https://doi.org/10.15388/TMP.2023.14

UNLOCKING THE FULL VALUE OF DATA – MISSION (IM)POSSIBLE?

Eglė Petrošiūtė, Justė Sabanskaitė

Vilnius University Faculty of Law
5th year students
Saulėtekio av. 9, I block, 10222 Vilnius
Email addresses: eglepetrosiute00@gmail.com, juste.sabanskaite@gmail.com
Academic supervisor of the paper lecturer Dr. LL.M. Paulius Jurčys
Email address: pjurcys@gmail.com
Practical supervisor of the paper lecturer Dr. Stasys Drazdauskas
Email address: stasys.drazdauskas@sorainen.com

Annotation. *The article analyses if and whether people can use the data, generated by various devices, effectively. One of the main goals of the European Union's legislators is to establish a system for individuals to successfully unlock their data from silos and eliminate limitations when it comes to sharing data with third parties and between different sectors. The authors of this paper argue that while the free flow of data offers benefits to businesses and individuals, there are a number of challenges that could arise. Hence, this paper analyses three practical situations regarding data sharing between different subjects and distinguishes the advantages, as well as ethical, legal and technical challenges.*

Keywords: *Data Act, GDPR, data, sensors, Internet of Things.*

DUOMENŲ VERTĖS „ATRAKINIMAS" – MISIJA (NE)ĮMANOMA?

Anotacija. *Straipsnyje analizuojama, kaip asmenys gali efektyviai panaudoti įvairių naudojamų prietaisų sugeneruotus duomenis. Vienas iš pagrindinių Europos Sąjungos teisės aktų leidėjo tikslų yra sukurti sistemą, kurioje individai galėtų sėkmingai „atrakinti" savo duomenis iš duomenų bazių (t. y. prieiti prie savo duomenų) bei pašalinti kliūtis dalytis duomenimis tarp skirtingų sektorių bei su trečiosiomis šalimis. Šio straipsnio autorės teigia, kad nors nevaržomas duomenų srautas yra naudingas tiek verslui, tiek ir asmenims, tačiau gali kilti nemažai iššūkių, siekiant užtikrinti laisvą duomenų judėjimą. Taigi, šiame darbe analizuojamos trys praktinės situacijos, kuriose pasireiškia duomenų dalijimasis tarp skirtingų subjektų, išskiriami privalumai bei etiniai, teisiniai ir techniniai iššūkiai.*

Pagrindiniai žodžiai: *Duomenų aktas, BDAR, duomenys, jutikliai, daiktų internetas.*

"Data is the new oil"
Clove Humby[1]

Introduction

Artificial intelligence (hereinafter referred to as **AI**)[2], sensors[3], deep fakes[4], Internet of Things (hereinafter referred to as **IoT**)[5], data[6]… These are the terms that nowadays frequently circulate in the media, various economic sectors and society in general. Rapid technology development prompts people to experience new things that otherwise could not be possible. To do that individuals incorporate as many inventions into their day-to-day life as possible. Nowadays people own multiple devices that make their life easier and more enjoyable: not only smartphones, automobiles, computers, and smartwatches, but also smart rings, smart door locks, smart bicycles, smart refrigerators or even smart toilets. Most of these new technologies have sensors that track various activities. As a result, it generates data. So much data that, according to the International Data Corporation, the Global Datasphere will grow from 33 zettabytes[7] in 2018 to 175 zettabytes by 2025 (Reinsel et al., 2018, p. 3). However, all this generated data is stored in closed, siloed databases of manufacturers of devices with sensors which leads to no access to the data that is enormously valuable for individuals and businesses. As a result, changes prompted by the increasing amount of data created and captured require a legislative framework which proves to be suitable for present times. That is why in 2022 the European Commission proposed a draft of a potential new regulation, i.e., Proposal for a regulation on harmonised rules on fair access to and use of data (hereinafter referred to as **Data Act**). It is one of the

---

1 Clive Humby is a mathematician who coined the phrase in 2006 (The Guardian, 2013).

2 Business Insider: Web search as you know it is dead: Microsoft's ang Google's new AIs are about to transform how you look for information online (modified 8 February 2023); Wired: The Case for Outsourcing Morality to AI (modified 2 February 2023); LRT: Dirbtinis intelektas įsitvirtina meno pasaulyje: kaip keliais paspaudimais telefone sukurti paveikslą? (modified 9 January 2023).

3 The Verge: How to use the Apple HomePod's temperature and humidity sensors (modified 30 January 2023); BBC: Baxter College installs toilet sensors to stop vaping (modified 23 January 2023).

4 Business Insider: Ukraine's deputy prime minister says it is educating its citizens about the dangers of deepfakes as it fights Russian disinformation in 'a war of technologies' (modified 20 January 2023); Wired: I Think My Face Was Deepfaked Into a Chinese Camping Stove Ad (modified 11 January 2023); LRT: Kinija imasi reguliuoti „deepfake" technologiją (modified 10 January 2023).

5 TechCrunch: Memfault raises $24M to help companies manage their growing IoT device fleets (modified 24 January 2023); LRT: 15 mlrd. prijungtų prietaisų: daiktų internetu naudojamės patys to nežinodami (modified 19 January 2023).

6 ZDNET: Unlock your trapped data: Driving insights from edge-to-cloud (modified 31 January 2023); Wired: All the Data Apple Collects About You–and How to Limit It (modified 16 January 2023).

7 One zettabyte is equivalent to a trillion gigabytes. It would take 1.8 billion years for one individual to download the full 2025 Global Datasphere (i.e., 175 zettabytes) at the average connection speed of 25 Mb/s (Reinsel et al., 2018, p. 7).

initiatives that the European Union (hereinafter referred to as **EU**) will try to enact in the next following years to promote free data flow within the EU and across different sectors, as well as establish an open approach to international data flows, based on European values. Hence, this article analyses not only the new proposed legal act but also discusses sensors and their importance nowadays, as well as presents practical situations on how unlocking the value of data could work in different sectors and what kind of challenges could arise.

