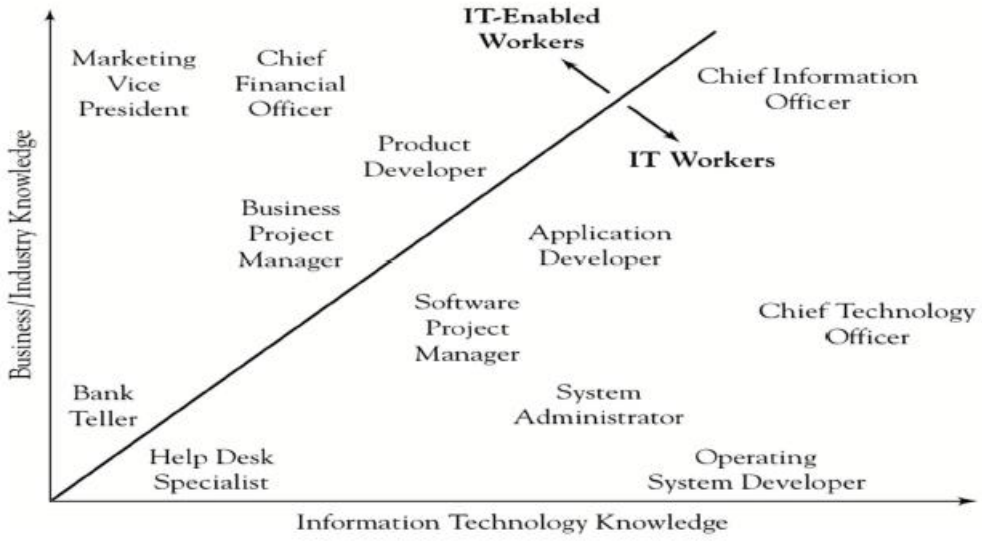
CHAPTER 3A.-PROFESSIONALISM IN ICT: A GENERAL APPROACH

1.- INTRODUCTION

Computer science is a very recent science that has a considerable **socioeconomic impact**. It is necessary to analyse this phenomenon from different points of view:

- Countries.
- Businesses.
- Professionals.
- Clients

2.- COMPUTER PROFESSIONALS OR ADVANCED COMPUTER USERS?



3.- IT WORKERS

IT workers categorisation:

- **Conceptualisers**: those who conceive of and sketch out the basic nature of a computer system.
- **Developers**: those who work on specifying, designing, constructing and testing an information technology artifact.
- **Modifiers/extenders**: those who modify or add on to an information technology artifact.
- **Supporters/tenders**: those who deliver, install, operate, maintain or repair an information technology artifact.

International Labour Organization (ILO) is the international organization responsible for drawing up and overseeing international labour standards. It is the only "tripartite" United Nations agency that brings together representatives of governments, employers and workers to jointly shape policies and programmes promoting Decent Work for all. This unique arrangement gives the ILO and edge in incorporating "real world" Knowledge about employment and work.

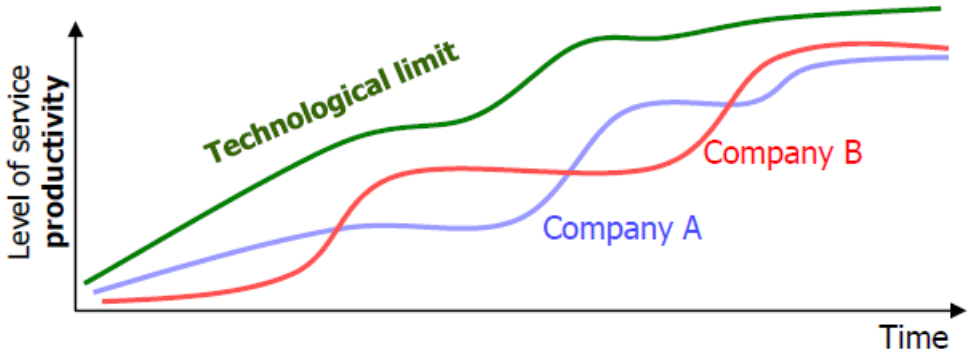
The **ISCO** is the International Standard Classification of Occupation.

Computer professionals become a basic element of an effective group work. **Interdisciplinary teams** compete more effectively and need individuals known as T-shaped people. The concept of **T-shaped skills** is a metaphor used in job recruitment to describe the abilities of persons in the workforce.

