LUISS

Dipartimento di Impresa e Management
Corso di laurea in
Management and Computer Science

Cattedra: Business Cyberlaw

Different perspective of data protection: in China and European Union

Prof. Eugenio Prosperetti
RELATORE

Matteo Riccobono 260971
CANDIDATO

Anno Accademico 2022/2023

CAP. 1 INTRODUCTION TO DATA PROTECTION

- ***What is Data Protection***

To talk about the different perspectives of data protection in different countries, which in our case are Europe and China, we first need to introduce and analyze in depth what is data protection, its various facets and why it is so important.

Nowadays we are very used to being protected, there are a lot of regulations and directives which keep us safe everywhere we go; or maybe not. The differences in data regulations across countries are several, and that is why I chose to dive into them and elaborate on how they differ in the two biggest and influential countries in the world.

We can define data protection as the process of safeguarding data from any type of compromise, corruption or loss, while also providing the capability to restore the data if, for whatever reason, it had been made inaccessible or unusable.

What we are trying to do here is analyze how with the various regulations, directives and laws, the different countries can manage and control all the aspects of data protection.

When talking about data protection, we are dealing with all the processes, tools and policies which are used to restrict access to data.

These tools and policies are numerous, and especially in a business scenario, companies used them a lot to protect, not only their data, but also their processes and their way of working.

In fact, the term “data” is a concept much broader and wider than people think.

Data can come in the form of anything, such as text, observations, figures, images, numbers, graphs, or symbols. For example, data might include prices, weights, addresses, ages, names, temperatures, dates and distances.

In simple terms, data can be seen as a simple and pointless form of knowledge until with the proper techniques it is analyzed and organized, with the support of some context behind it.[1]

Data exists mainly in two types:

- Qualitative data
- Quantitative data

In qualitative research, non-numerical data is gathered with the intention of learning more about people's beliefs, biases, motives, decision-making processes, perceptions, and attitudes. This kind of information examines how people behave and focuses on the most fundamental study question: "Why?"

The majority of qualitative research uses uncontrolled experiments or control groups instead of open-ended questionnaires, focus groups, or interviews.

So, for instance, a music teacher who is listening to his students singing, and giving them feedback on how they sing, based on fluency, intonation, throw of words, clarity in pronunciation, without giving them an actual numerical value as a grade, could be an example of qualitative data.

[1] https://bloomfire.com/blog/data-vs-information/

The other type of data is quantitative data. Quantitative data is information that is expressed as counts or numbers, each of which has a specific numerical value. Data is any quantifiable information that may be used by academics for statistical analysis and mathematical computations so that they can derive practical conclusions.
An example of quantitative data could be when analyzing the balance sheets of a company, getting all the values of the revenues of that company month by month.
Data protection is obviously referred to both the two types of data, as it is very important to protect both of them, each one on a specific scenario and for different reasons.
In a big company like Apple, there are so many aspects that can be look into. From the sellers' point of view, the company probably really cares about the protection of numerical and quantitative data, as they might not want to share how their products are made, not to give any type of ideas or advantages to their competitors.
But if we think about it from the buyers' point of view, privacy might be the most important thing, they don't care about how the product was made, they just want to keep their texts and pictures hidden and private. The protection of qualitative data is more important to them.
And that is why the protection of all types of data is important, there is always going to be someone who is interested in retrieving data, and that data has to be protected.

- ***Data Protection vs Privacy vs Security***

When we mention data protection, it's important to make some distinctions. A lot of people often confuse the latter with concepts such as data privacy and/or data security. In fact, these terms are often misused interchangeably, as understanding the difference between them is quite challenging.
Roughly speaking, we can say that data protection spans two broad categories:

- Traditional Data Protection
- Data Security

These two terms have the same importance if we are aiming at achieving a proper control mechanism. That's why we need to understand clearly how they differ.
The differences between them are very slim, but they are still very true and relevant.
The main objective of data privacy, which is another term for data protection, is to ensure the physical person's right to access their information and know how their data is used and for what purposes. In essence, it protects the rights of individuals relating to their personal information.
Data security instead refers to protecting all information, not just personal data, from unauthorized access, corruption, or theft. The information can be digital or analog and belong to the natural person, the corporation, or other legal entities.
The CIA triad is the primary data security model that guides a company's safety procedures and policies,

and it consists of three major components or three principles of information security:

Confidentiality

It indicates that the information is only available to authorized partakers and has not been compromised by other parties. In addition, it must not be disclosed to people who don't have access to the data.

Integrity

Data integrity guarantees that the information is not deliberately modified, changed, edited, destroyed, or tampered with.

Availability

This component means that the data is available to authorized users when required.

- ***The relation between data privacy and technology***

Digital technologies have altered the marketing landscape, driven by the explosion of data. Parallel to this, serious privacy issues have disrupted consumer-firm connections, resulting in changes to governmental actions as well as people's own privacy-protective habits.[2]

Digital technologies give businesses access to enormous volumes of data, which they can use to boost their revenue (data monetization) or enhance the efficiency of their larger corporate networks (data sharing). Data monetization specifically refers to the firm's use of data to generate direct or indirect financial benefits. These procedures could involve using data analytics-based insights to create novel goods and services for the clients the data are intended to represent (data wrapping).

For instance, Coca-Cola gathers data from self-service vending machines and social monitoring enabled by AI-driven picture recognition technology to enhance consumer service and performance, such as the development of a Cherry Sprite flavor.

Utilizing insights to develop value-added capabilities for additional clients, such as expanded data wrapping, is another aspect of data monetization. Facebook, for example, makes money by providing data analytics features to advertisers based on user data on its social network platform. Finally, a direct approach to data monetization is for firms simply to sell their data to other firms.

Instead, data sharing refers to resource exchanges in which businesses distribute the data they have obtained, to different network partners (such as suppliers, distributors, and partners) in order to promote collaboration in the larger ecosystem. Coca-Cola, for instance, discloses information to consultants, hosting companies, and IT service providers in order to facilitate the provision of its services.

Other companies like Apple work with networks of suppliers and developers who very often exchange information to make better products and services.

These types of collaborations improve the performance of the entire digital community. So, data monetization increases firm profitability more directly, whereas data sharing improves profitability via

[2] https://pubmed.ncbi.nlm.nih.gov/35281634/

network performance.

Data specialists practice high degrees of data sharing and monetization. They control most of the data flows in the digital ecosystem and own a lot of data due to their large digital technological resources. To draw in new clients, they mostly execute extended data wrapping.

In other words, data professionals provide the data of their clients to other clients, like advertisers, who then utilize the insights to connect with their own target audiences.

In general, data sharing and monetization methods incorporate a wide range of digital technologies, each of which has the potential to be advantageous but also to raise privacy concerns.

Digital technologies assist businesses by allowing them to share and monetize their data, but they come at a cost to customers, particularly in terms of privacy.

In contrast to Sam Altman[3], CEO of Open AI, who sees privacy as "the selective control of access to the self" through social interactions and personal space, Alan Westin who was a famous professor of Public Law at the Columbia University (1967) defines privacy as a person's right "to decide what information about himself should be communicated to others and under what conditions".

We can define three categories of consumer privacy: informational, communicative, and individual, adopting the definitional precepts of autonomy, access, and control.

When all three types are taken into account at once, it expands on the existing marketing studies on privacy, which frequently concentrate simply on information privacy.

Information privacy specifically refers to a user's ability to manage who has access to, uses, and disseminates their personal data. People can thus choose when, how, and to what degree others will be able to access their information.

Communication privacy shields private conversations or messages from listening in, scanning, or intercepting. People prefer to maintain the privacy of their interpersonal communications, which would be impossible if conversations with friends were recorded by social media and messaging apps, or their in-person discussions were recorded by smart devices with built-in microphones.

Lastly, individual privacy means being left alone without disruptions. Threats to individual privacy involve personal space intrusions, emotional manipulation, and physical interference, including spam emails and retargeting practices. Such violations are on the rise, due to the presence of IoT and smart home devices installed in consumers' personal, physical spaces. In turn, firms' data strategies, enabled by digital technologies, have implications for each type of consumer privacy.

Businesses can enhance their marketing and business performance by creating market segmentation and (re)targeting strategies, creating personalized content, products, and experiences, and creating and fostering stronger customer relationships. This is done with the help of user-generated social media content, location insights from geospatial technologies, biometric data, and web tracking technologies like cookies.