The purpose of this article is to analyse and present new proposed data legislation in the EU and provide an analysis of practical situations in the framework of this legislation. In order to achieve this aim, the authors have established the following **tasks**:

1. To present measures used to collect and process data.
2. To provide data legislation analysis in the EU and new initiatives.
3. To assess how unlocking the value of data would work in practice and identify the possible challenges.

The object of this article is to show how unlocking the value of data works according to the proposed Data Act.

The following research **methods** are applied in the article: the theological method was used to understand the substance of EU legislation; the legal document analysis method was applied to get an insight into data legislation in the EU; the interdisciplinary method was applied to analyse practical situations and to highlight the ethical, legal and technical challenges.

The article is **relevant** since the usage of sensors and sensorised devices is growing at a rapid pace. Hence, there is so much data that could be used in beneficial ways to improve the quality of life and generate profits for businesses. Thus, it is important to unlock the data from closed databases and take advantage of it by creating new products and services. However, every new initiative has its advantages and disadvantages. The paper analyses practical situations in different sectors in accordance with the new proposed regulation and assesses ethical, technical and legal challenges which show the **originality** of this paper.

The research analyses the works of authoritative legal scholars who explore the topic of unlocking the value of data, as well as the EU's initiatives to ensure free data flow. In addition, the legal documents which impact data management in the EU are discussed. Furthermore, the literature about IoT and sensors is analysed to better understand the importance of these innovations.

1. Age of sensorisation

Humanity has already experienced three industrial revolutions and mechanisation, as well as electrification and information, has already changed the world. Now, it is happening again, for the fourth time.

This time, the Fourth Industrial Revolution (also called and hereinafter referred to as Industry 4.0) is supported by technological pillars such as sensors and the IoT, AI, cloud computing, cybersecurity, etc. Industry 4.0 encourages physical objects, such as sensors, devices and business assets to be connected to one another and the Internet (Sipsas et al., 2016, p. 236). Therefore, it helps to connect the physical and digital worlds, as well as enable the development of smart applications or autonomous systems.

Sensor technologies play a key role in Industry 4.0. They can increase efficiency, reduce cost, determine failure, collect information and many other things in the manufacturing facilities. However, sensors are no longer used just in engineering or manufacturing. Innovative sensor technologies have transformed day-to-day lives and are used for daily life in almost all fields: to help clean the house, enhance safety, monitor environmental changes, promote fitness and healthcare etc. (Javaid et al., 2021, p. 6-7). Indeed, sensors are everywhere, from the dishwasher button to the video doorbell at home. With the advent of the IoT, new sensor-related applications are being introduced every day and it is driving sensorisation even more. Thus, what are sensors, the IoT and how do they work?

1.1. Sensors and their capabilities

Sensors are devices that can detect changes in the source or the environment, collect signals and respond accordingly, i.e., convert them into a form that can be understood and processed by electronic systems (Javaid et al., 2021, p. 2). There are many different types of sensors: temperature, proximity, gas, level, light, pressure, chemical, biomedical and so on (Sehrawat, Gill, 2019, p. 524-525).

The diversity of sensors enables the creation of many different things. For example, a French health company Withings recently introduced a bowl-affixed device called U-Scan to analyse biometrics from urine concentration (Fitt Insider, 2023). By observing and identifying a wide range of biomarkers present in urine, it is intended to give a quick glimpse of the body's balance. Another smart gadget is Muse 2, presented by Canadian company InteraXon (Choose Muse, n. d.). It is a multi-sensor meditation tool (headband) that offers real-time feedback on breathing, body movements, pulse rate and brain activity and guidance on how to achieve a more relaxed state of mind. Also, there are wireless leak detectors, i.e., Ukrainian company Ajax Systems created a product called LeaksProtect which is equipped with sensors to alert people about possible leaks (Ajax.Systems, n. d.). The company even provided and installed security and monitoring apparatuses in Ukraine to protect four Banksy murals that have become symbols of invincibility in and around Kyiv. To help detect efforts to harm or approach the objects, as well as to send notifications to the security company in case that occurs, they have a variety of sensors, including motion, shock,

temperature, humidity and CO2 sensors (The Art Newspaper, 2023). Essentially, the list is endless and there are smart gadgets for every possible occasion that a person can think of.

It is clear that sensors made a huge impact on many different industries and also generated countless benefits. This tendency of sensorisation has a huge impact on people's daily lives. To give an illustration of that tendency, today more than 100 million people wear Apple Watches (Above Avalon, 2021) which greatly contributes to awareness about health (it tracks daily steps, heart rate, burned calories, blood oxygen levels, sleep and more). Besides that, emails, texts, calls, music etc. are all accessible from a small device on a wrist which is very convenient. As an analyst Neil Cybart correctly pointed out, the Swiss watch industry missed the wrist's essential significance by selling prestige and wealth on the wrist and Apple took advantage of the underpriced "wrist real estate" (Above Avalon, 2021). And a lot more people own other sensor-equipped devices because the market offers a variety of them.

To sum up, the popularity of sensors is growing exponentially. However, the vital component of their popularity is the IoT and connectivity which will be presented in the following part of this article.

1.2. The main idea of the Internet of Things

All smart devices with sensors can be connected by a wireless network system - the IoT. The IoT, in its broadest terms, is a network of physical objects ("things") connected to the Internet. More precisely, IoT means that the objects are wired together and have sensors, software and other technologies that enable them to send and receive data. The IoT components are conceptually summed up in the equation below.

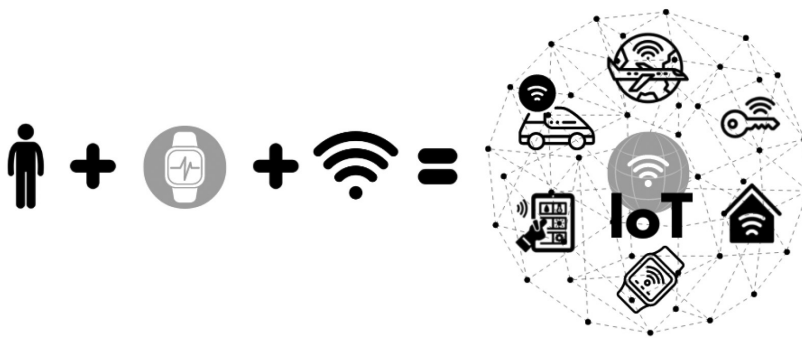

Figure 1. Visual representation of IoT (Farhan et al., 2017, p. 1)

Figure 1 illustrates that for the IoT to work there needs to be a person, a physical object (device, sensor, controller etc.) and the Internet. For example, even a smart light bulb is considered to be an IoT product because it is connected to the Internet and allows lighting to be customised, scheduled and controlled remotely via an app.

