Security and Privacy Concerns in IoT

"مخاوف الأمن والخصوصية في مجال إنترنت الأشياء"

أم.د.نبراس سالم خضير

كلية الكنوز الجامعة – قسم القانون

dr.nibrassalem@gmail.com
nibras.s@knuoozu.edu.iq

تاريخ استلام البحث ٢٠٢٤/٥/١٠ تاريخ قبول النشر ٢٠٢٤/٩/١٩

Abstract

In the last generation, the Internet has profoundly changed our lives and because our society has grown more reliant on information technology, we are now saving and transferring sensitive information online, we are paying greater attention to data protection and security issues. Governing authorities in many countries have enacted laws and regulations intended to address and influence privacy and security practises. This research analyses how businesses across the globe comply with the laws of various countries with their privacy notifications and whether organisations vary in their degree of compliance with their privacy regulations and their reading ability. The objective of this research is also to explore moral and ethical views. Laws and regulations are meant to maintain an order, justice and fairness in the society, while ethical laws are as such to establish standards of ethics and behaviour that enable individuals determine what's unjust and how to react to injustice. Legislations lay down basic norms for decent behaviour, the law and ethics should be followed 'anytime' and 'everywhere' on the internet in order to offer a safe and inclusive environment for everyone, including the marginalised ones. This calls for a new perspective on social and political environment, which calls for new increased legal and ethical privacy protection measures, data security, preservation of ownership, improved confidence, and the creation of appropriate standards of behaviour on the internet and social media space.

Keywords: Data Protection, Privacy, Ethics, Legal Compliance , Cybersecurity.

الملخص:

في الجيل الأخير، غيّر الإنترنت حياتنا بشكل جذري، ومع ازدياد اعتماد مجتمعنا على تكنولوجيا المعلومات، أصبحنا نقوم بتخزين ونقل معلومات حساسة عبر الإنترنت، مما جعلنا نولي اهتمامًا أكبر لمشاكل حماية البيانات والأمن. وقد أصدرت السلطات الحكومية في العديد من البلدان قوانينًا وتنظيمات

تهدف إلى معالجة وتأثير ممارسات الخصوصية والأمان. يحلل هذا البحث كيفية امتثال الشركات في جميع أنحاء العالم لقوانين مختلف الدول فيما يتعلق بإشعارات الخصوصية، وما إذا كانت المنظمات تختلف في درجة امتثالها للوائح الخصوصية وقدرتها على القراءة. كما يهدف هذا البحث إلى استكشاف الآراء الأخلاقية والمعنوية. تهدف القوانين والتنظيمات إلى الحفاظ على النظام والعدالة والإنصاف في المجتمع، بينما تهدف القوانين الأخلاقية إلى وضع معايير للسلوك والأخلاق تمكّن الأفراد من تحديد ما هو غير عادل وكيفية الرد على الظلم. تضع التشريعات معايير أساسية للسلوك اللائق، وينبغي الالتزام بالقانون والأخلاق "في كل وقت" و" في كل مكان" على الإنترنت من أجل توفير بيئة آمنة وشاملة للجميع، بما في ذلك الفئات المهمشة. يتطلب ذلك منظورًا جديدًا للبيئة الاجتماعية والسياسية، مما يستدعي زيادة التدابير القانونية والأخلاقية لحماية الخصوصية، وأمن البيانات، والحفاظ على الملكية، وتعزيز الثقة، وإنشاء معايير سلوكية مناسبة على الإنترنت وفي فضاء وسائل التواصل الاجتماعي.

الكلمات المفتاحية: حماية البيانات، الخصوصية، الأخلاقيات، الامتثال القانوني، الأمن السيبراني.

