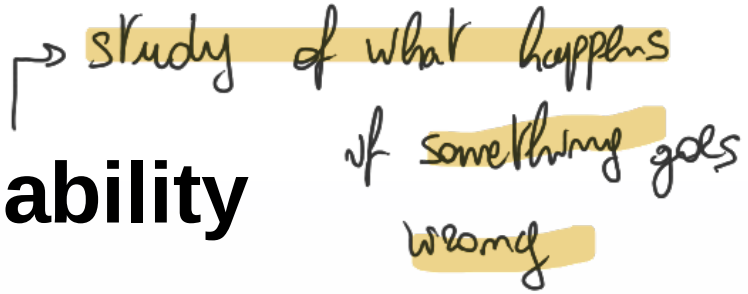
Msc Cybersecurity
UNIPI
28 November 2024–hybrid

BRIEF

Biorobotics Research &
Innovation Engineering Facilities

Internet of Things (IoT) & Liability



Francesca Gennari, PhD
Research Affiliate, Lider-Lab
Scuola Sant'Anna

Sant'Anna School of Advanced Studies – Pisa
Università degli Studi di Napoli Federico II
Politecnico di Bari
Finanziato dall'Unione europea NextGenerationEU
MUR

Presentation outline

Connection between Italian rules and EU rules that concern liability.

2 main groups of liability laws: private rules in case of contracts (ex. run over by someone).
↳ related to private people.

↳ Criminal law

State and individual concerning rules.

- IoT. Recap
- The IoT composition: hardware and software (preliminary outline)
- Types of liability in private law (preliminary outline)
- Structural problems and liability rules: contractual liability
- The EU digital policy
- Structural problems and liabilty: defective products
- Structural problems and liability rules: Tort liability and AI
- Future Perspectives

We will focus on the first one.

Finanziato dall'Unione europea NextGenerationEU

IoT: a technology as elusive as it is present

Difficult to define of course! Even from a technical PoV. Very versatile.

Definition problems from both a technical and legal point of view

Very versatile technology: can be applied from medicine to industry, from agriculture to the home

Structure: centralised, focused on the cloud layer

more vulnerable a cysec PoV

The peripheral part of the IoT system often lacks sufficient computational power and -especially in consumer applications- this prevents more extensive use of encryption and other technical protection measures

Problem: internet traffic (over-fitting) and data deluge

we don't want to overburden the traffic.

creation of devices, use of energy.