Nowadays one of the main goals for developers is to create not islands of isolated systems, but to integrate many islands of connected systems, applications, services and underlying devices (Farhan et al., 2017, p. 1), i.e., enable objects in IoT to communicate and exchange data with each other autonomously. That is where the concepts of smart cities, smart homes, smart offices, smart agriculture etc. emerge from. For instance, the concept of smart city explores IoT applications to manage traffic and control air quality and explores the possibility of smart parking, smart lighting, as well as a smart waste collection (Kumar et al., 2019, p. 5). According to the statistics, there were over 10 billion IoT devices in the world in 2021 and it is estimated that in 2030 the number of active IoT devices will surpass 25 billion (Data Prot, 2023). Therefore, people already use a vast amount of smart gadgets, so the idea of integrated islands of connected systems and autonomous communication between various devices does not seem so far-fetched.

With the wide adoption of IoT devices, the amount of data collected by smart devices is rising at an unprecedented rate, resulting in new insights, opportunities, and applications in a variety of fields. This is the main reason why the European Commission is trying to change data regulation in the EU and unlock the data to experience its full potential. Therefore, the next part of this article will provide an overview of data regulation in the EU and the European Commission's latest initiatives in this field.

2. Data in the European Union: new initiatives

Technology advancements and massive amounts of data collection prompt countries to recognise the need to provide appropriate measures to protect people's privacy, as well as personal data. In today's digital age, various data is collected and processed on a transnational scale and the data moves freely between different states and businesses. Precisely that is why the competent EU institutions must ensure consistent protection of personal data and privacy across the EU and establish a harmonised legal framework. One of the key pieces of legislation in this sphere is the 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, and repealing Directive 95/46/EC (hereinafter referred to as **GDPR**), which came into force in 2018 (Article 99(2)). Some authors, such as Tal Z. Zarsky, stated, that the GDPR is "the most comprehensive and forward-looking piece of legislation to address the challenges facing data protection in the digital age" (Zarsky, 2016, p. 995), while former member of the European Par-

liament Jan Philipp Albrecht claimed that GDPR will change not only the European data protection laws, "but nothing less than the whole world as we know it" (Albrecht, 2016, p. 287). GDPR is still one of the most talked about pieces of legislation that is best known for harming companies with huge fines for data breaches.

According to the Recitals 6 and 7 of GDPR, the scale of the collection and sharing of personal data has increased and both private companies and public authorities can make use of personal data on an unprecedented scale to pursue their activities. It is important to ease the free flow of personal data within the EU and third countries while ensuring an extremely high level of protection of personal data. Therefore, GDPR emphasises the need for a more coherent data protection framework, supported by strong enforcement. That is why GDPR establishes several key principles for the protection of personal data (e. g. lawfulness, fairness and transparency, data minimisation, storage limitation, accountability, etc. (Article 5)), data subject rights (e. g. right of access (Article 15), right to erasure (Article 17), right to data portability (Article 20), etc.) and, most importantly, forces member states to establish supervisory authority to monitor the application of GDPR (Article 51), as well as other abstract rules and principles.

From 2018 GDPR was (and still is) the main document, which protects people from the harmful influence that arises from data management. However, there have been some concerns raised by scholars and the European Commission about the implementation and enforcement of the GDPR. The Communication Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation evaluates and reviews the application and functioning of the GDPR rules. The Communication notes that the regulation requires member states to make laws in certain areas while giving them the option to add more specific details in others (e. g. member states have the option to lower the age of consent from 16 (Article 8(1)). As a result, this has led to a level of inconsistency between the states that creates challenges to conducting cross-border business and innovation. Moreover, to comply with GDPR, companies allocate a significant amount of time and resources towards improving the quality of their technology systems, revising privacy policies, making alterations to their data storage, etc. (Li et al., 2019, p. 2). In other words, GDPR is a complex and principle-based regulation that is difficult to interpret and requires a lot of resources to properly implement, however, it is formed in a technology neutral way in hopes to remain flexible and cover new technologies as they arise.

Recently data became a central part of people's lives, as more and more devices collect data and perform according to it. That is why in 2020 the European Commission issued another Communication, i. e., A European strategy for data, to establish the necessary action to maintain the EU's leadership in the data-driven economy. According to the Communication, one of the main objectives is to reap the benefits of better data usage in the EU, including improved productivity and competitiveness in markets. Le-

gal scholars Axel Metzger and Heike Schweitzer correctly distinguished the keywords of a mentioned document, which are "access", "availability", "flow" and "value creation" (Metzger, Schweitzer, 2022, p. 2). That is why the European Commission proposed to further improve the portability right for individuals under Article 20 of the GDPR giving them more control over who can access and use machine-generated data and for that matter propose new regulation, i.e., Data Act. Although the Data Act is just one of the initiatives that the European Commission plans to accomplish, it is a centrepiece to create a more data-dominant, innovative, and competitive society. Therefore, this document and proposed initiatives will be analysed in the following sections of this article.

2.1. Data Act: the possibility of data unlocking

As mentioned in this paper, more and more people tend to wear and use various devices that track their daily steps, sleeping patterns, burned calories, heart rate etc. to improve their quality of life. Those types of devices have apps or websites where individuals can log in and see collected data and their progress. However, all the value from collected data ends there: a person logs into the app (or a website), sees progress and daily achievements and later signs out. The outcome is that the individual has all the gathered data, but it cannot be extracted or shared with third parties which means that it is locked. Therefore, when a person buys a connected product (or service) generating data, it becomes unclear who can do what with the data and if that data belongs to the manufacturer or the user.