I-Introduction

The Internet has reached nearly all sectors of manking existence, e.g. commerce, industry, health services, educational services, etc. in our society. The interconnection of various things from electronic devices to sensors to monitor the garden is what is known as the Internet of Things or IoT. IoT may be defined as things/objects that are linked in our surroundings to offer seamless interaction and services. It includes a large number of nodes between objects and people. Kevin Ashton created the phrase Internet of Things in 1999, originally intended to improve radio frequency identification (RFID).[1]

As IoT does not only relate to things but also inter-relations between objects and people, the philosophical, ethical and legal problems of the Internet of Things co-existence with people have to be taken into consideration. The 'informed consent principle' is of greatest significance when contracts are concluded with 'use terms' that most of them usually do not completely comprehend. Very frequently, these words indicate that users have wide rights to acquire, share, and utilise data from businesses. If agreed and signed, probably. It is thus of main significance to look at IoT and to grasp the limits of legal and regulatory protective frameworks and to offer solid suggestions to maximise good and to minimise damage. The variety of IoT applications is steadily growing. Figure 1 shows eight areas of basic uses. Each domain has many separate apps. Other (non-exhaustively) IoT applications are: smart home, smart grid, smart supply networks, retailers, mobile banking, AI-enabled investment and insurance, and smart agriculture.

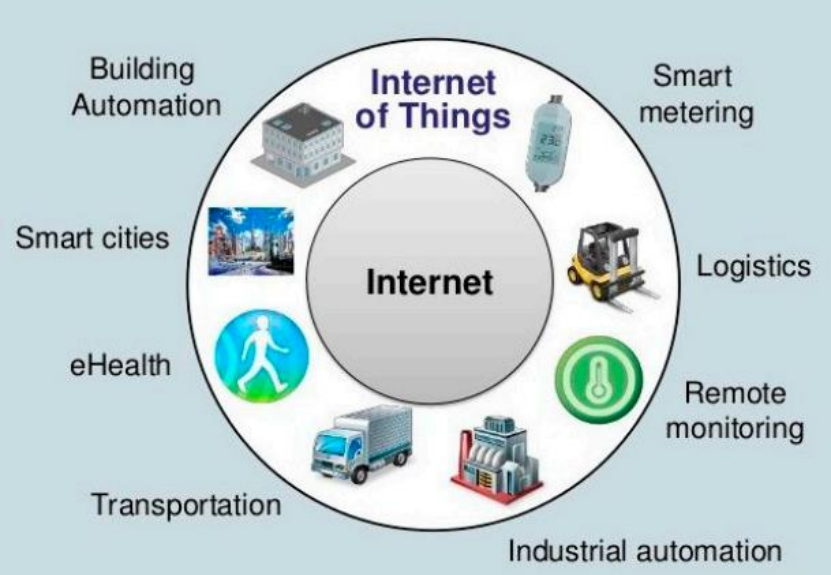

Figure 1 Application domains of the Internet of Things

IoT devices are computers which wirelessly connect to the network and can transmit data. The IoT extends internet access over traditional devices to all kinds of previously dumb or non-internet accessories and to everyday objects (Laptops, desktops, smartphones, and tablets). These technical devices may connect, engage, monitor and control through the Internet. A lot of IoT-accessible information was generated using coded RFID tags and IP protocols linked to the EPC network.[2] Management protocols like Open Mobile Alliance Device Management (OMADM) need to be used by large IoT users to enhance the security and operating efficiency of their operations across the whole life cycle.[3] The following capabilities for device management should be provided:

- Configuration of device
- Troubleshooting of devices
- Diagnosis of faulty devices
- Registration of device
- Monitoring of device
- Authentication and Authorization of device Challenges to the adoption of IoT include:
- Governance structures
- Privacy and security
- Lack of interoperability and sound business structures

