Journal of Politics and Ethics in New Technologies and AI

Vol 2, No 1 (2023)

Journal of Politics and Ethics in New Technologies and AI

IoT in Education: Implementation Scenarios through the Lens of Data Privacy Law

Konstantinos Kouroupis, Dimitrios Vagianos

doi: 10.12681/jpentai.34616

Journal of Politics and Ethics in New Technologies and AI
Volume 2, Issue 1 (2023)
e-ISSN: 2944-9243

https://doi.org/10.12681/jpentai.34616

RESEARCH ARTICLE

IoT in Education:
Implementation Scenarios through the Lens of Data Privacy Law

Konstantinos Kouroupis
Assistant Professor of European and Data Rights Law, Department of Law, Frederick University, Cyprus.

Dimitrios Vagianos
Laboratory Teaching staff, Department of International and European Studies, University of Macedonia, Greece.

Abstract
The Internet of Things (IoT) is today one of the most rapidly developing digital technologies and has managed to establish a solid presence in the academic realm. This article highlights the promising implications of IoT in Education including efficient school management, real-time data collection and analysis, resource management and global interconnectedness. Implementation scenarios are many and incorporate billions of devices that collect huge amounts of data that can be exploited for a wide range of educational purposes. In the post Covid19 era, the IoT as the so-called 3rd revolution of Information technology appeared to be able to support distance learning as well as to protect students in terms of virus spreading, guaranteeing a safe learning environment in their coming back to the classrooms. At the same time, all implementations scenarios raise concerns related to data privacy rights and data security. This article highlights the need for a legal context that protects privacy as well as fundamental rights and freedoms. Since the Internet of Things encompasses new technologies, such as Artificial Intelligence and Blockchain, the study of its regulatory framework is of primary interest. In addition, serious legal and ethical concerns arise which demand a relative critical approach. Therefore, it is pursued the proposal of fruitful guidelines which would lead to a powerful, productive and human-centric educational environment.

Keywords: Internet of Things (IoT), School Management, post Covid19 era, Data Privacy, Digital Rights, Privacy, Artificial Intelligence, GDPR, cybersecurity, NIS Directive

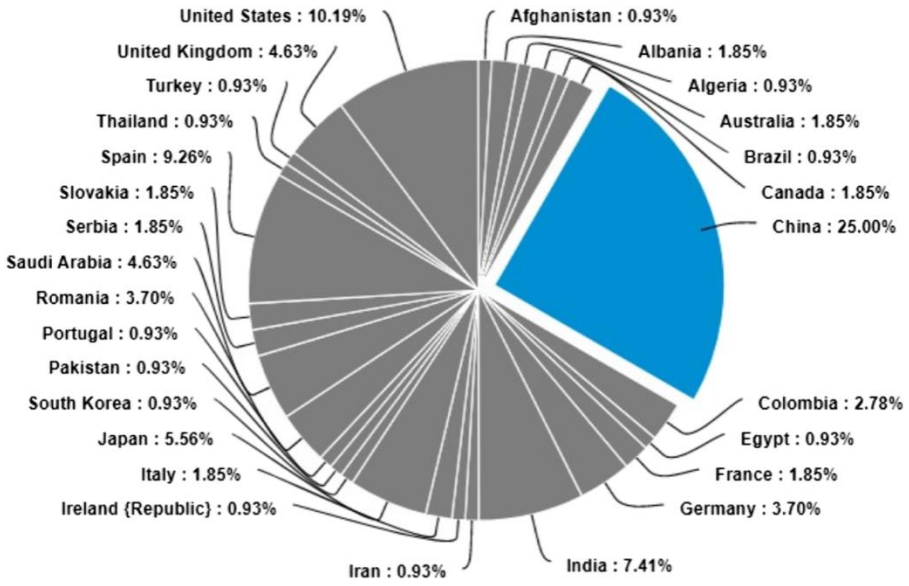
Introduction

The Internet of Things (IoT) is a complex, mainly wireless network of thousands of devices that have been introduced to generate, share, collect, create and receive all kinds of data that can further be analysed in a variety of ways. These devices range from biochips to mobile phones including a vast variety of sensors that feed data to huge monitoring systems for interpretation and decision-making through the aid of Artificial Intelligence (AI) algorithms.

Cisco defines IoT as a network of connected physical objects (Cisco, n.d.). It has also introduced the term “Internet of Everything” for both physical and virtual objects (Barakat, 2016). Cisco states that

"IoE brings together people, process, data, and things to make networked connections more relevant and valuable than ever before—turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunities for businesses, individuals, and countries".

Figure 1: IoT in Education Research, Authorship Geographical Authorship



(Source: Kassab et al., 2020)

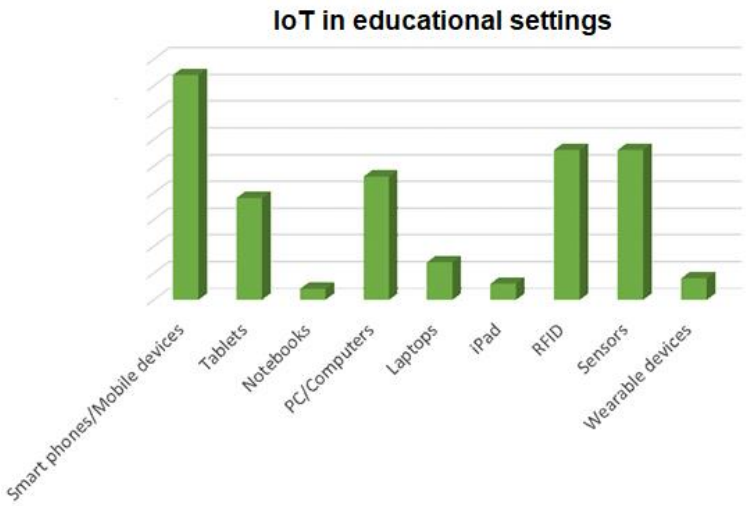
Today, the IoT technologies are motivating nations for digital transformation. This transformation is part of the so called Fourth industrial revolution. The field of Education could not be unaffected by this multifaceted technology with the first steps having been made a few years ago (Kortuem et al., 2012). The Covid19 Pandemic accelerated this trend. The effects and the implications in this field are numerous and so are the issues under investigation that have arisen in this process (Asseo et al., 2016). The global authorship geographical distribution (figure 1) stretches the importance of this scientific field with China, Unites States, India, Spain and United Kingdom being the countries with the highest rates of research over this field of Study (Kassab et al., 2020).

IoT and Learning Process

As stated above, the education sector is considered to be one of the most adaptive and effective fields in terms of deploying IoT in an attempt to make education more collaborative, interactive, and accessible to all (Akbarand and Rashid, 2018). IoT devices (figure 2) have the potential to give students reliable access to a variety of areas ranging from learning materials to communication channels while they provide educators with tools to measure student learning progress in real-time. Recently, the COVID-19 pandemic has sufficiently highlighted the essence of these tools and it was the IoT that,

smoothly or not, enabled the shift in teaching methodology from traditional to digital with several benefits and, in many cases increased efficiency (Bakla, 2019).

Figure 2: Tools used to Interact with IoTsystems in educational settings



(Source: Kassab et al., 2020)

Moreover, smart attendance devices, boards, integrated alarm systems in schools, assessment checking tools, cameras and school locks are examples of IoT devices that contribute to scenarios of central system-based control and automation in the academic environment (Tan et al., 2018).