---

[3] Sam Altman is an important programmer and entrepreneur, but most importantly he is the co-founder of OpenAI together with Greg Brockman, Reid Hoffman, Jessica Livingston, Peter Thiel and Elon Musk.

These practices threaten information privacy because consumers lose control over who has access to their personal information and communicative exchanges.

Geospatial data allows businesses to pinpoint the whereabouts of their clients; additionally, by tracking clients' digital footprints, they may follow them across other platforms, causing individual privacy problems.

Soft biometric data, such as those about moods or emotions, presents security and ethical issues because they are reflective of human feelings that might be exploited for profit, which would amount to invasions of personal privacy.

Due to the networked nature of social media, each user's information may also contain information about other users. When a user tags a friend in a public Facebook post, the two friends' communication privacy is violated if businesses look through these exchanges and profit from them.

Both data sharing and monetization practices in this domain can result in significant privacy tensions. An overall personal picture created through data aggregation and algorithmic profiling using big data analytics increases information privacy concerns, because it can reveal attributes which can be used to identify people such as personality, religious and political views or sexual orientation.

Furthermore, consumers are more susceptible to marketing effort when it is expected that their behavior will be accurately anticipated.

The enormous amount of historical and real-time data that links connected consumers, especially those who are close to one another through IoT devices. It increases the security concerns associated with identity theft, privacy violations, and intellectual property losses. Together, these behaviors pose a danger to both person and communication privacy because of their intrusiveness, invisibility, and extreme difficulty in being controlled.[4]

Also, especially in recent years, the development of high-tech tools and services as, for as Artificial Intelligence, robots and display technologies, made data free to be visualized through mixed, augmented and virtual realities. And obviously, in terms of data sharing this allows for immersive data presentation and experiences, which is a really vulnerable topic when talking about privacy issues; creating problems very similar to those created by the IoT services.

Information and communication privacy is at risk when the processed data is possibly also transferred to other applications such that the personal information of an individual is exposed to an unknown system.

Tensions over privacy are also a result of social behaviors that cause businesses and customers to react. As a result, even though legal frameworks and privacy norms have an impact on businesses and customers, those frameworks and norms are shaped and informed by consumer behavior.

So how can people and consumers react and actively protect their data?

The consumer protection behavior is not always the same and it varies as it needs in relation to the firm relationship with the customer, the level of fear of the firm and the level of trust that people have for a

[4] https://www.springer.com/journal/11747, “Digital technologies: tensions in privacy and data” article.

specific firm.

We can however identify four main protection strategies:

- *The reactive information protection strategy*
- *The proactive information protection strategy*
- *The reactive permission protection strategy*
- *The proactive permission protection strategy*

In response to privacy concerns, with the ***reactive information protection strategy*** customers can control immediate privacy dangers by modifying their digital footprint.

By deleting content from blog entries or Facebook postings, "untagging" themselves in pictures or posts, "unfriending" connections, or requesting that a company or social media platform remove their information, for instance, people can self-censor or filter content after it has been published.

Additionally, customers may purposefully withhold specific information in response to initial inquiries or otherwise falsify the data they do submit, such as by using a false name, address, date of birth, or profile picture. This tactic lessens their digital footprint by deleting or changing previously accessible content.[5]

A proactive information strategy instead, as opposed to managing already published content, defines consumers' ongoing behaviors of information withholding through constraint. Consumers limit activities like online check-ins that can reveal personal information, limit the quantity of personal content they publish online, and minimize their digital interactions.

To decrease the availability of data, they might also use encrypted communications or anonymous re-mailers (servers that receive messages with embedded instructions on where to send next and that forwards them without revealing where they originally came from). Some people look for non-digital substitutes for their purchases, information searches, and communications.

This tactic minimizes content and sociability since it limits information before sharing. Compared to a reactive information strategy, it typically requires more effort, complexity, and discomfort on the part of the user because it necessitates ongoing monitoring of the digital footprint.

When service providers request access to their personal information or act in response to an immediate hazard, such as a data breach that makes the risk apparent, customers who use a ***reactive permission strategy*** restrict that access.

Consumers frequently consent to granting access to their information, but they use this strategy to withdraw from risky situations. Examples of this include deleting apps that request location access, refusing or removing cookies from their computers, and blocking advertisements.

After threats or data breaches, a fortification of identity effort may involve doing things like changing passwords for example.

They can also reduce risk by ceasing company communications or by choosing not to participate in them

[5] https://www.springer.com/journal/11747, "Digital technologies: tensions in privacy and data" article.

in order to avoid intrusion and stop unauthorized access to information.

We observe more sophisticated measures and reactions such as ***the proactive permission strategy*** to secure personal information among customers who are more conscious of privacy issues and informed about digital privacy solutions.

With screening, they keep an eye on their own online behavior by confirming companies' privacy policies and safeguarding transactions (for instance, by utilizing https protocols).

Restriction is the process of controlling who has access to information by modifying privacy settings, such as disabling location-based access or modifying cookie preferences.

Another common tactic to avoid tracking is identity masking, which uses a security feature that prevents a browser from saving cookies and search history. Virtual private networks and The Onion Router are much more advanced tools that use encryption and build networks of virtual tunnels to anonymize internet conversations.

Lastly, if they adopt security consolidation, consumers install privacy-enhancing technologies, such as blockers and firewalls for third-party trackers, along with internet security programs. These strategies offer strong protection but also require substantial technological ability that is unlikely to be possessed by all consumers.[6]

In response to regulatory and consumer actions, firms might comply with privacy rules or go beyond them to engage in privacy innovation.

It is possible also for firm responses to define two main reactions:

- **Reactive response**
- **Proactive response**

A ***reactive response*** corresponds to the minimum expectation for a company to follow existing, regulatory frameworks. With this local approach to privacy regulation, firms only aim to meet specific, local privacy rules. This type of response is common among small and local businesses, but it also might be adopted by big companies, to take advantage in legal systems across specific markets.

For instance, businesses can address customers' reactive information strategies by enhancing their cybersecurity by reducing adverse occurrences like data breaches that could lead to consumers' falsifying, avoiding, withdrawing, or terminating communication acts. These businesses probably concentrate on technologies that allow them to follow regulations as well as possible.[7]

Privacy innovations are new or enhanced firm privacy management practices designed to benefit consumers, appease the government, or otherwise appeal to relevant stakeholders.

They appear when businesses actively incorporate compliance as a pillar of their operations and make an

---

[6] Zarouali, Brahim & Poels, Karolien & Ponnet, Koen & Walrave, Michel. (2020). The influence of a descriptive norm label on adolescents' persuasion knowledge and privacy-protective behavior on social networking sites. Communication Monographs. 88. 1-21. 10.1080/03637751.2020.1809686.

[7] https://www.springer.com/journal/11747, "Digital technologies: tensions in privacy and data" article.

effort to address privacy laws collectively by adopting a global perspective on privacy.
Firms identify critical compliance issues across regulatory frameworks instead of addressing each legislation and policy separately and establish a streamlined, uniform strategic plan that may direct all areas of their activity, as well as present and future standards.
By building a secure environment, pursuing privacy innovation can address the proactive privacy responses of even the most skeptical consumers and inspire trust, so it can decrease restraint and restriction behavior.
In this regard, privacy innovation presents an efficient way of dealing with both pro-active customer responses and legal requirements.
The resources that consumers have, like knowledge and self-efficacy, also influence their behavior. Reactive methods typically call for less technical knowledge, while proactive ones need more. Although they are still constrained by the structure, businesses can either take a reactive approach that regards privacy as a compliance issue or a proactive approach that sees it as a fundamental business value.
We rely on these trade-offs and tensions to provide an integrated framework that will enrich theory, practice, and policy. They characterize regulatory-consumer-firm interactions.