There is a clear gap between the requirements of privacy and security and

the ground reality and risk of exposure it comes with the IoT.Data protection is the control of its use and disclosure of personal information by consumers or users; but safety is described as policies, procedures and technology that must allow an organisation to electronically transact its business via networks with acceptable safety guarantees.Secure data and applications have two main purposes. Firstly, unlawful accessibility to IT resources such as customer information is prevented. The second thing is to keep IT services up-to-date. Access restrictions are an apparent instrument to avoid unauthorised access to meet the first objective, but less visible measures, such as unauthorised hardware audits, are also essential.[4]For example, consider an illegally operational wireless point where critical customer information is sent on an unsecured network. Someone may exploit this vulnerability to steal customer information. It emphasises the truth that any attempt to design, implement and maintain rules on access control may be compromised. The administrator's objective is to maintain IT services. This typically includes a multi-faceted approach, including firewalls and intrusion detection systems and anti-virus services, vulnerability screening and system monitoring settings. It is essential to test that the operating systems are up to date and appropriately patched. In order to secure data and to guarantee that the network functions efficiently, both these aims are critical. Even minor nuisances such as spyware implantation can cause major network issues due to a distributed denial of service (DOS).[5]

These internal measures are important but are insufficient to provide comprehensive protection in the constantly growing applications of the internet. Technology has advanced in every other area of contemporary life, and the government now regulates and legislates on how technology is used and protected, via communication and commerce between individuals, institutions, organisations, and businesses. In order to accomplish these goals and correct breaches, system administrators need to be informed of and manage applicable legislations and guidelines on privacy and safety concerns. The rise of IoT has prompted us to review internet security and privacy again. This review is particularly relevant since the application of the web is prevalent today and because some people use the internet also for unlawful purposes.In turn, this calls for ever more complex and restrictive law and regulation aimed at maintaining the obviously beneficial applications of the Internet while maintaining the desire to misuse and to breach private rights.

In order to confuse matters more, privacy programs differ by geographic

location. Privacy protection is predicated on 'freedom' protection in the US.6 In the US, privacy is only recognised if the authorities do not interfere. The legal foundation for anonymity in the U.S. is split and scattered because of the notion of private as liberty. Many fields of law emerge from of the germ of privacy, all with their own ideas as to what must be safeguarded.7 The approach to the question of privacy in the European Union is based on the person's 'dignity.' This regulatory regime acknowledges that the idea of privacy is about protecting personal dignity rather than civil liberties.8 Dignity is considered as a social concept, while freedom is an ideal of politics. Protecting dignity preserves a specific social position, a social image. The European Union's General Data Protection Regulation (GDPR) broadens the scope and enhances privacy obligations. Personal information may be protected outside the EU under stringent circumstances; when GDPR law is enacted outside the EU or businesses adopt Binding Corporate Rules (BCR) or employ standard contractual clauses (CCC) for particular business transactions.9

When data comes to privacy regulations, the disparities between the US and Europe are explained by these two different approaches. The private industry is more regulated in the United States, whereas the European Union does not oversee private sector data usage.10 Both systems are beyond the scope of this article to address in full.

by the way we can know IoT stands for the (Internet of Things). It refers to the network of physical devices, vehicles, appliances, and other objects that are embedded with sensors, software, and connectivity features, allowing them to collect and exchange data over the internet. This technology enables objects to communicate with each other and be monitored or controlled remotely, leading to improved efficiency, convenience, and automation in various applications, such as smart homes, healthcare, transportation, and industrial processes

II-Importance of Research

The importance of this research lies in its critical examination of the intersection between technology, law, and ethics in the context of the Internet of Things (IoT). As IoT devices become increasingly pervasive, the need for robust privacy and security measures becomes paramount. This study underscores the implications of these technologies on individual rights and societal norms, highlighting the urgent need for effective governance frameworks. By analyzing global compliance with privacy regulations, the research aims to contribute to a

deeper understanding of how organizations navigate the complex legal landscape while maintaining ethical standards. Ultimately, this research serves to inform policymakers, businesses, and the public about the evolving challenges and opportunities posed by the integration of IoT into everyday life.

III-Objectives of Research

1. Assess Global Compliance: To evaluate how businesses across different countries adhere to various privacy laws and regulations, and to identify discrepancies in compliance levels.

2. Analyze Ethical Perspectives: To explore the moral and ethical implications of privacy practices in the context of IoT, emphasizing the importance of informed consent and transparency.

3. Examine Regulatory Frameworks: To investigate the existing legal frameworks governing privacy and data protection, and their effectiveness in addressing the challenges posed by IoT technologies.