According to Shan et al. (2016), a learning model based on IoT is composed of four distinct layers (figure 3):

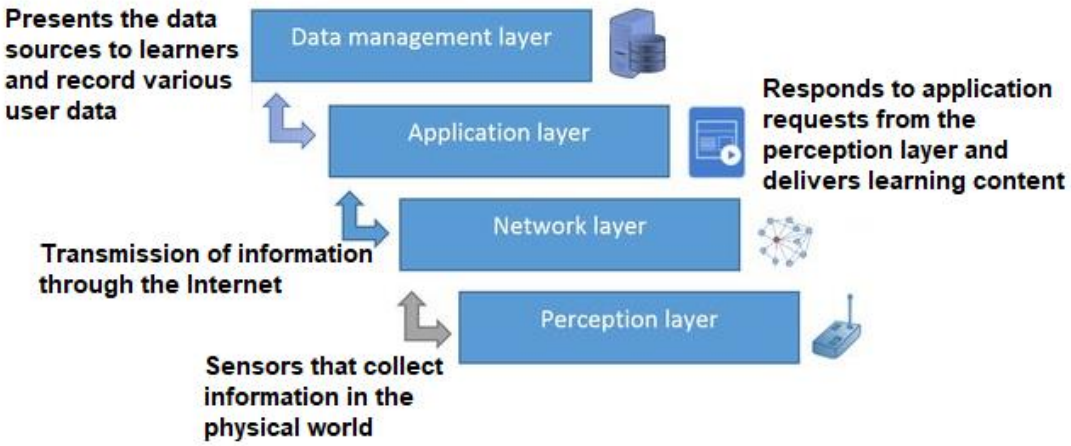
- The perception layer, which is composed of sensors, RFID tags, 2D barcodes, wireless sensor networks and electronic product codes that are used to identify the elements in the physical world, collect information about the environment and automatically control it and connect it to the other network devices and servers,

- The network layer which is responsible for the transmission of information through the Internet,

- The application layer, which responds to application requests from the perception layer and delivers learning content using a blended learning approach,

- The Data management layer, which presents the data sources to learners, record various user data, such as test scores, interests, preferences, achievements and so forth.

Figure 3: The four Layers of IoT supporting Learning



(Source: Shan et al., 2016)

The upsurge of interconnected IoT devices in educational contexts brought about new developments in the way teachers viewed education and how they carried out educational activities. Nowadays, IoT seems to alter education with respect to teaching and learning, school management, experimentation and training, school buildings and so forth (Cheng and Liao, 2012).

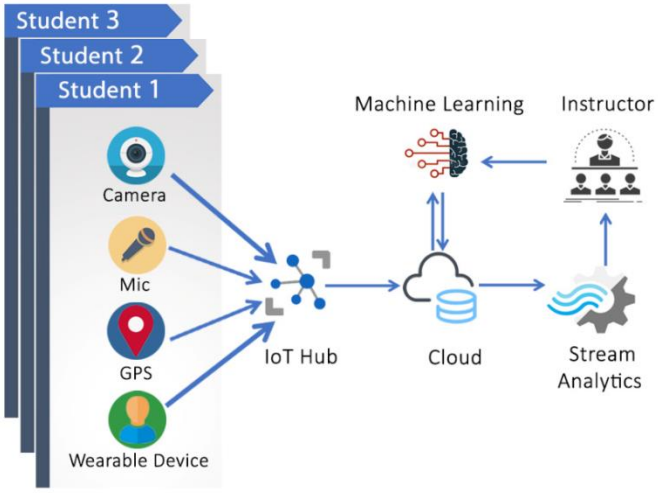
Applications of the IoT in Education

Practical applications of the IoT in educational environments basically fall into several categories including students' attendance (Alotaibi, 2015), engagement or any physical activity as well as school management processes. IoT can also be utilized to increase the effectiveness of learning through learner analytics, better access to information and individualizing learning through the use of smart devices (Charmonman et al, 2015). The smart devices in this design, which have a variety of capabilities for observation, monitoring, communication, and decision making, have the potential to revolutionize the training and evaluation model completely.

These IoT devices can be cameras, microphones, and wearables (Attallahand and Ilagure, 2018) that collect data from students in real time, which is then stored and analyzed (Gul et al., 2017). Students' pulse rates, brain waves, and skin resistance are measured in real time. Wireless technology such as Bluetooth, ZigBee, and other similar protocols is used for the transmission of data from sensors to receiving devices. The IoT hub (figure 4) links student gadgets to cloud storage (Nie, 2013), which allows for the storing and processing of data on a larger scale. The collected data are processed in real time in the cloud using machine learning (ML) algorithms, allowing faster decision making. The

teacher can obtain the outcomes on their unique profile and adjusts their educational approach during teaching or exams.

Figure 4: IoT-based model for e-learnin5



(Source: Rahmani et al., 2021)

It has been found that e-learning has a favorable and statistically significant impact on students' flexibility, learning experience, educational productivity, and overall quality of education. The IoT technology can contribute in several areas in the educational process with some of them being listed below (Gul et al., 2017).

Distance Learning

This includes the web-based systems that enable synchronous or asynchronous delivery of classes to users from anywhere in the world that possess the necessary equipment, Internet connection and personal credentials. This can help everyone who cannot be a part of a legit educational institution but still want to pursue its educational course (Meacham et al., 2018). Live classes, pre-recorded classes, online timer-based assessment questions, tracking of time spent on the portal can all help in creating a comprehensive approach for distance learners. During the COVID19 pandemic, this has beenthe standard procedure for millions of educational institutions, making material provision and students assessment online without the need for live meetings.

Enhanced Interaction and Productivity

Smartphone-based virtual application-based classes have the potential to make the students more interactive (Brown, 2017). They are also able to think beyond the horizons of the classrooms and communicate and voice their learning and doubts. This interaction-based learning can in turn students keener about participation and involvement in the assessments, activities, and even self-learning via

scanning codes in books (Thorne, 2016) and therefore accessing relevant digital content. They can also revise the taught topic again at their own convenience from possible teacher's web portal enhancing learning outcomes and feelings of productivity.

Automated Attendance Recording

Biometric attendance or barcode-based with the identity card number of students can be used for automatically recording the attendance as they enter the classroom (Sura and Nihad, 2021). In this way, there is barely any chance of discrepancy and storage. This can enable teachers to devote more time to their primary concern which is teaching. Some systems can go even further by sending a direct message to the pupil's parents referring their making them aware of the situation (Coffman and Klinger, 2015). The same feature can be used in taking the attendance and lecture count of the teachers themselves, along with their entry and leaving times using their id and biometrics so that there is a clear track record of everything (Wang, 2015).

Close Monitoring

These applications monitor the activities and time spent by students on a particular topic, no matter if we refer with remote or live students' attendance. The appropriate sensors can collect data and automatically suggest academic topics of interest to the students for further learning processes (Cajide, 2015). Also, there can be easily made out as to who has been a part of which assessment and even scoring and progress can be tracked. This technology can be also used to prevent misuse or inappropriate web content consumption by students' smartphones connected to school Wi-Fi. Devices can also be modified or designed in a way that only support certain kinds of applications and systems only with parental controls and teachers monitoring features.