In T-shaped skills, the **horizontal bar** on the T represents the depth of related skills as **expertise in a single field**. On the other hand, the **vertical bar** is the **ability to collaborate** across disciplines with experts in other areas, and to apply knowledge in areas of expertise other than their own.

4.- ICT

Business management is one of the oldest clients in the computing market.



The **technology gap** is the time lag between the appearance of a new technology and its acquisition.

The role of ICT professionals play in business are:

- **Technological support**:
  - Identify, analyse and innovate major business processes.
  - Design, development and deployment of applications.
  - Provide timely maintenance, when minor improvements are required in the current system.
  - Give support during in-use stability period.
- **Legal support**:
  - Legal consultant.
  - Judicial experts.

5.- SUPPORTING ICT PROFESSIONALS

The professional profiles in this workspace are varied, and it is even difficult to classify some practitioners. In recent years, there has been an international clamour to regulate the profession in some way.

Professional associations around the world: CEPIS, IEEE, ACM, CompTIA, etc.

Professional associations in Spain:

- Professional associations: ATI.
- Official associations: without recognized professional skills and not accompanied by European directives.

Today, many experts are available through **social networks**, either with their own blog or by participating in others.

Monographic associations: in many cases, due to the lack of regulation of the profession, specific associations are emerging for a type of work, tool or technology.

Training in the field of ICT:

- **Vocational training**: middle-level training cycles and superior-level training cycles.
- **Higher education**.
- **Non-formal training**: associations and private companies.

There exist magazines and publishers covering ICT topics as PC-World, Novatica, ACM Press, etc.

The standards for a global ICT profession:

- **De facto standard**: a custom, convention, product or system that has achieved a dominant position by public acceptance or market forces. Example: Java and C# languages.
- **UNE standards** (Una Norma Española).
- **ISO standards**.

CHAPTER 3B.-ICT PROFESSINALS COMPETENCES AND CERTIFICATIONS

1.- THE STARTING POINT

The **company** has a clear mission supported by "core competences" and formulates objectives. Work is necessary to achieve these objectives. The jobs require capable and competent people.

The **employees** (human resources) contribute with:

- Personal characteristics:
  - Physical.
  - Psychological.
- Competences:
  - Training.
  - Experience.

Core competences underpin the mission if the firm. They are those capabilities that are critical to a business achieving **competitive advantage**. It also can be defined as key ability or strength that an organisation has acquired that differentiates it from others, gives it competitive advantage, and contributes to its long-term success.

Competences can be determined by analysing previous (good) results. In dynamic environments, companies tend to question their own competences and consequently whether their employees need to change. As a consequence, we talk about **lifelong training**.

In many cases, **internal promotion** of employees is preferred for new jobs or vacancies.

Advantages:

- Very useful system to keep employees motivated.
- Maintain a healthy perspective that this can boost your professional career.

Disadvantages:

- Competences may change and the person may not be able to handle the new job.
- The competences which are good at this level are not always good at another.

The **Peter Principle** states than in a hierarchy, every employee tends to rise to his level of incompetence. Basically, it states that, generally speaking, incompetent workers will be promoted above competent workers to managerial positions where they thus don't have to do any real work and the damage they do can be limited.

In the **Dilbert Principle**, instead of people getting promoted to their lowest level of competence, any and all incompetent employees are placed in the one place where they can do the least damage, management.

2.- ABOUT COMPETENCES

A **competence** is the ability to do something successfully or efficiently. It can also be defined as the legal authority of a court or other body to deal with a particular matter.

Competence = Knowledge + experience + ability

Knowledge comprises a co-worker's training and qualifications.

Experience is framed by time and work content.

Ability refers to the capability to utilize knowledge and experience to solve problems.

Will is sometimes emphasized in definitions of competence. The concept of competence is also often referred to as:

- **Motivation**: a reason or reasons for acting or behaving in a particular way. Desire or willingness to do something, enthusiasm.
- **Attitude**: a settled way of thinking or feeling about something.
- **Potential**: latent qualities or abilities that may be developed and lead to future success or usefulness. The possibility of something happening or of someone doing something in the future.

Competence dimensions:

- Technical dimension: knows the work to be done and is very experienced.
- Collaborative dimension: knows how to collaborate with others and facilitates coordination among members.
- Directive dimension:
    - Personal: feels motivated.
    - Teams – groups:
        - Leads.
        - Manages the strategy.
        - Manages the work.
        - Solves problems.

