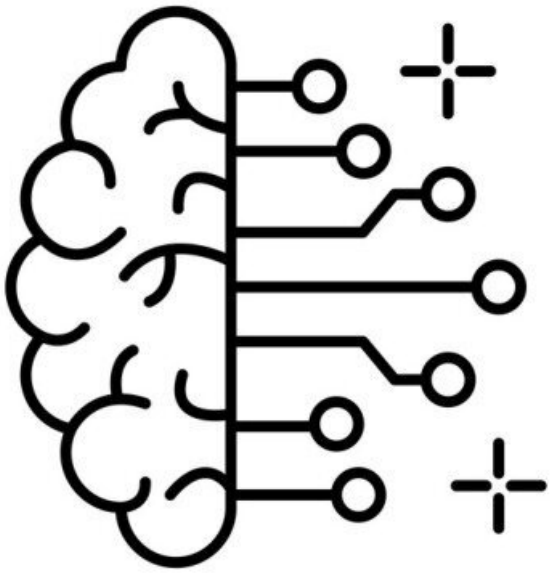
NOTES

Juridical Issues in Information Society

2223-1-FDS01Q005



myloview

Vittorio Haardt
853268
vittoriohaardt@gmail.com

December 4, 2022

Abstract

Notes from "Juridical and Social Issues in Information Society" lectures.

Contents

Chapter 1

Lecture 1: Ethics and law in information society

1.1 The fourth revolution

Due to the digitization man is no longer the center of reality, but just another node in an unlimited set of informational nodes.

The tree big revolution of the world were:

1. Copernicus: the man is not the center of the universe
2. Darwin: the man is not the center of the animal kingdom
3. Freud: the man doesn't master his mental life

The fourth revolution began with Alan Turing, and then it was fully explained by Floridi. A "mature information society" is characterized by living in an online context. Umans are now seen as informational organisms (*inforgs*) that leave interact as networked agents in a world and it's made of information. In this new world created by the fourth revolution information is what makes us healthy or sick, happy or sad.

1.2 Hyperhistory and Infosphere

According to Floridi "we are reminded of our deep technological debt when we divide human life into prehistory and history.

- Prehistory: was when man can't take records
- History: start with the invention of writing so man could finally have records and it is characterized by the possibility of telling the future through technologies
- Hyperhistory: technologies now con process information

Our society is dependent on the technological infrastructure that manipulates information.

Now that our society lives hyperstorically the cyber attacks are a real issues. If an hyperstorically society has to face a shift from one period to another it is required a huge levels of processing power and big quantity of data. This bring to the fact that memory and connectivity are the base of this shift.

The link between the cyber domain and the physical world crates new vulnerabilities and pose new legal and policy challenges.

1.3 Big Data

The Infosphere is a polluted area with tones of fake news, information overload and so on. It is still possible to fix it by changing those expectations and sensitivities on one hand, but also changing our business models in a practical way.

The real problem with big data is *small patterns*. Because of the huge quantity of data brought by Big Data is now very difficult to spot and were the new patterns with real added-value are in immense databases. To handle Big Data correctly is important to regulate personal data and the anonymisation, so there are regulation about it.

Two fundamental points for ethical discourse have now become crucial, it is how much in control we will be of our own informational essence (identity understood informationally), and manipulation. It is important to protect our selves and the way of doing it is through limitation made by law. The real-time bidding (aimed and in real time advertisement) is becoming more and more oppressing and our consumer profiles may come to define us in all of our interaction, both online and offline.

1.3.1 Data mining

Data mining methods:

1. Cookies: they are identifying pieces of data that a website can embed on a user's hard drive. Cookies can be used to let websites to track users' activities to develop rich profiles. Cookie-based data mining itself generally doesn't reveal personally identifying information, but it is possible to cross-reference that information with cookie-derived data.
2. Spyware: it is software that is installed on a device for tracking purpose. It is illegal to place spyware on user's devices, but users who clicks agreements without reading them may be consenting to downloading spyware.
3. Deep packet information: it is performed by the Internet service providers. To examine all the data going to and from their users' devices the providers have installed devices in their network infrastructures. It is impossible to track this operation and to know what data is being captured.
4. Direct collection: are the data collected by single website. Sometimes data are aggregated to improved user experience, but often it is for target advertising.

Data mining costs:

1. Eliminating users' ability to shield intimate and personal details of their lives from the view of profilers.
2. The potential for public disclosure of details that a user expected to remain private.
3. Identity theft.
4. The potential for users to suffer adverse consequences when entities make decisions based on their profiles.

Data breaches are a real issues for even the most sophisticated companies.

1.4 Ethics and Law

The role of ethics is changing and now it is a proactive task to help to understand what can be done and if it is good to do it.

The current norms are challenged by new technologies, this is interest to ethics. One a new technology is been fully understood in its context it is possible to include regulation and law.

- **Ethics**: it is a branch of moral philosophy that guides people about the basic human conduct, governed by individual and Professional norms. Ethics do not have a binding nature. There is no punishment for violation of ethics.
- **Law**: it is the systematic set of universally accepted rules and regulation created by an appropriate authority. Law has a legal binding. Violation of law is not permissible which may result in punishment.

Policy is a set of ideas or a plan for action followed by a business, a government, a political party, or a group of people. It is important to distinguish between soft law and hard law, for example policy is soft law.

- **Soft law**: it include recommendations, guidelines, codes of conduct, non-binding resolution, and standards.
- **Hard law**: it refers to legally binding instruments.

The legislation of this dynamic environment is difficult and has to be done constantly. New issues are born and with them the necessity to crate new laws. Some of this issues are the manipulation of behavior, the opacity of the system, the bias in decision system, and the human-machine interaction. The *manipulation of behavior* happen when algorithms are used to target peoples with just the kind of input that is likely to influence them. The *opacity of information-intensive systems* is with bias a central issues in "data ethics" because more complex is a model and less clear it is what cause the output of that model. This brings directly to *bias in decision system*, that it is when unfair judgments are made because the individual making the judgment is influenced by irrelevant things, if the judgment comes from a opaque model this bias are not recognisable. At least the *human-machines interactions* are a big issues of our era because of the loss of employment or other things like that.

1.4.1 Privacy

The most important problem of the Infosphere is the privacy. People want to be in control of their data, this implies data protection. Our online lives are based on the circulation of information, so having the information means having the control. The idea that we are running into trouble with an Infosphere that's polluted becomes a serious problem that we need to address. There are to ways to address it, one is make companies that control information less powerful, the second is to make the public pay for content. Unfortunately this will not happen.

The lost of privacy is now real, we have lost ownership of our data.

Chapter 2

Lecture 2: Privacy and identity for the information society

2.1 Big Data are the problem

Nowadays information is widely collected and available, the amount of data is growing in analytical capability. This bring some risks, because data can be use for political or commercial purposes and the infosphere can become like a "big brother" with no privacy for nobody.

There are two principal Big Data drivers, the increase in computing power, and the decreasing in data storage cost. The low has not fully understand the problem of this increment in calculation capacity and in fastness and because of that now privacy is a big issue.

As said before the lesson before the teal epidemiological problem with big data are small patterns.

2.2 Privacy for the infosphere

It is important to begin with some definition to fully understend what will come next

- **Processing**: it is almost anything you do with personal data.
- **Personal data**: it means information about a particular living individual called *data subject*. Id doesn't need to be private information and it doesn't cover truly anonymous information.
- **Data controller**: it is the person that has the power to decide how and why collect and use the data. It is usually an organization.
- **Data processor**: it is a separate person (or organization) who process data for the controller.