Evolving Methodologies

IoT in education primarily corresponds to the incorporation of digital and internet-based smart devices for the students and teachers in the educational institutes. Therefore, e-books can be downloaded that are available with zooming and saving features, smart boards can be used instead of blackboards which can operate as whiteboards to write with a marker and also can display topic related images and graphics to the students. Such devices are connected to a central server that can control and monitor the syllabus wise and topic-wise categorization for the students. Voice command systems for teachers, speech to text-based note-taking systems for the students (de la Guía et al., 2016), smart security cameras, GPS tracker equipped school buses, disaster alarms and tablets, and smartphones with educational applications are changing how the traditional schools and educational systems have always

operated. In such cases it is known that transition of ways of teaching and methodologies cannot be implemented immediately but is necessarily done slowly and gradually.

AR Equipped Systems

Augmented Reality can be envisaged as an enhanced version of the real and is implemented with with computerized tools support. IoT-based devices and systems can be made even more efficient with AR the use, with students having to scan a QR code related to the topic they are studying. AR with its graphics and sounds can provide enhanced details and 3D visions of the topic being taught. Such study materials can also be be slowly and gradually updated in the school systems or portals by the management authorities, enabling the students to find and see animated depictions of the topics wherever they deem fit.

Special Education

Some years ago, this was almost impossible and comparatively tough for the specially-abled students to get a normal and detailed education. By introducing IoT tools and smart devices, the educational curriculum is being specially modified and classroom environments are being made sound and light-sensitive to cater to the special needs of the students with sensory disabilities (Kurzweil and Baker, 2017). They can seek help from a system of sensor-connected gloves and a tablet to generate verbal speech, translated from sign language which the teachers can use while teaching the concepts extended to what's mentioned in the books.

Safety in Premises

Most schools do not have an infrastructure that detects red flags for theft, abuse, sexual assault, and other crimes that can occur within the institution, nor do they have a proper contingency plan in the case of a disaster or emergency. IoT can help in solving such issues at a vast level, in the case of any intolerable activity that gets monitored on camera; it can be immediately taken care of due to a network system that enables the camera recording to be displayed at various screens in the premises. In the case of any fire or short circuit, IoT-based sensors can activate alarms with the exact area of the problem so that there is less hassle and danger in resolving the issue. Additionally, if anyone tries to break in the school smart door lock, alerts can be turned on via sensors and help requests can be sent automatically ensuring safety in a great manner.

IoT Applications in the Education Service

EdModo is an asynchronous e-learning platform that helps teachers, students, and parents share advice, learning materials, keep track of students' progress, and improve the efficiency of education inside

and beyond the classroom. The tool has been running for twelve years now and is one of the poster cases of IoT in education.

C-Pen is a portable scanner tool that helps students share anything they write online or save it as a smartphone picture. The device is portable and easy to use. By bringing a *C-Pen* to classes, students can ensure that no lesson or lecture notes will be lost. The device can highlight the definition of a chosen word, help create memos and can translate it to over forty languages, and pronounce it correctly. The tool facilitates the education process for people with learning difficulties as well.

Locorobo, on the other hand is an IoT educational that helps programming students learn how to design Python, Java, JS, or C apps much faster. Using a connected tool that learns from its interactions with students to optimize the curriculum, people of all ages (K-12 and college students) can learn the basics of robotics, start coding for drones and design functional wearable applications. There is a connected coding platform and a lesson library that helps STEM teachers access and share worksheets or lecture notes, as well as monitor the learning progress of each student.

Magicard is a smart card implemented in the UK that helps monitor attendance, provide access to medical and transportation facilities and allow users to pay for goods in the cafeteria without having to carry cash around (Abuarqoub et al., 2017). Each tag is fully traceable and can help determine the student's location.

There are also IoT applications that have been designed to ensuring safe and comfortable student transportation. *Kajeet* is such a system that helps raise the bar for school bus system efficiency. The platform allows drivers to monitor the behavior of passengers onboard; Wi-Fi connectivity allows students to turn on homework or access learning materials on their way to school. *Kajeet* also allows parents to monitor their child's location in real-time and be confident that they made it to school safely.

Referring to managements' applications, the University of New South Wales has implemented its own efficient resource management. The institution leveraged the power of IoT for education to track and optimize energy consumption. The program collects real-time power data for HVAC systems and controls lighting, heating, and cooling remotely to avoid energy waste and reduce university operating costs. Based on the insights provided by the platform, facility managers can predict energy consumption expenses with astonishing accuracy and allocate budgets more intelligently.

Carnegie Mellon University, on the other hand is using IoT to improve student life by optimizing transportation, schedules' planning, and enjoying the time inside and outside the lecture hall (Cata, 2015). Thanks to connected systems, students can find out if there's a bus stop near their location, if

the laundromat is open, or if there's a study room available. All the data is collected in real-time and shown on interactive web portals for students.

VT Alerts, a platform designed and implemented at colleges in Virginia, helps identify potential security-threatening situations, sends immediate alerts to all students in case of an on-campus emergency, and optimizes the lighting around the campus so that the residents don't have to walk through poorly-lit streets after classes. *VT Alerts* is exploited only with a a smartphone or a smartwatch.

Finally, the "*How Do I"* app by *Digiteum* helps include people with learning difficulties in education or employee onboarding. The tool uses NFC technology to help those diagnosed with autism and other learning difficulties get practical guides on how to use daily objects and handle mundane tasks, such as cooking, cash withdrawal, moving between locations, etc. A user-friendly interface and gamification integration make the tool engaging and classroom-friendly.

IoT and the Post Covid19 Era

The Covid19has been an intensely rising virus that intentioned countries to utilize technologies to identify Covid19 disease and battle against it (Peeri et al., 2020). Numerous countries have been utilizing a range of gadgets to contest the pandemic, looking for data about growth, perceiving as well as the emancipating the personal data of the inhabitants. Legislative institutes all around the world made an effort to build a monitoring system that notified about declared cases throughout the world (Kumar et all, 2020) and this was the case for educational institutions as well. Three kinds of applications played a distinctive role in schools in this process: thermal detection cameras, Social Distancing measurements and Air Quality measurements (Ashraf et al., 2020).

Thermal detection cameras used AI algorithm and thermal technologies to detect elevated body temperatures to identify people in a crowd that can signal illness.

The end-to-end social distancing and contact tracing solution had usually three components: a tracking device that could be worn in a lanyard or around the wrist; a gateway; and cloud-based management software. When students or faculty came closer than six feet apart, special devices made an audible sound to alert the individuals that they were too close together and needed to move further apart.

Sensors had also been used to measure and transmit and store data about humidity, temperature, indoor air quality and the level of carbon dioxide or other pollutants.

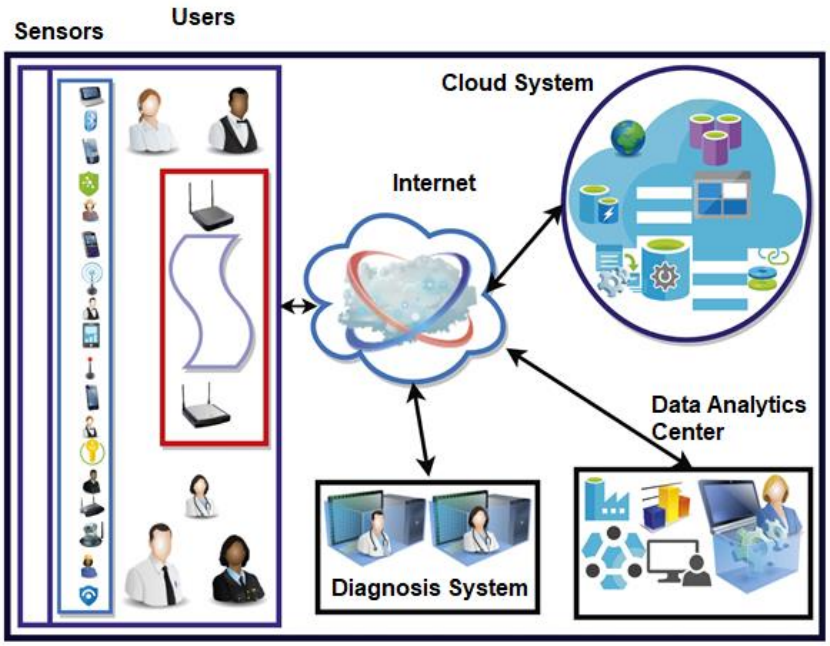
Eventually, frameworks compute the presence of Covid19 virus by mining the health parameters collected in real time from sensors and other IoT devices like biometric-based access controllers,

thermal detection or verification of mask protection cameras, air quality sensors, social distancing supervision, networked hand sanitizers and many other available applications (Mir et al., 2022).

