Vilnius University Faculty of Law
Department of Private Law

Heythem Abidat
2nd study year, International and European Law Study Programme Student

Master's Thesis

Legal Issues of Cybersecurity in Internet of Things
Kibernetinio saugumo teisiniai klausimai daiktų internete

Supervisor: Prof. Dr. Rimantas Simaitis

Vilnius
2025

Abstract and keywords

This thesis examines the legal issues of cybersecurity in the Internet of Things and evaluates how well current laws protect users and service providers. The study shows that Internet of Things creates new risks because it connects physical devices with data and services in ways that traditional legal rules did not anticipate. This paper reviews the main legal frameworks in the European Union and United States and at the international level and finds that most of these laws were not designed specifically for the Internet Of Things. As a result they often leave important gaps in security, responsibility and user protection. The research explores problems related to liability, consumer contracts, privacy and cross border data flows which become more complicated in a connected environment. The thesis invited to a clearer, updated and harmonized legal rules and stresses out that they indispensable. These rules should focus on security by design, stronger protection of personal data, better allocation of responsibility across the supply chain and more international cooperation. By addressing these issues the Internet of Things system can become safer, more reliable and more respectful of users' rights.

Keywords

Internet of Things, Cybersecurity, GDPR, NIS2, Cyber Resilience Act, Digital Data, Liability, Consumer Protection, Cross Border, Data, Human Centric Data, Legal Gaps, International Cooperation, Vulnerability.

Table of contents

Introduction

Relevance of the Topic

Nowadays The use of The Internet of Things (IOT) became crucial in our daily uses, it connects billions of smart devices, such as phones, watches, sensors, vehicles and machines that can collect, receive, send and share data automatically in a sophisticated way. These technologies make daily life easier and help users become more efficient. However, as more devices connect to the internet, new risks also appear. Weak security, data breaches, accountability… and the lack of clear rules make IoT systems easy targets for cyberattacks and cyber breaches.

Because of this, questions about the legal issues of cybersecurity in the internet of things have become very important. existing laws like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the United States and the Budapest Convention on Cybercrime NIS2 DIRECTIVE, Cyber Resilience Act and all relevant laws, were not created specifically for the internet of things, but in same time these laws help to protect user's data, they do not fully cover all the risks connected with the Internet of Things devices. Therefore, there are many legal gaps and missing improvements that must be addressed.

It is worth mentioning this thesis has a theory importance and practical as well, it consists all the theory concept on both cybersecurity and IOT and it allows any person interested in this topic to know how the practical issues of the respective thesis can be avoided

The legal issues of cybersecurity in the internet of things can be relevant and important for Lithuania, the country is working on digital transformation and smart city projects. Lithuanian law still needs clear rules for IoT devices, cybersecurity standards and the protection of personal data in connected devices. Studying these legal issues helps to improve both theory and practice of law, by showing how existing laws like GDPR or CCPA can be applied in new areas such as smart homes, health devices, or transport systems and even industries.

Aim and Objectives

The main aim of this thesis is to analyze how well current laws protect both users and service providers and what kind of legal reforms are missing in order to fill all gaps.

To reach this goal, the work sets five objectives:

1. Define IoT and cybersecurity and how it works.

2. Determine existing laws that deal with IoT cybersecurity.
3. examine who is responsible when IoT systems fail or are hacked.
4. identify gaps and differences between international and national laws.
5. suggest legal reforms, new approach that can make IoT safer, clearer and more reliable.

After analyzing and determining all these points we will be able to answer our main question: what are the legal issues of cybersecurity in the internet of things?

Object of the Research

This thesis focuses on the legal issues related to cybersecurity in the Internet of Things, including describing what is "IOT", what the legal instruments say about cybersecurity of IOT and how the law can protect users and define when and who is responsible when problems occur, it also ends with suggestions and possible improvements.

Research Methods

The descriptive, analytical and comparative methods were used because they are the most suitable for the nature of this research.

The descriptive method was applied by collecting different data and information which are highly related to the legal issues of cybersecurity in the internet of things and describing them in order to reach the desired results like giving definitions and determining different applicable laws.

The analytical method was also used by analyzing the previous studies and especially to analyze the respective laws to identify the specific legal issues of cybersecurity in the internet of things for the purpose of giving recommendation at the end of this thesis.

Finally, the comparative method was used to compare both of scholars opinions and international laws and understand the point of view of each legislator separately, so that it could be more efficient later to suggest effective solutions and fill all the gaps.

Originality (Novelty)

The originality and novelty of this thesis appear in two aspects:
The first aspect is the style and method used in this thesis. Unlike previous studies, it focuses on analyzing the technical aspects of the Internet of Things and combining them with the legal perspective. Therefore, this research is a comprehensive thesis from beginning to the end.

The second important aspect is that we are in a digital age and data is not only something personal, it is also commercial. People and companies are creating apps, algorithms, databases, digital artworks and other valuable digital assets every day. But the legal tools we use to protect these digital data are not always clear and even outdated sometimes.

At the same time, individuals are losing control over their personal data, which is often stored and used by centralized platforms containers, then they sell it to third parties. Therefore, there is an urgent need for an updated approach. An approach evolves in a way that protects digital data while giving individuals more control through a human-centric data model. Instead of centralized data model

What is happening is that we should trust companies when it comes to our data, because we don't know what they have collected and we don't know what they are doing with our data. However, by implementing a personal container which is controlled and owned 100% by users, we will even be able to reshape data's rights. To make it clear, users will be able to access, delete, control their data by default not by demanding these from companies.

Main Sources

This thesis consists of three main types of sources: legal instruments, books and articles (previous studies) and delivered lectures .

First, important legal regulations have been used, such as the General Data Protection Regulation (REGULATION (EU) 2016/679 GDPR) , California Consumer Privacy Act Of 2018 ,the Budapest Convention on Cybercrime, the NIS2 Directive, the Cyber Resilience Act. These are the main rules that address cybersecurity and data protection and tried to implement these legal instruments in the respective thesis.

Second, previous academic works like Cybersecurity in the Internet of Things: Legal Aspects by Rolf H. Weber and Evelyne Studer and the book :*Internet of Things and the Law* by Guido Noto La Diega. Their works were an eye opener to know the structure of this thesis.

Finally, lectures which have been delivered at Vilnius University, "cybersecurity Law and Cybercrime" by Dr. Joanna Kulesza and "Data Protection and Privacy Law "by Dr. Paulius Jurčys and Doctoral Candidate Goda Strikaitė Latušinskaja. These lectures gave me new and recent examples about data protection, cybercrime and helped to find the best recommendations.

In writing this thesis, AI was only to improve the language, correct grammar and help organize the list of sources. All legal arguments, explanations, and conclusions where prepared independently.

1-Part I conceptual Foundations of Internet of things and Cybersecurity

Part I gives the basic understanding of the Internet of Things and why cybersecurity is so important for it. As nowadays devises, watches, cars, home devices or medical tools are connected to the internet, and these smart devices indeed collect data also communicate with each other and make our lives easier and more convenient. As a result Internet Of things is becoming a big part of modern life going through smart cities and even e-commerce, healthcare and industry.

However, when more devices become connected the security risks and legal issues also going to appear, knowing the fact that connected devices are cheap and poorly protected or have weak passwords and do not receive updates, which makes them easy target for hackers. A simple attack on one device can affect a whole home, hospital, company, or even a city (smart cities), these issues show why understanding cybersecurity is essential.

In this part, an explanation of the Internet of Things will be given , how its systems work, where it is used and what benefits and problems it creates. also look at the main weaknesses of Internet Of Things devices and the common cyberattacks they can faced and how the digital world and the physical world become linked. So basically on overview regarding Internet Of Things will be given in order to reach out the legal issues and dive deep into solutions afterwards.

Chapter I Introduction to Internet of things

To know what are legal issues of cybersecurity in the internet of things, we should know first what is “internet of thigs”. Therefore, a definition will be addressed together with the most uses areas of internet of things finishing with the impact of this technology in the real, physical word.

1.1 Definition and architecture of internet of things

There are so many different definitions for the internet of things, legal scholars agreed that a unified definition is missing. However by describing the components of the internet of things a definition could be found easily

"Internet Of Things" first time was mentioned by Kevin Ashton on 1999, as a title of presentation that he made back that day.[1]

The internet of things is "an inextricable mixture of hardware, software, service, digital content and data with (inter)connectivity, sensing and actuation capabilities and interfacing the physical world".[2]

Or in another way, Internet Of Things is where the internet connectivity and computing capability Extend to different physical objects like devices and sensors. [3]

As a result and from two previous definitions, the main components of The Internet Of Things are: Internet, Devices, Sensors, Data and a software system .

The best simple example of the Internet of things are: smartwatches, smart glasses, , wearable health trackers. Each one of these devices has sensors, driven by a software, which going to collect Data from the physical environment, at the end it will be readable data to users.

Internet of things architecture is more complicated, legal scholars prefer to mention three main layer, the first layer is:

Perception layer, which includes sensors and devices which allowsto collect data from our physical world.[4]

Network is the second layer which transfer data through communication technologies, the most two popular are WIFI and BLEUTOOTH to the cloud systems or servers.[5]

Third one is called application layer, where all the collected data is processed and turned into practical service, for instance smart homes, smart cities monitoring.[6]

Everything together provides a full sense, communicate and transfer of data system connecting digital world with the physical one.[7]

---

[1] ASHTON, Kevin (2009). That "Internet of Things" Thing [online]. https://www.rfidjournal.com/that-internet-of-things-thing, p.11

[2] LA DIEGA, Guido Noto (2018). Internet of Things and the Law [online]. London: Routledge. ProQuest Ebook Central, p. 11.

[3] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p. 11.

[4] WU, Miao; LU, Ting-Jie; LING, Fei-Yang; SUN, Jing et al. (2010). Research on the architecture of Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) 2010, Vol5,[online].https://www.researchgate.net/publication/224175757_Research_on_the_architecture_of_Internet_of_Things, p. 1.

[5] Ibid, p1.

[6] Ibid, p1.

[7] Ibid, p1.

1.2 Internet of things uses

2025's technologies have been improved a lot compared to previous years, consequently the uses of the internet of things technology evolves in a way that we can find it anywhere, even i industry area , manufactures, and government section., it can be hard to list all different uses, therefore the most main uses of the internet of things are as follows:

- **Smart cities:**

A smart city uses digital technologies such as Internet Of Things Ecosystem, AI and big data to enhance urban living and making services more efficien and to reducing waste, improving safety and ensure better communication with citizens. It's about using tech to solve real life urban problems like traffic jams or pollutions even crimes and resource management while keeping human needs and rights at the center.

The Smart cities in general use their own systems, sensors and camera along with collecting data from private companies and individuals connected devices, which connected through the internet of things and because the Internet Of Things is a global network where all devices connected together, these devices will share information which can be studied for different purposes including solving crimes, making decisions, as a result the Internet Of Things can be a prominent solution for smart cities to resolve transport, energy, security issues because one of the most important goals is to keep citizens safe and efficient [1]

The using of this data can raise so many legal issues, cybersecurity issues especially, this issues will be addressed later.

Internet Of Things devices collect huge amount of information about people's everyday activities, hence it could help the judicial system to investigate in crimes or what truly happened during a crime because of the cameras footages and sensors.[2]

At some point we should agreed on that. Although the different legal issues come from the use of the Internet Things, this technology has so many benefits.

- **E-commerce and Payment**

in 2018 amazon opened it first store " Amazon Go" in USA. This store basically works fully automated without workers, cashiers, or even payment methods. It has a payment process deducting money from amazon app once the customer leaves the store, sensors

[1] LOSAVIO, Michael M.; CHOW, K. P.; KOLTAY, Andras et al. (2018). The Internet of Things and the Smart City:Legal challenges and possibilities. Security and Privacy, 1(3) [online]. https://doi.org/10.1002/spy2.23, p 1.
[2] Ibid, p 1.

including cameras and other devices detect what the customer took from the store, quantity, different types of products,,, by sharing all this data through a network in order to be saved and send to the internal server, just to track what each customer buys.[1]

However collecting vast amount of data can really arise lot of issues including tracking what the preferences of the customers, what type of product the customer A likes most, selling data to third parties, which means Data breaches, refund issues…

Nowadays not only personal AI exists but also Agent AI, which going to work fully on behalf of us, making transactions, paying subscriptions, buying tickets flights, searching for best offers… and as the market evolving , E-Commerce also has been touched by The Internet Of Things and and the AI Agent technology, the system will send/receive, buy, sell, order, count and refund Automatically.

- **Health care**

In the healthcare sector, the Internet of Things (IoT) connects different smart devices that allows information to move easily between patients and doctors, wearable or implanted sensors can measure health data such as heart rate, temperature or blood pressure and send it automatically to medical systems through wireless connections like Wi-Fi or Bluetooth, these connected devices help doctors monitor patients in real time and offer more personalized care. In smart hospitals, IoT technologies are already used for services such as assisted living, tracking medical supplies, supporting remote healthcare and improving emergency response.[2]

The Internet of things in the healthcare sector can be even only for individuals' use without the intervene of clinics or external doctors, like counting how many steps or how many kilometers the person has achieved per day, pressure blood…, apple watch can be a perfect example, where this watch has embedded sensors and a specific application, while it is connected with our phones, the transfer of our data will be through the network.

Possible legal issues related to cybersecurity could be arise, legal and ethical concerns regarding the protection and processing of sensitive health information, also accountability, for instance if we have two connected devices the chance of being hacked or facing any kind of cybercrimes is high, if the watch gave us wrong analyses about our health and

[1] AZNAG, Fatma and TAHANOUT, Kheira (2022). Internet of Things (IoT) Technology and the Future of Payments (Case of Amazon-Go). Administrative and Financial Sciences Review, 6(1) [online]. https://www.asjp.cerist.dz/en/article/187893, p. 477.