Problem: Technology-induced pollution

Finanziato dall'Unione europea NextGenerationEU

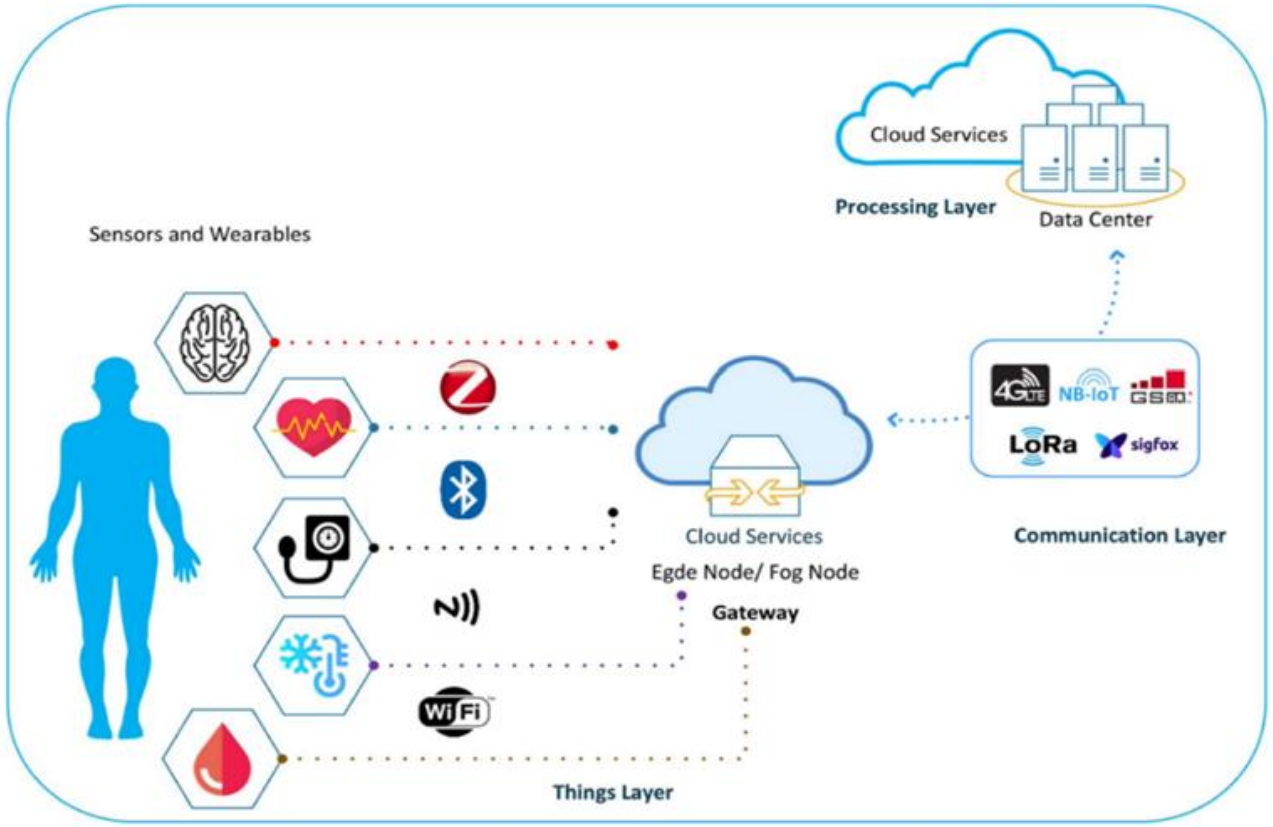


FIGURE 1. Three-tier architecture of the IoT healthcare system.[1]

Strategy is also giving more computational power to edges or fog.

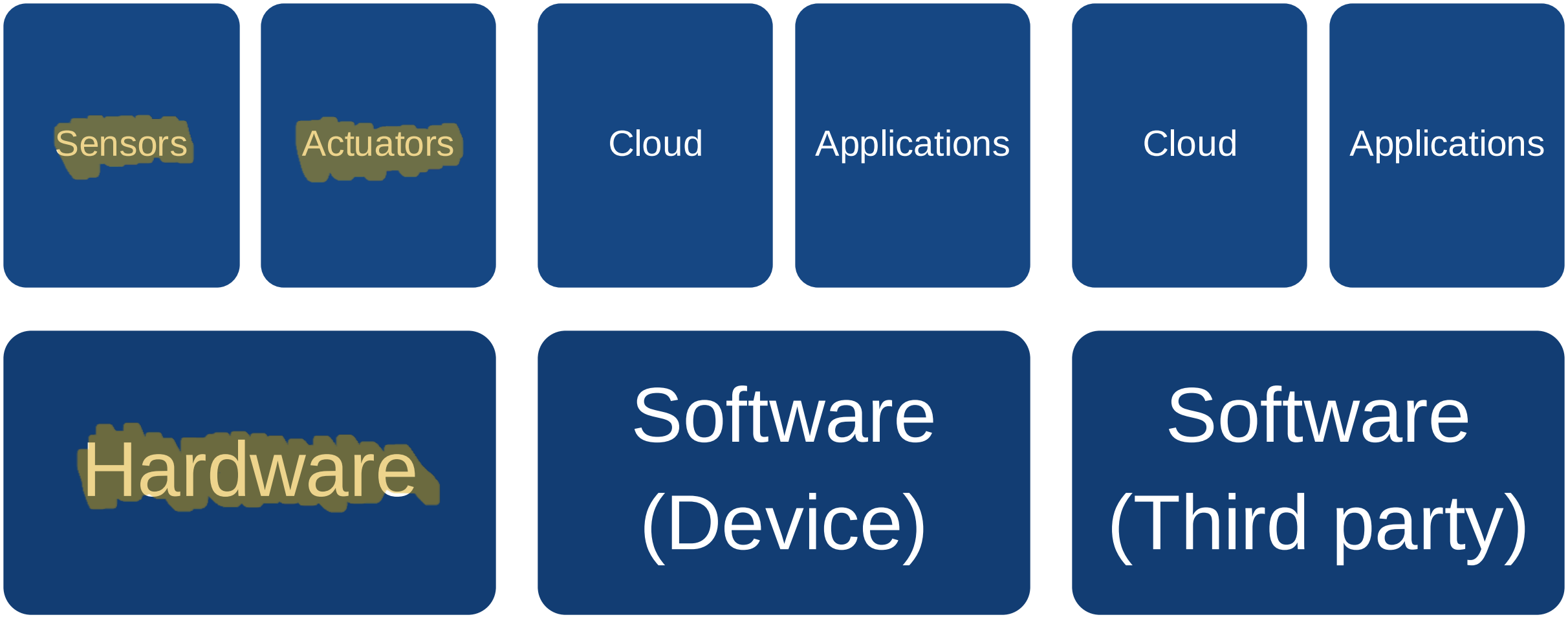
Finanziato dall'Unione europea NextGenerationEU

MUR

BRIEF

The IoT composition: hardware and software. A preliminary outline.

If we look at any device to understand where damages come from, a scheme is useful.



Finanziato dall'Unione europea NextGenerationEU
MUR
BRIEF

It so versatile that devices can have softwares, it can rely on cloud or on an application of the system. But it might be that on this device you have third parties providing SW, like apps for phone.

Third party softwares also are there.

Plus, there are medical applications that only have a SW. There's sw that interfaces and drives the HW, we have medical SW certified as medical devices.

Preliminary outline: the various types of liability in Italian and EU private law

1st Scenario

Negotiation before contract ex: one party unexpectedly withdraws → **pre-contractual liability** (Articles 1337-1338 Civil Code)

2nd Scenario

Existing contract but

1) non-performance (default),

2) delay in performance and

3) improper performance of the contract→ **contractual liability** (Articles 1218 et seq. 1321 et seq.)