Given the extreme complexity of many of the characteristics that are required today, **discrimination** can occur at many levels of screening. At the **corporate level** we talk about:

- **Specific competences of the organisation**: in business organisation and organisational structure.
- **Business-related competences**: facilitate business.
- **Personal competences**: place the employee in a good position to do the job, teamwork, good listener, delegate, effective communication.

Nowadays it has become fashionable to classify competences into:

- **Hard skills**: they are referring to the technical work developed and for many years, competences were focused on this area.
- **Soft skills**: they currently generate interest. Skills related to emotional intelligence, collaboration, teamwork, leadership, decision making, etc.

The technical ones are high perishable, but not soft skills.

A **competence GAP analysis** is a radar chart that shows the competences available and the needs to be covered. The analysis is to facilitate the selection and identification of areas of training.

3.- COMPUTER PROFILES

The **EUCIP** (European Certification of Informatics Professionals) is a European qualification developed by **CEPIS** (Council of European Informatics Societies). Overall goals:

- Define an industry-driven vocational structure and standards for the informatics profession.
- Establish a sustainable European services network for informatics competence development.
- Contribute to closing the ICT professional skills gap in Europe.
- Offer a vehicle for life-long learning and competency enhancement for the ICT profession.

The EUCIP covers a broad range of ICT knowledge on core topics relevant to all ICT practitioners:

- EUCIP Core: an introductory-level three-part ICT professional certification.
- EUCIP Professional: based around one of 21 different job profiles.
- EUCIP IT Administrator: a stand-alone certification focusing on the skills required by an IT administrator typically working for a small or medium-sized enterprise.

Hard knowledge areas:

1. **Planning area**: the use and management of information systems.
2. **Building area**: development and integration of information systems.
3. **Operation area**: operation and support of information systems.

Soft knowledge area: essential behavioural skills.

The **European e-Competence Framework** (e-CF) provides a reference of 40 competences as required and applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills and proficiency levels that can be understood across Europe.

The e-CF was developed through a process of collaboration between experts and stakeholders from many different countries under the umbrella of the CEN Workshop on ICT Skills.

CHAPTER 4.-BASIC CONCEPTS AND LEGAL FRAMEWORK IN THE DAY-TO-DAY ACTIVITIES OF IT PROFESSIONALS

1.- LAW BASIC CONCEPTS

Computer law does not exist as such. The rules affecting our profession are fragmented in different texts.

According to differing concepts of the state:

- The State as a body established by dominating class to maintain its dominance: the **law** is the regulatory artefact designed to organize and protect the state.
- The State as harmonizing and integrating some socially compatible groups: the **law** is the regulator artefact designed to prevent infighting to attain this *harmonious society*.

Attending to the RAE, a **law** is a set of principles and norms, expressing a sense of justice and order, which regulate human relations in every society, and with which compliance can be coercively imposed.

The Spanish constitution (1978) establishes the separations of powers:

- **Executive**: the government (law enforcement).
- **Legislative**: general court = congress + senate (law making).
- **Judicial**: judges and courts administer justice according to law.

The hierarchy of the set of laws:

- **Fundamental law**: in Spain it is the **Constitution**. It is above any other law.
- **Organic and ordinary laws**: organic laws concern the **fundamental rights and public freedoms**. The approval, amendment or repeal of organic laws shall require an **absolute majority in Congress**, in a final vote on the overall project. Ordinary laws are the rest of laws.
- **Decree-law**: **in case of extraordinary and urgent need**, the Government may issue temporary legislative provisions which take the form of decree-laws. Must be immediately submitted in full for debate and voting by the Congress.
- **Regulatory requirements**: the regulations emanate from the **executive branch power** and cannot contradict any law.

There is a **supranational legislation** as a result of the transfer of national sovereignty to perform common actions between a set of countries. In the case of the European Union, there is a transfer of power to the European Council, Commission and Parliament, which have legislative initiative. Supranational legislation goes beyond the European Union. We distinguish between:

- **Regulations**: legal standards issued by the European institutions that have **direct effect** in the member countries, which take precedence over national law.
- **Directives**: contain targets that countries must comply within a time specified, and each country **transcribe the directive** into their own legislation in their own terms.
- **Decision**: also have a direct effect, but in this case, they have a **more administrative nature** and are addressed to **particular recipients**.