[2] CASAROSA, Federica (2024). Cybersecurity of Internet of Things in the Health Sector: Understanding the Applicable Legal Framework. Computer Law & Security Review, 53 [online]. https://doi.org/10.1016/j.clsr.2024.105982, p. 4.

caused a physical harm, who could be responsible ? the watch manufacture or the application developer, or no one because the use does not precisely analyze the results?.

- **Industry and Manufacturing**

Industry 4.0, has been mentioned and repeated a lot in the previous studies and all scholars agreed that Internet Of Things can serve this area perfectly.

The Industry 4.0 means the fourth industrial revolution, where factories become smart and fully connected through the Internet of thigs instead of controlling machines by people, now machines can communicate with each other and share data and make automated decisions and this actually allows factories to work more efficiently and adopt automated decisions like adjusting manufacturing priorities to accommodate supply delays caused by weather [1]

- **Agriculture and Energy**

In agriculture, the Internet Of Things is used in smart farming as well, where sensors, drones and self driving farm machines which going to be work together to make farming system more efficient and to decrease the human interaction. [2]

In short the industry and manufacturing area become more intelligent network where connected machines uses data, automation and earning to make production line faster, safer and more efficient.

1.3 Impacts and Outcomes of the Internet of Things

At some point we should admit that the Internet of Things brings both progress and challenges, it creates economic and social opportunities while also it demands strong attention to cybersecurity.

From the previous sub chapter it can conclude so many points, the Internet Of Things technology could increase the:

- **economic and level of innovation** by making faster decisions and quick results also by

suggesting new products or services based on the given data.

[1] HUNT, Matthew and TREACY, Pat (2022). Internet of Things (IoT) — Key Legal Issues [online]. Lexis PSL: Technology, Media and Telecommunications, p. 4.
[2] Ibid, p 3.

- **social development** is the most pivotal axe, Internet Of Things can improve access or the uses of resources, energy and agriculture so a better services and life quality will improve as a result, which means Internet Of Things has a hand in developing both individuals and states.

The Internet Of Things does not has only a positive impact, there is also undesirable outcomes, this outcomes is inevitable and as follow:

- **human interference** could be less indeed but in same time it needs so much oversight,

because of the harm that could be made of it , it consumes energy, resources, big budget, a huge infrastructure and not all countries can offer that.

- **Cybersecurity legal issues concerns**

If there are so many devices and sensors that collect different data around us automatically through one network and if just one of the devices got hacked it means all collected data not under control anymore, and a very sensitive information is in danger, Including misuse of data, potential harm, security breaches and legal accountability should be applied because missing guaranties not reached yet.

Chapter II Cybersecurity Challenges in internet of things

This chapter explains the main cybersecurity problems that can appear when we use Internet of Things devices. Different IoT devices use weak passwords, cheap components, old software, or do not receive security updates, these make them easy for hackers to break through, especially when one device is hacked the attacker can access personal data or watch people through cameras, control smart home systems or even cause physical harm by attack smart cars or medical devices.

This chapter discusses the most common vulnerabilities in the Internet Of Things devices and systems, like poor authentication, lack of encryption, weak network security, and unsafe software, it also explains the most famous threats IoT faces, including ransomware, privacy breaches, botnet attacks, and unauthorized data collection,not only studying and analysing from technical perspective but also from the legal perspective

Finally, the chapter shows how Internet Of Things connect the digital world with the physical world, meaning that a cyberattack can now create real scene consequences.

2.1 Vulnerabilities of the internet of things

Lack of security standards: Internet of Things devices have serious security

weaknesses because most of them are not reliable, small, low cost products with very limited control. Sometimes they are designed to perform only simple functions, such as switching lights or recording temperature, manufacturers cannot support strong encryption systems. As a result, information can be send between devices, mobile applications, and cloud servers travels in plain text without protection, this lack of transport encryption exposes large amounts of personal and operational data to possible interception or manipulation during transmission.[1]

- **insufficient authentication and authorization** is Another major weakness.

Internet Of

Things systems often rely on weak or default passwords, which users rarely change, devices may not require regular password updates or reauthentication when accessing sensitive information. This careless handling of passwords changing makes them the easiest way for attackers to break into a system and gain control of connected devices, because once a hacker accesses one device, the whole network can be at risk.[2]

- **web interfaces** is a security problem that control Internet of Things devices.

Many

have poo management, weak credentials, or coding errors which allow attackers to take over user accounts, because these web panels are directly connected to the internet, a single flaw can open the door to remote exploitation and unauthorized access.

- **Software and firmware vulnerabilities** make the problem worse, to keep

production

costs low, most IoT devices are built without the ability to receive software or firmware update so when the weak points are discovered they remain unpatched, leaving permanent openings for attackers, even when updates exist some devices download them without using encryption, which allows manipulation of the update files. Since it is nearly impossible to create software completely free of vulnerabilities, the inability to update represents one of the most critical risks in Internet Of Things security.[3]

---

[1] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p.720.
[2] Ibid, p.720.
[3] Ibid, p.720.

Overall, the massive increase in connected devices combined with these weaknesses has shifted the focus of cybersecurity from individual hardware to the networks that link them. Every connected things becomes a potential entry point for an attack which creating an cdertain situation where defenders must secure every component, while an attacker needs to find only one weak spot. In this sense, the Internet Of Things environment clearly demonstrates that a system is only as strong as its weakest link.[1]

2.2 Common Threats and Incident

vulnerabilities are the weak points, in other meaning are the loopholes that the attackers can use in order to break the system. However, the threats are the set of operations increase the possibility that something bad can happen, for instance ransomware is a threat for the IOT devices, because the full system could be hacked and blocked. So, there is a need to prevent and fight all what can threaten Internet Of Thing system .

If cybersecurity is the set of tools which made to protect our data, it means the only way to prevent threats is by establishing a strong and consolidate cybersecurity tools.

Speaking about cybersecurity, the purpose always is to keep privacy, data, information in safe, as a result people concern about threats which is the leak or the breaches of their data-privacy.

In this sub chapter a group of threats will be mentioned, not focusing only on the technical aspect but also what the law can say about that ?

Cybersecurity in the internet of things aims to protect confidentiality, integrity, availability these are the most important cores all scholars have been stressed.

The Budapest convention on cybercrime 2001, does not directly mention the Internet of Things. However, the convention still applied to the different threats that can affect the respective object, also the convention identifies crimes which is considered as a threats to Internet Of Things system ,Under the chapter two: Measures to be taken at the national level, the most threats have been mentioned

- **Illegal access:** The article two states that Each Party shall adopt such legislative and

other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

[1] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p. 720.

- **Data interference** According to the article 4 from the same convention it means the

damaging, deletion, deterioration, alteration or suppression of computer data without right

- **Misuse of device** according to Budapest convention the misuse of device is when

someone intentionally and without right use passwords, devices, data, import data, to commit the offences on the respective convention.

The threats list is endless, in generale any act can effects and threats the Internet Of Things devices should be eliminated, threats concerning information modification or misuse, information, destruction, unauthorized access, data breaches, data theft and denial-of-service[1].

Different regulations speak about our Data threats such as CCPA and GDPR, the term of Internet Of Things is not mentioning but it applies also for it, because the internet of things is just part of the whole internet and technology.

The weak passwords, also cheap components, lack of updated software are sufficient to make the Internet Of Things vulnerable to get hacked.

Harmonization issues can be a threat to the internet things developing, the word is a group of countries as consequence the IOT could arise a cross border legal issues, if a manufacturer of a device in a place and the user in another place, also the application developer completely residing in a different country, how can we resolve a legal dispute effectively, as a result the existing instruments need an urgent update,

2.3 When Internet of things Meets the Physical World

The Internet of Things does not only exist in computers or online networks, it is now part of our daily life and the physical world, so many connected objects like cars, medical devices, or home systems can now act automatically, because these objects can move, control, or affect the environment, a cyberattack can also cause real physical harm. What was once only a data problem can now become a safety and liability issue.

The Internet of Things is not limited only to data or networks it extends digital systems into physical reality.

[1] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p.718.

Different examples of hacking in the IoT dedicated especially to automobiles, In 2015 Fiat Chrysler recalled 1.4 million cars in response to a widely publicized demonstration where

hackers took control of a Jeep Cherokee, simply they were able to turn the steering wheel, and disable the brakes, the worse thing they even shut down the engine.[1]

When the Internet Of Things meets the physical world could be beneficial, but can cause harm not only to objects but for people also.

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles. Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents.[2]

If the Internet Of Things got be hacked, the damage could be much more serious and could happen right away including death accidents, In the next few years, there will be about ten million self driving cars on the roads. If hackers find weak points in these cars, they could cause accidents and put people's lives in big danger.[3]

Speaking about health sector, "Two years ago, researchers Billy Rios and Jonathan Butts discovered disturbing vulnerabilities in Medtronic's popular MiniMed and MiniMed Paradigm insulin pump lines. An attacker could remotely target these pumps to withhold insulin from patients, or to trigger a potentially lethal overdose"[4]

Chapter III Risk and Security Perspectives

Chapter III focuses on how we can reduce the risks that come from using Internet Of Things devices. It explains simple ways to manage IoT security, like using stronger protections, regular updates, and safer system designs, also shows why standards, laws and rules are important for keeping critical infrastructure like hospitals and transport and energy systems in safe. Overall, it introduces the basic ideas needed to understand how IoT risks can be controlled and how security can be improved by addressing some of the legal issues

3.1 Managing the security of internet of things

[1] BEALE, Sara Sun and BERRIS, Peter (2017–2018). Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses. Duke Law & Technology Review, 16, 165, p. 165.
[2]Graeme Baker, Schoolboy Hacks into City's Tram System, THE TELEGRAPH, Jan. 11, 2008, http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacksinto-citys-tram-system.html.
[3] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p.721.
[4] NEWMAN, Lily Hay (2019). These Hackers Made an App That Kills to Prove a Point [online]. https://www.wired.com/story/medtronic-insulin-pump-hack-app/

One of the biggest issues slowing down the use of IoT in our daily lives is security, Internet Of Things devices are not protected, so they easily can be attacked, fix these issues and keep users safe should be a priority, Internet Of Things becomes more common and people need to trust the devices they use and they need to believe their data is in safe. this can create complicated security risks. Security attacks can happen in several ways: physical attacks, network attacks, encryption attacks, and software attacks and these problems can seriously affect users' trust. indeed trust is very important in any relationship so when trust is lost the relationship becomes weak especially the internet is already known for being unsafe, and people are becoming more aware of its negative effects, this is why, people try to protect their data and limit their online activity but in today's world, avoiding the internet completely is almost impossible. A survey by Allhoff and Henschke (2018) explain that trust depends on ethical issues like privacy and informed consent, information security and physical safety, so when there is a data breach or the users' privacy is violated or their safety is at risk and informed consent is ignored. This creates distrust and make users question who or what they can rely on, which can causing stress and insecurity. For people to use IoT with confidence they must trust that these devices are safe and protect their data and to solve this problem companies and governments are introducing trust Frameworks, these frameworks help show that the device or service follows certain security rules, for instance the U.S. government develops and uses Trust Frameworks, and other countries can also create laws to protect citizens, this can helps users feel more confident knowing that their smart devices are supported by strong legal protections.[1]

According to NIS 2 each EU country must make sure that such valuable institutions what is considered a something important to the government like hospitals, banks, or internet companies, take the right steps to protect their computer networks and information systems from cyber risks. These organisations need to use simple and effective technical and legal protection to prevent problems or reduce their impact on people and other services. The rules depend on the size of the institution or the organization also if it open to different risks or not and how serious the impact of an incident could be. The protection measures must cover everything from risk analysis, handling incidents and keeping business running in case of problems, to making sure their suppliers are also secure. They must also make sure their systems are safely built and updated and especially tested, the article stressed also the needed use of encryption . If a company finds it is not following these rules, it must fix the issues quickly.

[1] KARALE, Ashwin (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet of Things, 15, Article 100420. https://doi.org/10.1016/j.iot.2021.100420 , p. 10.

All new technologies bring some level of risk, and the Internet of Things has the same thing. Even though Internet Of Things devices can be attacked, this does not automatically mean that the overall danger is very high. Not every weakness will be used by hackers, and the results of an attack can vary, some may cause small problems, while others could be serious. What matters most is understanding how much extra risk Internet Of Things can add compared to existing cyber risks, and finding ways to manage and reduce it. At the same time, it is important not to overreact or create rules that slow down innovation, new business, or economic growth.[1]

"People accept and manage risk. Consumers and companies make decisions based on their tolerance for risk and their estimates of both risk and the value provided by the"risky" activity. Perceptions of risk are shaped by knowledge and assumptions about safety that manufacturers have made safe products, that standards and regulations provide guidance for production and use, and that courts will provide remedies if safety fails."[2]

Malfunction and the fair of being hacked and our efforts to protect privacy to make Internet Of Things devices more secure will create economic harm that can put extra burden to reduce risks[3]

It is also worth mentioning that "Most accounts of IoT vulnerability assume that a single hacking incident can be duplicated on a mass scale, but in most instances, the challenge is not hacking a single car or refrigerator, it is hacking several thousand in situations and circumstances that produce mass effect. The number of variables involved in this kind of mass incident suggests that this kind of IoT hacking is very improbable. We do not want to extrapolate systemic effect from an example where hackers, under ideal conditions, can cause a single device to malfunction, into some larger threat to safety or security. The average level of dissonance and even chaos that modern economies accept as normal is high. IoT hacks would have to exceed this threshold to be noticeable. Most IoT devices will not perform critical functions, nor will they generate or store critical data. This is particularly true for consumer IoT devices. This means that even if these consumer devices are hacked, the result is most likely to be annoyance. A nation with greater exposure to pranks does not face a surge in risk. It is systemic risk, the ability to create significant disruption by attacking a single critical node (like FedWire, the power grid, or a nuclear power plant) or by simultaneously attacking a large number of targets to produce significant

[1] LEWIS, James Andrew (2016). Managing Risk for the Internet of Things [online]. Center for Strategic and International Studies (CSIS). JSTOR, p. 1.
[2] LEWIS, James Andrew (2016). Managing Risk for the Internet of Things [online]. Center for Strategic and International Studies (CSIS). JSTOR, p. 3.
[3] Ibid, p. 5.

effect. A simple precaution would be to ensure that some critical systems, which are not now linked to the Internet, remain disconnected until we can better assess and control risk".[1]

A good way to manage Internet Of Things risks is to focus on what really matters, efforts should first focus on protecting systems that are important or high risk (like government systems, hospitals). Not every small weakness needs an immediate fix, It is also important to keep a balance like a strong security is needed, but too many rules can slow down new ideas and innovation. Security should improve step by step as technology develops and companies learn from experience. Laws and regulations should target the most serious risks, not every small problem[2], this is law instrument not an IT manual, law makers cannot fix everything, technicians will fit and fill the gaps when it comes to cybersucrity technics gaps.