3rd Scenario

Two parties, **lack of contract**, one harms the other→ **non-contractual liability** (Article 2043 of the Civil Code) (now also applicable to GDPR personal damages) it is also known as tort or extra-contractual liability

4th Scenario

Dangerous building, animal, exercise of a dangerous activity, subordinate worker, uncapable person injures someone → form of specific non-contractual liability (**quasi-objective** or **aggravated liability**, Articles 2047- 2054)

5th Scenario

Malfunctioning of a consumer object

→ **product liability** (Consumer Code Legislative Decree 206/2005, Articles 114-127, transposition Directive 85/374/EC)

Warning it will need to be changed because of the PLDU approval

Finanziato dall'Unione europea NextGenerationEU

To understand liability: EU law come way cuffer the national existing causes. We have similar laws in other EU MS but they also have differences for historical and cultural purposes.

* Cause of selling PC: I could have spent my time in looking for other people!

① Ex. I bought something and you don't send it.

② I don't have any relationship with the person that harmed me. It is a bit more complex to find liability: I have to explain the LINK OF CAUSALITY and the NEGLIGENCE or VOLUNTARY ACTION.

③ Bad condition buildings, fault of the owner. In this case: the owner needs to prove that they did anything they could to prevent the damage to the person. For this reason quasi-objective liability.

⑤ Malfunctioning of a product. Is more similar to the 3rd scenario, but also a bit about it, because manufacturer should be the point of contact.

This is at eu level. The implementation is in CODICE DEL CONSUMO, but we have a renewal now.

When do I apply a kind of liability instead of another?

It depends on the **procedural civil rule laws** of the country which we examine

For instance, in Italy, it is possible **to graduate and put an order to your claims** and request the judge to ascertain that the counterpart can be liable because of contractual liability, and/or tort or strict liability (1)

Generally, people will try to rely on **contract** (hence contract liability) as it is easier to demonstrate that the counterpart breached a duty or did not deliver an expected result. If we are talking about a consumer object that I bought and that injured me because of an internal malfunction I can also use the product liability rules. You can try both if procedural laws allow that because there was a **contract** at the beginning (contractual liability) and a **product** (**strict/extra contractual or tort liability**)

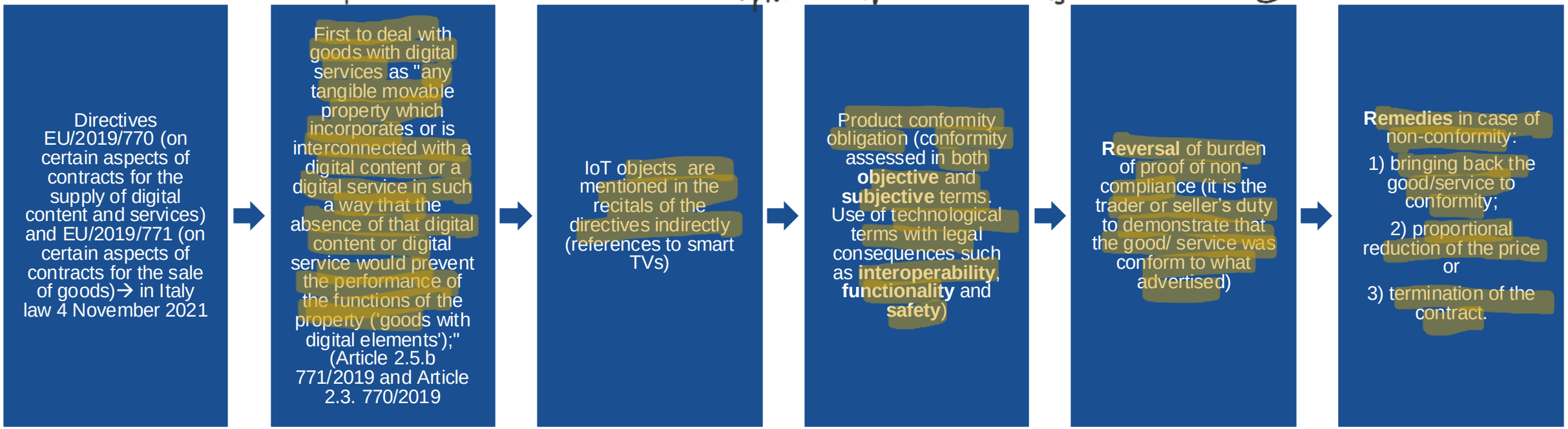
The rule described is not absolute: if I am run over by a **stranger** in a car there is no contract or product at stake. I will have to use non contractual liability

Finanziato dall'Unione europea NextGenerationEU

Is there a rule to choose liability rules? When I buy something, can I use contractual and product liability?

① Possible to go for different types of liability for liability. In other countries you can't.

Structural problems: IoT and contractual liability law



Finanziato dall'Unione europea NextGenerationEU

Manufacturers define what a product can do (define conformity requirements), that can be objective (can do this because it has this components) and subjective ones: for example usability of the device. Something that is related to the user.