The main idea of the Data Act is that the users of IoT devices and other companies should have more access to IoT data because the data is often solely controlled by the makers of these devices (Kerber, 2022, p. 1). Furthermore, Commissioner for Internal Market Thierry Breton stated that it is important to unlock a wealth of data in Europe because it benefits consumers, businesses, public services, and society as a whole (European Commission, 2022). Hence, the EU aims to establish its leadership in the global data market based on the principles of data accessibility, portability, and interoperability (Fenwick, Jurcys, 2023, p. 9).

Recitals 5 and 6 of the Data Act set out the aims of his document, i.e., it shall ensure that users of a product or related service in the EU can access the data generated by the use of that product or related service and that those users can share the data, including by sharing them with third parties of their choice. Furthermore, it shall require the data holder to make data accessible to users and third parties nominated by the users, thereby avoiding situations where the data is "locked-in". As a result, this initiative, according to the European Commission, will make it easier for users to move their data to other companies and encourage competition in the market for data-based services, as well as promote innovation and the creation of new products or services that are not connected to what the user initially bought or signed up for.

Overall, the proposed Data Act promotes data access and unlocking the value of generated data for the benefit of new inventions, a competitive market and a more conscious society. However, it is also important to understand the proposed right of access in the Data Act and consider the problem of data ownership.

2.2. Data Act: the right of access and Article 35

Articles 4 and 5 of the proposed Data Act refer to the right of access and the right to share data with third parties. These are the most important when talking about the Data Act and its purpose which was discussed earlier.

According to Article 4(1), the data holder is responsible for the availability of the user's generated data by the use of a product or a related service undue delay, free of charge, continuously and in real-time. As a result, to gain access a simple electronic request is enough. The product user's right to access includes a right to share the data with third parties (Article 5(1)) which means that upon request by a user or by a party acting on behalf of a user, the data holder is obliged to make available the data generated by the use of a product or related service to a third party. In any case, the involvement of a user is required for the use of data by third parties, and there are several restrictions and requirements outlined in Articles 5 and 6. For example, the third party cannot share the data it obtains with another third party or use the data to create a device that is in direct competition with the product from which the data was accessed (Article 6(2)(e)).

It should be noted that GDPR also enshrines a general access and data portability right (Article 20). However, to exercise this right, there are three requirements, i.e., data processing must be based on consent of the data subject or a contract, the form of processing must be by automated means and the object of the processing must be personal data provided by and concerning the data subject (Article 20(1)). The result is that the exercise of this right is largely theoretical because it does not cover continuous and real-time access to data (which is crucial for products that are always connected to the internet) (European Parliamentary Research Service, 2022, p. 2). That is why the Data Act is set to establish a harmonised legal framework for making data accessible to the users of certain products or services in real-time and continuously.

The proposed Data Act's Article 35 is critical. It clarifies that the sui generis database right (i.e., a property right that is similar to copyright)[8] does not apply to data-

[8] Article 7 of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on legal protection of databases (hereinafter referred to as Directive 96/9/EC) establishes that database makers may forbid the complete or significant portion of their database extracted and (or) reused if it can be demonstrated that a significant amount of money was spent gathering, validating, or presenting the database's contents on a qualitative or quantitative level. In other words, the Directive 96/9/EC grants sui generis right against unauthorised extraction of the contents of a database for a term of fifteen years from the date of creation of the database (Article 10(1)).

bases which contain data obtained from or generated by using a connected device in order to not hinder the right of access and the right to share data with third parties. It can be challenging to tell which databases may be covered by the sui generis right in today's digital world when data is often generated in vast volumes and automatically by sensors, machines and related technologies. There is a chance that data holders (such as original equipment manufacturers) could use their sui generis right to restrict access to the IoT data gathered in a database to any third party in a way that leads to lock-in scenarios (European Parliamentary Research Service, 2022, p. 3). As a result, this would hamper the sharing and use of data which is the opposite of what the EU is trying to achieve.

Many legal scholars express their concern about the understanding of Article 35 and its capabilities. International association COMMUNIA[9] even goes as far as to say that sui generis right should be repealed, since it "imposes additional restrictions to the use of data and information without demonstrating any benefit" (COMMUNIA, 2021, p. 1). Legal scholars Thomas Margon, Thomas Gils and Eyup Kun argue that based on the construction of the provision it is not fully clear who are the recipients of Article 35 (whether it is only beneficial to data users and data holders or also third parties) (Ku Leuven, 2022). While different organisations, for example EuroCommerce, express the need for the European Commission to clarify the definitions and the types of data and devices that fall under the Data Act to give businesses clarity in complying with the new rules (EuroCommerce, 2022, p. 3). Although Article 35 of the proposed Data Act is not the main object of this article, it is important to understand that the European Commission still has a lot to consider to accomplish the vision of easy data access and usage in the EU.

In conclusion, the EU is going in the right direction, i.e., creating a system to avoid data lock-in situations for businesses, as well as individuals to experience the full potential of the data, which is necessary in this technology-full world.

3. Unlocking the value of generated data: analysis of possible situations

As explained by the marketing commentator Michael Palmer, data is extremely valuable, as is oil, however, if unrefined it cannot be used, so data must be broken down and analysed for it to have worth (The Guardian, 2013). In other words, if all gathered data is just stored in closed databases with no access, then it brings no value to the businesses, individuals and even countries. To enable the full potential of data it needs to be

[9] COMMUNIA advocates for policies that expand Public Domain and increase access to and reuse of culture and knowledge. It unites researchers and practitioners based in Europe and the United States who strive to make data access and use more available.

easily reachable for the purpose of analysing it, processing it and creating new products or services based on it. Exactly that is why the European Commission took the initiative to encourage individuals to refine data and use it in beneficial ways.

Although data accessibility is needed in today's data-driven world, it also raises serious concerns because of the potential threats that could occur. That is why the authors of this article analyse three possible scenarios in different sectors where sensored devices and IoT dominate, i.e., healthcare, automotive industry and agriculture. Furthermore, the ethical, legal and technical challenges are discussed when data is shared and accessed freely, according to the proposed Data Act. The table below summarises the analysis of the three practical situations of data unlocking.