2.- LEGAL FRAMEWORK OF IT PROFESSIONALS

The most important regulations that affect our profession are:

- **Data Protection Law**.
- **Intellectual Property Law**.
- Law of Information Society Services.
- Citizens' Electronic Access to Public Services.

The Spanish "**Law of Information Society Services and Electronic Commerce**" (LSSI) arises to include in our legislation the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (**Directive on electronic commerce**).

The objective of the LSSI is to regulate the legal framework for information society services and electronic contracting insofar as concerns:

- The **obligation of service providers**, including service providers who act as middlemen in the transmission of contents by telecommunications networks.
- The **electronic commercial communications**.
- The information before and after the conclusion of **electronic contracts**.
- The conditions regarding the validity and efficacy of electronic contracts.
- The system of **sanctions** applicable to information society service providers.

Information society service means "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service". Example: a website that earns money through advertising almost certainly will constitute an information society service.

Infractions and sanctions:

- Very serious (penalties from 150.001 to 600.000 euros).
- Serious (from 30.001 to 150.000 euros).
- Minor (up to 30.000 euros).

The Law on Citizens' Electronic Access to Public Services (also known as "**Law on eGovernment**") entered into force on 24 June 2007. It officially recognised the right of citizens to communicate electronically with Public Administrators. The aim of the law was:

- To enhance efficiency by doing away with the need to present paper documents to authorities.
- To promote "closeness to the citizen and administrative transparency".
- To contribute to the development of eGovernment.

It also established the basic principles for the use of IT between citizens and the Administration, but also among Public Administrations.

The laws 39 / 2015 Common Administrative procedure of public administrations and 40 / 2015 Legal Regime of the public Sector, which replaces Law 30 / 1992 and the Law 11 / 2007, entered the fact that the **use of the electronic environment has to constitute the usual means in relations of administrations with citizens and those among themselves**.

Law 39 / 2015, Common Administrative procedure of public administrations, allows the that the electronic processing must constitute the usual performance of public administrators, in order to better serve the principles of effectiveness, efficiency, the cost savings, transparency obligations and guarantees of citizens.

3.- CIVIL LIABILITY

Civil liability is the **potential responsibility for payment of damages as a result of an action or omission**. In order to succeed with a claim for damages arising out of the action or omission of another, it is necessary to prove **fault** on the part of that person. Fault can take the form of either: **intent** or **negligence**.

From the point of view of intentionality, we may distinguish two types of behaviours:

- **Fraudulent behaviour**: events where the subject is aware that he will cause harm.
- **Negligent behaviour**: lawful acts that cause damage because the appropriate precautions are not taken into account, that is, for acting negligently.

A **compensation** involves **quantifying first the damages** suffered by the person or entity due to the activity of one individual who has personal liability for it, and second **repairing the damage caused**. The right to compensation could include not only the value of the loss suffered (**consequential loss**), but the gain the creditor has ceased to get (**ceasing gain**). The amount obtained is called **full reparation** so that the person suffering the damage is restored to the previous situation, before the occurrence of the act giving rise to compensation.

Civil liability differs from criminal liability in that the latter is intended to **designate the person who must answer for the damages caused to the society as a whole**, not to a particular individual. The damages in criminal liability are social, since they are considered as **violations of public order**. The civil liability is an attempt to repair the damage caused to victims, therefore, **the sanction of civil liability is in principle compensatory, rather than punitive**. Both responsibilities can coexist in the same event.

In contractual relationships we distinguish between:

- **The obligations of means**, whereby a party undertakes to use its best efforts, or **to use the appropriate means**, to do something for the other party. These only require a debtor to act prudently and diligently and to use all reasonable means so as to endeavour to achieve a certain result. **No result is guaranteed**, however.
- **The obligations of result**, whereby a party undertakes **to achieve a defined result**. These require a debtor to actually achieve the bargained for result expect only where the debtor can rightfully invoke a force majeure or the creditor's fault to be excused.

Professional liability can be defined as those legal obligations arising out of **professional's errors, negligent acts or omissions** during the course of the practice of his or her craft. Traditionally, the scope of professional liability was limited entirely to liberal professions. In the case of computer engineers, one of the typical cases where liability may be incurred is data protection.

The civil liability insurance is only responsible **for the other party's losses**. Your person and your property are unprotected, but liability insurance protects you from being held responsible for the other party's damages.