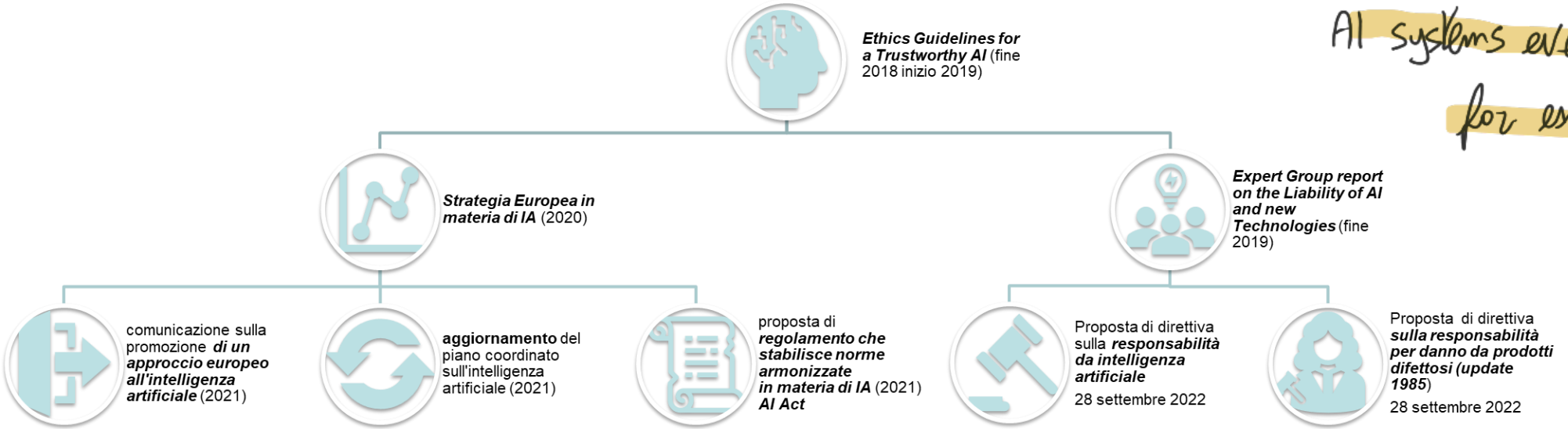
For the first time, there is the use of interoperability, functionality, safety are used in particular in this field.

① It's the part that had the damage that has to prove something, normally. Here not like that.
② Remedies that are linked to non-conf: manufacturer of IoT has different options.
(2) "I want back 80% of the money".

So this is a case of contractual liability and have these tools to file a liability lawsuit.

The European digital policy I.
IoT: between AI and product liability

IoT and AI have thinner and thinner differences.



AI systems even at the edge for example!

My was clear to the EU legislators there was a need to understand what happens before and until you put AI on the market (AI act) but also what to do in case AI brings damages.

Finanziato dall'Unione europea NextGenerationEU

The European digital policy II.
2024 a momentous year for digital policy

Approval of the AI act in March 2024→ Official publication in the EU Journal in July 2024 → Entry into force 1 August 2024.

Approval of the Directive on the non-contractual liability of AI→ ? (I will explain in a short while why it is not known what is going to happen with this project)

We do not know! Related a lot on 1st proposal of AI act. So this directive is a bit useless

Approval of the Product Liability Directive Update (PLDU) in March 2024→ Official Approval on 10 October 2024 by the council→ Official Publication in the EU Journal on 18 November 2024

Applicable in 2026

Finanziato dall'Unione europea NextGenerationEU

European Digital Policy III. The AI Act in short a)

'Horizontal' legislation concerning the use of I systems

New Definition of AI (very general): 4(1) AIA '*AI system' means a **machine-based system** designed to operate with **varying levels of autonomy**, that may exhibit **adaptiveness after deployment** and that, for explicit or implicit objectives, **infers**, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*;

Article 5: prohibited AI systems:, subliminal effects, vulnerability, social-scoring (reliability and trustworthiness)

Article 6: High-risk AI systems: if security component other product (Annex II) and conformity assessment considers it as high-risk + Annex III (e.g. biometric identification, management and operation of critical facilities)

Important high-risk AI systems: obligations on how to create and train AIs, obligations to certify algorithms with notified bodies, and registration in a common database

Finanziato dall'Unione europea NextGenerationEU

* JV is stated that any device/system that also falls under these regulations, then this is a high risk. PDR is between those regulations.

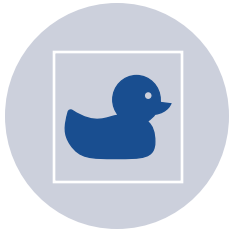
A lot of overlapping and obligations etc.

European Digital Policy IV. The AI Act in short b)

BUT… **CHAT GPT** HAPPENED, SO IN THE ORIGINAL PROPOSAL THE **GENERAL PURPOSE AI (GPAI)** MODELS WERE INTRODUCED. THEY CORRESPOND TO LLMS AND FOUNDATION MODELS.