3.2 Legal Protection of Critical Infrastructure and the Role of Standards.

The idea of critical infrastructures keeps changing over time to match new problems and security needs. In the last years , the number and types of these important infrastructures have grown a lot (health sector, transport system, government services...), therefore, protecting them from different risks and making sure they work without interruption has become a major priority. These infrastructures can stop working or be damaged because of many reasons: natural disasters like earthquakes or floods, mechanical problems, bad design, or human actions such as theft, or even terrorist attacks. Both public and private operators tried to protect these infrastructures from different kinds of attacks. However, the growing of threats and the weaknesses in the systems show that operators and governments must stay alert and keep updating their protection rules. In the last twenty years, a new major threat has become very common: cyberattacks. Recently, the number of cyber threats has increased sharply and they have become more diverse, more advanced and more complex.[3]

"Critical infrastructures consist of those physical and information technology facilities,

[1] LEWIS, James Andrew (2016). Managing Risk for the Internet of Things [online]. Center for Strategic and International Studies (CSIS). JSTOR, p. 7.
[2] LEWIS, James Andrew (2016). Managing Risk for the Internet of Things [online]. Center for Strategic and International Studies (CSIS). JSTOR, p.15-19.
[3] MARKOPOULOU, Dimitra and PAPAKONSTANTINOU, Vagelis (2021). The regulatory framework for the protection of critical infrastructures against cyber-threats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer Law & Security Review, 41, Article 105502 [online]. https://doi.org/10.1016/j.clsr.2020.105502 , p.1-2.

networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well being of citizens or the effective functioning of governments. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. Some critical elements in these sectors are not strictly speaking 'infrastructure', but are in fact, networks or supply chains that support the delivery of an essential product or service. For example the supply of food or water to our major urban areas is dependent on some key facilities, but also a complex network of producers, processors, manufacturers, distributors and retailers".[1]

The integration of Internet Of Things technologies into critical infrastructures such as energy networks, transport systems and healthcare services and government services, creates both opportunities and systemic risks. Not paying attention to the previous onces can disrupt essential services and threaten public safety.

The 2008 Directive is an important part of the Eu's EPCIP programme. It is the first step toward identifying and protecting European Critical Infrastructures. The directive uses a sector specific approach, which means it applies only to the energy and transport sectors. As a result, many other important sectors such as health or drinking water and finance are not covered. The directive itself admits this limitation. It even says that during its review, more sectors could be added, giving priority to the ICT sector. This is interesting because earlier EU documents, like the Green Paper and the draft proposal, listed eleven different critical sectors, but the final directive included only two. One possible reason is that energy and transport were chosen as a test phase,and the list would be expanded later during the 2012 review, however although the review process started in 2012, it has still not been completed.[2]

When we talk about cyber resilience and protecting Critical Infrastructures from cyberthreats, especially the network and information systems and the internet of things, they depend on we must also look at the NIS 2 Directive. Unlike the first NIS Directive, NIS2 covers many more sectors, The NIS Directive does not directly mention "Critical

[1] Commission of the European Communities (2004). Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism (COM(2004) 702 final) [online]. Brussels, 20 October 2004. CELEX 52004DC0702. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702 , p. 3-4.

[2] MARKOPOULOU, Dimitra and PAPAKONSTANTINOU, Vagelis (2021). The regulatory framework for the protection of critical infrastructures against cyber-threats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer Law & Security Review, 41, Article 105502 [online]. https://doi.org/10.1016/j.clsr.2020.105502 , p. 6.

Infrastructures," but it uses the term "Essential Services," which is basically the same idea. "Operators of Essential Services" are public or private organisations that provide services which are essential for society and the economy. The types of organisations covered by the NIS 2 Directive are very similar to the sectors listed by the EU as Critical Infrastructures.

A full analysis of the NIS 2 Directive is outside the focus of this paper. What is important to know here is that the NIS 2 Directive, Nis 2 currently is the main EU cybersecurity law requiring Member States to make sure that network and information systems especially those supporting CIs and essential services are well protected".[1]

ENISA has also recognised how serious cyberattacks on critical informations Infrastructures (CIIs) can be. ENISA believes that identifying which infrastructures are critical is the first step in protecting them. For this reason, it has published several reports on identifying and protecting CIIs. ENISA has also created guidelines to help Member States apply the NIS Directive. This includes a tool that links the security requirements for Operators of Essential Services to international standards and a detailed report explaining security requirements in specific sectors such as healthcare (which will be discussed later).

ENISA's role became stronger with the Cybersecurity Act (2019). The Act gave ENISA a permanent mandate and expanded its responsibilities, including helping develop EU-wide cybersecurity certification schemes for ICT products, services and processes.[2]

Directive (EU) 2016/1148 impose minimum security requirements on operators of essential services and digital service providers.[3] These instruments oblige entities take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

The Cyber Resilience Act complements this framework by lays down:

rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;[4]

---

[1] MARKOPOULOU, Dimitra and PAPAKONSTANTINOU, Vagelis (2021). The regulatory framework for the protection of critical infrastructures against cyber-threats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer Law & Security Review, 41, Article 105502 [online]. https://doi.org/10.1016/j.clsr.2020.105502, p. 7.

[2] MARKOPOULOU, Dimitra and PAPAKONSTANTINOU, Vagelis (2021). The regulatory framework for the protection of critical infrastructures against cyber-threats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer Law & Security Review, 41, Article 105502 [online]. https://doi.org/10.1016/j.clsr.2020.105502 , p. 7.

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, pp. 1-30, art. 14/16.

[4] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 ("Cyber Resilience Act"). OJ L 347, 20 Nov. 2024, pp. 1-79, art. 1 (a).

essential cybersecurity requirements for the design, development and production of products with digital elements and obligations for economic operators in relation to those products with respect to cybersecurity.[1]

There is what is called by the international standards such as ISO/IEC 27001 for information security management and ISO/IEC 27400 for IoT specific cybersecurity, these standards serve as a guidlines for compliance and demonstrate an organization’s due diligence in managing digital risks, but even though there is so many things to improve and create the cooperation between countries.

Negligence on critical infrastructure can lead to a famous case which happened before “Stuxnet (2010): A sophisticated cyberattack targeting industrial control systems, Stuxnet demonstrated the potential consequences of Internet Of Things related breaches in critical infrastructure. It was a computer worm that specifically targeted supervisory control and data acquisition (SCADA) systems, affecting Iran's nuclear program by causing centrifuges to malfunction”.[2]

[1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 (“Cyber Resilience Act”). OJ L 347, 20 Nov. 2024, pp. 1-79, art. 1 (b).

[2] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 5.

2-Part II Legal and Regulatory Issues of Internet Of Things

Internet of things has been built on the premise that a huge amount of data will be generated and that can be used and analyzed for the benefit for the consumer, the installer, for the product manufacturer and the network provider so everyone wants a piece of it, as a result of the explosion In data there's been a need to review data privacy and as a result we need always new, updated laws, regulations, policies and guidelines. [1]

Part II looks at the legal problems that appear when billions of Internet Of Things devices collect and share data within or across borders. Internet Of Things create a world where personal information move between companies and countries and cloud systems with no limits, this brings serious legal questions: Who controls the data? Who is responsible when something goes wrong? And how can privacy protected when IoT devices track users' behavior ? laws, such as GDPR in Europe or the NIS 2 Directive, try to protect people but they was not fully made for Internet Of Things. United States also uses rules like HIPAA for health or GLBA for finance but there is no unified national law. Globally, frameworks like the Budapest Convention help fight cybercrime, but there is still no international law that clearly regulates Internet Of Things.

Because Internet Of Things system easily cross border but laws do not sometimes, governments struggle to manage risks for instance surveillance, uncontrolled data flows, weak security standards and unclear liability. This part explains how current regulations work, where they fail, and why new, modern, and harmonized legal solutions are necessary to protect users and how we can define the cybersecurity legal issues of the internet of things

Chapter I Regulatory Frameworks for IoT Cybersecurity

As more cyber threats appear, laws and rules about online security generally and about the Internet Of Things specifically are changing quickly to try to keep up and protect people from these new risks.

[1] HowToAV (2019). How is the Internet of Things affected by GDPR? [video]. https://www.youtube.com/watch?v=Ji53_8vPVjo

1.1 European Union IoT Instruments

In this sub chapter, the main EU legislative documents that can be applied to Internet Of Things will be provided, and to know what is the actual efforts made by the EU in order to orchestrate the internet of things technology and how to make better cybersecurity.

- **GDPR**

The GDPR is applicable throughout Europe which applies to all EU member states and any company inside or outside the EU that process personal data of people in the Eu.[1]

As we know, the General data protection regulation is the main EU law that protects people's personal data, it also applies to all IoT devices that collect or use information about people for example, smart watches, cameras or home assistants.

Of course, the GDPR doesn't address the Internet of Things technology directly, but it is worth mentioning that IoT devices are just a tool used to transfer data from place to another, this is why GDPR Regulation applies 100 percent to Iot ecosysytem.

Under article 5 of the GDPR under name "principles", the article stressed that our data must be used fairly, lawfully, in a transparent manner[2] Therefore companies who are making IoT devices they have to be absolutely transparent about what data is being taken.

Iot manufactures should be clear when it comes to what are they going to do with the collected data or in another way, for which purposes[3] ?

Only collecting the necessary data and nothing extra, being accurate which means keep data correct and up to date, respecting storage limitation and not keep personal data longer than needed ans especially keep data safe. Last but not least data controller should be accountable, and be able to prove compliance.

Article 6 explains when companies are allowed to use personal data, or when the user gives clear consent. This is crucial to speak about, especially when users struggle to read the companies policies without understanding what the internet of Things devices will collect, in real life users use these devices without even giving consent.

consent must be freely given, specifically informed and clear, this is difficult for many IoT devices that work automatically without asking users directly.[4]

---

[1] HowToAV (2019). How is the Internet of Things affected by GDPR? [video]. https://www.youtube.com/watch?v=Ji53_8vPVjo

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). OJ L 119, 2016, pp. 1–88, Art. 5.

[3] Ibib.art 5(1)(b)

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). OJ L 119, 2016, pp. 1–88, art 7.

Even though article 25 requires privacy and data protection by design and by default and IoT devices must be built with strong privacy and security features from the beginning. Does this really align with our reality? the cheap component of devices forces the manufacturers to build bad quality with low privacy guarantee.

companies must use good security measures, such as passwords, encryption, and regular checks, to keep data safe and to report any data breaches, both to authorities and, sometimes, to the users.[1]

Without forgetting that there is general conditions for imposing administrative fines which is very high fines (up to €20 million or 4% of a company's total income) if they break these rules.[2]

- **The Cybersecurity Act and the Internet of Things (IoT)**

The EU Cybersecurity Act (Regulation (EU) 2019/881) defined 'cybersecurity' as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats[3]

This is broader than the older 2013 definition, which focused only on three basic goals known as the CIA triad : confidentiality, integrity, and availability, The new meaning includes not only systems but also the rights and freedoms of individuals like privacy, freedom of expression, and data protection as well.[4]

When it comes to IoT, the Act cover and applies to it because IoT devices are part of the category of ICT products and services. According to article 2 of the Act, an ICT product is any part of a network or information system. which includes connected IoT devices.

Several parts of the Act specifically mention the Internet of Things. For example, Recital 2 recognises that many IoT products do not use "security by design" meaning they are not built with strong security from the beginning[5]. It also noted that without proper certification, consumers can't easily understand whether the device is secure or not.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). OJ L 119, 2016, pp. 1–88, art .32-34.
[2] Ibid, Art 83.
[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. OJ L 151, 7.6.2019, pp. 15-69, art. 2.
[4] CHIARA, Pier Giorgio (2022). The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology, 36(2), 118–137 [online]. https://doi.org/10.1080/13600869.2022.2060468, p. 119.
[5] CHIARA, Pier Giorgio (2022). The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology, 36(2), 118–137 [online]. https://doi.org/10.1080/13600869.2022.2060468, p. 120.

Therefore, the certification system is designed to build trust between manufacturers and consumers or users in genral so when a product is certified, it shows that it has passed an evaluation which prove it meets cybersecurity standards. [1]

basically , certification equals proof of security, It helps users trust IoT products and services by making their security level visible and transparent.

- **NIS2**

This Directive (EU) 2022/2555 "lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market"[2]

And to achieve this, the directive sets obligations that require member states to adopt national cubersecurity strategies, cybersecurity risk management, theses obligations can be achieved only if member states put supervisory and enforcement bodies.[3]

Previous in part I, chapte 3, under "managing the security internet of things" we found the Directive NIS2 sets obligation and tools on how we can manage risks on Iot technology and how we can avoid all legal issues related to cybersecurity in the internet of things.