These Frameworks mainly had four main components: a user system or data collection center, a data analytic center, a diagnostic system and a cloud system (figure 5).

Examples of the systems described above were the IoT *Integrator&Intel* IoT with *TempWatchbeing* the system for thermal fever detection, *ContactWatch* being the system for social distancing and *NoviTizer*, a system for hand sanitizing with digital display (IoT Integrator, 2022).

Figure 5: IoT in the post Covid19 era



(Source: Mir et al, 2022)

IoT Benefits and Challenges in Education

Introducing a revolutionary and multifaceted technology like the IoT in education has a lot of benefits (Gupta, 2017). First it raises expectations for improving student outcomes. For example, studies have shown that the fluorescent lighting typically found in schools can have a negative impact on student performance. Installing programmable IoT-connected LED lighting is just one way to improve the student experience in an educational setting. Moreover, real-time data collection by countless IoT devices allows processing terabytes of data simultaneously, opening a lot of applications for schools and colleges — safety tracking, student progress monitoring, not to mention the professional training of teaching specialists, and many more. Ministries and principals can use real-time data to improve the efficiency of testing and grading or when looking for new ways to improve classroom engagement

(Meola, 2016). If we consider the global interconnectedness perspective, the IoT can help education professionals to create uniform teaching standards and ensure equally efficient school and college training worldwide. The IoT can support global peer-to-peer professional training tools, where educators all over the world can exchange tips and best practices (Peters, 2016). Students, on the other hand, will be able to share learning materials internationally, improving the accessibility of education all over the world (Marquez et al., 2016).

Moving to the management level, the IoT can enhance school management efficiency (Qi, 2020). Managing education institutions requires filling in a lot of paperwork, keeping track of supply management, and distributing funds properly. IoT solutions lay the groundwork for faster, risk-free, and interconnected decision-making framework where all the stakeholders (teachers, students, parents, public officials) are engaged in improving the state of the facility (Lu et al., 2017). Moreover, Energy Efficiency and Cost Savings can also be achieved. IoT connected lighting and other devices can be programmed and automated. For example, lights can be set to a schedule, or they can be connected to occupancy sensors and programmed to shut off when a classroom is empty. IoT connectivity improves building efficiency and reduces energy waste, resulting in cost savings (Rosales, 2017).

Additionally, IoT can make schools safer. IoT networks allow for customizable security plans that utilize connected devices such as colored lights, digital signage, door locks and sensors. Some schools use an IoT network to create different programs for severe weather threats, intruders and other security risks. IoT technology also enables solutions such as interconnected emergency alert buttons in classrooms. IoT security applications empower teachers to take action and keep their students safe.

However, there are also challenges involved. First of all, such a technology has a very high implementation cost. Implementing IoT solutions for education requires significant hardware and software power (Digiteum, 2020). To deploy a custom platform, or a connected device, public offices or school principals would have to hire a robust tech team skilled in software development, data science, and other fields. Hardware license fees and maintenance costs are other factors that increase the cost of an IoT product. Unfortunately, not all publicly funded schools can afford such expensive innovations and design custom IoT solutions.

Regarding the in-class ethics, an IoT-based tool needs to provide mechanisms that help prevent cheating, plagiarism, or other forms of academic dishonesty. Before implementing global IoT-based data sharing systems, the worldwide tech community needs to design a framework for fighting fraud and ensuring all shared data is tamper-proof (Shah and Yaqoob 2016).

But the most important challenge that the IoT in education introduces is the security and privacy concerns that this technology raises (O' Hearon, 2021). Collecting and processing various forms of digital data puts educational institutions on the map for hacking threats. Before deploying an IoT solution, project stakeholders need to build a contingency plan for data breaches, security attacks, and other threats (Cam-Winget et al., 2016). Increasing awareness regarding the importance of data security among students is an essential part of the innovation implementation process. Moreover, the collection of such amounts of personal data including biometric or behavioral data without their consent is a serious issue and therefore a pressing concern. A major question is if the GDPR that went into effect in May 2018 applies to these personal or non-personal data involved in the educational IoT processes where both developers and consumers of IoT devices are held responsible for their use of personal data. The passive nature of IoT devices makes it difficult for individuals to be informed that their personal information is being collected. In USA, the IoT Cybersecurity Improvement Act of 2020 requires government agencies to ensure the security of their IoT devices. Several states, including California and Oregon, have already passed IoT cybersecurity laws. Currently, security is not even an option for users of IoT devices where weak software systems are in many cases the rule while malware attack vulnerabilities are very frequent (De Donno et al., 2018).

The legal context should take into account questions like whether users should know where their data is sent or stored, how they will be used, how long they will be kept, how secure these data are during transfer or storage and how they will be notified if there will be a data breach.

While excellent technologies will emerge, such Blockchain technologythat enhance the level of Data Security acquired by IoT in education, the need for regulating this broad and sensitive field is and will continue to be indispensable (Campanile et al., 2020).

Regulating IoT: A Critical Approach

It has been thoroughly demonstrated through the first section of the paper that Internet of Things and its components, such as Artificial Intelligence, Cloud Computing and Blockchain technology, are omnipresent and have a strong interaction with the area of education. Furthermore, it has been clearly exposed the variety of services provided by new technologies, especially during the era of the pandemic due to COVID-19. Therefore, their use is considered inevitable and appears a natural consequence of the technological evolution as well as of the scientific progress. Besides that, the EU Digital Agenda puts the Internet of Things at the centre of the digitalization of the world economy, along with Artificial Intelligence and Big Data (European Commission, The next generation of Internet of Things).

However, serious concerns arise regarding the protection of privacy since the Internet of Things poses new challenges on this ground. Indeed, personal and sensitive data may be processed by the learning machine tools. Hence, in case an organization uses this technology it should accurately record, during the design phase, the systems used at the perception level and the categories of personal data collected directly and indirectly (Vousinas, Simitsi, Livieri, Gkouva, Efthymiou, 2022; Kanellos, 2020).

During the second section of the paper there will be attempted a critical approach of the legal governance of the Internet of Things in order to investigate the lawfulness of the use of such methods. Specific questions will be addressed focusing on the extent of lawfulness, accuracy and reliability of the results derived from such technologies.

Regulating the digital world seems to be a very hard process since technology always precedes law. Especially in the area of education this initiative hides several risks for our privacy. At first, it should be clarified that the legal governance of the IoT industry encompasses two distinct aspects: IoT cybersecurity and IoT privacy. Both of them are regulated by specific legal texts at european level.