THEY HAVE **SPECIFIC RULES** (E.G. NO DEEPFAKES, TRANSPARENCY OBLIGATION)

THEY ARE DIVIDED IN 2 GROUPS: ABLE TO CREATE **SYSTEMIC RISK OR NOT**. THE DEFINITION OF SYSTEMIC RISK IS VAGUE BUT IT ITS MEANS THAT THE NEGATIVE EFFECTS OF A GPAI CAN INTEREST A HUGE NUMBER OF EU CITIZENS AND ATTEMPT TO THEIR SECURITY, FREEDOM AND HEALTH

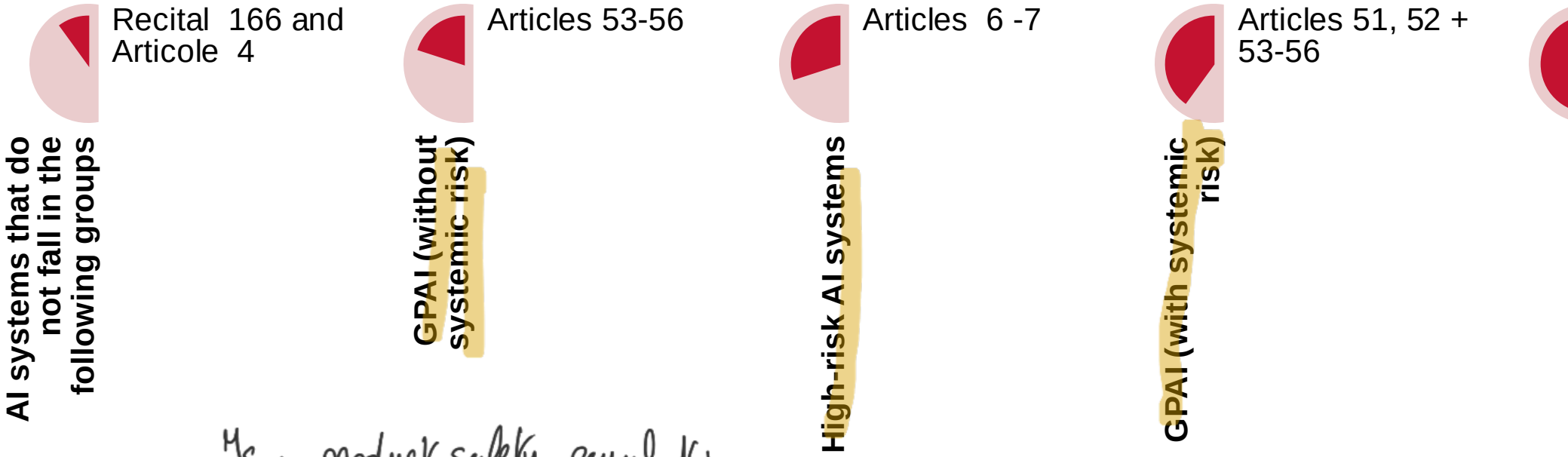


THE SYSTEMIC RISK IS PRESUMED ON THE QUANTITY OF FLOATING POINTS OF OPERATION (FLOPS) THAT THE MODEL CAN REACH. BEYOND 10 25 FLOPS A GPAI IS PRESUMED ABLE TO CREATE A SYSTEMIC RISK

HOWEVER… NOBODY KNOWS HOW TO ADAPT THESE RULES ESPECIALLY WHEN THE AI SYSTEM IS CONSIDERED AS HIGH RISK BY THE AI ACT (SUCH AS A MEDICAL SOFTWARE) AND USES A GPAI TO WORK (THE CHAT OF A CONVERSATIONAL AND REHAB ROBOT FOR KIDS WITH NEUROLOGIC DISORDERS). DOES THE RULE ON HIGH-RISK AI SYSTEMS COMBINE WITH THE ONES ON GPAIS? IT SHOULD BE BUT IT IS NOT CLEAR HOW

Finanziato dall'Unione europea NextGenerationEU

European Digital Policy V. The AI Act in short c)



Yes a product safety regulation.
Not so different from the MDR. The higher the risk, the more the manufacturer should be accountable and liable for damages.

The higher the risk, the more the AI providers risk will be

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
BRIEF

European Digital Policy VI. The AI Act in short d

not thought about at the beginning.

ex: taking a GPT and making your own from that one.

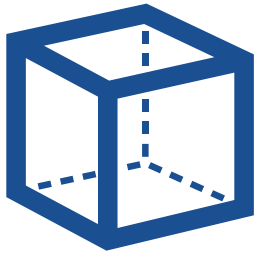
AI provider: creates the AI system

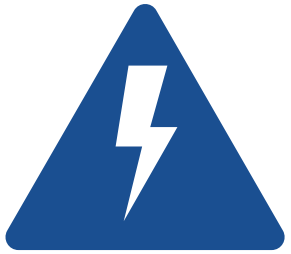
AI 'downstream provider' '*means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the model is provided by themselves and vertically integrated or provided by another entity based on contractual relations*.

AI deployer: who uses the AI system. It could be a professional user (hospital) but also consumer.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
BRIEF

Structural issues: the IoT and product liability I





real news of today: kind of ①.

Characteristics of product liability:

(*Quasi*-) **Strict liability:** Allegedly, more favourable for the consumer to prove against the producer than Non-contractual liability

They only have to prove damage, psychological damage, defectiveness but before, directive was of 1985, not up to date.

Elements to be proved:

Damage

Defectiveness of the product and

Causal link between the first two elements

(Possibility for the producer to exempt themselves)

Innovation from EU law:

the directive has remained unchanged for more than 38 years without major changes

BUT

Much contested by some states that had a more protective tradition of consummation law

AND

Radical technological change in the last 5 years with IoT and AI development made it necessary to modify the directive ①

Finanziato dall'Unione europea NextGenerationEU

① SW intended generally (AI or not) is considered a product! If a product is defective, the newly approved dir applies.