Speaking about the same Directive, it really helps internet companies to solve and avoid the hidden issues, loopholes, and he was like a guarantee to users, best example for that we find in article 23, which states that every EU country must make sure that important entities like hospitals, banks, and all internet companies, immediately inform the national cybersecurity team (called CSIRT) or another responsible authority if they have a serious cybersecurity incident that affects their services(like cybersecurity attack on their systems), and if the problem could also harm people who use their services, these entitiees should also inform those users as soon as possible.

The report must include information to help the authorities to understand if the incident also affects other countries which can cause cross border issue.[4]

---

[1] CHIARA, Pier Giorgio (2022). The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology, 36(2), 118–137 [online]. https://doi.org/10.1080/13600869.2022.2060468, p. 121.

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). OJ L 333, 2022, pp. 80–152, art. 1.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). OJ L 333, 2022, pp. 80–152, Art 21.

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). OJ L 333, 2022, pp. 80–152, Art 23.

Finally and what is importat the article mention that reporting the incident will not cause punishment or legal responsibility it just helps the authorities react and protect others.[1]

As already mentioned NIS 2 especially serve the essential services entities, like hospitals, banks, transport, and these sectors are part of IoT asa result NiS2 forcefully applies to IoT and is one of the main pillars to prevent the legal issues in the internet of things.

- **Cyber resilience act**

The Cyber Resilience Act is a new EU law that makes sure all products with digital parts like smart watches, baby monitors, or software are safe and protected from cyber risks, it requires manufacturers and sellers to keep their products secure from the designing stage passing through the product is in user's hand until the life cycle of the product, this means they must fix security problems quickly and provide regular updates, therefore some important products will also need to be checked by an independent expert before being sold in the EU, it is worth mentioning also that the law applies to almost all connected products, except some special ones like medical devices or cars that already have other rules and products that meet these cybersecurity standards will have a CE mark, showing that they are safe to use and follow EU rules. This helps people and companies trust that the digital products they buy are secure and reliable.[2]

Best legal issue that Cyber resilience act addressed can be found in annex I, Part II inder " **Vulnerability handling requirements" the respective article states :**

"Manufacturers of products with digital elements shall:

- identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products.
- in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). OJ L 333, 2022, pp. 80–152, Art. 23.

[2] European Commission. (2025, March 6). Cyber Resilience Act. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

- apply effective and regular tests and reviews of the security of the product with digital elements.
- once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities their severity and clear and accessible information helping users to remediate the vulnerabilities in justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixing vulnerability until after users have been given the possibility to apply the relevant patch.
- put in place and enforce a policy on coordinated vulnerability disclosure.
- take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.
- provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner.
- ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken".

From analyzing perspective, the cyber resilience act doesn't follow the old approach, it applied binding rules to manufacturers, service providers, third parties, to accomplish the purpose of IoT devices which is serve users and consumers without arise any legal issues.

if GDPR protects personal data collected or processed by IoT devices, the NIS2 Directive focuses on cybersecurity and incident reporting for essential and important services that IoT devices may rely on, and if Cybersecurity Act creates Eu wide certification standards for secure digital products and services including IoT components, the Cyber Resilience Act introduces mandatory cybersecurity rules for all connected products, which directly covers IoT devices.

EU DATA ACT

The main objective:

- to ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data.
- Applies to IOT device users Users (Businesses & Consumers)
- Access to (almost) all loT device-generated data[1]

1.2 United States' Internet of things instruments

In the U.S., there's no single binding law covering all IoT devices like in the EU, so they do not have one national law like the EU's Cyber Resilience Act or NIS2.

Instead, it uses a fragmented and different laws or agencies and states cover different parts of IoT and cybersecurity.

Although the number of Internet of Things (IoT) devices keeps growing everywhere around us, the laws and rules about IoT are still very new and limited, there are very few federal or state policies in the U.S. that directly control how IoT devices should be made or used.[2] Most of the existing guidance comes from the National Institute of Standards and Technology (NIST), but these are only recommendations and not mandatory rules, even the U.S. President's Executive Order 14028, which talks about improving cybersecurity, barely mentions IoT security, except to say that the public should learn more about it.[3]

Different regulations and documents also use different definitions of what an IoT device actually is even within NIST itself. Having one clear and unified definition would make it much easier for everyone to apply the same security standards.[4]

When policies talk about reasonable security features for IoT devices, they usually just mean basic protection, such as the option to set passwords and these responsibilities mostly fall on manufacturers, who must make secure devices and show customers how to use them safely and provide support after sale.[5]

---

[1] JURČYS, Paulius; STRIKAITĖ LATUŠINSKAJA, Goda (2024). Data Protection and Privacy Law lecture, Vilnius University, MS Teams, unpublished teaching material.
[2] BEYER, Jessica L. (30-03-2023). U.S. Federal and State Regulation of Internet of Things (IoT) Devices, 2019-2022 [online]. https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/
[3] BEYER, Jessica L. (30-03-2023). U.S. Federal and State Regulation of Internet of Things (IoT) Devices, 2019-2022 [online]. https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/
[4] Ibid.
[5] Ibid.

Rules about consumers mostly focus on large organizations or government agencies and not on ordinary people using IoT devices at home which leaves many personal security risks uncovered.[1]

Federal IOT Policies:

Law #	Title	Summary	Link
E.O. 14028	Improving the Nation's Cybersecurity	Acknowledges the need to improve national cybersecurity by removing barriers to reporting and sharing threat information, requiring federal agencies to adopt security best practices, educating the public on the security capabilities of IoT devices, and developing a standard playbook for federal response to cybersecurity vulnerabilities and incidents.	https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
PL 116-207	Internet of Things Cybersecurity Improvement Act of 2020	Requires National Institute of Standards and Technology (NIST) and the Office of Budget and Management (OMB) to review federal agency information security policies relating to IoT devices and establish practices for disclosure of security vulnerabilites relating to agency IoT devices.	congress.gov/bill/116th-congress/house-bill/1668/text/pl?overview=closed

Source: BEYER, Jessica L. (30-03-2023). *U.S. Federal and State Regulation of Internet of Things (IoT) Devices, 2019-2022* [online].https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/

[1] BEYER, Jessica L. (30-03-2023). U.S. Federal and State Regulation of Internet of Things (IoT) Devices, 2019-2022 [online]. https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/.

State IoT laws:

State	Law #	Title	Summary
California	SB-327	Information Privacy: Connected Devices	Requires manfacturers of connected devices to equip them with "reasonable security features", which can be met through a preprogrammed password or prompting the user to generate a new means of authentication prior to first use.
Oregon	HB 2395	Relating to security measures required for devices that connect to the Internet	Requires manufacturers of household IoT devices to include "reasonable security features", such as authentication and compliance with federal security regulations. Manufacturers are not responsible for third-party software or applications added by users. Inspired by California's SB-327 and AB-1906.
california	AB 1824	CALIFORNIA CONSUMER PRIVACY ACT OF 2018	Became effective on 1st January 2025, it considered as the 2nd versio of GDPR it applies only to people and companies in California, or to companies doing business with California resident.

Source: BEYER, Jessica L. (30-03-2023). *U.S. Federal and State Regulation of Internet of Things (IoT) Devices, 2019-2022* [online].https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/

US IoT guidelines and Standars:

Organization	Title	Description	Stakeholders
Federal Trade Commission (FTC)	Internet of Things - Privacy & Security in a Connected World	Identifies the benefits and risks of IoT, and strongly recommends steps that businesses can take to protect	Businesses and policymakers

		customer privacy and security in relation to IoT. Regarding legislation to regulate IoT, this report concluded it was too early for specific regulation, pushing instead for broad-based privacy legislation at a federal level.	
National Institute of Standards and Technology (NIST)	Considerations for Managing Internet of Things (IoT) Cybersecurty and Privacy Risks (NISTIR 8228)	Familiarizes federal agencies and other organizations with the cybersecurity and privacy risks associated with IoT devices throughout their lifecycles by highlighting differences between IoT and IT devices and their implications, then recommends three high level risk mitigation strategies: 1) protect device security, 2) protect data security, and 3) protect individuals' privacy.	Federal agencies and other organizations
National Institute of Standards and Technology (NIST)	Foundational Cybersecurity Activities for IoT Device Manufacturers (NISTIR 8259)	Recommends six cybersecurity-related activities for IoT manufacturers to perform prior to selling their devices to reduce security issues, Activities One through Four focus on pre-market impact, while the remainder are post-market oriented: 1) identify customer base and define expected use cases, 2) research customer	IoT device manufacturers and customers

		cybersecurity needs and goals, 3) determine how to meet needs and goals, 4) plan for adequate support of needs and goals, 5) define approaches for communicating to customers, and 6) decide what and how to communicate to customers.	
National Institute of Standards and Technology (NIST)	IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A)	Identifies and recommends IoT device manufacturers develop a cybersecurity capability core baseline, defined as a set of device capabilities needed to support common cybersecurity controls that protect IoT devices, device data, systems, and ecosystems. Used in conjuction with NISTIR 8259 and 8259B.	Primarily IoT device manufacturers
National Institute of Standards and Technology (NIST)	IoT Non-Technical Supporting Capability Core Baseline (NISTIR 8259B)	Identifies and recommends IoT device manufacturers with a non-technical supporting capability core baseline, defined as a set of non-technical supporting capabilities that manufacturers should possess to support common cybersecurity controls that protect IoT devices, device data, systems, and ecosystems. Used in conjuction with NISTIR 8259 and 8259A.	Primarily IoT device manufacturers

National Institute of Standards and Technology (NIST)	IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (SP 800-213)	Advises organizations on how an IoT device they plan to acquire can be integrated into a system, provides guidance on system security from a device perspective, and identifies device cybersecurity requirements that organizations should expect from IoT device manufacturers.	Federal agencies and other organizations
Prague 5G Security Conference 2019	The Prague Proposals	Acknowledges the importance of 5G and future communications technologies as vital to the efficient usage and security of IoT, provides proposals in four categories to help guide the development and implementation of 5G networks: 1) policy, 2) technology, 3) economy, and 4) security, privacy, and resilience. Adopted by the House of Representatives as H.Res. 575 in 2020.	National governments, 5G developers
U.S. Cybersecurity and Infrastructure Security Agency and the Department of Homeland Security	Internet of Things Security Acquisition Guidance	Highlights vulnerabilities and weaknesses associated with software-enabled and connected aspects of IoT technologies, especially when the physical nature of IoT devices is considered. Provides factors to consider prior to purchasing IoT devices, systems, and services, and	Manufacturers and sellers of IoT technology, as well as acquisition teams of organizations that intend to purchase IoT technology

		recommends ways to improve the effectiveness of evaluating such factors.	
U.S. Cybersecurity and Infrastructure Security Agency	The Internet of Things: Impact on Publics Safety Communications	Discusses the benefits IoT can bring as well as the concerns associated with implementing IoT within the public safety context, including cybersecurity and privacy risks. Recommends development of a framework for implementing IoT within the context of public safety, which should include training, standardization of security protocols related to IoT, and privacy regulation.	Industry, academia, public safety personnel
U.S. Department of Homeland Security	Strategic Principles for Securing the Internet of Things (IoT)	Highlights new risks emerging from the rapid growth of IoT and challenges to IoT security, such as the lack of widely-adopted international norms and standardization, and presents six principles to help address IoT security challenges: 1) incorporate security at the design phase, 2) advance security updates and vulnerability management, 3) build on proven security practices, 4) prioritize security measures according to potential impact, 5) promote transparency across IoT, and 6)	IoT developers, manufacturers, service providers, industrial and business-level consumers

		connect carefully and deliberately.	

Source: BEYER, Jessica L. (30-03-2023). *U.S. Federal and State Regulation of Internet of Things (IoT) Devices, 2019-2022* [online].https://jsis.washington.edu/news/u-s-federal-and-state-regulation-of-internet-of-things-iot-devices-2019-2022/.

As it was mentioned in the beginning of the sub chapter, there's no single binding law covering all IoT devices like in the EU, so they do not have one national law like the EU's Cyber Resilience Act or NIS2.

Instead, it uses a fragmented and different laws or agencies and states cover different parts of IoT and cybersecurity. Therefor users and consumers to protect themselves they use general laws.

Consumers and users can always use the Federal Trad Commission as a shield because they responsible for Protecting the public from unfair or deceptive acts or practices in the marketplace and they issuing reports, helping government in improving IoT regulations[1]

1.3 International approaches

"In broad terms, harmonization is essential for two reasons. The first is to eliminate or at least reduce the incidence of 'safe havens', if conduct is not criminalized in a specific country, persons in that country may act with impunity in committing offences that may affect other jurisdictionsn, Not only is there no ability to prosecute in the home jurisdiction, efforts at evidence gathering and extradition are likely to be thwarted in the absence of dual criminality and this raises the second and more far reaching rationale; that harmonization is crucial for effective cooperation between law enforcement agencies"[2]

[1] FEDERAL TRADE COMMISSION. About the FTC. [online] Available at: https://www.ftc.gov/about-ftc (Accessed: 05 oct 20225).

[2] CLOUGH, Jonathan (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. Monash University Law Review, 40 (3), 698-736. https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf .

The Budapest convention on cybercrime is the first international treaty on crimes committed via internet and other computer networks, dealing particulary with infringement of copyriths, fraud,child pornography, and violation of network security, and different cybercrimes like phishing, ransomware, misuse of devices, forgery…

Its main objectives is to set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation

The Budapest convention is related to IOT through so many articles. On Chapter II under Chapter II; Title 1- Offences against the confidentiality, integrity and availability of computer data and systems, we can find so many illegal actions which can be used and very relevant to IoT devices.

The convention prohibited and took actions to prevent Illegal access, Illegal interception, and put clear image about Data interference, System interference, Misuse of devices[1]

To conclude Budapest convention on cybercrime is binding, the remaining international co-operations are just like recommendations and guidelines, the world needs to create more updated and comprehensive, specific conventions related to IoT technology not just guidelines.