- ***First appearance of privacy and data protection***

Privacy had existed for a very long time prior to the 19th and 20th centuries, even though this is when it first became widely recognized as a right. The concept of privacy has a very long history, and its roots can be seen in ancient societies. Even in the Bible, there are several chapters when the invasion of privacy first took place and was met with humiliation and rage from the target. Just consider Adam and Eve, who first began to conceal their bodies with leaves to protect their privacy. From a legal perspective, the Code of Hammurabi featured a section prohibiting entering someone's home, and Roman law similarly addressed the same issue.
The concept of privacy comes from the distinction that has to be made by the individual, between himself and the rest of the world.
Obviously, the limits between public and private differ according to the specific society and also to the specific era, that’s why there is a constant change throughout the years of what is considered to be private and what is not.
Talking about privacy from a legal perspective, we cannot fail to mention the US Constitution that came into effect in 1789.
Even though it doesn’t explicitly mention and guarantee the right to privacy, the Supreme Court has found that the Constitution does provide for a right to privacy in its First, Third. Fourth and Fifth amendments.
But if we want to actually address the first appearance of privacy from a legal point of view, the article that has to be mentioned is the “Right to Privacy”.
The right to privacy is a law review article published in the 1890 Harvard Law Review. The writer of the

article is Justin Louis Brandeis but in the analysis of the latter, Samuel Warren was a very important contributor to the final version of it.

Samuel Warren and Louis Brandeis were two Harvard Law School grads who at the time were practicing counseling in Boston. Samuel Warren belonged to the Boston elite because of his family's prosperous lifestyle.

S. Warren came up with the topic for the piece, while L. Brandeis is most likely the author of the actual text. L. Brandeis was born in Louisville, a city in the South, and was the son of poor Jewish immigrants. L. Brandeis, in the words of D.J. Glancy[8], "brought a certain amount of objectivity and a more democratic approach to the argument for the right to privacy."

This well-known article was produced as a result of the two lawyers' collaboration. It is important to note that this was not their only joint venture; they also managed a law firm known as "Warren & Brandeis."

As previously indicated, one likely justification for the piece was the disclosure of details about S. Warren's personal life. However, it is difficult to say for sure whether that was the only factor. Literature suggests that there may have been others. For instance, the article might have been written to increase "Warren & Brandeis" brand recognition or just to create an engaging piece for the Harvard Law Review. Whatever the intentions, the effects it produced on the legal system unquestionably went above and beyond what the writers had anticipated.

The two lawyers said that the development of mechanical devices and the progress of technology had created great opportunities for interfering in the personal life of individuals. What the press did though was aimed at a different objective, and that is, using these new technologies to obtain great information to capture the attention of the readers. They didn't even think about the concept of privacy and permission.

According to the presumptions of S. Warren and L. Brandeis, privacy ought to be safeguarded by the law as a value in and of itself. They claimed that merely defending things like property and correspondence privacy wasn't enough. Instead, the right to privacy ought to be universal in scope[9]. The writers adapted T.M. Cooley's[10] definition of privacy, which he defined as the "right to be left alone."

This definition was adopted as the shortest and most frequent one.

The authors redefined what it means to defend oneself and one's property, laying the groundwork for the right to privacy. They considered a part of the right to life to be the right to enjoy life.

An important thing to say is that human feelings were starting to be considered as a legal protected value, and this is a great step up because finally personal inviolability was also being taken care of, not only bodily inviolability.

The publication of the article by Brandeis and Warren had a great impact on doctrine and society, in fact,

---

[8] https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1318&context=facpubs

[9] https://journals.akademicka.pl/adamericam/article/view/3223/2905

[10] Thomas M. Cooley was the Justice and Chief Justice of the Michigan Supreme Court between 1864 and 1885. He coined the phrase "the right to be let alone" in his treatise on the law of torts (1st ed. 1879)

it triggered an immediate response from people and numerous articles and publications started to come out on the same topic. People were debating a lot on the right to privacy itself, confronting theses, arguments and solutions to the problem of privacy.
This first idea of privacy and its legal protection was almost immediately put to the test by the American judicature.
In fact, in 1891 the Supreme Court of New York passed a judgement in the case of Schuyler vs Curtis, which deemed the publication of the image of a dead private person violation of law. The Supreme Court used the thesis of Brandeis and Warren to issue judgements in accordance with it.
From that point on, judgements based on "The Right to Privacy" were gradually spread throughout many state courts. We can mention for example cases such as Marks vs Jaffa or Roberston vs Rochester Folding Box Co.
Clearly though, data protection and privacy were still in their first phases, and they were still treated with caution and attentiveness. In fact, they were still trying to get the best legal conceptualization of data and privacy protection.
With the passing of time, the concept of privacy was being understood better and better and new regulations and laws came out that helped with the legal procedures for its protection.

CAP. 2 PIPL AND GDPR, DATA REGULATIONS IN CHINA AND EUROPEAN UNION

After describing in detail what is data protection, explaining every facet of it, talking about its types, how it was addressed first and how companies and customers faced it and dealt with it, with this chapter we are going to talk about the specific data protection regulations in two of the biggest and influential countries on the matter; that is Europe and China.

- **European Union**

The right to privacy was part of the 1950 European Convention on Human Rights, which stated, "Everyone has the right to respect for his or her private and family life, his or her home and correspondence[11]." From this basis, the European Union has sought to ensure the protection of this right through legislation.
For what concerns the European Union we need to start from far back. We can go back to the moment when the first data protection directive was made in Europe, in 1995.

- **Regulations of data protection before GDPR**

The first data protection directive was, in fact, issued on 24 October 1995, and it was called "The

[11] The European Convention on Human Rights (ECHR) protects the human rights of people in countries that belong to the Council of Europe. Art. 8

European Data Protection Directive". Officially it was Directive 95/46/EC, and it was about the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The directive came into force on 13 December 1995 and required all EU member states to implement the corresponding provisions in national law by 24 October 1998.

Let us briefly detail the contents of the first EU directive.

First, we need to state that in 1980, in an effort to create a better data protection system throughout Europe, the Organization for Economic Co-operation and Development, also called OECD, issued the "Recommendations of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data.

These Guidelines were primarily based on 7 principles that are:

- Notice: data subjects should be given notice when their data is being collected.
- Purpose: data should only be used for the purpose stated and not for any other purposes.
- Consent: data should not be disclosed without the data subject's consent.
- Security: collected data should be kept secure from any potential abuses.
- Disclosure: data subjects should be informed as to who is collecting their data.
- Access: data subjects should be allowed to access their data and make corrections to any inaccurate data
- Accountability: data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

The main issue with the guidelines, however, is that they were non-binding; meaning that they had no legal or binding force. This has led to data privacy laws still quite different across Europe.

The first six principles were incorporated into the European Data Protection Directive of 1995.

At the core of the Data Protection Act, in fact, there are eight principles which were used in the past by organizations and companies to design their own data protection policies. For companies complying with these principles was essential to meet their obligations.

The eight principles of the Act were as follows:

- **Principle 1 - Fair and Lawful**

- **Principle 2 - Purposes**

- **Principle 3 - Adequacy**

- **Principle 4 - Accuracy**

- **Principle 5 - Retention**

- **Principle 6 - Rights**

- **Principle 7 - Security**

- **Principle 8 - International transfers**

Now we will explain these principles in a more specific manner to understand them better.

Fair and Lawful

The first data protection principle gave individuals the right for their personal data to be processed fairly and lawfully by any organization.

"Personal data should be controlled and processed lawfully and fairly in relation to individuals".[12]

In this first principle is included the need to provide the data subject with a Fair processing notice, which contains various informations such as:

- The identity of the data controller
- The purposes for which the personal data is intended to be processed.
- To whom the personal data may be disclosed to.

Purposes

The second data protection principle placed a specific obligation on the controller to only use personal data for a lawful and justifiable purpose.

"Personal data should only be obtained if it will be used for a lawful purpose. It should not be processed for any means incompatible with the purpose[13]".

Adequacy

The third data protection principle placed an obligation on the controller to only collect the minimum amount of information required.

"Personal data should only be adequate to the purpose it will be used for. It must not be excessive to the purpose it will be used [14]".

Accuracy

The fourth data protection principle demanded the controller only collect, store and keep accurate information on the individual.

"Personal data should be accurate and up to date. If personal data becomes inaccurate, it can no longer be

[12] Data Protection Act 1998 principle 1
[13] Data Protection Act 1998 principle 2
[14] Data Protection Act 1998 principle 3

used for the purpose [15]".

Retention

The fifth data protection principle placed a limit on the amount of time the controller can keep personal information on the individual.