Structural issues: the IoT and product liability I

Just say SW because both AI and IOT have in common.

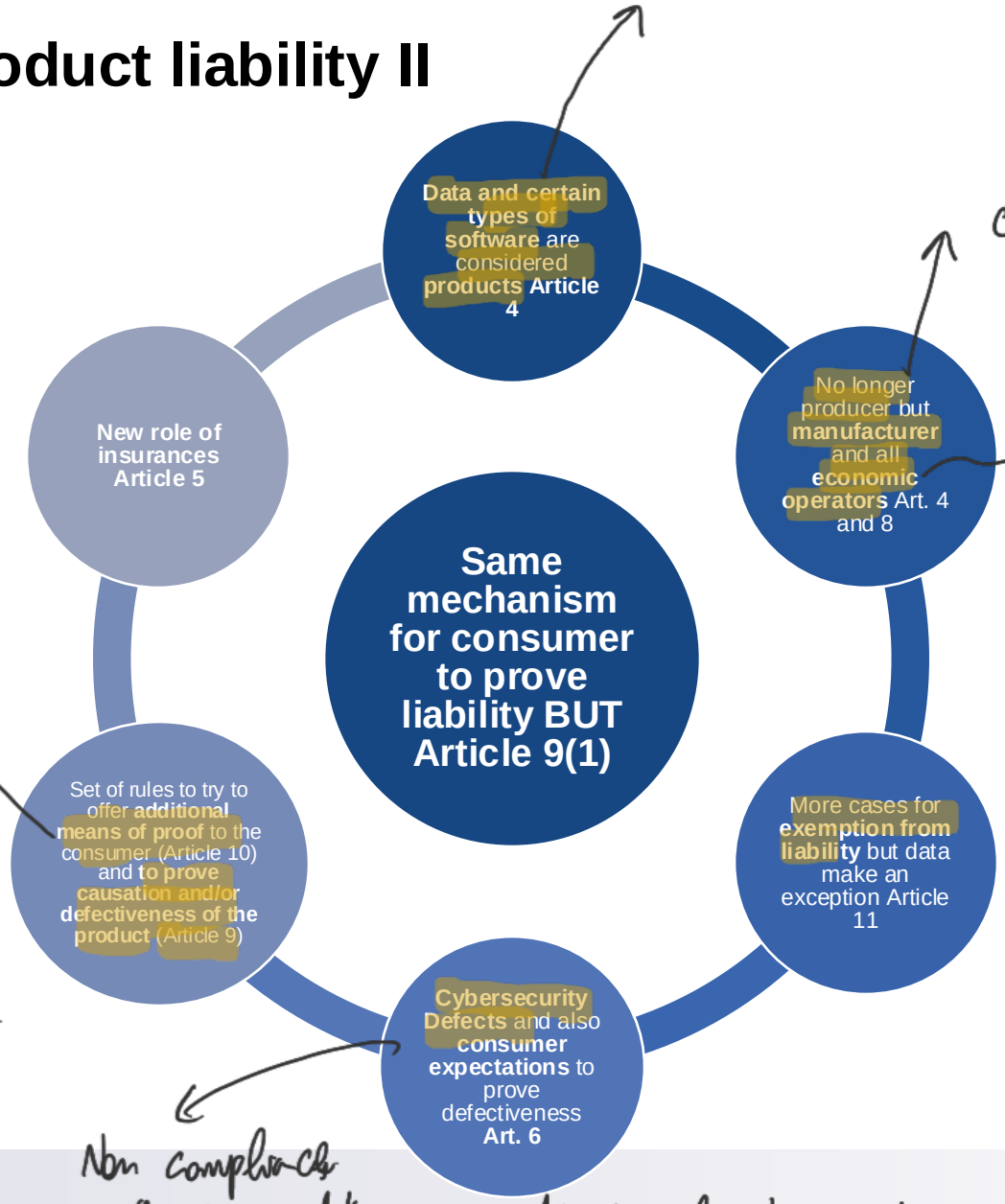
Software, included AI systems is considered a product which can be defective

In fact, the AI act can be considered a safety legislation and like all safety legislations it sets standards to produce products

If the said product is defective, despite the fact that it is an AI system, the newly approved product liability directive applies!