GDPR stand for "General Data Protection Regulation" and it is a European Union regulation on the processing of personal data and privacy. It has seven key principles.

1. *Lawfulness, fairness and transparency*: a data controller must identify the legal bases of collecting and using the data, for example the consent from the data subject. The second step is to use the data in a fair way for the data subject. The data subject expectation is important. The data controller has to be clear about the use of the data.

2. *Purpose principle*: The data data controller has to be clear and loyal about the purpose of the data. The purpose is changeable only with consent from the data subject or in some special circumstances.
3. *Data minimisation*: the data collected has to be adequate an relevant, so only the one necessary for the purpose and nothing else.
4. *Accuracy*: the data has to be more clear and correct as possible. The data need to be updated and corrected if it is necessary.
5. *Storage limitation*: the data controller must keep the data only for small amount of time, basically only for how long it is needed. The controller has to justify the amount of time. Individuals have a right to erasure if the controller no longer need the data.
6. *Security*: the data has to be securely processed, so the data controller must have appropriate technical and organizational measures. It is also important to take in account the security of the data processors. Some times it is necessary to use measures such as pseudonymisation and encryption. The measures must ensure the "confidentially, integrity and availability" of the systems and services and the personal data processed within them.
7. *Accountability*: the data controller has to take responsibility for what it does with personal data. The data controller also has to take records to be able to demonstrate its compliance.

The problem is that the ICTs (information communications technology) dismantle these types of rules, because technology is to advanced for a consistent application of this principles. The principles ar obsolete, so we need a new conception of privacy.

Privacy is now seen as divided in four parts:

- Physical privacy
- Mental privacy
- Decisional privacy
- Informational privacy

So privacy is seen as informational friction. Any factor decreasing or increasing informational friction will also affect privacy. Because of that to protect privacy it is necessary to consider anonymity and empowerment. It is important to know the consequence of processing the data, so a certain degree of anonymity must be guaranteed to protect privacy.

One of the most dangerous thing that can affect our privacy is a **data breach**. Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A data controller must consider the risk of this occurrence. The likelihood and severity of this risk must bee considered in order to protect people privacy and freedom. When this happens it is mandatory to notify the Data Protection Authority.

The new definition of privacy now has new rules and assumptions:

1. Rules are static and unchanging
2. Rules are a long and top-down process (authority)
3. Law requires and institutional oversight (law enforcement)
4. GDPR is also static and unchanging but:
    - Data protection authorities are independent from government and were created for istitutional oversight
    - GDPR requires accountability
    - GDPR requires a data protection officer

The **Data Protection Authority** (DPA) is an independent body set up that has the goal to protect rights in the public interest. In the EU member state is represented by the European Data Protection Board (EDPB).

A **Data Protection Officer** (DPO) advice the data controller to monitor internal compliance in data management. The DPO must be independent and can be done by existing employers or an external provider.

2.3 Identity for the information society

The gossip is now a way of enforcing communal norms. The infosphere has blurred the distinction between offline and online life (Onlife). The identity is at risk, because the infosphere never sims to forget, so is difficult to control our identity, to reinvent our selves or to overcome the past.

It is important to well understand the base rights in order to protect our identity.

1. **Right to be informed**: data subjects must be informed about the collection and use of their personal data. The data controller must provide people with privacy information.
2. **Right to access and rectification**: data subjects have the right to access and eventually correct their data.
3. **Right to be forgotten**: the data controller must erase the data of an individual. This right is not absolute and only apply in certain cases.
4. **Right to restrict processing**: when processing is restricted the data processor is permitted to store the personal data, but not use it. This is not an absolute right and only applies in certain circumstances.
5. **Right to data portability**: it allows to move, copy or transfer personal data without affecting its usability.
6. **Right to object**: in certain circumstance data subjects can object to the processing of their personal data.
7. **Rights related to automated decision making including profiling**: The GDPR has provisions on automated individual decision making and profiling. The additional rules are under Article 22. In order to use this tools the decision must be necessary, authorised by low and based on the individual's explicit consent. It is important to consider and address the risk and to use anonymised data in the profiling activities.

In order to be able to protect yourself technological solutions, privacy settings, reputation manager and expiration dates, must be adopted.

Chapter 3

Lecture 3: Freedom of speech and fundamental rights in the information society

3.1 Ethical and legal issues

There are several questions in the information society, such as if and when a government could track our movement, or how we can protect free speech online if the provider has all the power. All this questions and others lead directly to some of the most important ethical and legal issues in the information society. The ways that EU and US legislation has to cover those issues have some difference that will be highlighted.

3.1.1 The right to be forgotten

The most dramatic clash between privacy and free speech is *the right to be forgotten*. The right say that *individuals have the right to have personal data erased*. This right is not absolute and only applies in certain circumstance and it only applies on data held at the time the request is received.

It is very difficult for a provider to apply this right, so the solution adopted often conclude in an erasure of every content about the person making the request. The European approach is very different from the American one in this case.

The right to erasure doesn't apply if processing is necessary for one of the following reasons:

- to exercise the freedom of speech
- to comply with a legal obligation
- to safeguard public interest
- for the establishment, exercise or defence of legal claims
- if the processing is necessary for public health proposes
- if the processing is necessary for the purposes of medical and social care.

In Europe the approach is a balance with the right to be forgotten and other fundamental rights, such as the freedom of speech. This right is also important for people that want a second opportunity in life such as previous offender ones.

3.1.2 The liability of Internet providers

This theme is one of the most important different between the European's and the Unite State's prospective of the right to be forgotten. For the EU regulation the internet provider should put in act the erasure immediately unless there are some complications like the ones seen before.

The main point is that for the US the freedom of speech is a much more important issues than for EU. Before erasing a content is necessary to verify if the content is eligible for the right. Of course in this case the interest of the subject and the interest of the provider are at the opposite. The EU put the subject on the internet provider that has to prove that a content is right to prevent his the subject to claim this right. The right can also be calmed on any data controller that is carrying out any processing activity.

In the US there is an important factor in game: *the third party doctrine*. Basically you can't stop people from spreading a content. This is the main difference between the US and the rest of the world.

In the American approach is possible to declare *reputation bankrupt*, and it is applicable every ten years. Another proposal from US is to protect people from work implication, like loosing their jobs, based on internet information. One more proposal from US in technical point of view is an "eraser bottom" which could allowed subjects to erase data after a certain amount of time.

The difference is that EU approach is related to theoretical legal rights while the US one is more practical an is given to the individuals. To sum up:

American approach $\rightarrow$ the data subject is the core
European approach $\rightarrow$ the data controller is the core

The European approach to the issue compered the *accountability framework* whit its nine main principles, that will be seen later on.

3.1.3 Intellectual property rights

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his creation for a certain period of time. The internet services provider should check for this regulation but it can not have the liability if the eraser of a content that violate this principle is not fast enough.

This rights apply in the US as well in the EU. The real issues can be seen by an economic point of view.

3.1.4 Local laws and net neutrality

The providers have to obey also to local lows. The question is: how decide what type of content is displayable? Usually the judges and the government. An example of this laws are some sites of holocaust deniers which has to be closed because some local French lows.

Things tended to change after 2006 with the expansion of YouTube, obviously it is more difficult to regulate a video platform than a search engine. Because of this governments decided to block certain types of videos.