There is no global binding treaty on cybercrime. The Budapest Convention remains the main international agreement, but some countries (like Russia and China) want a new UN convention. The United Nations, through the World Summit on the Information Society (2003–2005) and the International Telecommunication Union promotes cooperation and legal harmonization, and capacity building, but all these efforts are not binding, also countries disagree even to have some support as global treaty while others (like the EU and the US) prefer improving existing frameworks.[2]

Creating a new worldwide convention is difficult and takes years, we are on 2026, while technology keeps changing faster than law, the world needs more comprehensive co-operation.

[1] Council of Europe. Convention on Cybercrime (Budapest Convention) (2001). ETS No. 185, 23 November 2001, Art. 2–6.

[2] CLOUGH, Jonathan (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. Monash University Law Review, 40(3), 698–736, p. 725-729.

Chapter II Liability and Accountability in the IoT misuse

"IoT devices pose legal liability concerns that need consideration, serious question regarding IoT devices is: Who is responsible if a person is harmed as result of an IoT function? there is not much case law to support this position. Currently, there is no defined statute as to who owns the data generated and collected by IoT devices, consumers or device manufactures? There are also concerns as to who is responsible or liable for patching IoT devices, routers, switches and cloud connections as well concerns if the user can view, edit, or delete sensor data from the manufacturer's servers if it is stored there. Does the IoT device have security controls built in? Is device information encrypted and how? Questions are asked about what exact information the device will collect about itself or its user, using what sorts of sensors? Is that information stored in the device itself, on the user's smartphone, on the manufacturer's servers in the cloud, or all of the above? Where will the information be stored? Does the device support an industry or regulatory function? What data will the device disseminate and what kind of security controls can the IoT device support? Consumers wonder if there are situations where IoT devices should not be collecting data and who exactly will the manufacturer or service share the data with, and whether the user have any right to opt out of such disclosures? Can the user gain access to the raw sensor data in order to export it to another service or device and what happens if the IoT product vendor goes out of

business or no longer supports the product? What happens when the Internet connection goes down? These are legitimate concerns and questions that continue to trail the adoption, growth and development of IoT unless regulations and device manufacturers properly address them".[1]

2.1 Product liability IoT devices

[1] CHIKE, Chike Patrick (2017). The Legal Challenges of Internet of Things. University of Maryland University College [online].
https://www.researchgate.net/publication/322628457_The_Legal_Challenges_of_Internet_of_Things , p 17-18.

Product liability is when manufacturers be accountable for defective products that harm consumers. [1]manufacturers, retailers and others may be held liable to compensate persons who are injured, or who incur financial loss.[2]

The product liability act (85/374/EEC) refers to the year 1985,and compared to 2025, so many things have been changed, technology of that time is completely different from know, thit instrument was addressing physical harm in first grade and consider the producer shall be liable for damage if caused by a defect in his product.[3]

The same directive on the second article states 'product' means all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. 'Primary agricultural products' means the products of the soil, of stock-farming and of fisheries, excluding products which have undergone initial processing. 'Product' includes electricity

In IoT, defects can be physical and can be digital as well likeWeak passwords set by default, or there's no security updates, no double authentication, no encryption, all these considered as defects and can cause real harm, data leaking, privacy issues.

The product liability directive ensure to define who is responsible and who could take the liability, Where the producer of the product cannot be identified, each supplier of the product shall be treated as its producer unless he informs the injured person[4]

Even though the directive still outdated, ant relevant to 2025, but it covers the basics, and enforce member states to adopt provisions concerning liability for defective products.

in the Internet of Things, products like the Amazon Echo are not just physical objects they combine hardware, software, data, and services. This makes it difficult to separate where the product ends and the service begins. When smart devices fail or are been hacked, the traditional idea of a defective product becomes more complicated.[5]

The EU Product Liability Directive (85/374/EEC) makes producers liable for harm caused by defective products, without needing even to prove fault. However, this law was

[1] BIREN LAW GROUP, P.C. (23-05-2025). The Hidden Dangers of Smart Home Devices: Product Liability in the IoT Era [online]. https://biren.com/the-hidden-dangers-of-smart-home-devices-product-liability-in-the-iot-era/ .

[2] FAIRGRIEVE, Duncan and GOLDBERG, Richard S. (2020). Product Liability [online]. Oxford: Oxford University Press. Oxford Academic.

[3] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. OJ L 210, 1985, pp. 29–33, art. 1.

[4] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. OJ L 210, 1985, pp. 29–33, art. 3.

[5] LA DIEGA, Guido Noto (2018). Internet of Things and the Law [online]. London: Routledge. ProQuest Ebook Central, p. 187.

written when products were tangible and more mechanical, not digital or connected. IoT devices constantly change through software updates and connectivity, so defects can be intangible.[1]

Also in cases of physical damages, the amount is easy to determine. However, in case of IoT hacks it becomes difficult to decide who to hold accountable for the leak. In addition, it becomes hard to calculate the loss amount.

To conclude, the current directive fully fit modern internet of things,and there is a need for legal updates to protect consumers in the IoT age.

Internet Of Things devices rely on sensors and automation so when something goes wrong the faul usually comes from the device or the network instead of the user, this can creates new responsibilitieto manufacturers and also service providers especially when they enter new industries with different rules because many parties are involved in an IoT system such as manufacturers and network providers and data storage companies or software developers and payment services it can be difficult to identify who is responsible when damage occurs. the different layers of devicesand the software or data and connectivity are all connected, which makes finding the root cause more complex, companies may also face unfamiliar contracts or standards when working in new markets. Some liabilities like death or personal injury caused by negligence can't be excluded by contract anit could be more relevant in IoT, it is important to ensure that IoT products remain safe throughout their lifetime and that all health and safety requirements are met, because IoT systems can cross sectors and jurisdictions, and for this companies must carefully find and map all parts of the product or service and identify the relevant laws and decide who is responsible for compliance and give long term support.[2]

2.2 Consumer contract in the internet of things

First of all, it should be mention that consumers have a lot benefits from the internet of things and the classic example is that someone has a driverless car then he can free up his time while the car using tangible sensors to drive by it self, the person can take over other things like attending meetings or whatever, so for sure he wins new functionalities, new services, accessible from everywhere, cost saving…

[1] LA DIEGA, Guido Noto (2018). Internet of Things and the Law [online]. London: Routledge. ProQuest Ebook Central, p 187

[2] Bristows (2022). Internet of Things (IoT) — Key Legal Issues [online]. Bristows. https://www.bristows.com/app/uploads/2022/10/Internet-of-Things-IoT—key-legal-issues-Lexis®PSL-practical-guida.._.pdf , p 36.

The most important consumer issues in the IoT is the contractual quagmire,

- **Contractual quagmire**

by asking Alexa: hey! What is the weather today ? we are triggering so many contracts and we are entering a number of terms of use, terms of services, terms and conditions, condition of use, notices, agreements[1] …, Because the IoT ecosystem is built on layers of interconnections, and as an example :

Amazone Echo device uses cloud, software which Alexa Voice Service, in order to give you data they should use Weather service provider like "Accuweather"

"In the IoT, consumers find themselves in a contractual quagmire in the sense that countless legals are attached to everything, and these are difficult to find, read, and understand. Stuck in the quagmire, the consumer feels that they do not have other choice but accepting all the legals, regardless of how unfair, opaque, and potentially unenforceable they may be."[2]

- **Consumer Autonomy Under Pressure and unfair practice**

Smart devices make it harder for people to make independent choices when buying products, they can also be used in unfair practices not only about the device itself, but also its software, it's also hard for consumers to get clear information, because smart devices are complex and need to be explained in simple language, because difficult technical words is used. [3]

Another issue is that smart products need regular updates and security fixes to keep working safely with time which raises the question of whether a smart device still meets quality and safety standards after purchase.[4]

The Unfair Commercial Practices Directive, The Consumer Rights Directive, The Unfair Contract Terms Directive, and The Sale of Goods Directive, In essence, these four directives add up to a coherent legal framework where each instrument complements the others adn they collectively ensure comprehensive protection for consumers

[1] UNSW COMMUNITY (14-11-2023). Internet of Things and the Law: Legal Strategies for Smart Technologies [video]. https://www.youtube.com/watch?v=ph5aaeVjJLM
[2]LA DIEGA, Guido Noto (2018). Internet of Things and the Law [online]. London: Routledge. ProQuest Ebook Central, p. 82.
[3]KOOLEN, Christof (2023). Protecting EU Consumers in Internet of Things Ecosystems: The Intersection between Consumer, Competition, and Data. In: [Book Title] [online]. Oxford: Oxford University Press. Oxford Academic, p. 56.
[4] Ibid, p. 57.

consumers rely on advertising, product information, and contractual documents to shape their expectations of a good or service, prior to their purchase, this why the consumer autonomy can be a legal issues which should be protected.

“Consumers are typically not very well-versed in contractual matters. It is therefore appropriate for EU consumer law to intervene when consumers nd themselves in a weaker or disadvantaged position vis-à-vis a business. For example, compared to professional traders, consumers tend to be less knowledgeable about the product being sold as well as the rights and obligations arising under the sales contract”[1].

General consumer protection laws also apply to Internet Of Things products, the European Commission said that in order to build consumer trust it is important for people to start using new digital technologies especiallyInternet Of Things interconnected devices and one major point is the need for a legal system that give solutions or compensation to people who have been harme, basically the current rules on liability are not mostly enough, but the EU understands that they must improve them in the future to give more clear protection for both companies and consumers. In October 2021 the European Consumer Organisation (BEUC) announced a document about how to protect european consumers who use connected devices, and it included recommendations on cybersecurity, data protection, contract rights, product safety, product durability, and competition, and the best example is The Consumer Rights Act 2015 (CRA 2015) which gives consumers protection and remedies when they buy goods and services or digital content, these rules also apply to IoT products so If a product includes digital content, that content shall follow the standards inside that Act for instance it must be good quality or suitable for its purpose and match its description. However if it doesn't meet the previous standards then it is considered not inline with the contract. In that case, the consumer has a short period to reject the product and can use the different remedies available for the defected goods. All terms and conditions (contracts or notices) must also follow the rules on unfair terms in that act and must be fair and easy to understand, it could be difficult when the product uses complex technology or when a lot of data is involved.[2]

Consumer law exists, nevertheless the term of conditions should be more clearer when it comes to cybersecurity issues such as :

---

[1] KOOLEN, Christof (2023). Protecting EU Consumers in Internet of Things Ecosystems: The Intersection between Consumer, Competition, and Data. In: [Book Title] [online]. Oxford: Oxford University Press. Oxford Academic, p. 59.

[2] Bristows (2022). Internet of Things (IoT) — Key Legal Issues [online]. Bristows. https://www.bristows.com/app/uploads/2022/10/Internet-of-Things-IoT—key-legal-issues-Lexis®PSL-practical-guida._pdf , p. 24/25.

- who is responsible for maintaining software updates ?
- how data breaches are handled ?
- and what remedies consumers have when cybersecurity failures occur?

2.3 Criminal liability and cybercrime law regarding IoT

Internet of Things devices are everywhere now and while they bring many benefits, they also face many cyber attacks. These attacks harm users, governments, and businesses around the world, cybercrime can cause huge money losses globally and in countries like Australia, many efforts have been made to stop attacks, but full success has not been reached yet. It is very important to make IoT devices safe and understand the threats they face, some reasons for cyber-attacks on IoT devices include:

- Countries with weak cybersecurity protection.
- Cybercriminals using new and advanced technologies.
- Criminals exploiting services and business models.[1]

"The most used IoT device in the business and every day in the Office space is IP-Phones which has 44% of enterprise IoT Devices but has only 5% of security issues when compared to other IoT devices. Most security issues are faced by cameras that have 33% of risk but only 5% of usage in the business world."[2]

as we know Budapest Convention on Cybercrime (2001) does not punish offenders directly but Instead it can acts as an international guidline or as a model that can tell each country what types of cyber activities must be treated as a crime. Every country that joins the Convention must include these offences like illegal access, data or system interference, and misuse of devices, in its own national criminal law, it means that when a cybercrime in the Internet of Things happenned, punishment is always based on the national criminal code, not on the Convention itself. The convention's role is to make sure that countries has a similar rules and can cooperate easily, In this way the convention helps to create a shared

[1] KAGITA, Mohan Krishna; THILAKARATHNE, Navod; GADEKALLU, Thippa Reddy; MADDIKUNTA, Praveen Kumar Reddy; SINGH, Saurabh (2023). A Review on Cyber Crimes on the Internet of Things. School of Computing and Mathematics, Charles Sturt University, Melbourne, Australia [online]. Available at: https://www.researchgate.net/publication/359708894_A_Review_on_Cyber_Crimes_on_the_Internet_of_Things , p. 2.
[2] Ibid, p. 3.

legal framework while each country keeps the power to investigate and punish under its own law.

The article 13 from the convention of cybercrime emphasized that “Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty”

Parties can punish criminals on her own jurisdiction, or even outside her jurisdiction if the conditions aligns with law, even the convention emphasized to create international cooperation, just in order to apply the criminal liability and make it more effetive[1], including extradition, mutual assistance, Spontaneous information[2]

main offences against Internet of things are : Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, Computer-related forgery, fraud[3]

What can be notified from the convention is the cross-border offences are regulated, but in the reality there is missing co-operation between countries in this metter, especially IoT is more broader and the user or consumer should be always protected or it will an visible unbalance between users and businesses.