There are different types of liability insurance, including:

- General liability.
- D&O liability.
- Employer liability.
- **Professional liability**.

The purpose of professional liability insurance is to protect those seen as professionals or "experts" in a given field, **who may not be protected by general liability due to their expertise**. When someone is seen as a professional, they are held to a higher standard and are therefore often considered to hold greater liability towards their clients. Consequently, **they need more coverage than general liability insurance offers**.

4.- COMPUTER CRIMES

An individual may incur criminal liability even where he or she was not aware that the activity constituted a crime. The Spanish Penal Code does not cover computer crimes as such. In summary, **the computer may have been used in the commission of a crime, or it may be the target**. Computer crimes refers to any crime that involves a computer and a network.

Computer crimes characteristics:

- **Imprudent acts**, which are not necessarily committed with intent.
- Can be performed **easily and quickly**.
- Can cause **serious economic losses**.
- Require some **technical skills** to be performed and can become quite sophisticated.
- **Do not require physical presence** to be performed.
- **Too hard to audit** because, in many cases, it is difficult to find the evidence.
- The **proliferation and evolution** of these crimes make their identification and subsequent persecution even more complicated.

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, this is the **first international treaty seeking to address computer crime and internet crimes** by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the **Council of Europe in Strasbourg** with the active participation of the Council of Europe's observer states **Canada, Japan and China**.

Computer crime classification:

- Offences against the **confidentiality, integrity and availability** of computer data and systems.
- Computer-related offences, such as **computer-related forgery and fraud**.
- Content-related offences, which include exclusively offe**nces related to child pornography**.
- Offences related to **infringements of copyright** and related rights, for example illegal copies of software or computer hacking.

- Dissemination of **racist and xenophobic** material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

CHAPTER 5.-PERSONAL DATA PROTECTION

1.- HISTORY OF DATA PROTECTION IN SPAIN

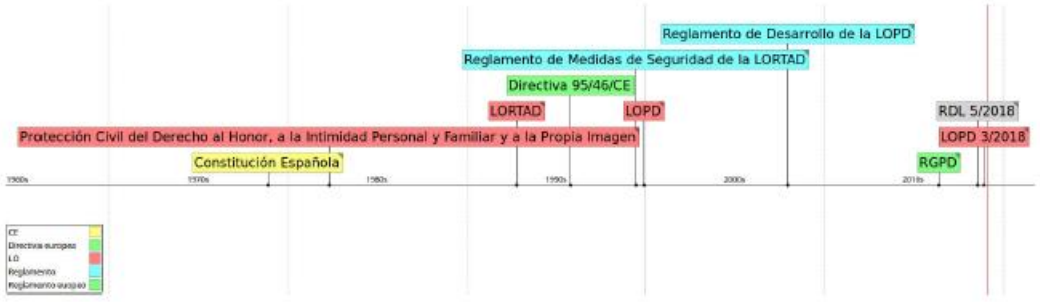
Article 18 of the Spanish Constitution:

1. The right to honour, to personal and family privacy and to protect one's own image is guaranteed.
2. The home is inviolable.
3. Secrecy of communications is guaranteed.
4. **The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights**.

Background:

- Organic Law 1/1982 of 5 May on the civil protection of the right to honour, to personal and family privacy and to protection of one's own image.
- Organic Law 5/1992 of 29 October regulating the automatic processing of personal data (**LORTAD**).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Organic Law 15/1999 of 13 December on the Protection of Personal Data (**LOPD**).

Timeline:



2.- GENERAL REGULATION OF DATA PROTECTION (GRDP)

The **General Regulation of Data Protection** entered into force on **25 May 2016**. But it was not applied until two years later, the **25 May 2018**. It repeals the Directive 95/46/EC and leads to an increased harmonisation of data protection law across the EU member states.

The period of two years until the implementation of the GRDP aimed to enable the adaptation of states of the European Union, the European institutions and also organizations.

The new Spanish Organic Law on Data Protection on Digital Rights Guarantee (**LOPDGDD**) **complements** the GDPD.

This Regulation lays down rules relating to the **protection** of **natural persons** with regard to the **processing** of personal data and rules relating to the **free movement** of personal data.

It also protects **fundamental rights and freedoms of natural persons** and in particular their right to the **protection** of personal data.