But unlike before Google decided to block users to access those contents that are illegal under their local lows. The system is that users can flag a content if they think that it violate the low in order to decide if a content have to be block in a country, after a content is flagged many times the provider has the authority to decide about it.

This case by case decision system is difficult for the internet provider, so other system are needed and made up.

3.1.5 Public interest and transparency

This two principles clash, the main example is Wikileaks and the anti terrorism agency. The freedom of speech in some cases clash and lost with public interest. In the example cited the publication of secrets about Afghanistan war overcome the freedom of speech, so the contents were erased.

3.1.6 Offensive speech

In general, speech that offends can be defined as speech that: "Causes someone to feel resentful, upset, or annoyed" . It is very common on internet and it is cause of depression and suicide mainly in the youngest users. It is important to prevent and block this type of beavers to prevent the bad effects. Depending on the country the users can be prosecuted by law for offensive speech. The internet providers put a special attention to this situation because of the image damage.

Chapter 4

Lecture 4: Data governance

4.1 Accountability

For the EU point of view the most important principle is *accountability*. In GDPR accountability is a principle that requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

As said accountability is a question of measures, this measure can be sum up in six point.

- Adopting and implementing data protection policies
- The data controller has to take data protection by design and by default
- Written contract with other organization, that contain the data controller's data are mandatory
- To have documentation about processing activity
- To carry out data protection impact in processing
- To appoint data protection office to comply lows and regulations

Accountability obligations are ongoing, so it is important to keep update this measures. A data governance framework is useful for build a trust relationship with the data subject and for mitigate enforcement action.

As mentioned in the chapter above the center of the EU regulation is the data controller, that in this case is the one that has to demonstrate its compliance. Accountability is important for taking responsibilities for what you do, as a data controller, whit personal data and the trust build with users.

Accountability is not only a juridical affair, but is something more deep.

4.2 Main problems in data governance

4.2.1 Jurisdiction

There are a lot of juridical authorities that can impact the data processing. Jurisdiction is handled at the level of the individual state and only for certain matters are EU courts competent on a subsidiary basis. The most important one is the *Data Protection Authority* (DPA), that in Europe is called European Data Protection Board (EDPB).

The DPA authority has the role of handling with data subject compliance, providing measures and adopting guidelines.

4.2.2 Laws

The problem with lows is that there are many different sources operating at different levels in different field.

The sources could be like "case law", "law and regulations", "official decisions by DPAs" or, "official guidelines by DPAs and EDPB". The levels could be like "EU GDPR", "EU ePrivacy", "UK post Brexit", "China PIPL and DSL" and "US privacy laws". At last the fields are things like "freedom of information act" or "codes of practice".

4.3 Lawful basis

Except for accountability the lawful basis are the key principle in GDPR. It is mandatory to have a valid lawful basis in order to process personal data. **No data processing without lawful basis**. There are six rules that only cover personal data.

- Consent
- Contract
- Legal obligation
- Vital interest
- Public task
- Legitimate interest

There is not a basis that is mote important than the others, the basis are all equal important. The data controller must determine its lawful basis before you begin processing, and it should document it. The data controller should not swap to a different lawful basis at a later date without good reason.

If the data that are been processed are *special category data* the data controller must identify both a lawful basis for general processing and an additional condition for processing this type of data. If the data that are been processed are *criminal conviction data*, the data controller need to identify both a lawful basis and a specific legal obligation in order to process this type of data.

The special category of data are more sensitive and need extra protection. The GDPR recognise as this type of data the following ones:

personal data revealing racial or ethnic origin
personal data revealing political opinions
personal data revealing religious or philosophical beliefs or trade union membership
genetic data or bio metric data where used for identification purpose
data concerning health
data concerning a person's sex life and sexual orientation

All of this special categories of data has political, religious or social belief and for that is required a data protection impact assessment.

4.4 Accountability framework

The accountability framework has some base principles.

1. **Leadership and oversight**
2. **Policies and procedures**
3. **Training and awareness**
4. **Individuals' rights**
5. **Transparency**
6. **Records of processing and lawful basis**
7. **Contracts and data sharing**
8. **Risk and data protection impact assessments**
9. **Security, breach response and monitoring**

4.4.1 Leadership and oversight

A fundamental building block of accountability is strong leadership and oversight (DPO). In few words they are organization for handling rules. The DPOs assist the data controller in support the practical implementation of data protection and information governance, DPOs assit to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessment and act as a contact point for data subjects and the DPA. DPO is linked with accountability principle and it is the core of a proactive approach.

4.4.2 Policies and procedures

Policies and procedures provide clarity and consistency, by communicating what people need to do and why. The GDPR requires the data controller to put in place appropriate technical and organizational measures to implement the data protection principles. This is *data protection by design and by default*. This means that data protection must be implemented from the design stage through all the life cycle. In other words, from the very beginning the data controller has to use measures to safeguard policies.

This consumption is common with all six principle from Article 5 and accountability principle. This will help the data controller whit the compliance.

4.4.3 Training and awareness

The training must be relevant, accurate and up to date. Training and awareness is key to actually putting into practice policies, procedures and measures. So it requires to put in place appropriate measures to implement data protection principle in an appropriate way. Then the data controller has to integrate this in the processing activity to meet all the requests made by laws and DPOs (the legal framework).

4.4.4 Individuals' rights

The individuals' rights are all the rights related to the data subject. There is a particular attention to personal information.

Personal information → Any kind of information that can be use to identify a leaving person.

The main rights in this section of the accountability framework are:

- Informed
- Access
- Erasure
- Restriction
- Object/Opt-out
- Data portability
- Automated decision

4.4.5 Transparency

The transparency is also referred to the data subject. The data controller must be clear in the communication about pretty much every thing.

In particular there are seven key point to follow:

- Insert contact detail of the data controller.
- What type of information does the data controller have.
- It must be specified how and way the data controller has the information. (Data transfer between two country caon be a problem).
- What the data controller do with the information.
- How the data controller store the information.
- How the info are stored. (The data controller mus protect information for all the process).
- The data controller must show a list of data subject's rights.
- The data controller must make clear to subjects how to complain. (Generally by contacting the DPA).

4.4.6 Record of processing and lawful basis

The GDPR contains explicit provisions about how the data controller must documenting its processing activities. Basically the data controller must maintain records on several things such as processing purposes, data sharing and consent from data subject. The DPA can request this documentation, and also the documentation can help the data controller comply with the GDPR and improve data governance.

Both data controller and data processor has this kind of obligations. Some other "tools" like data-mapping are not mandatory for the GDPR, but could help keep the documentation. The records must be kept in writing, generally they are kept electronically, because it is easier to kept them up to date.

4.4.7 Contracts and data sharing

Whenever a data controller uses a data processor, there must be a written contract in place. It is important also for both parties to understand their responsibilities and liabilities. If a processor uses another organization, called sub-processor, the data controller needs to have a written contract in places also whit that sub-processor.

4.4.8 Risk and data protection impact assessment

A Data Protection Impact Assessment (DPIA) is the most important part for the technical and organization methods. It is a process to reduce the probability or the severity of data protection risks.

The DPIA must describe all the processing (nature, scope, context and purposes); it must assess necessity, proportionality and compliance measures; it must identify and assess risks to individuals; and it must identify any additional measures to mitigate those risks.

It is important to give a score to the risk, to do so the data controller must consider both the likelihood and the severity of any impact on individuals. The data controller should consult its data protection officer (if it has one). If an high risk, that can't be mitigate, is identified, it is important to consult the DPA before starting the processing.