Countries are in need to update their national law, for instance although criminal liability for cybercrimes in the Lithuanian criminal code was determined by the harmonization process with the Budapest Convention and EU law standards, the analysis has showed that not all international standards are properly implemented in the Criminal Code. [4]

Chapter III Gaps, Fragmentation of iot’s regulation

3.1 Inconsistent regulations across jurisdictions.

Even though many countries are trying to improve cybersecurity, there is no global law that covers everything. However, each country or region creates its own rules, and they are not the same. This creates a fragmented system, where some countries follow certain

[1] Council of Europe. Convention on Cybercrime (Budapest Convention) (2001). ETS No. 185, Arts. 22–23.
[2] Ibid, art. 24-26.
[3] Ibid, art. 2-8.
[4] NEMEIKŠIS, Giedrius (2022). The Challenges of the Digital Age: The Problems of Criminal Liability for Cybercrimes in Lithuanian Law. Acta Prosperitatis, 13 (Issue 1), pp. 125-138 [online]. https://doi.org/10.37804/1691-6077-2022-13-124-138, p. 136.

agreements and others do not. As a result, cybersecurity laws around the world look like a patchwork, with different rules for different sectors and places.[1]

3.2 Gaps in existing laws

Internet of Things creates new legal issues such as discrimination, security and privacy and these problems can harm consumers. IoT devices also makes consent more difficult, just like they make privacy and security more complicated, current consumer protection laws are **not ready** to handle these new challenges. One big issue is that the different Internet of Things devices have no screen, no keyboard, and no way for the user to give consent directly. As a result companies usually put all the privacy and data information on their websites instead. But the language in IoT privacy policies is often unclear and confusing. It is not always clear whether sensor data or biometric data counts as "personal data," or how companies can share or sell this data to other businesses. Consumer protection laws also still struggles here. The FTC's job is to stop unfair practices, but IoT data is hard to anonymize and so easy to track and the worst is difficult to secure. which can creates big privacy risks, under privacy laws, the FTC can only act when a company breaks its own posted privacy policy but it have not given strong rules about how companies should explain IoT data practices.[2]

Even though there are many laws and frameworks about cybersecurity, significant gaps still exist when it comes to IoT devices. The following are some of the key areas that need further attention:

Lack of legislation specifically for Iot

Most cybersecurity laws today were written for traditional computers and networks, not for IoT. IoT devices are different because there are many, diverse, and always connected.

But there is no clear, complete law made especially for IoT.

---

[1] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p. 721.

[2] CHIKE, Chike Patrick (2017). The Legal Challenges of Internet of Things. University of Maryland University College [online].
https://www.researchgate.net/publication/322628457_The_Legal_Challenges_of_Internet_of_Things , p 16-17.

As a result, existing rules are general or old, and they do not fully solve modern IoT security problems.[1]

Insufficient Enforcement Mechanisms

Even when security laws exist, it is very hard to enforce them. IoT devices are spread across different countries and made by different companies, so no single authority can check them all and many IoT manufacturers are small companies that do not have the money or experts to follow all security rules, Because of this, some devices end up with weak protection or even with no compliance at all.[2]

Privacy Concerns and Data Protection

IoT devices collect a large amount of personal data, which increases privacy risks, the existing laws help protect users, but they do not cover all the special risks of the Internet Of Things especially when data from many devices is combined or shared across platforms. This raises concerns about constant monitoring, tracking, and data being used without proper consent, where our data will be transferred, who can guarantee ?[3]

Information security one of the concerns for the Internet of Things system IoT devices are very different from each other in size for instance the storage, computing power, and battery even life. Because there's different IoT devices in many different areas and security, privacy are often not properly protected. IoT devices are weak in processing power and operation, which makes them easy targets for cyberattacks and security breaches. And the Cia triad which is (to ensur confidentiality, availability, integrity) a model that have been used by so many companies is not enough because the issue is that there is no guarantees [4]

Fragmentation of Standards

IoT security rules are not the same from one country to another, this lack of unified standards makes it very difficult for manufacturers to built devices that work securely everywhere. It also confuses consumers, who may not know what rights they have or how well their devices are protected in different regions, this fragmentation creates a complicated and inconsistent global IoT security landscape. [5]

---

[1] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach, p. 7.

[2] Ibid, p. 7.

[3] Ibid, p. 7.

[4] KARALE, Ashwin (2021). IoT-based Application of Information Security Triad. International Journal of Interactive Mobile Technologies, 15(24), 61–76 [online]. https://online-journals.org/index.php/i-jim/article/view/27333 , p. 61/64.

[5] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach, p. 7.

Part III how to solve IOT and cybersecurity legal issues ?

nowadays we hear a lot about cyber attacks, data breaches, security issues, data leaking... and they keep increasing every year. These issues now affect everyone, normal people and small companies to big international companies, police, and even governments. In 2014, many people called it the Year of the Breach, and 2015 was even worse, these names might sound exaggerated, but they show one thing: cybersecurity issues are happening often and causing more damage. Experts also say that attacks are becoming more destructive and personal. There are many reasons why cyber attacks in general and Internet of things breaches are rising so fast: new technologies are spreade quickly, society depends heavily on connected devices,and hacking tools are easy to buy or to use, cyber criminals are becoming more skilled, and it's very easy to enter the cybercrime world.[1]

Given the current situation of the Internet of Things , what can we do as a community to move forward?

First, we must understand that the IoT world is still messy and will stay in that way for a long time. Big companies will continue fighting to control different parts of the IoT market, despite this chaos, researchers and policymakers can still take important actions. One of the of the steps for example is improving cybersecurity education for computer science students and Right now, many students can finish a computer science degree without taking any cybersecurity classes. Many experts see this as a big red flag. Different groups have suggested solutions. For example:

A 2012 national plan on cybersecurity education recommended offering more cybersecurity courses, creating competitions to attract students, and using these events for company recruitment, also a 2013 report by the Association for Computing Machinery said students should be required to take at least one cybersecurity related course and universities should offer certificates and be like a middle man to find them jobs. However these ideas remain just suggestion, they are not strongly supported or funded yet.[2]

[1] WEBER, Rolf H. and STUDER, Evelyne (2016). Cybersecurity in the Internet of Things: Legal Aspects. Computer Law & Security Review, 32(5), 715–728, p. 716.

[2] HONG, Jason (2016). Toward a Safe and Secure Internet of Things [online]. New America. https://www.jstor.org/stable/resrep10509.6 . P. 8.

Another important idea is to teach cybersecurity to people outside of computer science, not just to increase awareness but also to help them understand how cybersecurity affects product design, teaching only computer science students is not enough, because creating IoT products involves sp many fields. For instance psychology students can learn how people change their behavior in cybersecurity situations if an issue has been raised from nowhere, such as how social pressure or motivation works Industrial or graphic design students can learn how to design warning messages and understand how users think.

The main point is that we should not limit cybersecurity education to traditional academic approaches, the world is complex, and real problems do not align only one field.[1]

On this sub chapter a legal, technical solutions related to the Internet Of Things will be discussed accordingly

1.1 Security, private, privacy by design principles.

Privacy and security in the Internet of Things are major concerns because these devices collect and share large amounts of sensitive data, because different companies are involving like device makers, app developers, and online platforms, this makes it hard to know who is responsible for protecting the user's information. IoT devices can easily violate privacy rules and the data they gather may move across different countries with different laws, creating legal problems (cross border issue). Many devices also have weak security, cannot be updated, and are vulnerable to hacking. Current laws are not fully prepared for these issues, as some data breach rules do not cover the types of data IoT devices collect. To address these challenges, stronger regulations are needed to ensure companies apply privacy, security by design principles and add built-in protections to their devices from the start.[2]

But what is privacy, security by design principle ?

"Companies/organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way

[1] HONG, Jason (2016). Toward a Safe and Secure Internet of Things [online]. New America. https://www.jstor.org/stable/resrep10509.6 . P. 9.

[2] CHIKE, Chike Patrick (2017). The Legal Challenges of Internet of Things. University of Maryland University College [online].
https://www.researchgate.net/publication/322628457_The_Legal_Challenges_of_Internet_of_Things , p. 12-16.

that safeguards privacy and data protection principles right from the start ('data protection by design'). By default, companies/organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data isn't made accessible to an indefinite number of persons ('data protection by default')".[1]

in other meanng Besides taking basic safety steps with IoT devices, it's also important to implement security by design. This means the company builds its products to be safe from the very beginning on the earlier stages . in order to follow rules that helping to protect the system from attacks and keep user data safe. By doing this, the company can be sure that she's protecting its customers and following EU laws like the GDPR. Products designed this way use for instance good coding practices, strong login protections, and are tested regularly to find and fix problems.

Security, privacy design principle by default was just a theory or approach ti develop software and hardware systems in so many countries, but nowadays so many countries make it a s requirement in favor to protect users, government or even manufactures to avoid responsibility if they proved that the cybersecurity issues is not from their side and they have no hand on it .

the law in so many regions stressed that companies need to apply and implement this principle, but the question is: whether this principle is mandatory or not ?

according to the GDPR article 25 : " The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons, on the same article it was mentioned that: An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance" .

It is crucial that GDPR spoke about certification to prove compliance but it is not mandatory to have in order to start selling IoT devices and in our to EU countries. This principle should be mandatory and make it as a requirement to decrease the ambiguously legal issues, and at least to make someone responsible.

[1] European Commission . What does data protection 'by design' and 'by default' mean? [online]. Retrieved [insert date], from https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en .

This could be happened if Default Settings applied by Manufacturers and the should be required to set secure default configurations for devices, including strong, unique passwords rather than common or factory default credentials that are easily exploited by attackers.[1]

1.2 Prevent sharing data with third parties and companies

There is a well quote " If something is free, you are the product," in other words if we use any product, a software, a platform, social media apps for free and we don't pay any fees, simply it means this entities getting their profits by using and selling our data to third parties, this profits could be happen by making advertisement. The company or the app developer will collect different data, our preferences, our historical search, and based on this information the users will get advertisement based on their preferences.

Speaking to Alexa, using smartwatches, using our phones, these are interconnected devices working simultaneously together, actually it makes it even worst because instead of using one device, we use three or four or even more devises, which making scope range of collecting data process more widely.

Did we gave our consent ?

By using any of IoT devices we usually use them without reading their policies, because that policy is long and not clear, containing so many technical words, as a result the user will avoid reading those policies without thinking about the consequences or where their Data will be transmitted. The GDPR discussed about data minimization, Conditions for consent, but what are the mechanisms to apply these rules ?

A simple answer for the previous legal issues related to users themselves, people don't know how much their data are valuable.

Preventing selling data will create a big problem to so many companies, and of course we can't implement effective rules to eliminate completely selling data to third parties, despite technology is sophisticated and tech companies will always find new loopholes to extract this data. However there is alternative solutions and approaches to minimize and make selling data to other parties near to zero percent, this solution is make our data in one

[1] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 8.

place, centralized, in one container, each used data will be known where it will be used, going…

This idea means that we will own our data and moitor, control each step, this approach called the Human centric Data approach.

The legal framework should also make sure that different IoT devices and platforms can work together safely. Security rules must be flexible in order that devices can connect to each other while still keeping the communication secure for instance the law could encourage using common security protocols to protect data sent between devices, this can help to avoid problems that happen when devices use weak or incompatible communication methods, which means if our data in in safe the leak of our data to third parties will be reduce.[1]

1.3 Public and private partnerships and industry for better regulation

Governments should support cooperation between companies and other industry groups to create a good security standards for IoT devices. Industry programs, like certifications or self made rules, can work alongside government laws to increasethe efficiency of using IoT. These programs make sure that devices are built with security from the start and include ways to monitor them, fix security problems with updates, and respond quickly to any incidents. [2]

This solution will improve the IoT sector, of course policy makers in most cases don't have any computing skills, they know how to regulate, and set out instruments, when it comes to technical solutions there is a need for specialists. If the policy, legislation makers asks the intervention of companies' users, technicians' help. We are going to have better regulation, better protection.

Chapter II Future Directions to resolve legal issues of cybersecurity in internet of things

The rapid growth of the Internet of Things brought us many benefits, but it also created different legal and security problems that current regulations still struggle to address and to resolve. as discussed in the previous chapters on this paper , existing laws are fragmented

[1] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 8.
[2] Ibid, p. 18

also enforcement is difficult, and many IoT devices still lack basic security protections. Therefor it is clear that updating old rules is not enough, especially the IoT scope is expanding too fast, and the technology is changing every year. What is needed now is a new, updated approach that can respond to new risks before they become serious problems.

This chapter looks at future directions that could help reduce the legal issues which touch cybersecurity of IoT cybersecurity. Technology alone cannot guarantee safety if the legal framework does not support it, and law alone cannot solve the problem if the devices themselves remain insecure. For this reason, the goal of this chapter is to combine both ideas and both fields and offer practical paths for the future.

The first section examines new generation IoT security solutions. These include emerging technologies such as blockchain, which can improve transparency and trust, and artificial intelligence, which can help detect malicious behaviour in connected devices more effecient. These tools may support legal compliance by giving regulators and users stronger guarantees about data protection also authentication and to solve vulnerabilities issues. While these technologies are still developing, they show strong potential for strengthening cybersecurity in ways that current systems cannot.

The second section turns to the concept of human-centric data approach. Nowadays data from IoT devices is stored and controlled by different companies, which increases risks and reduces user control. A human-centric model targets a system where personal data is managed in a single, secure environment controlled directly by the user. This would help address many privacy and accountability problems by giving individuals more control over how their information is accessed .

Finally, the chapter discusses the need for global cooperation and adaptive regulation. Cybersecurity problems do not stop at national borders, and IoT devices operate internationally. laws differ from one country to another, creating confusion and gaps in protection sometimes.we need for better harmonisation of standards, more cooperation between states, and flexible regulatory frameworks that can evolve with new technological developments are essential for building a safer IoT environment. Without international cooperation, even the best national laws will not be enough to address global threats.

Overall, this chapter argues that the future of IoT cybersecurity requires a combination of innovative technology, strong user-centric data protection, and coordinated global regulation. By discussing these future directions, the chapter provides a foundation for understanding how legal and technological strategies can work together to create a safer and more trustworthy IoT ecosystem.