Table 1. Data unlocking challenges in practical situations.

	Healthcare	Automotive industry	Agriculture
Practical situation	Employer monitors the mental health of the employees	The insurance company collects data to calculate an adequate price	Devices measure the condition of soil and crops
Ethical challenges	Bias, discrimination, sensitive information	Borderline stalking, discrimination, biases	Unequal access based on investments (high cost), unfair competition
Technical challenges	Data management, connectivity and reliability, maintenance, data minimisation, probability of error	Secure data transmission and storing, proper assessment of collected data (tests, norms, criteria), data minimisation	Data management, security, secure data storing, proper placement of devices
Legal challenges	Personal data protection, multiple agreements with manufacturers, clear employment contract terms, privacy	Clear contract terms, providing information to clients, personal data protection	Multiple agreements with manufacturers, unfair competition

3.1. Data - a panacea for a better workplace

Before the advent of sensors and IoT, patients and doctors only interacted during visits. There was no possible way for doctors and hospitals to monitor patients'

health and offer recommendations regularly. IoT has revolutionised everything and now plays a special role in healthcare because it can provide real-time data and continuously monitor patient health. The IoT has many advantages in this field, such as it can help reduce the number of doctor visits, help diagnose diseases at an early stage, provide proactive treatment etc. (Wipro, n. d.).

One of the places where smart devices could be used to track health data that is not related to doctors and hospitals is the workplace. For instance, an employer could implement for employees to wear wearable healthcare monitoring systems that observe heart rate, neural activity, perspiration and respiration rate. Each of these measures would give insight into the workers' mental health. According to the World Health Organisation, in 2019 it was estimated that 15 per cent of working-age adults suffered from a mental disorder and it is estimated that 12 billion working days are lost every year due to depression and anxiety (World Health Organisation, 2022). Wearing devices that track important data and notify about the possibility of a deterioration in mental health could be just as helpful as other approaches to combating this phenomenon, such as educating workers and managers about mental health literacy and awareness or developing skills to manage stress.

Considering this scenario, the employer would be responsible for all the gathered data. Hence, she (or he) would be the one to receive highly sensitive personal data. That is why in this situation the GDPR would be widely applied (for example, according to Article 9, to process biometric data the data subject (in this case, the employee) should give explicit consent). Furthermore, all this collected data could lead to discrimination and biases in the workplace. That is why the employer needs to follow the rule of data minimisation, i.e., only adequate, relevant and limited to what is necessary in relation to the purpose personal data should be processed (Article 5(1)(c) of the GDPR). For instance, the employer could use a system that only allowed her (or him) to see a green, orange or red light next to an employee's name, indicating whether or not that person was displaying signs of a mental health worsening (for example, a worker's heart rate, sweating and respiration rate were higher than usual for a longer period of time, indicating that she (or he) may have been having an anxiety attack). Additionally, when hiring new workers, the terms of the employment contract must be clear and specify the type of purposes for which data will be gathered.

Moreover, the employer would have to contact multiple manufacturers of the devices to be able to access all data continuously (Article 5(1) of the Data Act). Depending on how many workers there are, the employer would be subjected to enormous quantities of data. In order to ensure proper data assessment and data security, the employer would need to have efficient data management and storage systems. The employer would also need to provide a reliable internet connection and ongoing wearables maintenance for the devices to function properly. Otherwise, the data may not be accurate and, consequently, the purpose of monitoring employees will not be achieved.

Although smart gadgets are advanced, they can mislead and process data incorrectly. Therefore, if an employer makes decisions based on inaccurate data, the worker will be impacted. For instance, she (or he) may be dismissed to fly a plane, attend a crucial meeting or perform other important tasks.

In conclusion, wearables and data could help to establish a more peaceful and mindful workplace environment, even though there are quite a few challenges. Immediately noticed changes in employees' health could prevent more severe diagnoses and ensure uninterrupted work.

3.2. Driving and data gathering: more precise payments for car insurance

Driving is a popular means to get around places. Nowadays vehicles have many sensors that collect various data, such as, they monitor the temperature, track the condition of tires, speed and emission levels, recognise any obstacle on the front or rear of the vehicle for easier parking and they can even detect when a driver may be distracted or intoxicated to avoid collisions (The Verge, 2022). Therefore, all this data could be used, for example, to offer suitable car insurance and determine motor insurance policy premiums. When it comes to the payment sizes for the insurance, companies take into consideration the driver's age, experience, previous accidents and the vehicle itself. If car manufacturers were able to share the data that is gathered while driving a vehicle with insurance companies then the premiums could be based on more variables (for example, considering the mileage, driver's liking to exceed the speed limit and average speed, driving time (i.e., if a person often drives at night), car care etc.) to offer an appropriate price. In other words, the insurance company could interpret the data that a user of a vehicle gathers and calculate variable charges. People would be encouraged to drive safely as a consequence because their premiums would be reduced.

Currently, as mentioned above, the impact of various potential driver behaviour features that can be extracted from the data that a car collects is not taken into account by offering insurance premiums. As a result, all drivers fall under the same criteria for when they want to purchase insurance for their vehicle, i.e., it does not factor in more accurate and personalised information on the actual vehicle usage. Doing that the insurance companies could divide lower-risk drivers and higher-risk drivers, although it could arise discrimination and biases. That is why it would be important to properly evaluate the received data, set specific norms and tests to accurately and without biases choose appropriate insurance charges for every policyholder. Furthermore, secure data transmission is also important not only for gaining the trust of the clients but also for ensuring that data breaches do not occur (i.e., companies should own secure databases).

Another issue that arises when applying an analysed insurance model is the quantity of data and the minimisation of it. The amount of data that the companies would collect would be enormous and, as a result, it could even be considered stalking (for example, the insurance company tracks driving routes to evaluate if a client most of the time drives in a city or countryside to calculate the chances of potential dangers). As a result, concerns about personal data, which is protected by the GDPR, would emerge. Insurance companies would have to develop, for instance, driving scores and "hide" each client under a number combination to minimise personal data that it holds. Although firstly the company would need to collect the personal data lawfully, i.e., follow Article 6 of the GDPR.