The case that can be considered an high risk can be: whitelist, profiling and automated decision making, systematic monitoring, datasets matched or combined, vulnerable data subjects, new technologies, cross-border transfer, service refusal, genetic or biometric data, location data, employment.

4.4.9 Security, breach response and monitoring

The GDPR obligate all organizations to report certain personal data breaches to the relevant supervisory authority. The notification must be done within 72 hours from when the data controller become aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the data controller must also inform those individuals without undue delay

This time limit exist because to main reason, on one hand to reduce risk for individuals, on the other hand to receive support from the DPA in compiling with the necessary improvement. In addition the data controller must keep a records of any personal data breaches, regardless of whether it is required to notify.

Chapter 5

Lecture 5: Data protection impact assessment

5.1 AI and data protection

There are two side of artificial intelligence, on the bright side the AI can be a gigantic benefit and can improve all systems, but on the other side the use of AI bring many risks.

A data governance framework is strongly related with AI and data protection, and it is build in four parts.

1. Accountability and governance
2. Fair, lawful and transparent processing
3. Data minimisation and security
4. Individual rights

A note to remember that data minimization is very complex to make, and it implies that the data used in a process are only the ones that are necessary for a specific goal and nothing more than that.

In the case of AI system the *accountability* requires that:

- The data controller to be responsible for the compliance of its AI system
- Assess and mitigate its risks;
- Document and demonstrate how your system is compliant and justify the choices

Risks are a real issue in this field, and so technical and organizational measures are the most important part of the process. Identify a specific risk related to an AI system is the key point. Some specific risk could be: the loss or misuse of the large amounts of personal data often required to train AI systems, or some software vulnerabilities in AI related code and infrastructure.

Carrying out this activities make possible to identify challenges to overcome, like data minimisation principle and individual rights.

It is interesting to see how the data protection law does not use the term "AI", so none of legal obligation depend on exactly how it is defined.

A risk-based approach requires to assess the risk involved in a process and then, starting from the risk, to implement technical and organizational measures. It is a case by case approach, so there isn't a list of measure or rules to follow.

If it is use well the AI has the power to make organization more efficient and it has a huge impact in productivity, but there are may risk with AI, especially related to data subject and individual rights, but also with the compliance. The DPIA (see section 4.4.8) require to involve of all the people in charge of an organization.

The risk has to be minimised but this means that the regulation says that some risk is tolerated. In other words it is not a zero risk approach. The data controller has to describe the particular context and the purpose of processing, in order to allow the data controller to identify the specific risks. It is a step by step operation to recognise the risks.

It is important to identify the **controller** and the **processor**. The controller is a legal person that can decide how and why carrying out a certain processing activity. He has the main responsibility in AI compliance. The processor has also some compliance but it is a different level of responsibility.

The risk mentioned until now are risk related to individual rights. The controller can decide how to handle this risks (accountability principle) and than the choices has to be described in the DPIA. As we have seen before the DPIA is a written document about the choices made by the organization, it is a legal tool and it is mandatory. It function as an oversight on the compliance. It is another consequence of the accountability principles.

5.2 Data protection impact assessment

A DPIA is a process to help the data controller to identify and minimise the data protection risks of a project. It is required by the article 35 of the GDPR. As seen in the section 4.4.8, it applies in every case of AI or any activity related to AI.

The DPIA must: describe the nature, scope, context and purpose of processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. This description need to clarify:

- How all the data involved are process: it means how they are collected, stored and used.
- What data are being processed: this is the case of data protection regulation it involves volume, variety and severity.
- A description of data subjects: like the number, the relationship, the source of data and expectation of individuals, which is very important to address in this case.
- The possible outcomes: outline all the benefit obtained through the system, and also outline the possible negative consequence. The law doesn't require a zero tolerance approach, so some risk are acceptable if the balance between good and bad outcomes is favorable.
- Data flows.
- Effects on individuals: it is very important to outline the consequence for individuals.
- Statistical accuracy and human involvement.

5.2.1 Necessity and proportionality

This is a more legal part. There are many problems related with Big Data and AI processing, especially in the EU. In order to use AI the data processor has to state that the AI solution is the only alternative available to achieve a certain goal. As the AI solution, also the collection of data has to be strictly necessary, the deployment of AI must be driven by the problem of an huge amount of data, and the way to solve it is to evidence that the goal can't be obtained in any different way.

The DPIA hallow ti to clarify also the proportionality between competing interests of data collector and rights of data subjects. This two aspects are very important for the DPIA.

5.2.2 Risks

Risk in this field are especially related with individuals' interests. It is important to measure with probability and severity each risk and each impact that that risk could have on individuals. There are many kind of risk but the two more related with individuals' interests are the *discrimination* and the *bias*.

5.2.3 Mitigating measures

In order to mitigate the risks related to AI, the ones just seen, there are a variety of measures that could be done. From a technical stand point the *anonymization* is a very effective solution. Another effective measure is a training and awareness of all the people involved in the process.

From a practical point of view a DPIA is the measures that the data processor has put in place before starting the processing. After this point the data controller is not able to reduce the risk. The data controller can ask for a prior checking of DPA if it is unable to sufficiently reduce the risk. In addiction the data controller should review the DPIA with some periodicity, it is considered a live document.

5.2.4 Controller/processor

In order to identify the right responsibility of every one how is involved in the process, it is important to identify the roles. It is important to have all organization involved in the AI system labeled as: data controller, data processor, join controller, sub-processor.

- **Data controller**: the controller has the control of the purpose and means of processing.
- **Data processor**: the processor doesn't have any independent purpose.
- **Join controller**: if there are many data controller they are called join controllers.
- **Sub-processor**: it is an organization that operate as a data processor to a data processor, usually on a specific part of the dataset.

This chain is very important in the field of responsibilities. The data processor can make some decisions about some technicality, but the responsibility remain to the controller, because it is the one that decide the purpose.

So what is on the DPIA is under the responsibility of the data controller. There is the possibility of a change of roles during the process and it is quite common in real life situations.

In order to clarify the decision making power of a processor we make some examples. A processor can decide, for example the IT system and the process to give to personal data. The processor can also decide how to

store the data, this is very important for security measures. So the processor has a very important role, but non the less it has no responsibility. The data controller must chose carefully its processor.

5.3 Lawfulness, fairness and transparency

It is a bit more difficult to handle the lawfulness, fairness and transparency principles when the AI is involve.

- **Lawfulness**: the development and deployment of AI systems involve processing personal data in different ways for different purposes. The data controller must break down and separate each distinct processing operation, and identify the purpose and an appropriate lawful basis for each one, in order to comply with the principle of lawfulness.
- **Fairness**: If the data processor use an AI system to infer data about people it deed to ensure that the system is sufficiently statistically accurate and avoids discrimination; and the processor consider the impact of individuals' reasonable expectations.
- **Transparency**: the data processor need to be transparent about how the it process personal data in an AI system, to comply with the principle of transparency.

5.4 Security and data minimisation

There is no "one-size-fits-all" approach to security. Record and document has to be done about all movements and storing of personal data. Any intermediate files containing personal data has to be deleted as soon as they are no longer required. Also an application of de-identification techniques to data, before it is extracted form its source and shared, is mandatory.

The processor has to pay attention to externally maintained software used to build AI systems, and it need to assess the security of any externally maintained code and frameworks.

In a model inversion attack, if attackers already have access to some personal data belonging to specific individuals included in the training data, they can infer further personal information about hose same individuals by observing the inputs and outputs of the AI system. So it is important to prevent it having a secure pipeline from development of deployment that will further mitigate security risks.