2.1 New generation IoT security solutions

So many IoT devices depend on parts made by other companies such as sensors, chips, software, and cloud services. third party companies may not always use the same security rules as the company that make the final devices. This mean that weaknesses that third parties do can affect the security of the whole IoT system. For instance, one security flaw in a popular chip or software tool can create a problem in many different devices, no matter who made them. Because of this, IoT cybersecurity laws must cover the entire supply chain and make sure all suppliers follow strong security standards. This is difficult to control because supply chains involve many companies in different countries, each with their own laws and rules, and this exactly what countries should focus on.[1]

The security problems of IoT devices also encourage researchers to look for new cybersecurity solutions. Some of the most important research areas related to IoT including:

- **Encryption**

most IoT devices have very limited power and memory, so they cannot use heavy encryption. Researchers are working on simpler, "lightweight" encryption methods that still protect data well but do not slow down the device[2]. But when it comes to safe users' data it doesn't matter the cost always users in first line. Improving encryption by forcing companies otherwise no license would be given to them .

- **Detection using AI**

Even though IoT devices are small, there is millions of them producing data all the time. This data can be used by artificial intelligence to automatically detect strange or dangerous activity. Machine learning helps find unusual patterns that may indicate a cyber attack, allowing faster detection and automatic responses.[3]

Artificial Intelligence and Machine Learning are now been added to many IoT devices to help them make smart decisions, predict problems, and work automatically, these technologies bring many benefits, but they also create new risks, ai powered devices learn from their surroundings and from users, which can accidentally reveal sensitive data or create weaknesses that hackers can use, also criminals can use AI to create smarter and

[1] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 12.
[2] KOŁACZEK, Grzegorz (2025). Internet of Things (IoT) Technologies in Cybersecurity: Challenges and Opportunities. Applied Sciences, 15(6), 2935 [online]. DOI: 10.3390/app15062935 . p 1.
[3] Ibid, p. 1.

more flexible cyberattacks that target IoT devices. Therefore, IoT security frameworks must update and adapt to face these new threats. The law will also need to make sure that AI and machine learning in IoT systems are designed and used safely, with clear rules for responsibility and what happens if a security problem happened.[1]

In 2025 it is crucial to speak about artificial intelligence, the implementation of AI is everywhere, creating jobs, teaching, finding solutions, industries machines…

AI can increases efficiency time, reduce costs, and even turnover millions of dollars. And IoT ecosystem needs this kind of technology to predict the potential cyberattacks, and create a self defense. This idea needs specialists of course but it helps law makers to encourage companies to implement certain cautions by default.

- **Blockchain**

We should know first what does it mean Blockchain ?

"Blockchain is one way that data is protected. In short, blockchain allows a transaction to be made between two nodes in a permanent way and doesn't require third-party authentication. An even simpler way to discuss blockchain is in terms of databases. Blockchain is a type of database that stores information, though the method of how it stores data is unique. Databases are designed to have a huge capacity for electronic storage while also allowing users to access, monitor, and modify data. To manage big amounts of information, databases use servers to house data. The main benefits of blockchain systems are security, transparency, reliability, and efficiency due to the ability to record digital transactions and interactions between devices".[2]

"Blockchain technology enables the establishment of decentralised trust frameworks in IoT solutions. Utilising such solutions provides the opportunity to enhance security in terms of data integrity and the secure authentication of devices in a decentralised manner without the need to rely on a single, common central source of trust. Blockchain also offers a potential solution to other issues related to cybersecurity and privacy that are inherently associated with IoT networks"[3]

Blockchain is a huge research topic around the world, some experts believe that blockchain could be a powerful solution for IoT security because it can help connect and

[1] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 14.

[2] SIMON IoT (2024). Everything You Need To Know About Blockchain and IoT [online]. IoT For All. https://www.iotforall.com/everything-you-need-to-know-about-blockchain-and-iot

[3] SIMON IoT (2024). Everything You Need To Know About Blockchain and IoT [online]. IoT For All. https://www.iotforall.com/everything-you-need-to-know-about-blockchain-and-iot , p. 1.

track devices safely within one network or even across the world, blockchain can also make it easier for manufacturers to protect their devices without spending a lot of money on creating new security standards.[1]

2.2 Moving to Human centric data approach

LinkedIn recently caused a lot of criticism because the platform used to collect user data from its platform and used it to trains its AI models without getting clear permission from users first. In September 2024, it was revealed that LinkedIn had been using data of 930 million users including profile information, posts, and interactions to train their models, and as a result musers felt surprised and concerned. LinkedIn collecting huge information, including profile details, posts, how much users interact, and their language preferences, the company said this data was used to improve services like content suggestions and personalized recommendations. However, the data scraping was not treated the same everywhere. Users in the U.S. and U.K. were included automatically, while users in the EU, EEA, and Switzerland were excluded, probably because of data protection laws like the GDPR, after regulators in United Kingdoms raised concerns, LinkedIn had to pause these practices, showing how different legal rules can affect how companies handle user data.[2]

The current "enterprise centric" model used by companies keeps personal data inside their own systems and limiting how users can move or control, monitor their informations. when digital services add new AI features, most people do not really understand how their data is used, the old idea of "consent and control" where users are expected to read long, confusing privacy policies and manage complicated settings puts too much responsibility on the user so this system shows the big power imbalance in the data market, where companies have much control and knowledge than individual users do.[3]

Today the way of handling personal data is mostly centered around companies. The idea of enterprise centric system is that people should have control over their own data and should be able to decide how it is used and who can access it, this is why laws like the

---

[1] AYED, A. B.; TAVERAS, Pedro; BENYOUNES, Tarek (2020). Blockchain and IoT: A Proposed Security Framework. In: S. Latifi (Ed.), 17th International Conference on Information Technology-New Generations (ITNG 2020), Advances in Intelligent Systems and Computing, vol. 1134, Cham: Springer. DOI: 10.1007/978-3-030-43020-7_17 . p. 3.

[2] JURCYS, Paul; FENWICK, Mark; KOZUKA, Souichirou (2024). "Private-By-Default": A Principle & Framework for Designing a New World of Personal AI [online]. SSRN: https://ssrn.com/abstract=4839183 , p. 3.

[3] JURCYS, Paul; FENWICK, Mark; KOZUKA, Souichirou (2024). "Private-By-Default": A Principle & Framework for Designing a New World of Personal AI [online]. SSRN: https://ssrn.com/abstract=4839183 , p. 4.

GDPR and the California CCPA use a consent and opt out model. The technology behind these laws is designing to give users the power to agree or refuse certain types of data collection and use. In this model, “user control” mainly means that people can choose to opt out of tracking, or ask companies not to sell their data. even under this focused system, LinkedIn should have asked users for clear permission before using their data. Because Consent is not just a small stepit is a basic legal requirement when personal data is involved.[1]

When companies collect data by default, it becomes almost impossible for them to offer honest on what they are collecting, and they offering the option to opt out from their service if you didn’t like the they working.

In other words, companies nowadays once we are using their provided services, they start collecting data automatically and you cant track what is happening with these data in most time, if they using them to develop their models? Or just keeping them in their container without further streps? Or selling them to third parties to make advertisement and making profits since in most times we use different platforms and services for free ?

Indeed we cannot ddeny the fact that the current laws like GDPR and CCPA reshape and protected our digital data rights. However the legal question is: do we own our data ? if someone’s own his data, why he would ask and demand and take permission to get access for his data? Several rights related to Data are mentioning in both GDPR and CCPA, but these are outdated ways on hoe to get access to our data, for instance any one can ask any kind of company whose holding his data, a copy or a version about what data they been keeping about him for the entire time, and the process is that the company should provide a not ambiguous steps to users allowing them how to ask about their data.

If a user own something why he needs to go through a long, difficult and in most times a not clear procedure just to get what he owns.

What are the guarantees if users ask their data to be deleted and companies will completely delete these data ? once data is outside, there is no way to get them back again, internet is a huge connected network.

It confusing sometimes that experts calling digital data as the new oil while users and people don’t appreciate and they can not evaluate the worth of their data, like how much their data is worthing ?

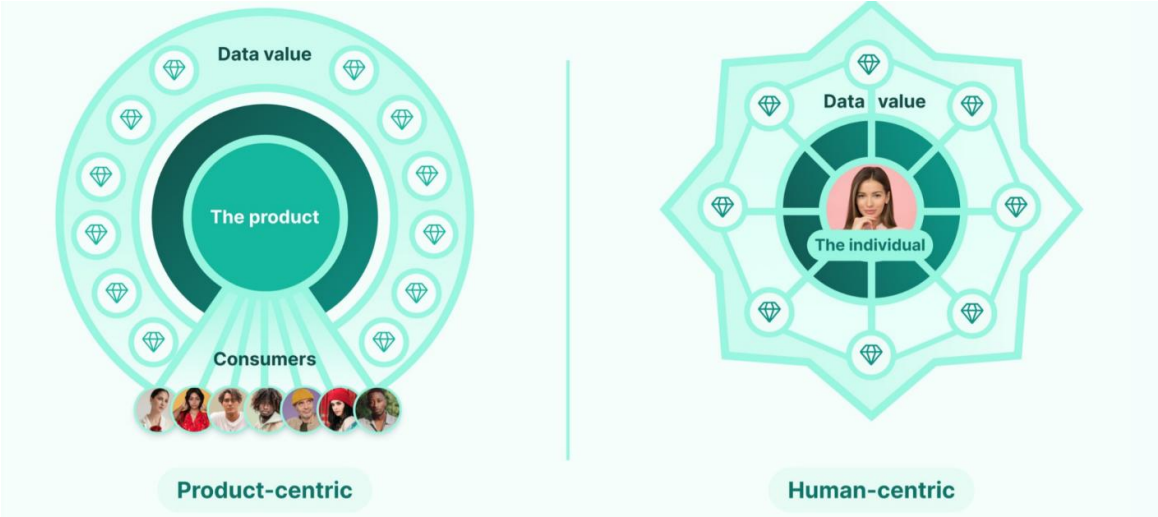
[1] JURCYS, Paul; FENWICK, Mark; KOZUKA, Souichirou (2024). “Private-By-Default”: A Principle & Framework for Designing a New World of Personal AI [online]. SSRN: https://ssrn.com/abstract=4839183 , p. 9.

Speaking about previous issues have really something to do with the respective paper. Internet of things based on interconnected devices, these devices using sensors, cameras, audio recording, programs… and the main responsibility is to collect as much data they can in order to give automation solutions to users.

If millions of data are being collect everyday, the existing approach does not align with this new generation.

For this reason, there is a solid reason to highlighted Human-Centric Data model, and make the distinguish between enterprise-centric.

We are entering a new era of digital communication where the way data is collected, organized, and shared is changing everyday and new system is starting to appear one that puts the individual at the center. This new human-centric data model is based on the idea that people should have real control and ownership over their data. In this system, your data stays with you, and apps or services only get access if you invite them into your personal data space, or your personal container. This is completely different from today's enterprise-controlled model. Right now, people must give their data to companies and accept whatever rules the companies set, this creates closed systems where big platforms control the data and act like they own it. The "opt-out" rights that exist today often give users only the illusion of control, moving to a human-centric data model would change everything. It would strengthen privacy, increase personal freedom, and shift power from companies back to individuals. Instead of companies owning user data, people would keep their data and decide who can access it and for what purpose. This gives users real control and makes data sharing safer and more transparent.[1]



[1] JURCYS, Paul; FENWICK, Mark; KOZUKA, Souichirou (2024). "Private-By-Default": A Principle & Framework for Designing a New World of Personal AI [online]. SSRN: https://ssrn.com/abstract=4839183 , p. 12.

Source : JURCYS, Paulius and STRIKAITE-LATUSINSKAJA, Goda (2025). Data Privacy Law: Human-Centric Approaches – Lecture 3 [unpublished teaching material]. Vilnius University, Faculty of Law.

Applying Human centric data approach means we will not only change technology, but also changing the existing laws to be aligned and have a updated version which serve companies but will put users in first line.

2.3 global cooperation and adaptive regulation

Because IoT technology changes so quickly, the law also needs to be flexible and able to adapt fast. traditional laws often become outdated before they can protect people from new security risks, a modern legal approach should respond quickly to new threats, set clear rules for IoT companies, and make sure they keep their devices secure. This means regularly updating security laws, working closely with governments, tech companies, international organizations, and consumer groups, and creating global standards so devices meet the same security level everywhere. It also requires setting clear security rules for every stage of an IoT device's life from its design and production to software updates and maintenance. [1]

Since IoT devices operate across borders, countries must cooperate to create shared global standards through organizations like ISO and IEC, and to protect data between countries with clear rules for privacy and security. Industry cooperation is also essential, because governments cannot solve these problems alone, companies can help by creating their own security guidelines, best practices, and certification programs that show devices meet strong security requirements. International bodies such as the UN, WTO, and ITU will need to work together to harmonize regulations and to reduce confusion for manufacturers and consumers, and fight cross-border cyberattacks through shared information and coordinated responsesnl through global cooperation and flexible, strong laws can we ensure that IoT devices remain safe and trustworthy as technology continues to evolve.[2]

[1] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 7.

[2] ROXANNE, Delores Glynis (2025). The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach[online].https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach , p. 10/16.