4. Identify Best Practices: To propose recommendations and best practices for organizations to enhance their compliance with privacy regulations and ethical standards.

5. Enhance Public Awareness: To raise awareness among consumers about their rights and the implications of data sharing, fostering a more informed public discourse on privacy issues.

6. Promote Inclusivity: To advocate for measures that ensure privacy and security protections are inclusive, addressing the needs of marginalized communities in the digital space.

By achieving these objectives, the research aims to provide a comprehensive understanding of the interplay between technology, law, and ethics, paving the way for more effective privacy and security measures in the IoT landscape.

VI-Background

In 1957, President Dwight Eisenhower started the Advanced Research Projects Agency (ARPA) in order to re-establish technological superiority in the arms race.[11]The new organisation, with a mission to continue the study into the semi-automatic environment programme to assist defend the United States from a nuclear space-based assault, was assigned to J.C.R. Licklider by the ARPA.[12] Licklider evangelised the potential advantages of a nationwide communication network that influenced Lawrence Roberts' successors in order to execute his ideas. He has been at the forefront of the network's advancement based on the innovative packet

switching idea of Paul Baran and Donald Davies. A desktop called the Interface Message Processor was designed and in October 1969 ARPANET was inaugurated.[13] The first contact took place between the Research Center of the University of California and the Research Institute of Stanford. The Network Control Program (NCP) was the original connection-oriented protocol, but TCP/IP (which stands for Transmission Control Protocol/Internet Protocol) soon had become the world's most used communication network.[14] The NSFNET became linked with the CSNET, connecting North American and EUnet universities connecting European research institutions.[15] The use of the Internet has grown after 90s due in part to the wise management of the NSF and fueling the popularity of the web, which have prompted the US authorities to transfer controls to independent organisations since 1995.[16] While nobody owns the internet, there are organisations involved in Internet administration and operation. There is a coalition of similar organisations working democratically together to boostdevelopment and the availability of information and resources on the world wide web.

As stated before, the Internet was established in the 1950s as a network of military communications, and it had become an education-purpose entity that connected university campuses throughout the US.[17] When the internet was made available to the public at the beginning of the 1990s, it was an immediate success, full of huge quantities of information and grew rapidly. This development has led to growing privacy and security-related problems.[18] The tremendous popularity of the Internet was not predicted and there were no limits or regulatory requirements at the beginning, leading to an early era of uncontrolled development. Even now, the general governing body does not restrict what can and cannot occur on the Internet. If the Web had rules and limitations in place throughout its rapid development, the Internet would never have been as large and popular as it is now.

V-Privacy Protection Laws and Regulations in the US and Europe

HIPAA 1996

Every US health organisation which handles patient’s details must duly by the Health Insurance Portability and Accountability Act of 1996[19]. HIPAA safety requirements demand the adoption of policies and procedures by health agencies which demonstrate how security measures are applied in a "reasonable and acceptable" manner. Like other organisations, health agencies wanting to safeguard

their information have used techniques such as password authentication, which act as a barrier to most computer systems in the 'outside world'. If hackers can identify a legitimate user id and password, then they may mimic your employee and enter the computer system of an agency. Unfortunately, this infiltration frequently goes undetected when legitimate credentials are provided. HIPAA consists of three standards sets, including: 1) Proceedings and codes 2) Database 3) Safety.[20]These claims-processing suggestions are meant to reduce the expenses and improve administration and supervision for patients while safeguarding them from vulnerability or loss. Under the HIPAA, it is imperative that healthcare organisations institute effective controls for restricting the collection of sensitive medical information to individuals, including the implementation of privacy training programmes, the assignment of a manager to oversee privacy efforts, and the provision of electronic records access for patients. The deadline for security under HIPAA was April 2005, but the date for HIPAA privacy laws was April 2003.[21]