"Personal data should not be kept longer than it is needed for. Personal data cannot be stored indefinitely until such a time it may serve a purpose [16]".

Rights

The sixth data protection principle gave individuals the right to choose how their personal data would be used. People could choose how organizations who held data about them used that data in their activities.

"Personal data should be processed in accordance with the rights of individuals".

The Directive therefore provides the data subjects with the following rights:

- Access to personal data
- Preventing process likely to cause damage or distress.
- Prevent direct marketing.
- Automated decision making
- Correcting inaccurate personal data
- Compensation

Security

The seventh data protection principle placed a legal obligation on the controller to secure data against unauthorized or unlawful processing and against accidental loss or destruction.

"Personal data should be protected using reasonable and practical means to maintain its integrity and people's rights and freedoms [17]".

The Directive specifically states that controllers must adopt measures to prevent the following:

- Unauthorized processing of personal data
- Unlawful processing of personal data
- Accidental destruction, damage or loss to personal data

International transfers

The eighth data protection principle requires the controller to inform the individual of their intent to transfer their data overseas and to ensure the country it is being transferred to can adequately protect the data under their own laws.

"Personal data should not be transferred outside the EU unless the country it is being transferred to can ensure adequate protection of the data in order to maintain the rights and freedoms of data subjects and

[15] Data Protection Act 1998 principle 4
[16] Data Protection Act 1998 principle 6
[17] Data Protection Act 1998 principle 7

their personal data [18]".

After the Data Protection Act, there were a lot more directives to add some knowledge and importance to data protection, as the Directive 97/66/EC, on the protection of consumers in respect of distance contracts, which, adopted in 1997, by explicitly referencing Article 8 of the European Court of Human Rights (ECHR), implied the recognition of a 'consumer's right to privacy', protecting consumers against particularly intrusive means of communication.

To give a more formal definition, it defines its object as to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

With this Directive there were two main topics that were incorporated into the 1995 European Data Protection Directive, to increase its consistency and value.

The first one is a reference to the protection of fundamental rights and freedom in general, and the second one is an important mention of "free movement" of personal data.

Directive 95/46/EC, by its nature, obliged Member States to enact laws that implement its provisions, but It had no legal effect on the institutions and bodies of the Community. The Commission was aware of this and had included a statement stating that Community institutions must adhere to the same data protection rules as those established in the Directive with its 1990 draft Proposal.

To solve this issue, almost two years after the introduction of the European Data Protection Directive, the Treaty of Amsterdam was signed.

The Amsterdam Treaty[19] ensured that the legal implications of any provisions that time had rendered invalid or out-of-date were preserved while removing them from the European Treaties.

But what we want to focus on about the Amsterdam Treaty is Article 286.

This article stated that starting from January 1999, "Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data" shall apply to the institutions and bodies set up by the European Community Treaty.

So, Article 286 laid down the obligations of the European Community Treaty, but to implement them, in the same year, the European Commission adopted a proposal for a regulation on the protection of the individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data[20].

Following the path detailed above, the EU then adopt Regulation No 45/2001.

With this regulation, the purpose is to ensure that Community institutions and organizations uphold the

[18] Data Protection Act 1998 Principle 8

[19] The Amsterdam Treaty was signed on October 2nd 1997, member states agreed to transfer certain powers from national governments to European Parliament across the diverse areas.

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A11997E286

privacy rights of natural persons with regard to the processing of their personal data, and "shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC".

During the year 2000, the Directive 95/46/EC was the one which ruled over every facet of data protection. In the early 2000's, however, the Internet was morphing into the data giant that it is today. The 2000s, in fact, was an amazing decade for technology and forever established broadband as a necessity. There were approximately 21 million broadband users worldwide, and the number continued to increase year over year as new users signed up and dial-up internet users were migrating over to broadband service.

The years 2000-2003 gave us camera phones, USB flash drives, Bluetooth, iPods, the video gaming revolution, LinkedIn, and more[21].

All of these revolutionary changes set up the perfect stage for a data protection update that was needed from the Directive 95/46/EC.

In 2000, many financial institutions offered online banking. In 2006, Facebook opened to the public. In 2011, a Google user sued the company for scanning her emails. It was after that, that Europe's data protection authority declared the EU needed "a comprehensive approach on personal data protection" and work began to update the 1995 directive[22].

That is why to safeguard online privacy rights and advance Europe's digital economy, the European Commission (EC) recommended a thorough update of the EU's 1995 data protection laws on January 25. The GDPR Draft Regulation [23]was warmly received by the European Data Protection Supervisor (EDPS) since it represented a significant improvement in European data protection. Individual rights would be strengthened under the proposed regulations, and controllers would be held more liable for how they handle personal data.

Additionally, the function and authority of national supervisory authorities are effectively strengthened, both individually and collectively.

- **The General Data Protection Regulation**

In place of the 1995 Data Protection Directive, the GDPR[24] was approved in 2016.

It is the outcome of a difficult negotiation process that took four years before the approval of the finalized Regulation and involved multiple revisions to the legal text.

The dispersion of data privacy laws among EU Member States and the ensuing legal ambiguities were seen as obstacles to the development of the EU's economy and a source of competitive distortion.

The Regulation, unlike the Data Protection Directive, is self-executing, necessitating no additional implementation by EU Member States.

---

[21] https://connectednation.org/blog/2021/04/20/technology-throughout-the-2000s/

[22] https://digitaleducation.tdm2000.org/topic/topic-1-introduction-to-the-european-general-data-protection-regulation-g-d-p-r/

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011 2012

[24] Published April 27 2016

The GDPR increased legal clarity by equating the data protection laws and eliminating any potential barriers to the free flow of personal data.
With GDPR, more and more companies faced not only new data protection obligations but also a reinforcement of updated pre-existing obligations.
As legal obligations were updated, also the pertinent fines were significantly increased, that is why companies would have to be a lot more careful and reorganize their internal data protection procedures in order to reach compliance with GDPR.
To better understand its revolutionary contents, let us examine the material scope of the regulation itself. We can examine Article 2, which reads as follows:

"This Regulation 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."
The GDPR, therefore, applies to any processing of personal data. We can see that the material scope of the regulation can be interpreted in a very broad manner, this is done on purpose so that a high level of protection can be ensured.
From the above definition we can notice two main words which are very important, and it is important to clearly understand the exact meaning of it.
The first word is "processing". This can be automatic or manual but in the GDPR both types are included. "Processing" means any operation or set of operations that is performed on personal data or on sets of personal data. Therefore, any treatment of data such as organizing, storing or collecting, is considered as "processing".
The other important word is "personal data". Data is said to be personal if the information relates to an identified or identifiable individual. In fact, according to Article 4 of the GDPR, Data is therefore personal if the identification of a person is possible based on the available data, meaning if a person can be detected, directly or indirectly, by reference to an identifier.
Example of personal data could be something very basic such as a person's name or something like a location data or maybe a social insurance number.
Diving down into the topic of personal data, it could be useful to mention the concepts of anonymization and pseudonymization.
Anonymization is a way of modifying personal data so that as a result there is no connection of data with an individual, so the persons whose data belongs to is no longer identifiable.
Anonymization of personal data can happen in different ways.
The first example is the generalization of data; this means generalizing characteristics of data subjects by changing the scale or order of the data. An example could be using months as an attribute instead of using weeks.

Another example is the randomization of data; modifying the accuracy of data in order to remove the link between the individual and its data.

If the anonymization of personal data is done properly, then the GDPR does not apply. Nevertheless, if anyone can restore the original information then data will be deemed as personal data under the provision of the GDPR.

Data anonymization obviously has some benefits, for example the possibility for companies to collect anonymized data reducing the risk for data misuse and preventing data breaches victims.

That is why entities should take the coming into force of the GDPR as an opportunity to consider using anonymization as a tool to safeguard privacy.

The other important concept is Pseudonymization; this process is defined as "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.[25]"

This process can be done in many ways, e.g by alternating particular information in the data with certain indicators.

The additional information or indicators which allow for the identification of the data need to be kept separately.

An interesting technique used for pseudonymization is called "encoding", that is the process of putting a sequence of characters into a specialized format for efficient transmission or storage.

These characters then, can only be read with a special key that can be shared with whoever you want to be able to read your data.