Finanziato dall'Unione europea NextGenerationEU

Structural problems: the IoT and the new product liability II



change from producers

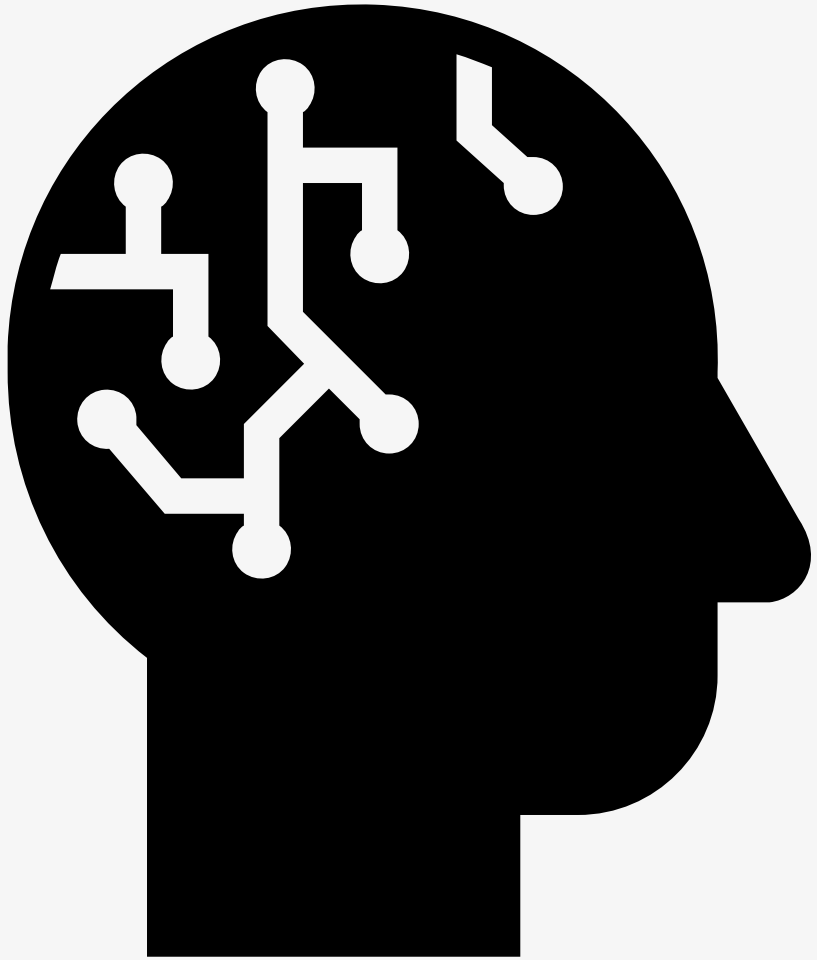
They can be importers, platforms etc Despite the manufacturers are liable, IoT devices are very very complex systems! HW made by someone, SW by someone else etc.

Introduced procedural rules on presumptions: how can someone that knows nothing about AI prove causality links? Even experts have problem!

Providing a plausible cause of damages, without being able to prove link is okay. As long as you give plausible cause. BUT, presumption will not be applied easily, you need serious or certified psychological evidence.

Non compliance with CS safety requirements can also be proved

Finanziato dall'Unione europea NextGenerationEU



Structural issues: IoT and non-contractual liability and the case of AI part I. The proposed directive on the civil (= tort, extracontractual) liability of AI

- **Complementary** to the AI act
- **High v. low-risk** AI systems
- *IoT and AI: what is their relationship? Important to decide which set of liability rules to apply* ***What about the GPAI***
- AI act concerns **software** *not covered by producer responsibility* and those types of AI systems that are described as *high-risk* in the AI act
- The draft directive is very short, but two articles are crucial (3 and 4)

Finanziato dall'Unione europea NextGenerationEU

Structural issues: the IoT and non-contractual liability. The case of AI part II

- Article 3(1): **Disclosure of evidence**→ on condition that *facts and evidence supporting the plausibility of the claim for damages* are brought to support it
- Article 3(4): **Balance** between **disclosure** of evidence and **confidentiality** to also protect **intellectual property**
- Article 3(5): if a defendant refuses to submit the evidence requested, their AI system is presumed to have caused the damage (simple presumption)

Finanziato dall'Unione europea NextGenerationEU

Structural issues: IoT and non-contractual liability and the case of AI part III

- Article 4: divided into two parts depending on whether the AI system is considered high-risk by the AI act

Presumption for causal link, not fault.

- Part 1: Rebuttable presumption of causation in the case of fault only if all the following conditions are met:

You have to demonstrate of all 3

(a) the claimant has demonstrated or the court has presumed pursuant to Article 3(5), the fault of the defendant, or of a person for whose behaviour the defendant is responsible, consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damage that occurred;

(b) it can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output;

(c) the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage.

Finanziato dall'Unione europea NextGenerationEU

Structural issues: the IoT and non-contractual liability. The case of AI part IV

- Part two: if the IA system is high-risk and if the following requirements are not met, the IA system is presumed to have caused the damage First condition proved but what about the other two?

(a) the AI system is a system which makes use of techniques involving the training of models with data and which was not developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in [Article 10(2) to (4) of the AI Act];

(b) the AI system was not designed and developed in a way that meets the transparency requirements laid down in [Article 13 of the AI Act];

(c) the AI system was not designed and developed in a way that allows for an effective oversight by natural persons during the period in which the AI system is in use pursuant to [Article 14 of the AI Act];

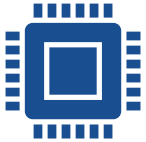
(d) the AI system was not designed and developed so as to achieve, in the light of its intended purpose, an appropriate level of accuracy, robustness and cybersecurity pursuant to [Article 15 and Article 16, point (a), of the AI Act]; or

(e) the necessary corrective actions were not immediately taken to bring the AI system in conformity with the obligations laid down in [Title III, Chapter 2 of

Finanziato dall'Unione europea NextGenerationEU

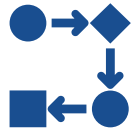
Structural issues: the IoT and non-contractual liability. The case of AI part V

What is the problem with this proposal?