Chapter 6

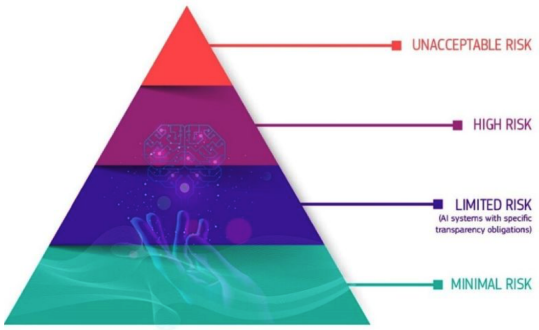
Lecture 6: Artificial Intelligence Act

6.1 AIA proposal

The artificial intelligence act (AIA act) is the first comprehensive attempt, made by EU, at regulating the uses and risks of AI. It is just a proposal, but it helps to understand the EU prospective about AI.

AI may affects many field and is nowadays used by companies to optimize their activities and operations, but as seen in GDPR framework it also bring many risks. Because of that finding a balanced approach to regulate AI has become a central policy question, it is important to minimize risks and protect users without reducing innovation and the uptake of AI.

The answer is a pyramidal approach.



The pyramid is divided in:

- **Unacceptable risk**: banned form the EU market
- **High risk**: most important legal requirement in order to reduce the risk for users
- **Limited risk**: no straights limit requirement but only basic obligations
- **Minimal risk**: no particular legal obligation related to AIA proposal

The core of the AIA are the AI that has high risk, 90% of this proposal is referred to them. The main points of the EU draft regulation are:

1. Lay down a common legal framework for the development the marketing and the use of AI products and services in the EU, in order to set out the specific rules for AI systems, so operators can rely to that. Also to create trust for users.
2. Risk-based approach. The same approach in GDPR, the risk is what matter.
3. AI systems can create the risks in the pyramid.
4. High risk requirements on:
    - data governance
    - documentation and recording keeping
    - transparency and provision of information to users
    - human oversight
    - robustness, accuracy and security
5. Low or limited risk: no additional legal obligation (just basic transparency obligations)

Typically the European artificial intelligence board is composed by the *national market surveillance authorities* and *European artificial intelligence board*. Another approach is the issues of the compliance of this type of rules, we have an independent body with specific rules to provide guidelines for AI.

6.1.1 Codes of conduct

Another milestone is the codes of conduct. It is a bottom up approach to regulation encourage providers of non-high-risk AI systems to apply voluntarily the mandatory requests for high-risk AI systems, in order to have more trust with users; it work like a sort of guidelines for the market.

6.1.2 Conformity assessment (CA)

The Conformity Assessment (CA) is a legal obligation designed to foster accountability under the proposed AIA that only applies to AI systems classified as 'high-risk'. It is very similar to the DPIA. According to its AIA definition, CA is the 'process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled'.

6.1.3 The difference between low and high risk AI systems

In order to distinguish high risk between low risk AI systems, the EU has chose a practical approach with a lost of those characteristics which automatically make an AI system considered high risk. The list is called **Annex 3**. Those are referred to some definitions, by default this kind are considered high risk, such as: related to biometric processes, management and operation of critical infrastructures (like road traffic electricity and water management), education and vocational training, employment and workers management, access to private and public services (like the ask of a loan in a bank).

6.2 Specific articles in the AIA

6.2.1 Risk management system (art. 9) and data governance (art. 10)

Requirement for a risk management system, it is been already seen in the accountability framework/

1. Purpose principle

2. Risk assessment
3. Technical and organisational measures to mitigate the risks

Which can have tree type of risks:

- Health risk
- Security risk
- Risk to fundamental rights and freedoms

6.2.2 Documentation (art. 11) and record keeping (art. 12)

1. Fine tuning (statistical accuracy / data quality)
2. Documentation (accountability - annex 4)

6.2.3 Transparency (art.13)

- Explanation (to users in order to give trust and internal governance)
- Trust
- Internal governance
- Informed public
- Better outcomes

That lead to six explanations:

1. Rationale explanation
2. Responsibility explanation
3. Data explanation
4. Fairness explanation
5. Safety explanation
6. Impact explanation

6.2.4 Human oversight (art. 14)

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.
2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.
3. Human oversight shall be ensured through either one or all of the following measures:
    - identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service
    - identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user
4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:
    - fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible

- remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons
- be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available
- be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system
- be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.

6.2.5 Robustness, accuracy and security (art. 15)

1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their life-cycle.
2. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.
3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans. High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures.
4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.

6.2.6 Quality management system (art.17)

This article is also important because it say that any providers of high-risk AI system has to put in place a quality management system (accountability principle).

Data Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

- a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;
- techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system

- techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system
- examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out
- technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title
- systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems
- the risk management system referred to in Article 9
- the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61
- procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62
- the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties
- systems and procedures for record keeping of all relevant documentation and information
- resource management, including security of supply related measures
- an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph

6.3 Providers of high-risk AI systems shall

All obligation are clear specify with refers form other articles.

- ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title (the five requirements that we have analyzed before)
- have a quality management system in place which complies with Article 17
- draw-up the technical documentation of the high-risk AI system
- when under their control, keep the logs automatically generated by their high-risk AI systems
- ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service
- comply with the registration obligations referred to in Article 51
- take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title
- inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken
- to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49
- upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title

Chapter 7

Lecture 7 (extra): Blockchain and smart contracts

7.1 Introduction to blockchain

Blockchain technologies are included in the broader family of Distributed Ledger Technologies (DLT). They are systems based on a distributed ledger, which can be read and modified by multiple nodes in an network. To validate the changes made to the ledger, in the absence of a central entity, nodes must reach consensus. The way in which consensus is reached and the structure of the register are some of the features characterising the different DLTs.

The technological prerequisites are a peer-to-peer and open source structure. The characteristics are:

- immutability of the register
- transparency
- traceability of transactions
- security based on cryptography

7.2 Smart contracts

Smart contracts are neither smart nor contracts. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises. A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

Basically they are software or application or script that are event-driven. Contractual obligations expressed in computational logic (ITTT) and then in programming language, that use self-execution for automated fulfilments and self-enforcement in case of default.

A decentralised application (DApp, dApp, Dapp, or dapp) is an application that can operate autonomously, typically through the use of smart contracts, that run on a decentralized computing, blockchain or other distributed ledger system. Like traditional applications, dApps provide some function or utility to its users.

Oracles are offchain information sources to provide input to onchain smart contracts. Mass users trusted third parties.

In Italy, the Ministry of Economic Development appointed a group of experts to develop a national strategy. In February 2019, with the Law converting the simplification decree-law (Decree-Law n. 135/2018), the Italian legislator formulated a definition of smart contract. According to the regulatory text, a smart contract, to be defined as such, must simultaneously have the following characteristics:

- being a computer program
- operating on technologies based on distributed ledgers
- whose execution automatically binds two or more parties
- based on effects predefined by them

A "smart contract" is defined as a computer program operating on technologies based on distributed ledgers and whose execution automatically binds two or more parties on the basis of effects predefined by them. Smart contracts fulfil the requirement of written form after computer identification of the parties concerned, through a process having the requirements set out by the 'Agenzia per l'Italia Digitale' with guidelines to be adopted within 90 days from the entry into force of the law converting the decree law.

Decentralized finance offers financial instruments, without relying on intermediaries such as brokerages, exchanges, or banks, by using smart contracts on a blockchain.