Conclusion

1. the Internet of Things is not just a technical idea but also considered as a complicated system that connects physical devices, data and services, therefore, the Internet Of Things create new types of risks and legal issues that traditional legal rules on cybersecurity and data protection was not designed to address. Existing concepts of networks, systems and data are often too narrow for the reality of the Internet Of Things.
2. The analysis confirmed that current legal instruments in the European Union, such as the GDPR, NIS2 Directive, Cybersecurity Act, Cyber Resilience Act and the Data Act, allready give an important level of protection for the Internet Of Things users and providers. However, these acts was not created specifically for Internet Of Things and therefore cover it indirectly. As a result, the protection is sometimes fragmented and important questions about responsibility, security duties and data control remains unclear.
3. The comparison with the United States showed that a fragmented sector based and state level approache to Internet Of Things cybersecurity creates many legal uncertainties. Without one unified federal framework similar to the EU approach, users and companies must rely on different rules in different states, like the soft law documents and guidelines from agencies such as NIST and the FTC. This makes it harder to create stable and predictable standards for IoT security.
4. The research on international law have demonstrated that there's still no global, binding framework focused on Internet Of Things cybersecurity. The Budapest Convention on Cybercrime remains the main instrument for offences against data and systems, but it was drafted long before the rise of Internet Of Things and does not directly address the specific risks of connected devices and the attempts to create broader UN instruments are slow, which means that cross-border cyber incidents involving Internet Of Things devices are still difficult to investigate and prosecute in practice.
5. The analysis of liability showed that traditional product liability and consumer protection rules do not fully fit the Internet Of Things environment. In Internet Of Things, harm can come not only from physical defects but also from software issues, weak security settings, missing updates, misuse of data and failures of cloud services. It is often difficult to identify who is responsible: the device manufacturer, the software developer, the platform operator, or other actors in the supply chain and this can create a legal uncertainty for both users and businesses.

6. Consumer contracts and terms of use in the Internet Of Things ecosystems often place users in a weak position, they are confronted with long and complex conditions, multiple overlapping contracts and unclear information about security, data sharing and updates. In this situation, consent is often formal but not meaningful and consumers cannot realistically negotiate or understand all risk related with clauses, for sure this affects autonomy, fairness and trust in Internet Of Things services.
7. Privacy and data protection rules, although strengthened by instruments such as the GDPR and CCPA, still rely on an enterprise centric model, where companies control data and users must “opt out” or make access requests after the fact. In a world where Internet Of Things devices collect continuous streams of personal data, this model does not give individuals real control. Human-centric data approaches, based on personal containers controlled by users, would better reflect the realities of modern data flows and reduce many risks and legal issues related to profiling, tracking and data using.
8. The study of critical infrastructures and standards confirmed that instruments such as NIS2, ENISA guidance and international standards (ISO/IEC 27001 and 27400) are important steps towards a more secure Internet Of Things environment. However, their effectiveness depends on how statess and companies implement them in real practice, because not all sectors, especially those related to Internet Of Things in everyday consumer life, receive the same level of attention as traditional critical infrastructure such as energy or transport.
9. The research showed that the technical solutions are not enough if they are not supported by clear and enforceable legal duties. Concepts like security by design and by default, strong encryption, regular updates, AI based detection of anomalies, can reduce the Internet Of Things issues, but they must be embedded in binding rules which allocate responsibilities along the whole supply chain and ensure that non compliance has real consequences.
10. Finally, this thesis concluded that the future of Internet Of Things cybersecurity must be based on three combined elements, firstly: strong legal frameworks specifically adapted to Internet Of Things, secondly: a shift towards human-centric data governance, Thirdly: deeper international cooperation. Without these three pillars working together, Internet Of Things will continue to bring benefits, but the legal protection of users, the clarity for businesses and the overall trust in connected devices and the Internet Of Things will remain incomplete.

Proposals

1. Lawmakers should further clarify and extend existing cybersecurity and product safety rules so that they explicitly cover Internet Of Things devices, cloud components and related services, this also includes adapting liability rules to digital and data driven harm, not only to physical defects.
2. The European union and other jurisdictions should update product liability by including software and security failures in Internet Of Things devices, responsibility should be shared in a fair and transparent way between manufacturers, software developers, platform operators and other actors who have real control over risks.
3. Security and privacy by design and by default should become a practical, enforceable obligation for all high risk Internet Of Things products, not only a recommendation. For certain categories of devices, especially those used in health, transport, energy, or smart cities, independent certification should be required before products are placed on the market.
4. Policymakers should support the development of human centric data infrastructures, like personal data stores or containers controlled and owned by users. Also legal rules on access, deletion, portability and reuse of data should be adapted so that individuals can exercise these rights directly through such tools, instead of relying only on slow and complicated procedure requests to companies.
5. States should strengthen international cooperation in the field of cybercrime and Internet Of Things security by building on the Budapest Convention and related initiatives, this includes faster mutual assistance, better sharing of technical information on Internet Of Things incidents and also long term work towards harmonized global standards for Internet Of Things cybersecurity and data protection.
6. Finally public authorities, industry and even consumer organisations should work together in partnerships to improves Internet Of Things security, this cooperation can help to develop technical standards, improved the guidelines and education programs that support innovation and the protection of digital data.

LIST OF SOURCES

I. Legal Acts

- Commission of the European Communities (2004). *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism (COM(2004) 702 final)* [online]. Brussels, 20 October 2004. CELEX 52004DC0702. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0702
- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. *OJ L 210*, 7 August 1985, pp. 29–33.
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *OJ L 345*, 23 December 2008, pp. 75–82.
- Council of Europe (2001). *Convention on Cybercrime (Budapest Convention)*. ETS No. 185, 23 November 2001.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *OJ L 194*, 19 July 2016, pp. 1–30.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *OJ L 333*, 27 December 2022, pp. 80–152.
- European Commission (2025). *Cyber Resilience Act*. Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *OJ L 119*, 4 May 2016, pp. 1–88.
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. *OJ L 151*, 7 June 2019, pp. 15–69.

- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 ("Cyber Resilience Act"). *OJ L 347*, 20 November 2024, pp. 1–79.

II. Books & Book Chapters

- AYED, A. B., TAVERAS, Pedro, & BENYOUNES, Tarek (2020). *Blockchain and IoT: A Proposed Security Framework*. In S. Latifi (Ed.), *17th International Conference on Information Technology–New Generations (ITNG 2020)*, Advances in Intelligent Systems and Computing, Vol. 1134. Cham: Springer. https://doi.org/10.1007/978-3-030-43020-7_17
- FAIRGRIEVE, Duncan & GOLDBERG, Richard S**.** (2020). *Product Liability* [online]. Oxford: Oxford University Press. Oxford Academic.
- KOOLEN, Christof (2023). *Protecting EU Consumers in Internet of Things Ecosystems: The Intersection between Consumer, Competition, and Data* [online]. Oxford: Oxford University Press. Oxford Academic.
- LA DIEGA, Guido Noto (2018). *Internet of Things and the Law* [online]. London: Routledge. ProQuest Ebook Central.

III. Scientific Journal Articles

- AZNAG, Fatma & TAHANOUT, Kheira (2022). *Internet of Things (IoT) Technology and the Future of Payments (Case of Amazon-Go)*. Administrative and Financial Sciences Review, 6(1) [online]. https://www.asjp.cerist.dz/en/article/187893
- BEALE, Sara Sun & BERRIS, Peter (2017–2018). *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*. Duke Law & Technology Review, 16, 165–204.
- CASAROSA, Federica (2024). *Cybersecurity of Internet of Things in the Health Sector: Understanding the Applicable Legal Framework*. Computer Law & Security Review, 53 [online]. https://doi.org/10.1016/j.clsr.2024.105982
- CHIARA, Pier Giorgio (2022). *The IoT and the New EU Cybersecurity Regulatory Landscape*. International Review of Law, Computers & Technology, 36(2), 118–137. https://doi.org/10.1080/13600869.2022.2060468

- CLOUGH, Jonathan (2014). *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*. Monash University Law Review, 40(3), 698–736. https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf
- KARALE, Ashwin (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet of Things, 15, Article 100420. https://doi.org/10.1016/j.iot.2021.100420
- KAGITA, Mohan Krishna; THILAKARATHNE, Navod; GADEKALLU, Thippa Reddy; MADDIKUNTA, Praveen Kumar Reddy; SINGH, Saurabh (2023). *A Review on Cyber Crimes on the Internet of Things*. Charles Sturt University [online]. https://www.researchgate.net/publication/359708894_A_Review_on_Cyber_Crimes_on_the_Internet_of_Things
- KOŁACZEK, Grzegorz (2025). *Internet of Things (IoT) Technologies in Cybersecurity: Challenges and Opportunities*. Applied Sciences, 15(6), 2935. https://doi.org/10.3390/app15062935
- LOSAVIO, Michael M.; CHOW, K. P.; KOLTAY, Andras; et al. (2018). *The Internet of Things and the Smart City: Legal Challenges and Possibilities*. Security and Privacy, 1(3) [online]. https://doi.org/10.1002/spy2.23
- MARKOPOULOU, Dimitra & PAPAKONSTANTININOU, Vagelis (2021). *The Regulatory Framework for the Protection of Critical Infrastructures Against Cyber-Threats: Identifying Shortcomings and Addressing Future Challenges: The Case of the Health Sector in Particular*. Computer Law & Security Review, 41, Article 105502. https://doi.org/10.1016/j.clsr.2020.105502
- NEMEIKŠIS, Giedrius (2022). *The Challenges of the Digital Age: The Problems of Criminal Liability for Cybercrimes in Lithuanian Law*. Acta Prosperitatis, 13(1), 125–138. https://doi.org/10.37804/1691-6077-2022-13-124-138
- WEBER, Rolf H. & STUDER, Evelyne (2016). *Cybersecurity in the Internet of Things: Legal Aspects*. Computer Law & Security Review, 32(5), 715–728.
- WU, Miao; LU, Ting-Jie; LING, Fei-Yang; SUN, Jing; et al. (2010). *Research on the Architecture of Internet of Things*. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE 2010), Vol. 5 [online]. https://www.researchgate.net/publication/224175757_Research_on_the_architecture_of_Internet_of_Things

IV. INTERNET SOURCES

- ASHTON, Kevin (2009). *That "Internet of Things" Thing* [online]. https://www.rfidjournal.com/that-internet-of-things-thing
- Bristows (2022). Internet of Things (IoT) — Key Legal Issues [online]. Bristows. https://www.bristows.com/app/uploads/2022/10/Internet-of-Things-IoT—key-legal-issues-Lexis®PSL-practical-guida.._.pdf

- BIREN LAW GROUP, P.C. (2025). *The Hidden Dangers of Smart Home Devices: Product Liability in the IoT Era* [online]. https://biren.com/the-hidden-dangers-of-smart-home-devices-product-liability-in-the-iot-era/
- European Commission (n.d.). *Cyber Resilience Act* [online]. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- European Commission (n.d.). *What Does Data Protection "By Design" and "By Default" Mean?* [online]. https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en
- FEDERAL TRADE COMMISSION (n.d.). *About the FTC* [online]. https://www.ftc.gov/about-ftc
- SIMON IoT (2024). *Everything You Need to Know About Blockchain and IoT* [online]. IoT For All. https://www.iotforall.com/everything-you-need-to-know-about-blockchain-and-iot
- UNSW COMMUNITY (2023). *Internet of Things and the Law: Legal Strategies for Smart Technologies* [online]. (upstream page exists; main content is video)
- WIRED (NEWMAN, Lily Hay) (2019). *These Hackers Made an App That Kills to Prove a Point* [online]. https://www.wired.com/story/medtronic-insulin-pump-hack-app/

V. OTHER

VIDEOS

- HOWTOAV (2019). *How Is the Internet of Things Affected by GDPR?* [video]. https://www.youtube.com/watch?v=Ji53_8vPVjo
- UNSW COMMUNITY (2023). *Internet of Things and the Law: Legal Strategies for Smart Technologies* [video]. https://www.youtube.com/watch?v=ph5aaeVjJLM

RESEARCH REPORTS & WORKING PAPERS

- HONG, Jason (2016). *Toward a Safe and Secure Internet of Things* [online]. New America. https://www.jstor.org/stable/resrep10509.6
- JURCYS, Paul; FENWICK, Mark; KOZUKA, Souichirou (2024). *"Private-By-Default": A Principle & Framework for Designing a New World of Personal AI* [online]. SSRN. https://ssrn.com/abstract=4839183
- LEWIS, James Andrew (2016). *Managing Risk for the Internet of Things* [online]. CSIS.
- ROXANNE, Delores Glynis (2025). *The Internet of Things (IoT) and Cybersecurity Laws: An Adaptive Approach* [online]. https://www.researchgate.net/publication/387971241_The_Internet_of_Things_IoT_and_Cybersecurity_Laws_An_Adaptive_Approach

DELIVERED LECTURES

- JURCYS, Paulius and STRIKAITE-LATUSINSKAJA, Goda (2025). *Data Privacy Law: Human-Centric Approaches* – Lecture [unpublished teaching material]. Vilnius University, Faculty of Law.
- KULESZA, Joanna (2025). *Cybersecurity Law and Cybercrime* – Lecture [unpublished teaching material]. Vilnius University, Faculty of Law.

Summary

Title: Legal Issues of Cybersecurity in the Internet of Things
Student: Heythem Abidat

This thesis examines the legal issues of cybersecurity in the Internet of Things and explain why this topic is important as billions of devices became connected together. Interent Of Things creates new risks because it links physical devices with data and services in ways that traditional laws did not expect even, the work reviews the most important legal frameworks in the European Union and the United States and at the international level to understand how well they protect users and service providers. The analysis show that laws like GDPR, NIS2, the Cyber Resilience Act, the CCPA, and Budapest Convention provide some protection but they not designed specifically for the Internet Of Things. Therefore there is many gaps in security, responsibility, accountability and data protection.

This thesis finds also, it is unclear who is responsible when Internet Of Things systems fail, when software is insecure or when data breaches misuse happens, it also shows that consumer contracts and privacy rules still rely on old models where companies control user data, which does not fit the modern connected devices model, indeed the research argues that a new approach is ofcourse needed including clearer legal rules, stronger security by design and better protection of personal data and a humancentric data model that gives users real control over their information and data to accomplish the idea of owning our data , it also highlights that international cooperation is necessary because Internet Of Things isuues easily cross borders. Overall, the thesis concludes that while Internet Of Things bring benefits, the updated and harmonized legal solutions are crucial to make Internet Of Things systems safer, fairer and more trustworthy for everyone.