Moreover, it is important to consider the contracts between a client, an insurance company and a car manufacturer. Firstly, the car user should empower a third party (i.e., the insurance company) to access and use the relevant data on the driver's behalf (Article 5(1) of the Data Act). Secondly, there needs to be an agreement between the client and the insurance company. The contract should clearly state what kind of data the company will evaluate and how it will be assessed. The outcome is that there is a lot of information and the goal is for policyholders to not get lost, as well as trust the company and entrust their data for personalised car insurance.

To sum up, modern vehicles are equipped with features that enable a wide range of driving-related data to be gathered. Car manufacturers enjoy exclusive control over most in-vehicle data and resources, giving them a position to dominate aftermarket service, not provide access to users (or third parties) and make the competition more difficult. Although sharing data with a third party in an analysed scenario promotes safe driving and brings more caution to proper driving etiquette, insurance companies must accurately inform drivers, ensure data protection and reduce the amount of data it collects to make data beneficial.

3.3. Modern solutions in agriculture to combat climate change and food production

There is no doubt that humankind today experiences global warming, global hunger problems and an outbreak of diseases. With a population of over 8 billion people, the world is under constant damage from human activity. As a result, climate change is currently just one of the challenges facing the planet. Climate change certainly cannot be stopped or slowed down by a single action, however, too many small contributions from different sectors can make a shift for the better (El-Mawla et al., 2019, p. 7). It should be noted that the technology field can also play an important role, especially the IoT. As the founder of Urban Data Collective Alex Gluhak stated, people can become aware of current problems and track them over time by measuring the actual state of the world using sensors (Raconteur, 2020). Furthermore, the ag-

ricultural sector is directly linked to food production. As explained by the Food and Agriculture Organisation, by 2050 there will be a need to produce 60 per cent more food to feed a world population of 9.3 billion (United Nations, 2012). Hence, it is vital to properly utilise the innovations to combat climate change and produce enough food for the people.

Using smart devices is the best way to ensure that there is enough food for everyone at a time when climate change is a major issue. There are many useful gadgets that measure temperature, soil moisture, humidity, and soil pH balance, as well as agricultural equipment that, for example, do pest control, when spotting unwanted living beings. All these devices collect data that, according to the Data Act, should be easily acceptable for the farmers. As mentioned earlier, the Data Act also promotes innovations, so this is the area where developers could create new opportunities for farmers to valuably use all the collected data, i.e., they could receive customised advice on how to act according to the gathered data. Hence, innovations could alert farmers to take action to prevent crop failures.

Even though collected data would be sent to a specific company to store and process it, there could still occur some technical challenges. Firstly, one of the biggest challenges is data management. It might be overwhelming and challenging to make sense of the vast amount of data that sensors collect. That is why the developers would need to properly sort all the data, ensure secure data storing and create a useful tool for farmers to track their crop and soil status at any time. Secondly, typically farms are located in distant areas, so there could be an issue with the Internet connection which could impact the results. Additionally, strategically positioned smart devices with sensors are necessary to collect data as precisely as possible, which may be challenging depending on the location.

Smart gadgets and equipment are expensive, which means that smaller farmers may not invest in it, therefore have access to it. This could provoke existing inequalities in the agricultural sector and limit the benefits of IoT only to large farmers. Aside from that, the competition between farmers would be unfair. One farmer would have all the innovations at his disposal, be able to monitor the growth of crops, check that the soil contains enough minerals etc., to produce a large amount of the best crops and easily sell them. On the other hand, there would be a farmer without advanced technology who would have to take all the necessary actions by hand when he felt it was necessary and in comparison grow not so good quality crops.

Regarding potential legal issues, it is important to note that, according to Article 5(1) of the Data Act, a product developing company on behalf of a user (in this case, a farmer) would have to contact multiple manufacturers (i.e., data holders) to be able to access all possible data continuously and in real-time. Hence, it confirms that there is a tremendous amount of data that developers would need to process in the analysed scenario.

To summarise, the main challenge in gathering, processing and using data in agriculture is to concur technical issues, so farmers could enjoy the full value of collected data. As the Data Act promises, the analysed situation opens an opportunity for developers to invent new technologies and unlock data from manufacturers to assist farmers in growing enough crops in the face of climate change.

Conclusions

1. The use of sensors and IoT is growing rapidly, as well as the volume of data they generate. When discussing data management, storing, assessment etc. law cannot keep up at such a pace and address all potential situations and difficulties that might arise. The Data Act is one of the long-awaited initiatives from the EU that aims to distribute control over data to generate profit from it, as well as deal with other relevant problems.
2. The Data Act expands the right of data portability that is established in the GDPR which is only limited to personal data. It creates an opportunity for data generated by devices and services connected to the IoT to flow freely in order to guarantee more benefits. Despite this, most of the time the product or service user lacks the desire, competence or qualifications to develop services for aftermarkets, where the Data Act aims to encourage new innovations and services that use mentioned data. Therefore, the right to share data with third parties is crucial, as it is significant not only to developers, but also to countries to boost their economies and attract investments.
3. The value cannot be created by the data that is just simply stored in closed databases. Hence, data work, not ownership, makes data beneficial and useful.
4. All analysed practical situations distinguish the need to always consider data security and privacy in order to make sure that the free flow of data and its value unlocking works properly. Furthermore, some additional issues, such as evaluating how much data is needed and thoroughly informing subjects about data assessment and how the process of it works, possible discrimination cases should also be considered. In conclusion, successful data unlocking faces many technical obstacles that must be overcome, but most importantly, resolving these problems would put people at ease and ensure that innovations would be enthusiastically adopted which is the main goal of unlocking the value of data.

List of sources

Legal normative acts

1. Regulation (EU) 2016/679 of the European Union 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, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, p. 1.
2. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on legal protection of databases. OJ L 77, p. 20.