Pseudonymized data, in contrast to anonymous data, nonetheless falls under the GDPR's purview of applicability because there is a greater chance of re-identification with pseudonymized data than with anonymous data. However, pseudonymization represents one way for processors and controllers to comply with their GDPR data protection obligations because it makes it easier to demonstrate compliance with the Regulation.

We answered the question that asked in which case the GDPR applies, now to clarify everything we need to know to whom the regulation applies to.

From earlier we know that the GDPR applies to anyone processing or controlling the processing of personal data. From this we can extrapolate the words "processor" and "controller".

We will start with the definition of controller as the definition of processor is easier to be stated when we already have the one of the controller.

The legal definition of controller is: "a natural or legal person, public authority, agency or other body that alone or jointly with others determines the purposes and means of data processing[26]".

Controllers make decisions about processing activities. They exercise overall control of the personal data

[25] GDPR art. 4 comma 5

[26] GDPR art 4 comma 7

being processed and are ultimately in charge of and responsible for the processing.[27]
Processors instead act on behalf of the relevant controller and under their authority.
In doing so, they serve the controller's interests rather than their own.
Even though also processors can make some operational decisions, if we look at the GDPR we find out that there is a specific article, that is, Article 29 that says that the processor should only process personal data in line with a controller's instructions, unless it is required to do otherwise by law.
As it is clear by now, the beneficiaries of the GDPR are individuals in general. All individuals, regardless of their age, benefit from protection under the GDPR.
It's important to say that children benefit from specific protection under the GDPR because they may be less aware of the risks that they can face, and they may not know all their rights in the relation to the processing of personal data.
A very interesting thing is that legal entities are not entitled to benefit from protection under the GDPR. This is because the GDPR wanted to enforce the protection of individuals.
Nonetheless, if the legal entities data contains information on the individuals associated with the legal person, then data could be seen as personal data and fall under the provision of the regulation.

- **The concept of accountability**

Whereas the former Data Protection Directive did not explicitly emphasize on accountability, the GDPR introduces the general principle of accountability in Art. 5, which imposes the responsibility for the compliance of processing with the GDPR and the burden of proof for said compliance onto the controller.
The controller basically had to do two important things; the first one is to be able to ensure compliance with the GDPR and the second one is to be able to prove compliance to any Supervisory Authorities.
The concept of accountability principle is a major one as it is enforceable, and fines can be applied to the controller or processor.
The accountability principle will increase the controller's comprehension of and actual commitment to data protection because it will be required to put in place the proper organizational and technical safeguards before starting its processing operations in order to prevent GDPR violations.

- **The main points of GDPR**

After clarifying the main definitions, I want to talk about the main points and articles of the General Data Protection Regulation.
For the purposes of this analysis, we shall exemplify and group the most important concepts contained in the GDPR in the three main rights of the data subject:

- **The right of individuals**

- **The right to be informed**

[27] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/

- **The right to erasure**

Right of individuals

As we already stated, protection of individuals and personal data is one of the main concepts of the GDPR and there are many articles that can confirm it.

Mentioning the most important articles:

ART 6 Lawfulness of processing

"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 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.*
- *processing is necessary for compliance with a legal obligation to which the controller is subject.*
- *processing is necessary in order to protect the vital interests of the data subject or of another natural person.*
- *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.*
- *processing is necessary 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, in particular where the data subject is a child."*

This article basically states that processing of data subject's personal data is lawful only under certain circumstances, including when the individual gives consent to the processing of the personal data for a specific purpose.

ART 15 Right of access by the data subject

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- *the purposes of the processing.*
- *the categories of personal data concerned.*
- *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations.*
- *where possible, the envisaged period for which the personal data 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 of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.*
- *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;"*

This article states that clients can ask if the company gathers and uses their personal information, and if they do, companies are obliged to tell their costumers why they process their data, which types of personal data is being processed and how long the data will be stored.

Right to be informed

Recital 58

"The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used.
Such information could be provided in electronic form, for example, when addressed to the public, through a website.
This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.
Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

I think it's great to cite this recital because it obliged the company to tell its customers how their personal data is being used and it touches the principle of transparency.

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 where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent on which the processing is based according to Article 6, or Article 9, and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21.
- the personal data have been unlawfully processed.

- Personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- the personal data have been collected in relation to the offer of information society services referred to in Article 8".

This article gives the right to customers to have their personal data erased in certain circumstances.

- When their personal data is no longer needed for the purpose, it was originally collected.
- When they withdraw consent
- If they object to the processing of their data
- If their personal data has been unlawfully processed
- If their personal data must be erased in order to comply with a legal obligation.

- **The differences with the Data Protection Law of 1998**

There are some important differences between the two regulations and some of them are key updates that revolutionize the way of looking at Data Protection.
Since we already mentioned it earlier, we can start with the principle of **accountability**.
Businesses must demonstrate their adherence to GDPR principles by, among other things, putting in place the necessary organizational and technical safeguards (such as internal data protection policies), keeping accurate records of their processing activities, and, where necessary, appointing a data protection officer. Compliance is no longer just an easy task that can be overlooked. It requires constant knowledge and accountability.
Another important change regards the way **consent** is looked at.
This must be freely supplied and unmistakable for a certain goal by a definite, deliberate action. Businesses will need to be able to establish that consent was lawfully obtained, and that the data subject supplied this consent. The information gathered must only be utilized for the intended reason and kept on file for as long as it takes to complete that purpose. Additionally, specific information about how to opt out or request that personal data be removed must be made available.
If we look at the territorial scope, there has been a key update, especially with the introduction of Art 3 of GDPR.
This article applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to, either 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 behavior as far as their behavior takes place within the Union.
The last two major changes were the increased **enforcement powers**, as GDPR significantly increase the maximum fines for non-compliance up to €20 million or four per cent of global turnover, and the

new obligations for data processors as GDPR introduced direct compliance obligations for processors (those who process personal data on behalf of another person who controls the data) meaning that processors may be liable to pay non-compliance fines.

- **Italian updated privacy code**

  Italy amended its Personal Data Protection Code (the Code) to comply with the General Data Protection Regulation (GDPR).

  The Italian Data Protection Authority, also called "Garante per la protezione dei dati personali", which oversees the GDPR and the Code, also handles complaints from data subjects, offers specific data protection measures for data controllers and processors, and adopts guidelines to help organizations comply with personal data protection laws.

  The main reason for the Italian personal data protection law being introduced was in order to abandon the implementation of the previous Data Protection Directive (Directive 95/46/EC) and to implement the new provision of the GDPR.

  Most of the article in Italy presents no differences with the GDPR.

  One of many roles executed by the Garante was enacting a general guide on the application of the GDPR, which provides a very helpful guidance on how to apply it to specific cases in Italy.

- **China**

  The internet law

  The history of China regarding data protection has been processed differently with respect to the one of the European Union but there is one thing that can be said that is very important for the concept of data protection, and that is the relation between China and the Internet.

  The Great Firewall[28] is the People's Republic of China's combination of domestic Internet regulation technology and legislative measures. Its function in China's internet censorship is to impede cross-border internet traffic and prohibit access to particular foreign websites.

  The great firewall uses transmission control protocol packets to scan for keywords or sensitive terms; if these keywords are found, the access will be blocked.

  As a result, international firms are compelled to obey local regulations, access to foreign information sources is restricted, and foreign internet tools (such as Google Search, Facebook, Twitter, and Wikipedia) are barred.

  China believes that the internet should be managed by its own government and be considered part of its sovereignty.

  The following factors contribute to Internet restriction in China:

- Social control: The Internet allows for freedom of speech, and the spread of campaigns may spark protests against the administration.

[28] The Great Firewall was deployed in China as early as 1996, under the direction of the Chinese Ministry of Public Security.

- Sensitive Content: Controlling information on the Chinese government.
- Economic protectionism: Because they have more control over them, China wants to use domestic businesses that are subject to Chinese regulations.

We understood that China processes the topic of internet access in a stricter way than the European do. This means that the Chinese government has implemented its own type of internet into their community with their own rules and regulations.
In fact, if in Europe we have Google as the most used search engine, in China the most used search engine is called "Baidu".
Even with the limited access and even though only 50% of the population uses internet, China is the country with the largest number of users in the world. In fact, there are more than 650 million internet users in China today and the number keeps increasing.
The Chinese government's targeted policies are the reason for the Internet user base's rapid expansion. The most recent Five-Year Plan gives the economy's overall digitization and the expansion of the internet sector top priority. The internet China policy, which the government also unveiled, aims to achieve nationwide internet coverage by 2020. This indicates that the number of Internet users is growing and is unlikely to slow down soon.