Strengthening security research and innovation

Cybersecurity is, perhaps, tied the most and relies heavily on the advancement of science. EU research, innovation and technological development offers the opportunity to take the security dimension into account as these technologies and their application are developed. Indicatively, there can be mentioned the Commission's proposals for Horizon Europe, the Internal Security Fund, the Integrated Border Management Fund, the EU Invest Programme, the European Regional Development Fund and the Digital Europe Programme which will all support the development and deployment of innovative security technologies and solutions along the security value chain.

The ability to overcome security challenges and crises is heavily dependent on the EU's ability to generate innovation, attract talent and use it to create new tools to help law enforcement and other security actors.

While ongoing efforts to empower researchers across Europe, through various programs, are underway, the EU is, currently, a net importer of cybersecurity products and services.

Skills and awareness raising

Even basic knowledge of security threats and how to combat them can have a real impact on society's resilience. Consciousness of the risks of cybercrime and the need to protect oneself from it can work together with protection from service providers to counter cyber-attacks. Challenges to IT infrastructure and e-systems have, subsequently, revealed the need to improve our human capacity for

cybersecurity preparedness and response. The pandemic has also highlighted the importance of digitalisation across all areas of the EU economy and society. It is for this reason, as part of the strategy, the Commission has set out improve upon the security matters through the Digital Education Action Plan. Updating the aforementioned document will present a vision for improving digital literacy, skills and capacity at all levels of education and training and for all levels of digital skills (from low to advanced). Based on lessons learnt from the COVID-19 crisis in areas such as online learning (Diareme et al., 2022), the Action Plan aims to support the development of robust digital competences and organisational capabilities in education and training systems (including for distance-learning) while fully harnessing the potential of emerging technologies, data, content, tools and platforms to make education and training fit for the digital age (European Commission, 2020a).

The reinvigoration of European Research Area and European Education Area, alongside the Digital Europe Programme, will contribute to the unfolding of this theme.

Key actions under the strong European security ecosystem pillar are resumed to:

- Strengthening of Europol mandate
- Exploring an EU 'Police Cooperation Code' and police coordination in times of crisis
- Strengthening Eurojust to link judicial and law enforcement authorities
- Revision of the Advance Passenger Information Directive
- Communication on the external dimension of Passenger Name Records
- Strengthening cooperation between the EU and Interpol
- A framework to negotiate with key third countries on sharing of information
- Better security standards for travel documents
- Exploring a European Innovation hub for internal security

An overview of the EU cybersecurity strategy

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy (European Commission, 2020b). The strategy represents an integral part of European's security, being a continuation of the EU Security Union Strategy.

The aims to safeguard a global and open Internet, while at the same time offering safeguards, not only to ensure security but also to protect European values and the fundamental rights of everyone.

Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments –regulatory, investment and policy instruments – to address three areas of EU action – *(1) resilience, technological sovereignty and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace.*

Resilient infrastructure and critical services

As mentioned in the overarching EU Security Strategy, at the core the cybersecurity paradigm lies the Network and Information Systems Directive (NIS) (European Union, 2016b). In order to ensure a consistent approach as announced under the Security Union Strategy 2020-2025, the reformed Directive is proposed together with a review of the legislation on the resilience of critical infrastructure. Energy technologies embedding digital components and the security of the associated supply chains are important for the continuity of essential services and for the strategic control of critical energy infrastructure. The Commission will therefore propose measures, including a 'network code' setting rules for cybersecurity in cross-border electricity flows for adoption by the end of 2022. The review is necessary to reduce inconsistencies across the internal market by aligning scope, security and incident reporting requirements, national supervision and enforcement and the capabilities of competent authorities. The draft proposal of NIS 2 will be presented through a separate part in this section.

Building a European Cyber Shield

With the spread of connectivity and the growing sophistication of cyberattacks, Information Sharing and Analysis Centres, or ISACs, perform a valuable function, including at the sectoral level, in allowing information exchange between multiple stakeholders on cyber threats. In addition to this, networks and computer systems require constant monitoring and analysis to detect intrusions and anomalies in real time. Many private companies, public organisations and national authorities have therefore set up Computer Security Incident Response Teams (CSIRTs) and Security Operations Centers, or 'SOCs'.

The Commission proposes to build a network of Security Operations Centres across the EU, and to support the improvement of existing centers and the establishment of new ones. It will also support the training and skill development of staff operating these centres.

Through sustained collaboration and cooperation, this network will provide timely warnings on cybersecurity incidents to authorities and all interested stakeholders, including the Joint Cyber Unit. It

will serve as a real cybersecurity shield for the EU, providing a solid mesh of watchtowers, able to detect potential threats before they can cause large-scale damage.

An ultra-secure communication infrastructure

The European Union Governmental Satellite Communications, a component of the Space Programme, will provide secure and cost-efficient space-based communication capabilities to ensure the security- and safety- critical missions and operations managed by the EU and its member states, including national security actors and EU institutions bodies and agencies.

In this perspective, and going further, the Commission will explore the possible deployment of a multi-orbital secure connectivity system. Building on GOVSATCOM and QCI, it would integrate cutting edge technologies (Quantum, 5G, AI, edge computing) adhering to the most restrictive cybersecurity framework in order to support secure-by-design services such as reliable, secure and cost-effective connectivity and encrypted communication for critical governmental activities.

Securing the next generation of broadband mobile networks

EU citizens and companies using advanced and innovative applications enabled by 5G and future generations of networks should benefit from the highest security standard. Member states, together with the Commission and with the support of ENISA, have established with the EU 5G Toolbox (European Commission, 2020c) of January 2020 a comprehensive and objective risk-based approach to 5G cybersecurity that is based on an assessment of possible mitigation plans and identification of the most effective measures. Moreover, the EU is consolidating its capabilities in 5G and beyond to avoid dependencies and to foster a sustainable and diverse supply chain.

Looking forward, the EU should ensure that the identified risks have been mitigated adequately and in a coordinated way, in particular as regards the objective of minimising the exposure to high-risk suppliers and of avoiding dependency on these suppliers at national and Union level, and that any new significant development, or risk, is taken into account.

An Internet of Secure Things

Every connected thing contains vulnerabilities that can be exploited with potentially widespread ramifications. As the Internet of Things proliferates, enforceable rules require strengthening, both to ensure overall resilience and boost to cybersecurity.

The Commission will consider a comprehensive approach, including possible new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market (Council of the European Union, 2020). Such rules could include a new duty of care for

connected device manufacturers to address software vulnerabilities including the continuation of software and security updates as well as ensuring, at the end of life, deletion of personal and other sensitive data.

Greater global Internet security

A set of core protocols and supporting infrastructure ensures the functionality and integrity of the Internet worldwide (European Union, 2019). This set includes the DNS and its hierarchical and delegated system of zones, starting, at the top of the hierarchy, with the root zone and the thirteen DNS root servers on which the World Wide Web depends. The Commission intends to develop a contingency plan, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system.

With a view to reducing security issues related to market concentration, the Commission will encourage relevant stakeholders including EU companies, Internet Service Providers and browser vendors to adopt a DNS resolution diversification strategy.

The Commission will also, in liaison with member states and industry, accelerate the uptake of key internet standards and will consider the need for a mechanism for more systematic monitoring and gathering of aggregated data on Internet traffic and for advising on potential disruptions.