Special literature

3. Albrecht, J. P. (2016). How the GDPR Will Change the World. European Data Protection Law Review, 2(1), p. 287-289, https://doi.org/10.21552/EDPL/2016/3/4
4. El-Mawla, N.A, Badawy, M. and Arafat, H. (2019). IoT for the Failure of Climate-Change Mitigation and Adaptation and IIoT as a Future Solution. World Journal of Environmental Engineering, 6(1), p. 7-16 [online]. Available at: http://pubs.sciepub.com/wjee/6/1/2 [Accessed 12 February 2023].
5. Farhan et al. (2017). A Survey on the Challenges and Opportunities of the Internet of Things (IoT). Eleventh International Conference on Sensing Technology (ICST), p. 1-5 [online]. Available at: https://ieeexplore.ieee.org/document/8304465 [Accessed 20 February 2023].
6. Fenwick M. and Jurcys P. (2023). Building a "Green Data" Future: How a human-Centric Approach to Data and Nudges Helps Fight Climate Change, http://dx.doi.org/10.2139/ssrn.4326718
7. Javaid, M. et al. (2021). Sensors for daily life: A review. Sensors International, 2, p. 1-10, https://doi.org/10.1016/j.sintl.2021.100121
8. Kerber, W. (2022). Governance of IoT Data: Why the EU Data Act Will nor Fulfill Its Objectives. GRUG International, p. 1-16, https://doi.org/10.1093/grurint/ikac107
9. Kumar, S., Tiwari P. and Zymbler M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6, p. 1-21, https://doi.org/10.1186/s40537-019-0268-2
10. Li, H., Yu, L. and He, W. (2019). The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management, 22(1), p. 1-6, https://doi.org/10.1080/1097198X.2019.1569186
11. Metzger A. and Schweitzer, H. (2022). Shaping Markets: A Critical Evaluation of the Draft Data Act, http://dx.doi.org/10.2139/ssrn.4222376
12. Sehrawat, D. and Gill, N. S. (2019). Smart Sensors: Analysis of Different Types of IoT Sensors. 3rd International Conference on Trends in Electronics and Informatics (ICOEI), p. 523-528, https://doi.org/10.1109/ICOEI.2019.8862778
13. Sipsas, K. et al. (2016). Collaborative maintenance in flow-line manufacturing environments: An Industry 4.0 approach. Procedia CIRP, 55, p. 236-241, https://doi.org/10.1016/j.procir.2016.09.013

14. Zarsky, T. Z. (2016). Incompatible: The GDPR in the Age of Big Data. Seton Hall Law Review, 47(1), p. 995-1020 [online]. Available at: https://scholarship.shu.edu/shlr/vol47/iss4/2/ [Accessed 3 February 2023].

Electronic publications

15. Above Avalon. Apple Watch Is Now Worn on 100 Million Wrists. [online] (modified 11 February 2021). Available at: https://www.aboveavalon.com/notes/2021/2/11/apple-watch-is-now-worn-on-100-million-wrists [Accessed 8 February 2023].
16. Ajax.Systems. LeaksProtect. [online] (modified n. d.). Available at: https://ajax.systems/products/leaksprotect/ [Accessed 20 February 2023].
17. BBC. Baxter College installs toilet sensors to stop vaping. [online] (modified 23 January 2023). Available at: https://www.bbc.com/news/uk-england-hereford-worcester-64322698 [Accessed 10 February 2023].
18. Business Insider. Ukraine's deputy prime minister says it is educating its citizens about the dangers of deepfakes as it fights Russian disinformation in 'a war of technologies'. [online] (modified 20 January 2023). Available at: https://www.businessinsider.com/ukraine-is-educating-its-citizens-to-recognize-russian-deepfakes-2023-1?_gl=1*nvshpy*_ga*MTg0MTA0MDQ5My4xNjc2MDE4ODQ2*_ga_E21CV80ZCZ*MTY3NjAyMTI4NC4yLjEuMTY3NjAyMTI5MS4wLjAuMA.. [Accessed 10 February 2023].
19. Business Insider. Web search as you know it is dead: Microsoft's and Google's new AIs are about to transform how you look for information online. [online] (modified 8 February 2023). Available at: https://www.businessinsider.com/google-microsoft-ai-transform-search-web-bing-chatgpt-bard-lamda-2023-2 [Accessed 10 February 2023].
20. Choose Muse. Introducing Muse 2. [online] (modified n. d.). Available at: https://choosemuse.com/muse-2/ [Accessed 20 February 2023].
21. Data Prot. Internet of Things statistics for 2022 - Taking Things Apart. [online] (modified 20 January 2023). Available at: https://dataprot.net/statistics/iot-statistics/#:~:text=In%202021%2C%20there%20were%20more,to%20the%20internet%20per%20minute [Accessed 2 February 2023].
22. European Commision. Data Act: Commission proposes measures for a fair and innovative data economy. [online] (modified 23 February 2022). Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 [Accessed 15 February 2023].
23. Fitt Insider. Withings Launches Diagnostic Toilet Device for Nutrition and Hormone Health. [online] (modified 17 January 2023). Available at: https://insider.fitt.co/withings-launches-diagnostic-toilet-device-for-nutrition-and-hormone-health/ [Accessed 20 February 2023].
24. Ku Leuven. Chapter X of the Data Act and the Sui Generis Database Right. [online] (modified 14 June 2022). Available at: https://www.law.kuleuven.be/citip/blog/chapter-10-of-the-data-act-and-the-sui-generis-database-right/ [Accessed 15 February 2023].
25. Leverege. IoT Explained - How Does an IoT System Actually Work? [online] (modified 29 October 2016). Available at: https://www.leverege.com/blogpost/iot-explained-how-does-an-iot-system-actually-work [Accessed 3 February 2023].