- **Cybersecurity law**

Missing important regulations for internet access in China, one of the first law that was introduced is called the Cybersecurity law.
Before explaining what, the Cybersecurity law is and what it is about, we need to mention and introduced the China's Cyberspace Administration (CAC)[29].
This entity is involved in the implementation and formulation of policies regarding a variety of issues related to the cyberspace and more in general the internet in China. It is under the jurisdiction of the Central Cyberspace Affairs Commission, which is a subordinated party institution of the Central Committee of the Chinese Communist Party.
Its main function is to centralize, coordinate and rationalize administrative measures and regulations regarding online content.
In fact, although prior to 2012 the Chinese was largely unregulated, several State authorities, such as ministries, had been competing, in order to gain control and competences over the booming digital economy. Although the Ministry of Industry information and technology (MIIT), had been formally appointed to coordinate interventions by other State authorities, a satisfactory degree of coordination was never achieved, until the creation of the CAC.
The Cybersecurity Law of the People's Republic of China, commonly referred to as the Chinese Cybersecurity Law, was enacted by the National People's Congress with the aim of increasing data

[29] The Cyberspace Administration of China is the national internet regulator and censor of the People's Republic of China. Founded in 2014 by the Central Cyberspace Affairs Commission.

protection, data localization, and cybersecurity, in the interest of national security. The law is part of wider series of laws passed by the Chinese government in an effort to strengthen national security legislation.

Cybersecurity is acknowledged as a fundamental right. This places the statute at the summit of the pyramid-shaped framework of cybersecurity legislation. The law is an outgrowth of the cybersecurity rules and regulations that already existed at different levels and in different industries, incorporating them to produce a macro-level, structured law.

The cybersecurity law was enacted in 2016 with the goal of being put into force on June 1, 2017.

It is composed of 7 chapters and 79 articles, but it is fundamental to report the most important concepts in my opinion.

Network operators are officially required to censor content and remove any prohibited material. The law states that "any person and organization shall, when using the network, abide by the Constitution and laws, observe public order and respect social morality".

It also expands to what is considered illegal content to be circulated online: "activities harming national security, propagating of terrorism and extremism, inciting ethnic hatred and ethnic discrimination, dissemination of obscene and sexual information, slandering or defame others, upsetting social order, harming the public interest, infringing of other persons' intellectual property or other lawful rights and interests"[30].

If we look at Chapter 4 of the Cybersecurity law, it prescribes punishments and penalties for people who violate the law. This chapter provides great insights for legal responsibility in China. It provides the regulations for fines that can go up to one million dollars and can be applied to both individuals and organizations. Repeated violations will result in temporary or permanent service suspensions, revoking business licenses, freezing assets and criminal responsibility.

When examining the cybersecurity law, we should consider the idea of anonymization. This is as a result of its intriguing perspective. In fact, you might believe that making online users anonymous would aid in preventing attacks on personal data, but this rule is applied differently in China.

As a matter of fact, the legislation ensures that users' online anonymity will no longer be tolerated; as a result, all social networks and messaging services operating in China now require users to provide identity verification.

Only real names must be used, and providers are expected to verify customer personal information and reject service to anyone who does not comply.

Before the regulation went into force, several Chinese internet companies were gradually following these criteria. Retroactive action was taken against past users who weren't properly verified once it became official. Account suspension now usually follows failure to pass verification.

Another important concept comes from Article n. 31 that states that people's personal information

[30] https://sampi.co/china-cybersecurity-law/

must be stored within China borders. In addition to personal data, the regulation loosely defines "other important data gathered and produced during operations" which must also be stored on local servers.

Companies who now have to send customer data overseas for processing have already been impacted by this necessity. These businesses will no longer be able to carry on like this without requesting a government permit. Some consumers were not very happy when some international tech companies, like Apple for example, were obliged to store their customer data locally.

- **E-commerce law**

Before analyzing the main and biggest regulation about data protection in China, the PIPL, it is interesting to take a look at a law that became effective from the very first day of 2019, the E-commerce law.

The traffic of users in the e-commerce world was becoming heavier and heavier, there was a need for a regulation to contain all the problems related to it.

In order to conduct business in China, e-commerce operators must act as a legitimate business entity and abide by all applicable legal and administrative requirements. In reality, all e-commerce providers of goods and services must register as a business in accordance with applicable laws, obtain a business license (save for situations where registration is not required by applicable laws and administrative regulations), obtain the necessary administrative licenses, and pay taxes. E-commerce platforms are responsible for providing open, fair and just services to third-party businesses on the platform.[31]

The department of market regulation must get business and tax identification from third-party firms. The e-commerce operators will issue a warning to any unregistered firm using the platform and require it to register in accordance with all applicable statutes, laws, and regulations. The platform must notify any violations of business and tax registration to the appropriate government agency.

For what concerns consumers, they are entitled to a right to know and right of choice. Information of commodities or services shall be disclosed in a comprehensive, accurate and timely manner. And false or misleading publication, such as fictitious deals and fabricated user comments, is forbidden. Equally, comments on services or goods provided by an e-commerce operator on e-commerce platforms cannot be deleted.

- **Personal Information Protection Law (PIPL)**

After describing important data protection laws and regulations, we are going to analyze the most important one:

the Personal Information Protection Law (PIPL).

[31] http://mg.mofcom.gov.cn/article/policy/201912/20191202923971.shtml

This law was adopted on August 20, 2021, and became effective on November 1, 2021[32]. It builds on top of the previously described Cybersecurity law, and it is similar to and partly based on the GDPR. It comes clear that, it brings updated on the protection of personal information rights and interests, standardization of personal information handling activities and promotion of the rational use of personal information. It also addresses the handling and transferring of personal data outside of China.

We can see the PIPL as the thing that made to refine and improve the old regulations. In fact, although China's fundamental laws, such as the Civil Law and the Criminal Law, include provisions for personal information protection, most of these rules are dispersed and do not offer a comprehensive or systematic protection of personal information.

The specialized personal information protection legislation now has a legal and logical foundation thanks to these sporadic measures. The PIPL has created a comprehensive system of methodical, specific, and workable specialized regulations on the basis of these regulations.

- **Scope of application**

The PIPL applies to the handling of personal information of people within the People's Republic of China and also outside the PRC, where all kind of personal information is handled for the purpose of providing products or services within the territory of China, or also to analyze and assess the conduct of people within the territory of China.

- **Key principles**

The PIPL establishes several principles that must be complied with when processing personal information.

Personal information processing principles

Article 5 to 9

The criteria of legality, propriety, necessity, and creditworthiness must be respected when processing personal information, and controllers must avoid using deceit, fraud, or coercion.

In addition to the aforementioned, the PIPL mandates that processing of personal information adheres to the principles of purpose specificity, usage limitation, transparency, quality, and accountability. More specifically, the PIPL states that treatment of personal information must be done with the least amount of interference to people's rights and interests and with a purpose that is both explicit and fair. Additionally, responsible parties must assure the quality of the personal information, including making sure it is correct or full, and the processing of personal information must adhere to the principles of openness and transparency.

Retention and storage limitation

[32] https://www.cyberlaws.it/en/2021/personal-information-protection-law-pipl-china/

According to Article 19, except as otherwise permitted by laws and regulations, the PIPL mandates that personal information must only be kept for as long as is necessary to achieve the handling purposes.

According to article 10, the PIPL sets a general ban on unauthorized processing that jeopardizes public interest and/or national security. More specifically, the PIPL states that businesses and individuals are prohibited from buying, selling, disclosing, or otherwise using someone else's personal information. It also prohibits them from engaging in personal information handling activities that jeopardize public safety or national security.