VI-The Gramm-Leach Bliley Act 1999

As the Internet develops, it is continuously uploaded with more and more data. It should thus not surprise that all kinds of information from personally identifiable data to finances are stored on computing devices connected worldwide through the Internet. Such a connection has dramatically impacted the safety of the Internet. In the late 1990s, a citizen called Joe Barton started a campaign demanding improved security for financial data stored by businesses, especially online ones.[22]When Barton's financial details, unbeknownst to him, were transferred to the Secret Intimate Clothing Merchant by his credit union, Barton understood that legal proceedings had to be taken. Not only did Barton get catalogues from Victoria's Secret, although his spouse and relatives started to ask him if he had a secret lover to whom he supplied lingerie. Barton's legal fight, tired of having been hounded by his personal information being sold. The US Congree from Massachusetts, Mr Ed Markey suggested a revision which'd put restrictions to safeguard personally identifiable data and those related to finances such as credit card details, etc. Particularly, his suggested changes were intended to protect people such as Joe Barton who found financial information transferred to retailers for a bounty. The Markey amendment was approved, and the Gramm-Leach Bliley Act was renamed after Barton's testimony in court about his secret Victoria catastrophe (GLBA).[23] The GLBA specifies three sub-sets: the Financial Privacy Regulation, the Safeguard Rule and a Federal Trade Commission (FTC) pretext described as an act to obtain financial information under false pretences.[24] The Financial Data Protection Regulations limit the authorities of finance-

related institutions and corporates acquiring finance-related data may do with a person's personal data. Financial information cannot be transmitted to other entities through the Internet anymore under the amendment. Such details provided herein cannot be sold alone; they could not even be shown on public platforms or to another organisation on or off the Internet. Unless a signed waiver in accordance with Financial Privacy Rule specifies, account numbers cannot be shared with related enterprises. The final GLBA provision protects people from attempts of misleading a person in order to get financial information. In no case may a person, company or organisation use inadequate techniques to acquire information that may disclose sensitive details (FTC, 2005). In the instance of Joe Barton, the Financial Privacy Rule was breached in a variety of ways. The credit union sold its information not only to a credit agency, and also sold its information to Victoria's secret in return.[25]In this situation, it can be deduced that a lot of mail advertisements are de facto a consequence of an infringement of the GLBA Financial Privacy Regulation.A thorough examination of another extremely comprehensive Internet legislation is necessary if financial data is secured.

VII-United States Patriot Act 2001

The US Congress passed this act during the tenure under President George Bush, strengthening America in public law by providing necessary instruments for the 2001 Internet and Obstruct Terrorism Act 45 days after the 9/11 incident.[26] The following sections of the Act with specific data security and protection connections are included:

- Section 204 – gives room for saved voicemails to not satisfy the more rigorous wiretap standards to be acquired by means of a search warrant messages on a reply machinetape are nevertheless inaccessible under section 204.[27]
- Section 210 — Extends the kind of data which could be disclosed by telecom service providers. It includesdetails on sessions and durations, sporadicallyIP address and payment methods used. This section is not limited only to suspected terrorist activities being investigated and can be broadly applied.28
- Section 211 – brings cable providers offering telecom and internet facilities under the ambit of current regulations covering providers of telecommunication and Internet services (ISPs).29
- Section 215 — empowers public authorities to ask for an order by the Court to acquire personally identifiable details such as bank and telephone documents, travel history and medicinal data. It is be done by modifying the Foreign

Intelligence Surveillance Act and is based on a much lesser suspected cause than normal warranty.30

- Section 216 – Applies to Internet traffic telephone surveillance legislation, comprising emails, webpages, and IP details to the Internet.31
- Section 314 – provides for the exchange of information between financial organisations and amongst public and financial entities.32
- Section 319(b) – amends Title 31 of the U.S. Code Section 5318 to add a 120-hour regulation. This clause compels a financial organisation, on request of an authorised federal bank agency, to provide documents pertaining to "any established, maintained, administered or managed in the United States." This section also offers instructions on keeping records of international banks.33
- Section 326 – Mandates financial organisationsto check a user'sidentification details.34
- Section 505 — Empowers the government, via administrative subpoena, to get personal data without court authorization. This clause expires not at the end of 2005 and has been used on numerous occasions since 2001. However, in September 2004, it was ruled unlawful by a New York Federal District Court.35