A reinforced presence on the technology supply chain

With its planned financial support for cyber-secure digital transformation over the 2021-2027 Multiannual Financial Framework, the EU has the unique opportunity to pool its assets to propel its Industry Strategy (European Commission, 2020d) and leadership in digital technologies and cybersecurity across the digital supply chain (including data and cloud, next generation processor technologies, ultra-secure connectivity and 6G networks), in line with its values and priorities.

Special focus will be put also on the Technical Support Instrument (European Commission, 2020e) and best use of the latest cybersecurity tools by SMEs - especially those not falling under the scope of the revised NIS Directive - including through dedicated activities under the Digital Innovation Hubs in the Digital Europe Programme.

A Cyber-skilled EU workforce

Similar to the embedded theme in the EU Security Strategy, there is an effort to upskill the workforce, to develop, attract and retain the best cybersecurity talent and to invest in world class research and innovation, form an important component of protecting against cyber threats generally. This field offers great potential. Hence specific attention must be paid to developing, attracting, and retaining

more diverse talent. The Revised Digital Education Action Plan will raise cybersecurity awareness among individuals, especially children and young people, and organisations, especially SMEs (European Commission, 2020f).

Strategic initiatives:

1. Adoption of revised NIS Directive;
2. Regulatory measures for an Internet of Secure Things
3. Through the CCCN investment in cybersecurity (notably through the Digital Europe Programme, Horizon Europe and recovery facility) to reach up to €4.5 billion in public and private investments over 2021-2027;
4. An EU network of AI-enabled Security Operation Centres and an ultra-secure communication infrastructure harnessing quantum technologies;
5. Widespread adoption of cybersecurity technologies through dedicated support to SMEs under the Digital Innovation Hubs;
6. Development of an EU DNS resolver service as a safe and open alternative for EU citizens, businesses and public administration to access the Internet; and
7. Completion of the implementation of the 5G Toolbox by the second quarter of 2021.

NIS 2 Directive Proposal

In 2016, the EU placed the first legal building block of cybersecurity by enacting the Directive on security of network and information systems (NIS Directive) (European Union, 2016b). The document enshrines the responsibility that all member states adopt national strategies on the security of network and information systems (article 1), while also defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering the following sectors: energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, as well as digital infrastructure. NIS enabled member states to adopt a culture of security across all vital sectors, cooperate among themselves, by means of information exchange. Furthermore, it required member states to think proactively about cybersecurity and be equipped appropriately for emerging threats.

One of the key features of NIS is that it enforces a viable security requirements and incident notification system, under which (Article 14): (1) *member states shall ensure that operators of*

essential services 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. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed; (2) *ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services*; and (3) *ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide*.

In respect to the overarching goal of European security, NIS achieved the following:

(1) contributed to improving cybersecurity capabilities at national level by requiring member states to adopt national cybersecurity strategies and to appoint cybersecurity authorities;

(2) increased cooperation between member states at Union level by setting up various fora facilitating the exchange of strategic and operational information; and

(3) improved the cyber resilience of public and private entities in seven specific sectors and across three digital services by requiring member states to ensure that operators of essential services and digital service providers put in place cybersecurity requirements and report incidents.

Notwithstanding its notable achievements, NIS has also proven its limitations. The digital transformation of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges which require adapted and innovative responses. The number of cyber -attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources inside and outside the EU.

The ex-post evaluation has highlighted the following drawbacks:

- The scope of NIS is too limited in terms of the sectors covered, mainly due to: (i) increased digitisation in recent years and a higher degree of interconnectedness, (ii) the scope of the NIS Directive no longer reflecting all digitised sectors providing key services to the economy and society as a whole.

- NIS is not sufficiently clear when it comes to the scope for operators of essential services and its provisions do not provide sufficient clarity regarding national competence over digital service providers.

- NIS allowed wide discretion to the member states when laying down security and incident reporting requirements for operators of essential services.
- The supervision and enforcement regime of the NIS Directive is ineffective.
- The financial and human resources set aside by member states for fulfilling their tasks, and consequently the different levels of maturity in dealing with cybersecurity risks, vary greatly.
- Member states do not share information systematically with one another, with negative consequences in particular for the effectiveness of the cybersecurity measures and for the level of joint situational awareness at EU level.

In order to respond to the growing threats due to digitalisation and interconnectedness, the proposed Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or *NIS 2*) (European Commission, 2020g).

Both EU Security and Cybersecurity Strategy identify NIS as cornerstone legislation when tackling threats to infrastructure and critical services and rely heavily on it in building up resilience and cooperation. In line with Article 23 of NIS that requires the European Commission to review the functioning of this Directive periodically, as well as in line with key policy objectives of the aforementioned strategies, a proposal to revise NIS by introducing systemic and structural changes to the document (through a new directive) envisaging a more fundamental shift of approach towards covering a wider segment of the economies across the Union, yet with a more focused supervision targeting big and key players.

The proposal aims to address the deficiencies of the previous NIS Directive, to adapt it to the current needs and make it future-proof. To this end, the proposal expands the scope of the current NIS Directive by adding new sectors based on how crucial they are for the economy and society, and by introducing a clear size cap — meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.

The proposal also eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance, and divided into essential and important categories, which will be subjected to different supervisory regimes.

NIS 2 covers the following entities:

Essential entities: energy (electricity, district heating and cooling, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health; manufacture of pharmaceutical products including vaccines; drinking water; waste water; digital infrastructure (internet exchange points; DNS providers; TLD name registries; cloud computing service providers; data centre service providers; content delivery networks; trust service providers; and public electronic communications networks and electronic communications services); public administration; and space.

Important entities: postal and courier services; waste management; chemicals; food; manufacturing of medical devices, computers and electronics, machinery equipment, motor vehicles; and digital providers (online market places, online search engines, and social networking service platforms).

The proposal strengthens and streamlines security and reporting requirements for companies by imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

Furthermore, the Commission proposes to address security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. At European level, the proposal strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, may carry out coordinated risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. It also enhances the role of the Cooperation Group in shaping strategic policy decisions and increases information sharing and cooperation between member state authorities. It also enhances operational cooperation including on cyber crisis management.

The Commission proposal also establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates EU registry in this area, operated by the EU agency for cybersecurity (ENISA).

Being a central piece in the security paradigm of the EU, NIS 2 wears a heavy burden. It is detrimental to the overall success of (cyber-) security policy mix in several ways. Firstly, critical infrastructure resilience is primordial in ensuring security in member states and at EU level. For this reason, the

achievement of desired legislative and policy outcomes is closely linked with the efficiency and impact that NIS 2 will have, as well as to what extent it will be able to foster cooperation. Secondly, the successful implementation of the directive is dependent on the swiftness of member states in implementing new regulations, one of the lackluster aspects of its predecessor. Lastly, having in mind the framework in which NIS 2 is proposed – as a nimble tool able to adapt to an evolving landscape of threats, it remains to be seen if it will not suffer from legal lag, falling behind on challenges, condition by bureaucracy within EU institutions. A key role in this regard will be played by ENISA, which under NIS 2 has a coordination role (Kouroupis and Serotila, 2022).

It has been clearly demonstrated during the previous analysis that the EU legislative package on cybersecurity intends to build an homogenic environment for all ICT products, services and processes. Indicatively, the Cybersecurity Act strengthens the European Union Agency for Network and Information Security (ENISA) mandate to help Member States address cybersecurity threats. An issuance of an EU-wide cybersecurity framework for ICT products, upon a request from ENISA, is of primary interest since it enables the creation of tailored and risk-based EU certification schemes. Initially, manufacturers and vendors will be able to have their products and services meet the EU cybersecurity pending standards voluntarily. The certification may eventually be compulsory and will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures (European Commission, 2022).