NFTs are unique tokens stored on smart contract blockchains, like the Ethereum blockchain. NFTs can represent an extraordinary range of intangible objects and, with appropriate bridges, tangible objects, too. The potential addressable market for NFTs is very large, but this is contingent on successful development and adoption. The NFT market is still immature and experimental. Initial progress has been made in collectibles and art, but most other categories are mostly unexplored.

Chapter 8

Lecture 8: A guide to "the fourth revolution"

The fourth revolution chapters:

1. Time
2. Space
3. Identity
4. Self understanding
5. Privacy
6. Intelligence
7. Agency
8. Politics
9. Environment
10. Ethics

8.1 Time

Hyperhistory: from prehistory to hyperhistory.

- Big data
- Small patterns
- Cyber attack and cyber war (chapter 8)
- Life cycle for information
- The age of zettabyte
- The growth and drivers of Big Data

- *The target case*
- *The stuxnet case* (not in Floridi's book)

Information society: Only very recently has human progress and welfare begun to be not just related to, but mostly dependent on, the successful and efficient management of the life cycle of information. (p.3)

Epistemological problem: The real epistemological problem with big data is small patterns. Precisely because so many data can now be generated and processed so quickly, so cheaply, and on virtually anything, the pressure both on the data nouveau riche, such as Facebook or Walmart, Amazon or Google, and on the data old money, such as genetics or medicine, experimental physics or neuroscience, is to be able to spot where the new patterns with real added-value lie in their immense databases, and how they can best be exploited for the creation of wealth, the improvement of human lives, and the advancement of knowledge. This is a problem of brainpower rather than computational power. (p.16)

Digital memory: Our digital memory seems as volatile as our oral culture was but perhaps even more unstable, because it gives us the opposite impression. (p.18)

Perpetual present: The risk is that differences are erased, alternatives amalgamated, the past constantly rewritten, and history reduced to the perennial here and now. When most of our knowledge is in the hands of this forgetful memory, we may find ourselves imprisoned in a perpetual present. (p.18) In hyperhistory, saving is the default option. The problem becomes what to erase. (p.21)

From hyperhistory to infosphere: The question to be addressed next is: given all the variables we have seen in this chapter, what sort of hyperhistorical environment are we building for ourselves and for future generations? The short answer is: the infosphere. (p.24)

8.2 Space

Infosphere or information society

- Technology in-between (first, second and third order)
- Interfaces and protocols
- Design
- Politics of technology
- Informational friction (chapter 5)
- Onlife

- *Silk road and bitcoins*
- *Fidelity cards*
- *Pirate bay*
- *BitTorrent*
- *Cyber insurance*

Technology: Second-order technologies are those relating users no longer to nature but to other technologies; that is, they are technologies whose prompters are other technologies. (p.27) Some first-order technologies (recall: these are the ones that satisfy the scheme humanity–technology–nature) are useless without the corresponding second-order technologies to which they are coupled. Roads do not require cars to be useful, but screws call for screwdrivers. (p.27-28)

Off the loop: Essentially, third-order technologies (including the Internet of things) are about removing us, the cumbersome human in-betweeners, off the loop. (p.31)

Politics of technology: At one extreme, one may interpret technology's in-betweenness as a deleterious kind of detachment and a loss of pristine contact with the natural and the authentic. (p.39) At the other extreme, there is the enthusiastic and optimistic support for the liberation provided by technology's in-betweenness. (p.39)

Infosphere: ICTs are modifying the very nature of, and hence what we mean by, reality, by transforming it into an infosphere. (p.40)

Money: Even money is becoming increasingly virtual. On any sterling banknote, one can still read 'I promise to pay the bearer on demand the sum of...', but the fact is that Britain abandoned the gold standard in 1931, so you should not expect to receive any precious yellow stuff in exchange. The euro, you may notice, promises absolutely nothing. Since currencies are free-floating nowadays, money may well be just a pile of digits. (p.46)

Informational flow: However, what we still experience as the world offline is gradually becoming, in some corners of the world, a fully interactive and responsive environment of wireless, pervasive, distributed, a2a (anything to anything) information processes, that works a4a (anywhere for anytime), in real time. (p.48)

Virtual materialism: Less emphasis on the physical nature of objects and processes means that the right of usage is perceived to be at least as important as the right to ownership, with an interesting twist. It may be called virtual materialism. (p.50)

Fairness and transparency: When free online services promote consumerism about purchasable physical products through advertisement, the process can easily generate confusion or mistaken expectations about what is and what is not free of charge, even whether it should be free. This confusion contributes to explaining why the more-or-less legal sharing of contents online is so popular. (p.51)

8.3 Identity

ICTs as technologies of the self

- Personal identities
- Hyper-self-consciousness
- Virtual bubbles
- The right to be forgotten
- The paradox of identity
- Our informational nature
- It from bit
- Perception: the digital gaze
- E-health
- E-ducation

- *Stacy Snyder's the drunken pirate photo* (not in the Floridi's book)
- *Tinder*

The right to a second choice: There are some classic puzzles about personal identity. They are linked to continuity through time or possible scenarios: are you the same person you were last year? Would you be the same person if you had grown up in a different place? (p.61)

Identity: In a nutshell, your identity is grounded in the unity of your consciousness and the continuity of your memories. (p.68) Then there is a second approach, more recent, known as the Narrative theory of the self. According to it, your identity is a 'story', understood as a socio- and/or auto-biographical artefact. (p.68)

8.4 Self understanding

The fourth revolution

- The first three revolutions
- Human intelligence
- Inforgs
- Enhancing and augmenting
- Technologies

- *Turing machine*

Human intelligence: We could still hold on to the view that our special place in the universe was not a matter of astronomy, biology, or mental transparency, but of superior thinking abilities. This was the implicit line of defence of our exceptional place in the universe which was still standing. Intelligence was, and still is, a rather vague property, difficult to define, but we were confident that no other creature on Earth could outsmart us. (p.91)

Computer: The history of the word 'computer' is indicative. Between the seventeenth and the nineteenth century, it was synonymous with 'a person who performs calculations' simply because there was nothing else in the universe that could compute autonomously. (p.39)

Inforgs: Rather, we are informational organisms (inforgs), mutually connected and embedded in an informational environment (the infosphere), which we share with other informational agents, both natural and artificial, that also process information logically and autonomously. (p.94) We are regularly outsmarted and outperformed by our ICTs. (p.96)

8.5 Privacy

Informational friction

- The ethical problem of privacy
- Privacies as freedom from
- Informational friction
- Anonymity
- Privacy enhancing technologies
- Cookies, monitoring software, malware
- Databases
- Empowerment (inclusion and improvement)
- Why privacy matters and the self-constitutive value of privacy
- Biometrics

- *Physical privacy*
- *Mental privacy*
- *Decisional privacy*
- *Informational privacy*
- *Bentham's panopticon*
- *Asimov's The Dead Past*
- *Warren and Brandeis "The Right to privacy"*
- *Orwell's "Nineteen Eighty-Four"*

- *Alfred Hitchcock "Rear window"*
- *Odysseus*

Informational friction: Put simply and more generally, privacy is a function of the informational friction in the infosphere. Any factor decreasing or increasing informational friction will also affect privacy. So it may seem that we have an answer to our first question. ICTs have made privacy one of the most obvious and pressing issues in our society because they unquestionably and influentially affect informational friction. (p.105)