In July 2005, the United States Senate adopted a re-authorization measure with major amendments to a number of clauses of the legislation, with the House renewal bill maintaining most of the original language of the legislation.[36] The two versions were harmonised and a "compromise bill" was drawn up to remove most changes from the version of the Senate. The amended legislation was adopted in March 2006 and was given green light by George Bush sooner.[37]

VIII-Sarbanes-Oxley Act 2002

The regulatory changes in the beginning of the 1990s mostly were concentrated on Information Technology concerns and important usage relating to internal computer systems.[38] Following the century of data changes, more focus was placed on risk management in the regulatory approach to Information Technology assessments and in particular risk governance, which addresses in-house core processing duties in contrast to a third party's exterior operations. The Sarbanes-Oxley Act (SOX) in its new law in July 2002 mandated stringent corporate governance procedures, including financial transparency, audits and accounting, to public companies.[39] Section 404 of the SOX in particular requires management to

review internal financial reporting checks.[40]Technology plays a vital role in the financial reporting of most firms, and IT is typically contracted by financial institutions. SOX standards apply to the outsourcing of operational transactions. According to 404, when a financial transaction is moved to another firm, management is held responsible for making sure all parties are adhering to these rules.[41]In order for banks to verify if a network operator is in the organization's corporate revenue recognition control, the company must be assessed. The management of the company may not be aware of any subcontractor hired by the institution.

IX-Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003

The 2003 Law to Control the Unwanted Pornography and Marketing Assault (or CAN-SPAM) started at the end of the yearbecause of the fast rise in spam cases.[42] Spamming is the emailing of large promotional messages in the expectation that every wave "grows" a number of purchases. Such emails or spams generally include contents which could deceive regular users and infect harmful programmes on their PCs. The newest email spam wave comprise of pornographic and other adult contents not suitable for young users. The FTC has implemented the CAN-SPAM Act 2003 To help safeguard the interests of people from spamming, the system is outfitted with anti-spam features in the defence of consumer rights. In accordance with the 2003 CAN-SPAM Act, numerous issues, from discouraging sending personal details over emails, are required for email users. The header of each emailsalso comprise ofdomain information. Aside from fulfilling the new validity criteria of the CAN-SPAM Act, e-mail topics cannot be deceiving or deceptive with respect to e-mail content. Pursuant to the Gramm-Leach Bliley Act, the CAN-SPAM Act currently mandates that publishing or promotional e-mail provide the opportunity to cancel the e-mail address of each receiver. Perhaps, the greatest challenging phase of the CAN-SPAM Act is the requirement for physical attention.[43]

X-California's Breach of Security Act 2003

A requirement of other states has been set out in the 2003 California Breach of Security Act to oblige companies holding consumer information to disclose any security breach that is reasonably suspected to have given vital information to unauthorised staff.[44] The legislation stipulates that essential information refers to information including the identity of a person and to sensitive information which cannot be accessed via a public record. The

legislation also states that the stolen information must be unencrypted in order to constitute a violation of security. If such corporate notifications cost more than $250,000, or the total number of impacted persons exceeds $500,000.[45] the firm must be permitted to utilise the media or other methods (including e-mail) to notify its consumers to a violation. Finally, any company that causes harm to people by not complying with the regulations laid out in the law may be penalised by civil action filed by the individuals affected. In addition to prior punishments under California state law, this threat is permitted.

XI-The Personal Data Privacy and Security Act 2005

The United States Senate brought the Privacy and Security Act 2005 on personal data in order to detect security breaches and to manage sensitive information such as HR4127.[46] In the Senate proposal, however, further modifications were made. In the first place, someone who deliberately disguises a security breach that harms users may be penalised and/ or detained upto 5 years. Secondly, people who engage in stealing and fraudulently utilize customer's personal data may apply the mandatory penalty, which has been in effect for up to two years. Thirdly, the proposal is supposed to fund$25 million yearly for national deployment of the act.[47] This distribution of money, in combination with the rest of the complex regulations, is a decent first effort to demand corporate accountability.