The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

It does not apply:

- In the course of an activity which falls outside the scope of Union law.
- By the member states when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU.
- By a natural person in the course of a purely personal or household activity.
- By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminals.
- Offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The GDPR applies to business that are:

- Established in any EU Member State and that process PD (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of this establishment.
- Outside the EU if they process the PD of data subjects who are in the EU in relation to:
    - The offering of goods or services to data subjects who are in the EU.
    - The monitoring of the behaviour of data subjects who are in the EU.

Some definitions:

- **Personal data** is any information relating to an identified or identifiable natural person. One can be identified by an identifier or one or more factors specific of that natural person.
- A **processing** is any operation or set of operations which is performed on personal data, whether or not by automated means.
- A **controller** is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- A **processor** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- A **data subject** is an individual who is the subject of the relevant personal data.
- **Sensitive personal d**ata is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership. Data concerning health or sex life and sexual orientation. Genetic or biometric data.
- A **data breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Pseudonymisation** is the processing of personal data in such 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.

The **key principles** are:

- Transparency.
- Lawful basis for processing.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Retention.
- Data security.
- Accountability.

The **transparency principle** is based on that PD must be processed lawfully, fairly and in a transparent manner. Controllers must provide minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The **lawful basis for processing principle** is based on prior, freely given, specific, informed and unambiguous consent. Contractual necessity, compliance with legal obligations and legitimate interests.

Types of consent:

- **Express consent**:
  - **Explicit** agreement generally documented in writing.
  - **The default option**, in the absence of express consent.
- **Implied consent**:
  - **Presumed** consent or implicit consent.
  - **Tacit** consent: consent that is expressed silently or passively by omissions or by failures to indicate or signify dissent.

The age at which minors may provide for themselves their consent for the processing of their PD in the area of the information society is **16 years**. Establishing a lower limit of **13 years**. In the case of Spain, **14 years**.

The **purpose limitation principle** is based on that PD may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

The **data minimisation principle** is based on that PD must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the PD that it actually needs to process in order to achieve its processing purposes.

The **accuracy principle** is based on that PD must be adequate, accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that PD that are inaccurate are either erased or rectified without delay.

The **retention principle** is based on that PD must be kept in form that permits identification of data subjects for no longer than is necessary for the purposes for which the PD are processed.

The **data security** principle is based on that PD must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful

processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The **accountability principle** is based on that the controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The **individual rights** are:

- Right of access to data / copies of data.
- Right to rectification of errors.
- Right to deletion / right to be forgotten.
- Right to object to processing.
- Right to restrict processing.
- Right to data portability.
- Right to withdraw consent.
- Right to object marketing.
- Right to complain to the relevant data protection authorities.
- Right to basic information.

The **right of access to data / copies of data** is when a data subject has the right to obtain from the controller the following information:

- Confirmation of whether, and where, the controller is processing data.
- Information about:
    - The purposes of processing.
    - The categories of data being processed.
    - The categories of recipients with whom the data may be shared.
    - The period for which the data will be stored (or the criteria used to determine that period).
    - The existence of the rights:
        - To erasure, to rectification, to restriction of processing and to object to processing.
        - To complain to the relevant data protection authority.
    - The source of the data, where the data were not collected from the data subject.
    - The existence of, and an explanation of the logic involved in any, automated processing that has a significant effect on the data subject.

The data subject may request a copy of the PD being processed.

The **right to rectification of errors** is when controllers must ensure that inaccurate or incomplete data are erased or rectifies. Data subjects have the right to rectification of inaccurate PD.

The **right to deletion / right to be forgotten** is when the data are no longer needed for their original purpose. The lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists. The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing. When the data have been processed unlawfully, erasure is necessary for compliance with legislation.

The **right to object to processing** is when data subjects have the right to object, on grounds relating to their particular situation, to the processing of PD where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such

processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

The **right to restrict processing** is when the data may only be held by the controller, and may only be used for limited purposes if:

- The accuracy of the data is contested (and only as long as it takes to verify that accuracy).
- The processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure).
- The controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights.
- Verification of overriding grounds is pending, in the context of an erasure request.

The **right to data portability** is when data subjects have a right to receive a copy of their PD in a commonly used machine-readable format and transfer their PD from one controller to another or have the data transmitted directly between controllers.

The **right to withdraw consent** is when a data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed or the right to withdraw consent. It must be easy to withdraw consent as to give it.