Anonymity: Sometimes, it seems that the privacy we miss nowadays is really nineteenth-century anonymity. Because digital ICTs are modifying our informational environments, our interactions, and ourselves it would be naïve to expect that privacy in the future will mean exactly what it meant in the industrial Western world in the middle of the last century. [...] In a way, a different kind of privacy is the price we pay to enter into hyperhistory. Society cannot depend so widely and deeply on ICTs without allowing them to reshape the environment and what happens within it. (p.106)

A-Anonymity: Some steps forward into the information society are really steps back into a small community and, admittedly, the claustrophobic atmosphere that may characterize it. (p.108)

PET's: The trouble with this reasoning is that, contrary to old ICTs, new ICTs empower users in both directions, as they can both increase and decrease informational friction. (p.113) At the point of data generation, digital ICTs can foster the protection of personal data, especially by means of encryption, anonymization, password encoding, firewalling, specifically devised protocols or services, and, in the case of externally captured data, warning systems. (p.115)

Fundamental rights: We never stop becoming ourselves, so protecting a person's privacy also means allowing that person the freedom to construct and change herself profoundly. (p.124)

8.6 Intelligence

Inscribing the world

- Intelligence
- Intelligence and big data
- The stupidly smart
- The Turing test
- Two AIs

- *Bacon vs Plato*
- *The Loebner Prize*
- *Deep Blue and Garry Kasparov*

Intelligence: With some differences in vocabulary, the passage could have been written by the English philosopher Francis Bacon (1561–1626). Bacon was a great supporter of huge collections of facts, believing that if one accumulated enough of them they would speak for themselves, and was suspicious of hypotheses. He underestimated a fundamental point that was clear to Plato: that knowledge is more than information, because it requires explanations and understanding, not just truths or correlations. (p. 129-130)

Intelligence and small patterns: If you recall, the problem with big data is small patterns. So, ultimately the knowledge game will still be won by those who, as Plato puts it in one of his famous dialogues, 'know how to ask and answer questions' critically, and therefore know which data may be useful and relevant, and hence worth collecting and curating, in order to exploit their valuable patterns. (p.130)

The two AIs: I prefer to use the less loaded distinction between light vs. strong AI. The misalignment of their goals and results has caused endless and mostly pointless diatribes. Defenders of AI point to the strong results of reproductive, engineering AI, which is really weak or light AI in terms of goals; whereas detractors of AI point to the weak results of productive, cognitive AI, which is really strong AI in terms of goals. Many of the pointless speculations on the so-called singularity issue—a theoretical moment in time when artificial intelligence will have surpassed human intelligence—have their roots in such confusion. (p.141)

8.7 Agency

Enveloping the world

- An ICT friendly environment
- The machine's use of human inforgs
- Artificial companions (ACs)
- The semantic web
- Web 2.0 and its semantic engine
- Webs in the infosphere

- *CAPTCHA*
- *Amazon Mechanical Turk*
- *Tamagotchi*
- *Folksonomy*

The winning formula: The winning formula is simple: smart machine + human intelligence = clever system. (p.148) **Relationship problems**: Two people A and H are married and they really wish to make their relationship work. A, who does increasingly more in the house, is inflexible, stubborn, intolerant of mistakes, and unlikely to change. Whereas H is just the opposite, but is also becoming increasingly lazier and dependent on A. The result is an unbalanced situation, in which A ends up shaping the relationship and distorting H's behaviours, practically, if not purposefully. If the marriage works, that is because it is carefully tailored around A. Now, light AI and smart technologies play the role of A in the previous analogy, whereas their human users are clearly H. (p.150)

Who is going to adapt to whom?: There are many 'roundish' places in which we live, from igloos to medieval towers to bay windows. If we spend most of our time inside squarish boxes that is because of another set of technologies related to the mass production of bricks and concrete infrastructures, and the ease of straight cuts or encasing of building material. It is the mechanical circular saw that, paradoxically, generates a right-angled world. (p.151)

Design: Following this example, it is easy to see how the opportunity represented by technologies' power comes in three forms: rejection, critical acceptance, and proactive design. (p.151)

Folksonomy: A folksonomy (from folk and taxonomy) is the aggregated result of the social practice of producing information about other information (e.g., a photograph) through collaborative classification, known as social tagging (e.g., the photograph receives the tags 'New York', 'Winter', 'Statue of Liberty'). (p.161)

Web 2.0: Web 1.0, but by an ecosystem friendly to, and inhabited by, humans as inforgs. Web 2.0 is a part of the infosphere where memory as registration and timeless preservation (the Platonic view) is replaced by memory as accumulation and refinement, and hence search replaces recollection. It is an environment characterized by its time-friendliness: time adds value and Web 2.0 applications and contents get better by

use, that is, they improve with age, not least because the number of people involved is constantly increasing. (p.162)

8.8 Politics

Multi-Agent Systems

- The sovereign States
- The four factors of the hyperhistorical order
- The multi-agent system
- Infraethics
- Cyberwar

- *Westphalian doctrine* (The Peace of Westfalia)
- *The Leviathan*
- *The passport*
- *Montesquieu*
- *Washington consensus* (post-Bretton Woods)
- *The stuxnet case* (not in Floridi's book)

The role of the State: But it did rise to the role of the binding power, the system able to keep together and influence all the different agents comprising it, and coordinate their behaviours, as long as they fell within the scope of its geographical borders. (p.169-170) States became the independent agents that played the institutional role in a system of international relations. (p.170)

The features of the State: And the principles of sovereignty (each state has the fundamental right of political self-determination), legal equality (all states are equal), and non-intervention (no state should interfere with the internal affairs of another state) became the foundations of such a system of international relations. (p.170)

The age of the State: The state arises as the information agent, which legislates on, and at least tries to control, the technological means involved in the information life-cycle, including education, census, taxes, police records, written laws, press, and intelligence. (p.171)

The purposes of the State: As the information agent, the state fosters the development of ICTs as a means to exercise and maintain legal force, political power, and social control, especially at times of international conflicts, frequent unrests, and fragile peace. [...] Through the centuries, the state moves from being conceived as the ultimate guarantor and defender of a laissez-faire society to a Bismarckian welfare system, which takes full care of its citizens. In both cases, the state remains the primary collector, producer, and controller of information. (p.171-172)

The emerging of others agents: However, by fostering the development of ICTs, the state ends by undermining its own future as the only, or even the main, information agent. This is the political apoptosis I mentioned earlier. For in the long run, ICTs contribute to transforming the state in an information society, which makes possible other, sometimes even more powerful, information agents, which may determine political decisions and events. And so ICTs help shift the balance against centralized government, in favour of distributed governance and international, global coordination. (p.172)

The four factors of the hyperhistorical order:

- Power
- Geography

- Organizations
- Democracy

The political multi-agent system:

- Theological
- Interactive
- Autonomous
- Adaptable

Serious questions for the multi-agent systems

- Identity
- Cohesion
- Consent
- Social and political space
- Legitimacy
- Transparency

8.9 Environment

The cost and risks

- Metatechnologies
- Prevention
- Limitation
- Compensation

- *Three Mile Island accident*

Metatechnologies: Together, legal systems and safety technologies constitute what may be called metatechnologies. These are the kind of second- or third-order technologies that operate on (rather than with) and regulate other technologies. (p.207) However, what I have in mind here is something slightly more inclusive. It is the view that a metatechnology should be understood as comprising not only the relevant technologies that regulate the appropriate technologies to which they apply, but also the rules, conventions, laws, and in general the sociopolitical conditions that regulate technological R D and the following use or application of technologies. (p.207)