Therefore, all institutions and organizations in the area of education which adopt new technologies and IoT in their processes shall meet the aforementioned standards9of the relative EU legislation. In terms of privacy, the General Data Protection Regulation is considered the most appropriate regulatory framework since it establishes a harmonized status within the European Union (Kotsalis and Menoudakos, 2020).

As far as concerns the use of the IoT in education it should be noticed the following:

- Any educational institution shall adopt a transparent, complete and clear privacy policy. That corresponds to the respect of all fundamental principles relating to processing of personal data (principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality according to article 5 of the GDPR).
- Any use of the IoT or other similar learning machine educational tools shall be lawful only if the data subject has given consent to the processing of his or her personal data for one or more specific purposes (article 6 of the GDPR). It should be equally underlined that the request for consent shall be presented in a manner which is clearly distinguishable from the other matters,

in an intelligible and easily accessible form, using clear and plain language. In addition, the data subject shall have the right to withdraw his or her consent at any time (article 7 of the GDPR). It shall be clarified that during the pandemic providing education via physical presence was impossible in favor of the protection of public health. Tele-education was widely applied. As legal basis could be evoked the case (e) of the article 6 of the GDPR where it is explicitly declared that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; In any other case where the educational organization uses tools of the IoT prior consent shall be the necessary prerequisite.

- In terms of the data controller responsibilities, all provisions regarding impact assessment, data protection by design and by default have to be respected.
- Accordingly, to the GDPR provisions (Kuner et al., 2020), all rights of the data subject must be respected, such as the right to transparent information, of access and to be forgotten (articles 12-23 of the GDPR). Special focus shall be given on article 22 of the GDPR concerning the automated individual decision-making, including profiling. The first paragraph of the article establishes a general prohibition for decision-making based solely on automated processing. According to the special guidelines issues on this subject by the Article 29 Data Protection Working Party, profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards. These processes can be opaque. Individuals might not know that they are being profiled or understand what is involved. In addition, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data. As part of their DPIA, the controller should identify and record the degree of any human involvement in the decision-making process and at what stage this takes place. Consequently, any use of the IoT shall not constitute the only basis or criteria for the evaluation of the student. Besides that, the educational process is an ongoing interactive process which implements the vivid interaction between student and teacher.

Conclusions

In terms of conclusions, it has been clearly pointed out that the massive use of digital technologies and the invasion of internet in all levels of private and public life mark the nature of modern societies. As Stephen Hawking once said, "*We are all now connected by the Internet, like neurons in a giant brain*". Especially in education, the connection of devices and the use of numerous learning machine tools are

numerous providing a huge variety of services. The rise of mobile technology and the IoT allow educational institutions to improve the safety of their campuses, keep track of key resources, and enhance access to information in the learning environment. During the period of the pandemic due to COVID-19 e-learning has become a common practice facilitating the educational process.

However, digital transformation and the upcoming reality bring a large series of risks and challenges for fundamental rights and freedoms due to its components such as the encouragement of the development of trustworthy technology, the need to produce a fair and competitive environment under a human-centric approach. Despite the existence of many legal sources, regulating the Internet of Things constitutes a very difficult task since technology always precedes law. In addition, the adaptation to the current digital age urges for expertise and familiarization with new technologies. Nevertheless, it's time to go in the right direction. The most important pillars of the policy are managing privacy, eliminating discrimination and fostering security and human-centric approach. Especially in the area of education, new technologies, computer machines and algorithms may constitute an important and essential part of the educational process but they should not be considered its central core. Human intervention as well as legal regulation of technology are of primary interest and shall be the decisive criteria for any scientific evolution.

References

Abuarqoub A., Abusaimeh H., Hammoudeh M. and Uliyan M., (2017). A survey on internet of things enabled smart campus applications. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, pp. 1–7.

Akbar M. A. and Rashid M. M. (2018). Technology based learning system in internet of things (iot) education. In *7th International Conference on Computer and Communication Engineering (ICCCE*), pp. 192–197.

Alotaibi, S. J. (2015). Attendance system based on the Internet of Things for supporting blended learning. *In 2015 World Congress on Internet Security (WorldCIS)*, pp. 78–78.

Ashraf M. U., Hannan A., Cheema S. M., Ali Z., Jambi K. M., and Alofi A. (2020). "Detection and tracking contagion using IoT edge technologies: confronting COVID-19 pandemic. In *Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, Istanbul, Turkey.

Asseo, I., Johnson, M., Nilsson, B., Neti, C., and Costello, T. J. (2016). The Internet of things: Riding the wave in higher education. *Educause Review, 51*, 11–33.

Attallah B. and Ilagure Z. (2018). Wearable technology: Facilitating or complexing education. *Int. J.Inf. Educ. Technol.*, *8*(6), 433–436.

Bakla, A. (2019). A Critical Overview of Internet of Things in Education. *Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi, 49*, 302-327.

Barakat S. (2016). Education and the internet of everything. *Int. Bus. Manag.*, *10*(18), 4301–4303.

Brown, J. L. (2017). *How will the internet of things impact education?* EdTech Magazine. Available at: https://edtechmagazine.com/k12/article/2017/03/how-will-internet-things-impact-education

Cajide, J. (2015). *The connected school: How IoT could impact education*. Available at: https://www.huffingtonpost.com/jeanette-cajide/the-connected-school-how-_b_8521612.html

Campanile L., Iacono M., Marulli F. and Mastroianni M., (2020). Privacy Regulations Challenges on Data-centric and IoT Systems: A Case Study for Smart Vehicles. in *IoTBDS*, pp. 507–518.

Cam-Winget N., Sadeghi A.-R and Jin Y. (2016). Can IoT be secured: Emerging challenges in connecting the unconnected. *In 2016 53rd ACM/EDAC/IEEE Design*

Cata, M. (2015). Smart university, a new concept in the Internet of Things. In *2015 14th RoEduNet International Conference - Networking in Education and Research (RoEduNet NER),* pp. 195–197.

Charmonman S., Mongkhonvanit P., Dieu V. N., and Linden N. (2015). Applications of internet of things in e-learning. *Int. J. Comput. Internet Manag.*, *23*(3), 1–4.

Cheng H. and Liao W. (2012). Establishing an lifelong learning environment using IOT and learning analytics. In *Advanced Communication Technology*, pp. 1178–1183.

Cisco. (n.d.). *The Internet of Everything Global Public Sector Economic Analysis*. [ONLINE] Available at: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf. [Accessed 6 December 2022].

Coffman, T. and Klinger, M. B. (2015). *Google Glass: using wearable technologies to enhance teaching and learning*. Paper presented at the Society for Information Technology & Teacher Education International Conference 2015. Las Vegas, NV, United States.

Council of the European Union, (2020). *Council Conclusions call for horizontal measures on the cybersecurity of connected devices 13629/20,* 2 December 2020.

Diareme K.C., Liapakis A.M., Efthymiou I-P., (2022). Big Data, Sentiment Analysis, and Examples during the COVID-19 Pandemic. *HAPSc Policy Briefs Series, 3*(2), 21–30.