The **right to object to marketing** is when data subjects have the right to object to the processing of PD for the purpose or direct marketing including profiling.

The **right to complain to the relevant data protection authorities** is when a data subjects have the right to lodge complaints concerning the processing of their PD with the competent data protection authority in Spain, if the data subjects live in Spain or the alleged infringement occurred in Spain.

The **right to basic information** is when data subjects have the right to be provided with information on:

- The identity of the controller.
- The reasons for processing their PD.
- Other relevant information necessary to ensure the fair and transparent processing of PD.

Outside the European Economic Area, if the transfer is to an “Adequate Jurisdiction” or the business has implemented one of the required safeguards as specified by the GDPR. Most of the safeguards outlined in the GDPR will need initial approval from the data protection authority.

Companies must take reasonable **measures** to ensure that they are in a position to comply with the principles, rights and guarantees that the Regulation states:

- Data protection by **design**.
- Data protection by **default**.
- **Security measures**.
- Maintenance of a processing of data **register**.
- **Impact assessments** on data protection.
- Appointment of a data protection **delegate**.

- Notifying **violations** of data security.
- Promoting **codes of conduct** and **certification schemes**.

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

An appointment is mandatory in some circumstances with a **data protection officer** (DPO):

- Large-scale regular and systematic monitoring of individuals.
- Large-scale processing of sensitive personal data.

The appointment must be notified by the controller or the processor. An DPO has some minimum tasks:

- Informing the controller, processor and their relevant employees who process data of their obligations.
- Monitoring compliance with legislation and internal policies including internal audits.
- Advising on data protection impact assessments and the training of staff.
- Cooperating with the data protection authority and acting as the authority's primary contact point.

A **one-stop shop** is a system designed to ensure a single data protection authority as an interlocutor. It does nor affect companies that are only in a member state and make data processing affecting only data subjects in that state

3.- LOPDGDD

The new **Spanish Organic Law on Data Protection and Digital Rights Guarantee** (LOPDGDD) complements the GDPD. Although they have the characteristic of being directly applicable, regulations may in practice require other complementary internal rules in order to make their application fully effective. In this sense, rather than transposition, we can speak of "development" or complement to European Union law. Its objectives are:

- Adapt the Spanish legal system to Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of their personal data and on the free movement of such data and complete its provisions.
- Guarantee the digital rights of citizens in accordance with the established mandate in Article 18.4 of the Constitution.

One of the biggest changes that the LOPDGDD introduces is new citizen rights for the internet age. Although many of them only constitute a reinforcement from the digital point of view to the rights regime already established in the GDPR, others are completely original.

List of digital rights:

- The right to universal access to Internet.
- The right to digital education.
- The right to privacy and use of digital devices in the workplace.

- The right to digital disconnection in the workplace.
- The right to privacy in front of video surveillance and sound recording at work.
- The right to digital will.

The GDPR does not apply to the personal data of deceased persons. Member states may provide for rules regarding the processing of personal data of deceased persons.

LOPD recognizes individuals have the right to digital testament. Moreover, the heirs of the deceased are entitled to exercise the rights to access, erasure and rectification of data unless the deceased person would have prohibited it, or this is not in line with applicable law.

The LOPDGDD includes a list of entities that must appoint a DPO as mandatory for their activity:

- Professional associations.
- Education centres, public and private universities.
- Entities that operate networks and provide electronic communications services.
- Providers of information society services when they develop large-scale profiles.
- Insurers.
- Credit finance institutions.
- Investment service companies.
- Health centres.
- Private security companies.

Competent authorities:

- Main data protection authority: **Agencia Española de Protección de Datos** (AEPD).
- Regional data protection authorities.

The **AEPD** is the body under public law, with its own legal personality and unlimited public and private legal capacity, **which acts fully independently of the public administrations** in the performance of its tasks. Its main function is **to ensure compliance with the legislation on data protection** and ensure its application, in articular as regards the rights of information, access, rectification, objection and cancellation of data. **The General Data Protection Register** is the data relating to files which are necessary to exercise rights of information, access, rectification, cancellation and objection.

Security measures:

- **Royal Decree 994/1999**, of 11 June, approved the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data. There were three levels of applicable security measures for files and processing: basic, medium and high. It was repealed by Royal Decree 1720/2007.
- **Royal Decree 1720/2007**, of 21 December, approved the Regulation implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data. It covered the area previously protected by Royal Decree 994/1999.