26. LRT. Dirbtinis intelektas įsitvirtina meno pasaulyje: kaip keliais paspaudimais telefone sukurti paveikslą? [online] (modified 9 January 2023). Available at: https://www.lrt.lt/naujienos/mokslas-ir-it/11/1860970/dirbtinis-intelektas-isitvirtina-meno-pasaulyje-kaip-keliais-paspaudimais-telefone-sukurti-paveiksla [Accessed 10 February 2023].
27. LRT. Kinija imasi reguliuoti „deepfake" technologiją. [online] (modified 10 January 2023). Available at: https://www.lrt.lt/naujienos/mokslas-ir-it/11/1863650/kinija-imasi-reguliuoti-deepfake-technologija [Accessed 10 February 2023].
28. LRT. 15 mlrd. prijungtų prietaisų: daiktų internetu naudojamės patys to nežinodami. [online] (modified 19 January 2023). Available at: https://www.lrt.lt/naujienos/mokslas-ir-it/11/1870887/15-mlrd-prijungtu-prietaisu-daiktu-internetu-naudojames-patys-to-nezinodami [Accessed 10 February 2023].
29. Raconteur. Is IoT a silver bullet for climate change? [online] (modified 18 February 2020). Available at: https://www.raconteur.net/technology/internet-of-things/industrial-iot-climate-change/ [Accessed 2 February 2023].
30. TechCrunch. Memfault raises $24M to help companies manage their growing IoT device fleets. [online] (modified 24 January 2023). Available at: https://techcrunch.com/2023/01/24/memfault-raises-24m-to-help-companies-manage-their-iot-devices/ [Accessed 10 February 2023].
31. The Art Newspaper. High-tech security systems installed on Banksy's Ukraine murals. [online] (modified 24 February 2023). Available at: https://www.theartnewspaper.com/2023/02/24/ukraine-security-company-banksy-murals-kyiv [Accessed 24 February 2023].
32. The Guardian. Tech giants may be huge, but nothing matches big data. [online] (modified 23 August 2013). Available at: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data [Accessed 12 February 2023].
33. The Verge. Volvo's EX90 electric SUV will have laser sensors and cameras that can detect drunk driving. [online] (modified 21 September 2022). Available at: https://www.theverge.com/2022/9/21/23363673/volvo-ex90-electric-suv-lidar-sensors-drunk-driving [Accessed 20 February 2023].
34. The Verge. How to use the Apple HomePod's temperature and humidity sensors. [online] (modified 30 January 2023). Available at: https://www.theverge.com/23574268/homepod-temperature-and-humidity-sensor-how-to-use [Accessed 10 February 2023].
35. United Nations. Feeding the World Sustainably. [online] (modified June 2012). Available at: https://www.un.org/en/chronicle/article/feeding-world-sustainably [Accessed 5 February 2023].
36. Wipro. What can IoT do for healthcare? [online] (modified n. d.). Available at: https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/ [Accessed 28 January 2023].
37. Wired. I Think My Face Was Deepfaked Into a Chinese Camping Stove Ad. [online] (modified 11 January 2023). Available at: https://www.wired.com/story/china-deepfake-advertising-policy/ [Accessed 10 February 2023].

38. Wired. All the Data Apple Collects About You–and How to Limit It. [online] (modified 16 January 2023). Available at: https://www.wired.com/story/apple-privacy-data-collection/ [Accessed 10 February 2023].
39. Wired. The Case for Outsourcing Morality to AI. [online] (modified 2 February 2023). Available at: https://www.wired.com/story/philosophy-artificial-intelligence-responsibility-gap/ [Accessed 10 February 2023].
40. World Health Organisation. Mental health at work. [online] (modified 28 September 2022) Available at: https://www.who.int/news-room/fact-sheets/detail/mental-health-at-work [Accessed 28 February 2023].
41. ZDNET. Unlock your trapped data: Driving insights from edge-to-cloud. [online] (modified 31 January 2023). Available at: https://www.zdnet.com/article/unlock-your-trapped-data-driving-insights-from-edge-to-cloud/ [Accessed 10 February 2023].

Other sources

42. COMMUNIA (2021). Subject: Public consultation on the proposed Data Act - Additional remarks [online]. Available at: https://www.communia-association.org/wp-content/uploads/2021/09/Data%20Act%20consultation%20response%20COMMUNIA.pdf [Accessed 14 February 2023].
43. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data (2020). COM(2020) 66 final.
44. Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation (2020). COM(2020) 264 final.
45. EuroCommerce (2022). Proposal for a Data Act: Promote measures for an innovative data economy [online]. Available at: https://www.eurocommerce.eu/app/uploads/2022/08/EuroCommerce-comments-on-the-Data-Act.pdf [Accessed 15 February 2023].
46. European Commission's Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). COM(2022) 68 final.
47. European Parliamentary Research Service (2022). The Data Act [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI(2022)733681_EN.pdf [Accessed 14 February 2023].
48. Reinsel, D., Gantz J. and Rydning J. (2018). The Digitization of the World: From Edge to Core [online]. Available at: . https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [Accessed 13 February 2023].

UNLOCKING THE FULL VALUE OF DATA – MISSION (IM)POSSIBLE?

Summary

The article provides insights into the growing popularity of new technologies and the amount of data that is being generated worldwide. Therefore, legislators are obligated to issue laws that are up to date. Hence, this article analyses the new proposed legislation in the European Union that ensures the possibility for individuals and businesses to gain access and exert control over data and share it with third parties. The authors of this paper conclude that the opportunity of freely sharing generated data is worthwhile, however, the drawbacks, such as concerns about privacy, potential discrimination and biases, as well as lack of infrastructure and personal data protection, should also be considered.

DUOMENŲ VERTĖS „ATRAKINIMAS" – MISIJA (NE)ĮMANOMA?

Santrauka

Straipsnyje pateikiamos įžvalgos apie didėjantį naujų technologijų populiarumą ir jų generuojamą duomenų kiekį. Įstatymų leidėjai privalo atsižvelgti į naujoves bei jų įtaką asmenims ir verslui bei priimti tokius teisės aktus, kurie atsispindėtų šias naujoves. Šiame straipsnyje analizuojamas naujas Europos Sąjungos siūlomas teisės aktas, užtikrinantis galimybę asmenims ir įmonėms gauti prieigą bei kontroliuoti duomenis, taip pat jais dalintis su trečiosiomis šalimis. Darbo autorės daro išvadą, jog galimybė laisvai dalintis duomenimis yra sveikintina, tačiau reikėtų atsižvelgti ir į kylančius iššūkius, tokius kaip privatumo trūkumas, galima diskriminacija ir šališkumas, taip pat tinkamos infrastruktūros nebuvimas bei asmens duomenų apsaugos neužtikrinimas.