It is already old! It was presented in September 2022 and took into consideration the first AI Act proposal

In that proposal there was no mention of generative AI and the GPAI of the then approved AI Act

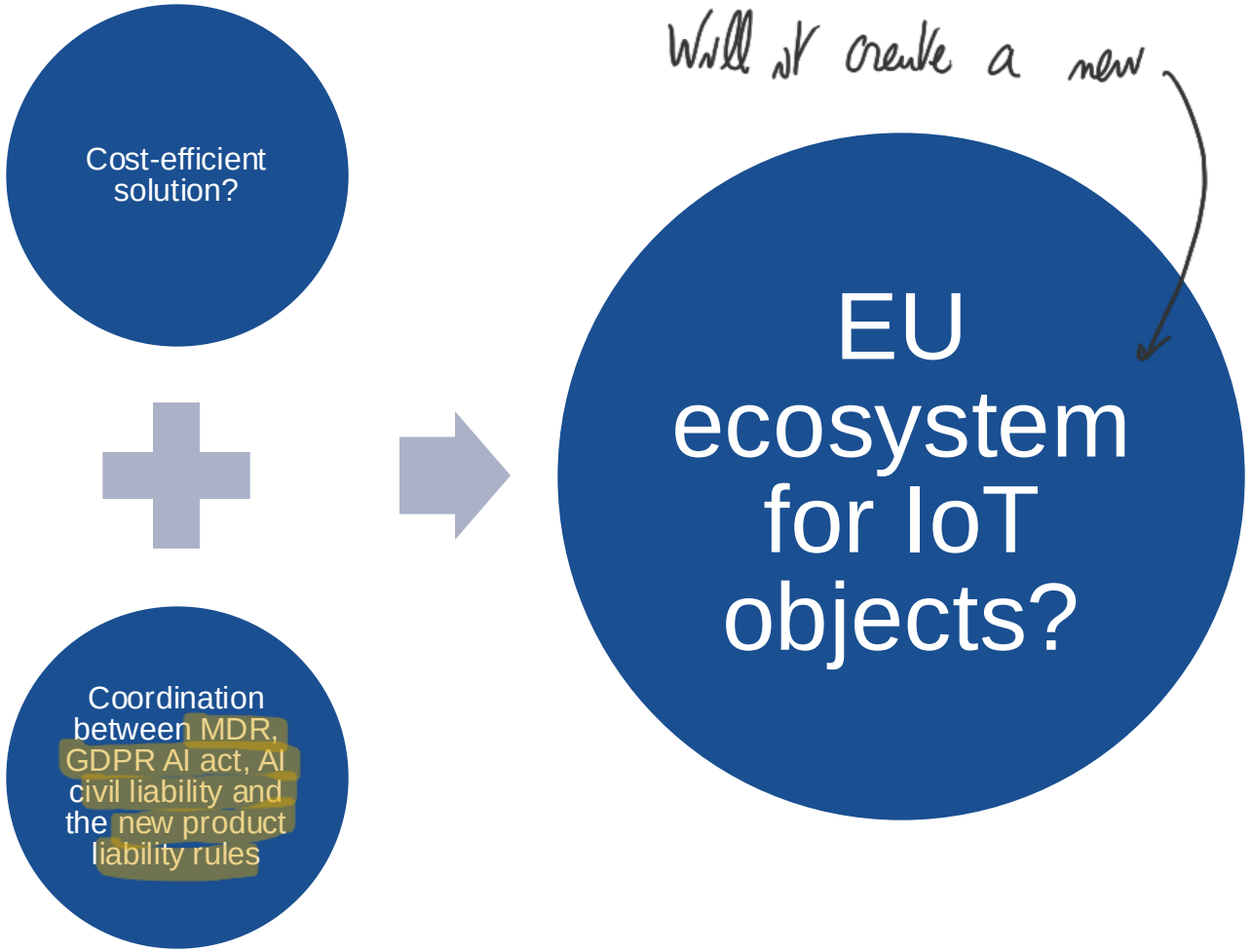


It needs to be updated and modified→ But will it? It is a lengthy process

It is a minimum harmonization directive, that means that

Finanziato dall'Unione europea NextGenerationEU

Structural problems:
the IoT and product liability III (update proposal)



Finanziato dall'Unione europea NextGenerationEU

Future perspectives: policy and technology

Until now there has been a need to regulate technology to avoid regulatory gaps and cause material and non-material damage (e.g. data breaches or cyber attacks)

Need to adapt existing legislation to the GDPR and to technological progress

A shared technical-legal language is being created and solutions are being reshaped according to needs (e.g. operator obligations, presence or absence of notified bodies as in the medical device regulation and the cybersecurity regulations)

Many of these are still proposals, one cannot be sure that they will not change between now and their approval, but the theoretical framework will not change that much

Legislation has taken stakeholders' opinions into account, and proposals have been approved and will be applied shortly

Work in progress: hybridisation of IoT technology with others (AI, DLT/Blockchain, Digital Twins) that may require regulatory adaptation

Finanziato dall'Unione europea NextGenerationEU

Any questions?

Finanziato dall'Unione europea
NextGenerationEU

Thank you for your attention

Francesca.Gennari@santannapisa.it

Finanziato dall'Unione europea NextGenerationEU

MUR

BRIEF