Information and technology law course

LECTURE 18 – 21 NOVEMBER 2024

FEDERICA CASAROSA – 2024/2025

Internet of Things

Different devices speak to each other, but they are not from the same manufacturer

Goal is to achieve efficiency and sustainability

IoT a definition

No universally accepted definition

Elements may be different:

- Technology
- Tools and application

Recommendation of the International Telecommunication Union:

"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"

* either you are at the center of the communication, or devices can speak to each other.

→ for the end user usually

IoT

Ecosystem composed of

- objects connected to the network through sensors → they can be whatever
- that interface with the physical world and interact with each other * is able to
- exchanging information on their status and the surrounding environment → DATA
- without the need for human intervention

Imagine the fridge recognising that we do not buy lactose products and that can be used for informing that we're lactose intolerant.

Technical structure

Perception layer

(Wearable) devices

Processing layer

middleware service (e.g. Cloud computing)

Application layer

High-level services

Challenges and risks regarding IoT devices. We are exchanging info. Worst case is the medical devices. But also storage bottles in a box; imagine an attack that makes it impossible to change what is in a box. Economic damage. We have three levels to be protected.

IoT technical architecture – security risks

Information level

- Integrity of data
- Anonimity
- Confidentialy
- Privacy protect sensitive data!

Access level ①

- Access control
- Authentication
- Authorization

Functional level ②

- Resilience
- Self organisation

② System of the medical device is still able to react and work.

↓

Be resilient, signal problems for example.

① The ones that access to data do so with this

Products that are connected = IoT! So Cyber resilience act should apply.

	Data protection	Cyber-security
General data protection regulation	√	√ of personal data
Cyber-resilience act		√
Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence		?

↱ Presented 2 years ago, will never end up in a legislation probably

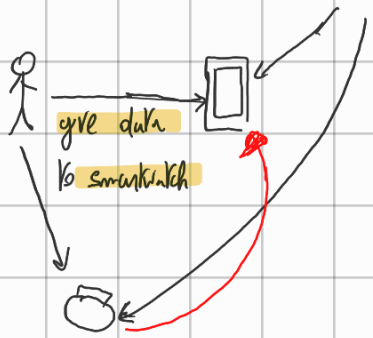
↰ Whenever there is an unjustified interference in the sphere of another individual that damage needs to be paid by the one that caused it

What are the problems?

IoT and data protection

- No binary connection between a data processor and a data subject
- Collected data can yield «fruits»
- Subjective and objective complexity
- Different types of data can be collected

App that is running (ex. Fitness app connected to smartwatch)



My smartwatch collects like: geographical pos., heartrate, running activity etc...
And the smartwatch sends this information to my smartphone.

Who's the data subject? Me. But who's the data controller? How many of them are here?
Smartwatch collects data, processed by manufacturer of smartwatch. What if I have synchronized my smartwatch with my phone, who gives me the certainty that data is not shared with the phone? Is it a joint process? Or are they two diff. controllers? It is a case by case situation. It's hard that data stays in a single silos, if a different DC gets access to data they probably use it too.
Who do I go to if I want to excercise my rights?
With the interconnectivity, there is joint connectivity with unclear relations: I don't know who are the controllers (subjective and objective complexity).
Plus I have no idea of data being collected.
* "hints": inference possibility for data,
*2 Different types of data collecting different kind of info connected to each other has a lot of inference possibility.

IoT and data protection

WP 29 - Opinion 8/2014 on recent developments in the field of the Internet of Things

- IoT "poses a number of significant privacy and data protection challenges, some new, some more traditional, but then amplified with regard to the exponential increase of data processing involved by its evolution".
- Eight main issues :
  - Lack of transparency;
  - Existence and involvement of various actors (often unknown to users);
  - Loss of control over data processing through IoT devices;
  - Difficulty in getting users' consent and quality of consent undermined;
  - Lack of granularity of the services provided by the IoT devices, with the consequence that users may be obliged to refuse the whole service if they do not accept a particular data processing aspect of the device;
  - The possibility to process more data than required for the original purposes;
  - The use of data collected from different sources and devices for different purposes than the original;
  - Security risks in the transmission of personal data (from personal devices to central services or to other devices).

① Problem: how many times do we really look at policies and not give consent?
Dark patterns are the way UI triggers consumers to a kind of choice (in general buying)
Those are not perceived by the users!

② Either you accept everything, if you want to use your smartwatch, you have to agree to every single request. You cannot say yes to some, no to others.

③ Ex: Smartphone getting access to GPS and heartrate

④ All these info are shared! Between devices, clouds etc!

Possible elements to think about:

Compatibility level

Specific and adequately informed consent: Very difficult to know this in advance
- Compare with Regulation 1807/2018 on the free flow of data

Purpose principle: what is the purpose of the processing? Make sure that users know for what data is collected

Data storage limits: how long do you need to save my data for?

Trasfer to third countries

Identification of data processor: Who is processing the data? Lots of question!