De Donno, M., Dragoni, N., Giaretta, A. and Spognardi, A. (2018). DDoS-capable IoT malware: Comparative analysis and Mirai investigation. *Security and Communication Networks*, 2018, 1-30.

de la Guía, E., Camacho, V. L., Orozco-Barbosa, L., Luján, V. M. B., Penichet, V. M. R. and Pérez, M. D. L. (2016). Introducing IoT and wearable technologies into task-based language learning for young children. *TLT, 9*, 366–378.

Digiteum. (2020). *How IoT Is Used in Education: IoT Applications in Education*. [ONLINE] Available at: https://www.digiteum.com/iot-applications-education/. [Accessed 6 December 2022].

European Commission (2020a). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Skills Agenda for sustainable competitiveness, social fairness and resilience. COM (2020) 274 final.

European Commission (2020b). Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. JOIN (2020) 18 final.

European Commission (2020c). Communication on Secure 5G deployment in the EU - Implementing the EU Toolbox, COM (2020) 50.

European Commission (2020d). Communication on a New Industrial Strategy for Europe, COM/2020/102 final.

European Commission (2020e). Proposal for a Regulation of the European Parliament and of the Council establishing a Technical Support Instrument. COM/2020/409 final.

European Commission (2020f). Digital Education Action Plan (2021-2027). [ONLINE] Available at: https://education.ec.europa.eu/focus-topics/digital-education/action-plan. [Accessed 20 March 2023].

European Commission (2020g). Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. COM/2020/823 final.

European Commission (2022). The EU cybersecurity certification framework. [ONLINE] Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. [Accessed 20 March 2023].

European Union, (2016a). 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. Official Journal of the European Union. L 194/1.

European Union, (2016b). 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. Official Journal of the European Union. L 194/1.

European Union, (2019). 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Gul, S., Asif, M., Ahmad, S., Yasir, M., Majid, M., Malik, M., and Arshad, S. (2017). A survey on role of internet of things in education. *International Journal of Computer Science and Network Security*, *17*(5), 159–165.

Gupta, P. (2017). *Internet of things (IoT) and its significance in education*. Available at: http://edtechreview.in/trends-insights/trends/2855-internet-of-things-iot-in-education

IoT Integrator. (2021*). 3 Must-Have Technologies to Help Protect Schools from COVID-19*. [ONLINE] Available at: https://www.theiotintegrator.com/education/3-must-have-technologies-to-help-protect-schools-from-covid-19?itc=refresh. [Accessed 6 December 2022].

Kanellos, L., (2020). *The GDPR Handbook*. Nomiki Bibliothiki.

Kassab, M., DeFranco, J. and Laplante, P. (2020). A Systematic Literature Review on Internet of Things in Education: Benefits and Challenges. *Journal of Computer Assisted Learning*, *36*, 115-127. 10.1111/jcal.12383.

Kortuem, G., Bandara A. K., Smith N., Richards M., and Petre M. (2012). Educating the Internet-of-Things generation. *Computer (Long. Beach. Calif).*, *46*(2), 53–61.

Kotsalis, L., Menoudakos, K., (2020). *General Data Protection Regulation*. 2nd edition, NomikiBibliothiki,

Kouroupis, K and Serotila, I., (2022). *Privacy and security in light of the European Digital Agenda*. Nomiki Bibliothiki, p.18-36.

Kumar, K., Kumar, N., and Shah, R. (2020). Role of IoT to avoid spreading of COVID-19. *International Journal of Intelligent Networks*, *1*, 32–35.

Kuner, C., Bygrave, L. A., Docksey, C. and Dreschler, L. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

Kurzweil, D., & Baker, S. (2017). *The Internet of Things for Educators and Learners*. Available at: https://er.educause.edu:443/articles/2016/8/the-internet-of-things-for-educators-and-learners

Lu, Y., Zhang, S., Zhang, Z., Xiao, W. and Yu, S. (2017). A framework for learning analytics using commodity wearable devices. *Sensors*, *17*(6), 1–25. https://doi.org/10.3390/s17061382

Marquez, J., Villanueva, J., Solarte, Z., and Garcia, A. (2016). IoT in education: Integration of objects with virtual academic communities. In *New Advances in Information Systems and Technologies*, Springer, pp. 201–212.

Meacham, S., Stefanidis, A., Gritt, L., and Phalp, K. T. (2018). *Internet of Things for Education: Facilitating Personalised Education from a University's Perspective*.

Meola, A. (2016). *How IoT in education is changing the way we learn*. Available at: http://www.businessinsider.com/internet-of-things-education-2016-9

Mir, M., Jamwal, S., Mehbodniya, A., Garg, T., Iqbal, U. and Samori, I. (2022). IoT-Enabled Framework for Early Detection and Prediction of COVID-19 Suspects by Leveraging Machine Learning in Cloud. Journal of Healthcare Engineering. 1-16. 10.1155/2022/7713939.

Nie, X. (2013). Constructing Smart Campus Based on the Cloud Computing Platform and the Internet of Things. In *Proc. 2nd Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE 2013)*, pp. 1576–1578.

O'Hearon, K., Mckee, M., Hossain, N. and Canbaz, M. A. (2021). *IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond*. American Society for Engineering Education,

Peeri, N. C., Shrestha, N., Rahman, M. S. (2020). The SARS, MERS and novel coronavirus (COVID-19) epidemics, the newest and biggest global health threats: what lessons have we learned?. *International Journal of Epidemiology*, *49*(3), 717–726.

Peters, J. (2016). *What will be the impact of IoT on education?*. Available at: https://www.geektime.com/2016/03/07/what-will-be-the-impact-of-iot-on-education/

Qi, X. (2020). University Education Management Based on Internet of Things Technology. In *International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy*, 2020, pp. 805–810.

Rahmani, A.M., Ali Naqvi, R., Hussain Malik, M., Malik, T.S., Sadrishojaei, M.,Hosseinzadeh, M. and Al-Musawi, A. (2021). E-Learning Development Based on Internet of Things and Blockchain Technology during COVID-19 Pandemic. *Mathematics*, *9*, 3151. https://doi.org/10.3390/math9243151

Rosales, C. (2017). *The Internet of things and how it will impact education – IE University Driving Innovation*. Available at: http://drivinginnovation.ie.edu/whats-the-internet-of-things-how-it-will-affect-education/

Shah, S. H. and Yaqoob, I. (2016). A survey: Internet ofThings (IoT) technologies, applications, and challenges. In *2016 IEEE Smart Energy Grid Engineering (SEGE)*, 2016, pp. 381–385.

Shan, Y., Wang, J., and Hao, F. (2016). Research on mobile learning model based on Internet of Things. DEStech Transactions on Social Science, Education and Human Science. Available at: http://dpi-proceedings.com/index.php/dtssehs/article/viewFile/5202/4826

Sura, I., Ali, M., and Nihad, M. (2021). Internet of Things for Education Field. *Journal of Physics: Conference Series. 1897*. 012076. 10.1088/1742-6596/1897/1/012076.

Thorne, T. (2016). Augmenting classroom practices with QR codes. *TESOL Journal*, *7*(3), 746-754. https://doi.org/10.1002/tesj.257

Vousinas, G.L., Simitsi, I., Livieri, G., Gkouva, G.-C., Efthymiou, I.-P. (2022). Mapping the road of the ethical dilemmas behind Artificial Intelligence. *Journal of Politics and Ethics in New Technologies and AI, 1*, e31238. https://doi.org/10.12681/jpentai.31238

Wang, J. (2015). The design of teaching management system in universities based on biometrics identification and the internet of things technology. In *International Conference on Computer Science & Education (ICCSE)*, pp. 979–982.