Risks: A metatechnological legislative approach is often at its best not when it provides affordances by offering incentives to counterbalance negative risks, but when it imposes constraints by enforcing disincentives to cope with positive risks, that is, when it focuses on the don'ts rather than the dos. (p.208)

- risks prevention
- risks limitation and repair
- risks compensation

8.10 Ethics

E-nvironmentalism

A new approach: As we saw in Chapter 3, the information society is better seen as a neo-manufacturing society in which raw materials and energy have been superseded by data and information, the new digital gold and the real source of added value [...] ICTs are creating the new informational environment in which future generations will live most of their time. Previous revolutions in the creation of wealth, especially the agricultural and the industrial ones, led to macroscopic transformations in our social and political structures and architectural environments, often without much foresight, normally with deep conceptual and ethical implications. The information revolution—whether understood as a third one, in terms of wealth creation, or as a fourth one, in terms of a reconceptualization of ourselves—is no less dramatic. (p.218-219) The task is to formulate an ethical framework that can treat the infosphere as a new environment worthy of the moral attention and care of the human inforgs inhabiting it. (p.219) This sort of synthetic (both in the sense of holistic or inclusive, and in the sense of artificial) environmentalism will require a change in how we perceive ourselves and our roles with respect to reality, what we consider worth our respect and care, and how we might negotiate a new alliance between the natural and the artificial. (p.219)

Chapter 9

Lecture 9 (extra): Security Measures

9.1 A change of paradigm

The legislator identifies the goals to be pursued and lives it up to recipient to determine which means to use to achieve the goals.

The minimum security measures were about: the authentication system, the adoption of credential management procedures, the implementation of an authorization policy, the periodic updating of the identification of the scope of processing allowed to individual appointees and officers in charge of the operation or maintenance of electronic instruments, protection against unlawful data processing, unauthorized access and the adoption of data backup and recovery procedures.

There were some specific rules security measures, but there was a partial paradigm shift with the **Security measures under the GDPR (art.32)**, from a *right based approach* we passed to a *risk based approach*.

The GDPR brought new things, when choosing security measures, one must take into account:

- State of the art technology
- Costs of implementation
- Nature of processing
- Object of processing
- Risks and severity of consequences on rights and freedoms to individuals

9.2 Security Measures Under The GDPR (Art. 32)

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

- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

This opens the door to so-called "*soft law*. Reference must be made to:

- Sector specific regulations
- technical regulations (ISO/UNI, etc.)
- voluntary guidelines and frameworks
- case law

In the first point, *encryption* are referring to encryption of storage systems, encryption of virtual machines, encryption of connections and VPN.

In the second point:

- *Confidentiality* is preventing unauthorized access to or use of personal data and equipment used for processing. Therefore, it is necessary to adopt: authentication systems, adoption of multi-factor authentication systems (MFA and Passwordless), authorization system, information classification systems (Information classification).
- **Integrity** is ensure changes to data and systems only to authorized individuals. It is therefore necessary to adopt: appropriate authorization system; systems for tracking changes to data and systems - log management systems (SIEM); essential for compliance with GDPR, the PCI/DSS standard, and the Privacy Guarantor's orders on AdS; information classification systems.
- **Availability** is data and systems must be accessible and usable when requested by an authorized party. Therefore, it is necessary to adopt for example baxkup systems or redundancy systems.
- **Resilience** is to withstand data breaches and restore the state prior to the breach. Therefore, it is necessary to adopt, for example vulnerability assessment and anomaly detection systems, anti malware or SIEM.

In the fourth point **organizational security measures** are:

- Drafting of policies/procedures
- Identification of roles/organizational chart
- Education/Training

9.3 EU Cyber Resilience Act

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity.

Eu Cyber Resilience act is a proposal for a regulation on cybersecurity requirements for products with digital elements. The Cyber Resilience Act mandates security-by-design by creating a list of essential cybersecurity requirements for manufacturers, importers, and distributors of connected devices and services to comply with through certification, reporting, and conformity assessment. Two main objectives were identified aiming to ensure the proper functioning of the internal market:

- Create conditions for the development of secure products with digital element
- Create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements

Eu cyber resilience act covers products with digital elements. i.e. any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.

The cyber resilience act categorize covered products in:

- **Class I**: class I products have a lower cybersecurity risk level than Class II products but a higher level of risk than the unclassified or default category.
- **Class II**: class II are higher-risk products with digital elements with regard to critical cybersecurity vulnerabilities.
- **Undefined/Default**: The Default category applies to products without critical cybersecurity vulnerabilities.

Class I and Class II products are splitted in these categories based on their level of risk. Risk factors for products include:

- Whether it runs with privilege, privileged access, or performs a function critical to trust
- Whether it is to be used in sensitive environments as described by NIS2
- Whether it is to be used to process personal information or other sensitive functions
- Whether its vulnerability can affect a plurality of people
- Whether it has already caused adverse effects when disrupted

Class I must adhere to the application of a standard or complete a third-party assessment to demonstrate conformity, while Class II must complete a third-party conformity assessment. Annex III of the Cyber Resilience Act currently splits critical products with digital elements into these categories. The Default category applies to products without critical cybersecurity vulnerabilities. Companies responsible for these products will have to self-assess their vulnerabilities for improvement. According to the Commission, this category will cover 90 percent of connected devices, including photo-editing software, video games, and other commonplace software and devices.

The product of class I and II are listed in the Annex 3. Manufacturers will have to undergo a third-party conformity assessment or apply harmonized standards or European cyber security certification schemes for Class I products. Class II product manufacturers can only demonstrate conformity through third-party conformity assessment. The specific requirements for third-party conformity assessments are described in Annex VI. For Unclassified or Default Category products, manufacturers will be responsible for determining and declaring their products satisfy all essential security and vulnerability requirements. These manufacturers will have to provide technical documentation, affix the conformity mark, and draw up a written EU declaration of conformity.

The Cyber Resilience Act creates reporting obligations for manufacturers to notify the European Union Agency for Cybersecurity (ENISA) within 24 hours after becoming aware of "any actively exploited vulnerability contained in the product with digital elements" or "any incident having impact on the security of the product with digital elements." The manufacturers will also inform the users of the product of the incident as well as corrective measures that can mitigate the consumer impact. Similarly, importers and distributors of products with digital elements must inform manufacturers of cybersecurity vulnerabilities without delay. If there is a significant cybersecurity risk, importers and distributors must also inform national market surveillance authorities of the non-conformity and the corrective measures taken.

The penalties for violation are:

- Non-compliance with Annex I's essential requirements and obligations in Articles 10 and 11 subjects offending businesses to the highest fine of either administrative fines of up to €15 million or 2.5 percent of their global annual turnover for the previous fiscal year, whichever is greater.

- Non-compliance with other obligations within the Cyber Resilience Act will lead to administrative fines of up to €10 million or 2 percent of global annual turnover for the previous fiscal year, whichever is higher.
- Misleading market surveillance authorities with incorrect, incomplete, or manipulated information will lead to a fine of €5 million or 1 percent of global annual turnover for the previous fiscal year, whichever is greater.
- Member states can lay down effective, proportionate, and dissuasive rules on penalties applicable to businesses that fail to comply with the Cyber Resilience Act. Still, they must notify the Commission of the rules, measures, and subsequent amendments. National market surveillance authorities can also prohibit or restrict products from being available if the manufacturer, importer, distributor, or other responsible business proves non-compliant.