Here: even if I consent without reading, I know that I am working within some limits (GDPR): for example my shared data is pseudonymised.

Privacy by design and security by design

Accountability standards

- Pseudonyms and Reducing the Amount of Data Collected
- Consent to Transparent Terms of Processing
- Design of Privacy Policies
- Secure Transmission and Retrieval of Data

Work to give our better info to users and make it more accessible.

CyRes Act

is better to ensure security

We move from Data security to more netw. and inf. security. Also in this case I have to follow regulations:

Cybersecurity issues:

In this case I'm only looking at the manufacturers instead of data subject too. But products are connected, supply chain goes crazy.

Article 13 Cyber Resilience Act

1. When placing a **product with digital elements** on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Part 1 of Annex I.

2. For the purposes of complying with paragraph 1, manufacturers shall undertake an **assessment of the cybersecurity risks** associated with a product with digital elements and take the outcome of that assessment into account during the **planning, design*, development, production, delivery and maintenance phases of the product with digital elements** with a view to **minimizing** cybersecurity risks, **preventing** security incidents and **minimising the impacts** of such incidents, including in relation to the health and safety of users.

We have a set of requirement (Article 13, might be, not sure)

*Make a season not expected

Cybersecurity issues

Security requiriments and vulnerability handling requirements ANNEX I

Security requirements ↱ PoR: but vague as shs. I should evaluate what I do *

- risk based taking into account CIA triad
- Ensure data minimization (Vague! I don't have clear requirements) We will probably have standards that tell us this.
- Resilience against DoS attack
- Avoid network effects
- Security by design including mitigation measures
- Record of internal activity
- Updates (including automatic ones)

Vulnerability handling requirements

- Risk based
- Tests and security updates to be carried out (free for users)
- Information sharing (in particular with third party components' manufacturers)

* Ex: my smart fridge can record items, can show expiring items on the fridge exc. What could the risks be? Maybe I'm not reading things correctly and the person eats it regardless, for example! One risk. So I would want to avoid attacks related to that.

This exercise has to be done by manufacturers!

Privacy by design and security by design

Market interventions:

- ioXt Security Pledge adopted by an association ↑ group of market IoT manufacturers of IoT: avoid security problems
  - 1. No universal passwords: The product shall not have a universal password; unique security credentials will be required for operation.
  - 2. Secured interfaces: All product interfaces shall be appropriately secured by the manufacturer.*
  - 3. Proven cryptography: Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.
  - 4. Security by default: Product security shall be appropriately enabled by default by the manufacturer. ↳ as soon as you have a new device, the security level is the highest, then up to you to lower it.
  - 5. Signed software updates: The product shall only support signed software updates.
  - 6. Automatically applied updates: The manufacturer shall act quickly to apply timely security updates.
  - 7. Vulnerability reporting program: The manufacturer shall implement a vulnerability reporting program, which shall be addressed in a timely manner.
  - 8. Security expiration date: The manufacturer shall be transparent about the period of time that security updates will be provided.

* Make sure that intervention by user is secure

Liability for damages of IoT

Liability for damages

- Article 82 GDPR (liability for the parties involved in the processing of personal data)
- Coordination with Product liability directive
  - Compensation for damage deriving from a defective product
- Ai based IoT?

Liability in Artificial intelligence

Proposal for an AI Liability Directive

Purpose : improve the functioning of the internal market by laying down uniform requirements for non-contractual civil liability for damage caused with the involvement of AI systems.

- Promote the rollout of trustworthy AI,
- Harvest its full benefits for the internal market by ensuring victims of damage caused by AI obtain equivalent protection to victims of damage caused by products in general.
- Reduce legal uncertainty for businesses developing or using AI regarding their possible exposure to liability and prevent the emergence of fragmented AI-specific adaptations of national civil liability rules.
  - However, being a proposal for a directive, it leaves the Member States some flexibility for their internal transposition of the legislation

Liability in Artificial intelligence

- 'extra-contractual' civil liability rules (rules providing a compensation claim irrespective of a contractual link between the victim and the liable person)
- Any type of victim (individuals or businesses) can be compensated if they are harmed by the fault or omission of a provider, developer or user of AI resulting in a damage covered by national law (e.g. health, property, privacy, etc.).
  - Scope of application excludes liability in the field of transport, the proposed revision of the Product Liability Directive or the Digital Services Act, as well as criminal liability.

Liability in Artificial intelligence

Article 4 : presumption of causality

- causal link between non-compliance with a duty of care under Union or national law (i.e. the fault) and the output produced by the AI system or the failure of the AI system to produce an output that gave rise to the relevant damage
- claimants seeking compensation for damage caused by AI systems have a more reasonable burden of proof and a chance of a successful liability claim.

It will be easier for people alleging injury from AI to succeed in bringing claims, given the complexity of the AI environment (i.e. 'black box').

- if a victim can show that someone was at fault for not complying with a certain obligation relevant to their harm, and that a causal link with the AI performance is reasonably likely, the court can presume that this non-compliance caused the damage.
- NB no full reversal of the burden of proof