The handling of personal data is, therefore, executed lawfully only if one of the following circumstances are met:

- the individual's consent is obtained.
- as necessary to conclude or perform on a contract to which the individual is a party, or as necessary for carrying out human resource management in accordance with lawfully formulated labor rules systems and lawfully concluded collective contracts.
- as necessary for the performance of legally prescribed duties or obligations;
- as necessary to respond to public health incidents or to protect natural persons' security in their lives, health, and property in an emergency.
- handling personal information within a reasonable range in order to carry out acts such as news reporting and public opinion oversight in the public interest.
- for a reasonable scope of handling of personal information that has been disclosed by the individual or otherwise already legally disclosed in accordance with this Law; and
- other situations provided by laws or administrative regulations.

Also, the PIPL states that consent must be given explicitly and voluntarily by people who are fully aware when it comes to handling personal information based on consent. Additionally, if laws and administrative rules stipulate that a third party's written or independent authorization is required before handling personal information, those rules must be observed. Additionally, agreement must be obtained anew if the intent behind, the procedures for processing, or the categories of personal information involved change.

Data subjects also have the right to revoke their consent, and this process must be simple and convenient. However, the validity of personal information processing actions carried out prior to the people’s consent withdrawal is unaffected by it.

Information disclosure and sharing

The PIPL forbids controllers from exposing the personal information they hold, except with agreement or as otherwise permitted by laws and administrative regulations.

Within a reasonable extent and unless the individual specifically objects, controllers may process personal information that has been legally disclosed or disclosed by the individual themselves. When

handling disclosed personal information that materially affects a person's rights or interests, however, personal information handlers are required to get that person's consent in compliance with the PIPL's rules.

Sensitive personal information

The PIPL provides that controllers may only use sensitive personal information for predetermined objectives, when absolutely necessary, and with the use of stringent security controls.

In addition to the aforementioned, controllers handling sensitive personal information must get separate consent and, if laws and administrative regulations permit it, written consent. In addition, when handling sensitive personal information, controllers are required to notify individuals of the necessity of handling sensitive personal information as well as the impact on their rights and interests, unless this Law specifically states that such notice is not required to be given to individuals.

- **The most important differences between GDPR and PIPL**

Scope of application

The GDPR places additional emphasis on the "establishment" of the business that processes personal information, and most of the time, this "establishment" refers to the location of the firm. If the business is based in the EU, the GDPR will govern any personal information processing activities carried out by the business, whether they take place inside or outside the EU.

The PIPL, in contrast, is more concerned with the location of the personal information processing activity. The PIPL is relevant if the personal information processing activity takes place on Chinese territory, either by a Chinese corporation or a foreign company without an office there.

This entails that if a company established in China processes personal information of people in countries that are not China itself, the PIPL does not apply to the company’s processing activity, because it does not take place in China.

Data controller and processor vs Personal information Handler

In article 4 of the GDPR, there are described the roles of the data controller as the one who chooses method and purposes for processing personal information, and the data processor as the one who handles that information on the controller’s behalf.

The PIPL instead specifies the duties in a different way, defining the role of a "Personal information handler". In fact, there are various situations where the handler's duties overlap with those of the controller and processor.

Personal information

Both the GDPR and the PIPL have a similar definition of personal information, but the PIPL explicitly excludes “anonymized” personal information from the definition.

Also, the scope of sensitive personal information under the PIPL is much broader than the special category data under the GDPR. In fact while the GDPR lists all special category data in a clear way, the PIPL does not include a full list on what to identify as processable personal information.

PIPL has a descriptive article about it, Article 28 that cites "Personal information that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property once disclosed or illegal used".

Consent

One common legal justification for processing personal information under both the GDPR and the PIPL is consent from persons or data subjects.

However, the PIPL specifies additional conditions for consent based on the sensitivity of the personal information and the context of the processing. When processing sensitive personal information, especially in situations like sharing the personal information with another party or transporting it outside of China, for instance, the PIPL mandates that the personal information handler seeks separate agreement from the individuals involved.

The GDPR allows companies to process PI for the purpose of legitimate interest pursued by the controller or by a third party.[33]

Authorities for supervision

Each EU member state is required by the GDPR to set up its own monitoring authority for the protection of personal information.

In order to ensure uniformity, it also governs the qualifications of lead supervisory authority when there are multiple supervisory authorities present. This is established so that, that while conducting business in an EU nation, enterprises may only have to deal with one supervisory entity.

In China, the situation is more complicated since different laws and regulations overlap, different supervisory bodies are appointed, and multiple authorities have the authority to enforce privacy protection rules.

Three main entities, in fact, share different level of authority in the field of privacy: the Cyberspace Administrator of China (CAC), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Public Security (MPS).

Data localization

The main difference is that the GDPR implements the requirements by country while the PIPL implements them on a case-by-case basis.

Data localization, if we talk about cross-border data transfer, is really a problem in China. This is because by being a case-by-case process, it takes a long time to be possible.

In fact, to be able to cross-border data there are a lot of requirements and also the application of other laws, such as the Cybersecurity law, that we have talked about earlier, and the Data protection law.

CAP. 3 CASES OF IMPORTANT DATA BREACHES

- Europe

[33] GDPR art 6 lawfulness of processing.

Before dealing with two cases of important data breaches in Europe and China, it is mandatory to explain how these two big countries handle data breaches as well as the differences and similarities between them.

Guidelines on personal data breach notification for European Union Institution and Bodies

In 2018, the Guidelines on personal data breaches were issued, with the scope of providing advice to the European Union Institutions and bodies, intending to help them to respond effectively to personal data breaches. The Guidelines make it easier for EUI[34] to adapt and develop their processes for the management of personal data breaches, to fulfill their obligations and to comply with them towards the EDPS[35] and the individuals.

It is also key to say that these guidelines will be updated as the European Union Institution develops experience and learn how to deal better with data breaches and communication pursuant to the Regulation.

We can also state that these Guidelines are an integration of what the GDPR already had regulated concerning data breach rules. Their main procedures are, in fact, just slightly different and updated with respect to the GDPR ones.

Assessing the risk

The first thing to do when a data breach happens is understanding how much risk there is behind it.

To do so, there is the need to conduct a research case by case, as every case can be different and procedures may differ.

The first article that has to be mentioned is Article 34 of the Regulation, that follows the risk based approach adopted by the GDPR.

Article 34

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.

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures written below.

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular*

[34] European Union Institutions.
[35] European Data Protection Supervisor

those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

- *the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*
- *it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.*

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

This article, that helps in the assessment of risk is crucial as a starting point, because it will determine if the data breach has to be communicated to the data subject, in fact this happens only if it is a very high-risk personal data breach where the safety of the data subject is threatened.

Right after the assessment of the risk, there is the procedure which concerns the notification to the EDPS.

The EDPS will be notified also in order to enabling him to verify compliance of the European Union Institution also for data breaches which were not notified.

Notification to the EDPS

Unless it is highly unlikely to put people's rights and freedoms at risk, an EUI must notify the European Data Protection Supervisor of a personal data breach no later than 72 hours after it occurs. An EUI should additionally inform data subjects if the personal data breach poses a "high risk" to their rights and freedoms.

The notification procedure to the EDPS involves: on one hand “the controller” on the other hand, the person in charge of data protection matters, like the Data Protection Officer (DPO).

As a controller, it's crucial to include personal data breach clauses in contracts with any vendors who serve as processors, obliging them to alert you right away in the case of a breach and provide all pertinent details.

In the event that you discover a breach of personal data, you have a responsibility to notify the relevant controller(s) very away and to provide all pertinent information.

Following after, the controller is required to immediately notify the DPO and make sure that they are both involved in the management of the breach and the reporting procedure (both to the EDPS and the data subject).

[36]

Communication to the data subject

When a breach of personal information poses a significant risk to the rights and liberties of natural beings, as defined by Article 35 of the Regulation, the controller is required to notify the data subject of the breach without undue delay.

The message should include information on the type of personal data breach and suggestions for the natural person affected to reduce any potential negative impacts.

Such notifications to data subjects should be sent as soon as it is practical to do so, in close coordination with the EDPS, and in accordance with its recommendations.

The EUI should also, when necessary, give individuals detailed information on how to safeguard themselves from any potential negative effects of the incident, such as resetting passwords in the event that their access credentials have been compromised. Again, in addition to what is necessary above, a controller may opt to submit additional information.

COSMOTE Mobile Telecommunications

COSMOTE Mobile Telecommunications is the largest mobile network operator in Greece with its headquarter in Athens.

It is an owned subsidiary of the Hellenic Telecommunications Organization (OTE), a telecommunication provider.

Personal data breach

Between 01/09/2020 and 05/09/2020, there has been a subscriber call data leakage of COSMOTE Mobile Telecommunications, which has put in danger the privacy and safety of most of its subscribers.

This caused a big investigation to start, which revealed violations on behalf of COSMOTE, for what regards the principles of legality and transparency, due to incomplete and unclear information to subscribers. COSMOTE has also been filed for faulty conduct of the impact assessment, faulty implementation of the anonymization procedure and insufficient security measures.

[36] Diagram for controller accountability.

This resulted in The Hellenic Data Protection Authority (HDPA) to publish on January 31st, 2022, its decision, in which it fined COSMOTE Mobile Telecommunications $6,000,000 for the violations of Articles of Laws such as:

- Articles 5 and 6 of the Electronic Communications Law, concerning the permissibility of the handling of personal information in the context of the offering and utilization of electronic communications services.
- Article 12 of the Electronic Communications Law, for failing to put in place the proper organizational and technical security safeguards to ensure both the security of the public electronic communications network and the security of its services.
- Article 35 of the GDPR, for the Data Protection Impact Assessment's inadequate content, particularly with regard to determining the necessity and appropriateness of the processing.
- Article 5, 13 and 14 of the GDPR, because of the unclear and insufficient information given.
- Article 25 of the GDPR, for failing to put in place the proper organizational and technical security controls to guarantee the effective execution of the anonymization process.
- Article 25 and 28 of the GDPR, due to the OTE Group's lack of a comprehensive understanding of the roles involved in the procedure in question. In this regard, the HDPA stated that, in the case of joint controllership, the division of labor and cooperation between the two businesses should have been based on an agreement in accordance with Article 26 of the GDPR, or, in the case of a processor, on another agreement or legal act in accordance with Article 28 of the GDPR.

Noticeably the HDPA in deciding the fine, it has taken into account and consideration the long duration of the infringement (6 years), the high number of affected users (over 10,000,000) and the fact that even after calls were made, there was no implementation of pseudonymization measure.

- **CHINA: General data Security Breach Notification Requirements**

  The PIPL offers a comprehensive procedure for breach notification.

  Personal information processors must take immediate corrective action and notify the relevant individuals as well as the personal information protection authorities in the event that personal information is lost, leaked, altered, or otherwise compromised.

  The notification should contain details like:

- categories of personally identifiable information at risk, reasons for occurrences, and consequences of a data breach incident

- remedial actions done by personal information processors, potential mitigation actions from affected individuals, and

- the personal information processor's contact details.

Personal information processors may decide not to notify the individual in question if they believe that the precautions adopted can stop any harm brought on by the leakage, tampering with, or loss of information. However, if personal information protection authorities believe that the leak of personal information may harm the individuals affected, the authorities may still demand that the processors of personal information notify the individuals.

Controllers and Processors notification procedure

The CAC and its local counterparts are the bodies in charge of managing and monitoring the protection of personal information generally under the PIPL. It is unclear under the PIPL which regulators are accountable for the handling of data breach notifications, however, given there are other Chinese regulators who are also vested with the task of protecting personal information.

Affected individuals

No particular requirements are stated. According to the PIPL, the personal information processor may be excluded from notifying the affected individuals if efforts have been taken to effectively stop the information leak, unauthorized alteration, or loss from causing harm. However, the competent authority may order the personal information processor to notify the affected individuals if it determines that further harm could result from the occurrence. As a result, corporations now have some discretion to decide whether or not to notify the affected individuals, unless expressly obliged by the relevant authorities.

In accordance with the PIPL, controllers are required to inform by default. However, because the CSL's notification requirements apply to all network operators, without distinguishing between controllers and processors, it is also acknowledged that controllers and processors may agree on who will notify individuals in the event of a personal data breach.

Chinese TikTok app data regulation controversy

Due to its potential to jeopardize Western security, the popular social media app TikTok has raised questions. The Chinese government allegedly has the capacity to use the application for data collecting, algorithmic control, and interference with personal devices.

Twelve nations have outright or partially outlawed the usage of this software as of this writing. The main justifications mentioned cover worries about espionage, national security, and violations of the data protection and privacy of their residents and their governments.

ByteDance, the parent company of TikTok, has proposed proposals for the construction of regional data centers, Project Clover in Europe and Project Texas in the US, in order to allay these worries. These data centers will require large investments of €1.2 billion and €1.5 billion, respectively, and will be situated in Ireland and Norway for the storage of European data and in Texas for the storage of US data. Oracle, a software corporation, will oversee the infrastructure in an effort to strengthen security protocols and add an extra layer of management.

These facilities, however, will only keep legally "protected data," leaving the rest of the users' data accessible. As a result, a sizable amount of data might still be gathered and utilized in accordance with the objectives of the Chinese government. Due to the thin line separating the private sector from the CCP and China's Personal Information Protection Law of 2021, which gives the government access to both personal and non-personal data stored by domestic businesses under the guise of national security, ByteDance would still be obligated to comply with any requests from the government, posing a serious threat to TikTok users.

Following the steps of the United States, the European Union banned the use of TikTok in February 2023. This ban applies to devices registered with European institutions, including the European Commission, the Council of the EU, the European Parliament, the European External Action Service and the European Court of Auditors.

With the GDPR enacted in 2016, the EU operates under a strong regulatory framework, which includes guidelines and controls to control how organizations both inside and outside the EU handle data.

The GDPR requires that the types of data gathered, the reasons for processing them, the receivers of the data, and any potential cross-border data transfers be made public. Importantly, recipient nations are required to provide an adequate degree of protection or put in place suitable safeguards in accordance with the provisions of the GDPR.

Beyond that, the Digital Services Act (DSA), which was released in 2022, aims to create a secure digital environment and mandate the annual risk analysis of major platforms with more than 45 million users, including TikTok. Under the DSA, the EU released a list of 19 digital platforms in April 2023, including TikTok, that will be subject to more stringent regulations and yearly audits as of this August, when the law takes effect.

The importance of privacy has increased in the era of data exploitation. The ways in which we can be tracked and identified, as well as the types and scale of information that is available about us, have exploded in recent years, putting our privacy at greater risk than we could have ever imagined 20 years ago, outside of science fiction.

Privacy is having the freedom to choose; it is the right to set boundaries, to control who has access to our bodies, our homes, our possessions, our conversations, and our information. It gives us the

freedom to decide how we want to relate to the people and things around us and to define those relationships on our own terms.

Controlling what can be known about us and done to us, as well as defending us from those who want to assert control over our data and ultimately all parts of our life, is how we seek to safeguard ourselves and society from the arbitrary and unjustified use of power.

Our right to privacy is fundamental to who we are as people, and it shapes how we interact with the outside world on a daily basis. It permits us to think freely and without bias while giving us the freedom to be who we are. It allows us the autonomy and dignity to conduct our lives.

Last but not least, As such, the right to privacy also allows us to enjoy other rights, and interference with our private frequently opens the door to other rights being violated.[37]

BIBLIOGRAFIA/SITOGRAFIA

- https://bloomfire.com/blog/data-vs-information/

[37] https://privacyinternational.org/learning-resources/privacy-matters

- https://pubmed.ncbi.nlm.nih.gov/35281634/
- https://www.springer.com/journal/11747, “Digital technologies: tensions in privacy and data” article.
- Zarouali, Brahim & Poels, Karolien & Ponnet, Koen & Walrave, Michel.(2020).
- https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1318&context=facpubs
- https://journals.akademicka.pl/adamericam/article/view/3223/2905
- Data Protection Act 1998 principle 1-8
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A11997E286
- https://connectednation.org/blog/2021/04/20/technology-throughout-the-2000s/
- https://digitaleducation.tdm2000.org/topic/topic-1-introduction-to-the-european-general-data-protection-regulation-g-d-p-r/
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011 2012
- GDPR ART 4 COMMA 5,7
- https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/
- https://sampi.co/china-cybersecurity-law/
- http://mg.mofcom.gov.cn/article/policy/201912/20191202923971.shtml

- https://www.cyberlaws.it/en/2021/personal-information-protection-law-pipl-china/

- GDPR ART 6

- https://privacyinternational.org/learning-resources/privacy-matters