XII-The Financial Data Protection Act 2005

In 2005, several US Congressmen suggested legislation targeting personal financial data brokers in particular. In essence, the aim of H.R. 2997 is to prevent data leaks by creating a nationwide standard concerning the security of sensitive consumer details.[48] For this purpose, the Act mandates that organizations must disclose to their customers if their personal data could be used to perpetrate criminal activity, and it also demands that institutions give customers unfettered access to their personal data, national credit tracking service for a period of six months upon notification of a violation.[49]

XIII-General Data Protection Regulation (GDPR) 2016

The General Data Protection Regulation has been implemented in the European Union.[50] GDPR concludes personal information as "any data relating to an identify or recognisable natural person," generally defined as "a person who is identified directly or indirectly by reference to an identification device in particular, such as name, identifying number, location data, online identification device or single or more physical, physiological, genetic and psychological

factors."[51] Personal data are collected online in a wide range of methods, including via email, social networking, twitter, web browser data and location data for smartphones. Personal information may also be collected and analysed to build a personal profile of non-personal information.

The allocation of GDPR personal data rights and responsibilities differs from data subjects, processors and controllers. Under the GDPR a controller must be defined as "a natural or legal person, public body, agency or other entity that determines on its own purpose and method of processing or in cooperation with another entity of the personal data."[52] A processing unit is said as a legal, governmental or other entity which is tasked with processing personal information for some other entity. The GDPR requires legal reason for personal data processing, namely consent or contracts. The users' consensusmust be'unambiguously there. The political opinions or religious belief data, for 'particular categories of personal information must be 'explicitly permitted.' In other limited circumstances, data processing is allowed such as, if important, for the purpose of complying with a contract according to his legal responsibility to protect the fundamental interests of the data subject, or in the public interest. It is also allowed for the purposes of the legitimate interest of the controller, other than where the fundamental rights and freedoms of subjects are obscured by these interests.

The GDPR sets forth five principles for the handling of personal information.[53] The key principle is that the data are processed fairly and legally; collected and not processed for a special, explicit, legitimate purpose in a manner which contradicts that; appropriate, relevant and not excessive for the purpose that the data are accurat and updated, where necessary. The GDPR also grants data subjects a range of rights to personal data. The most important are the right to information on the personal data of the controller, including its maintenance, the right to correct (so-called forgetting) and the right to erase any personal information.

In instance, the GDPR is now applicable to personally identifiable data processing. It also concerns the handling of personal data by an non-EU controller or processor of data subjects, if (a) activities relate to the provision of goods or services in the Union to such data subjects, regardless of whether payment is required for the data subject or (b) monitoring their conduct with regard to their behaviour.[54] If the controller does not, however, reside in the EU, the legislation mandates that the controller designate a Union representative.

Recitals 23 and 24 of the GDPR offer further context.[55] According to recital 23, the offer of goods or services online along with the use of an EU

Member State's language and buying choices may constitute an offer for GDPR sales. Recital 24 of the Regulation gives an outline of the definition of "surveillance" when "individuals are followed on the Internet using data processing methods comprising in particular in profiling a person to decide on him/her and analyse or forecast his or her preferences, conduct or attitudes." Taken together, that appears to be a lot of what happens when people use the Internet.

XIV-Conclusion

It is clear that governments of many different countries (primarily the United States and the European Union) are seriously trying to solve problems of personal data protection and security. Unless several laws, such as the EU GDPR or the Gramm-Leach Bliley Act, are proposed and ultimately implemented, which have improved financial data security and ensured that customers are protected from sharing information on the Internet. The Directives of the European Union have impacted private information gathered at EU level activities and transmissions. With these Guidelines in place along with US laws and regulations, researchers will be able to assess the economic and juridical ramification of these laws as well as future studies in the fields of safety and privacy. Governments across the world have to take global trade, user dignity and freedom into consideration in terms of internet privacy and security in legislation.Protection and security regulations will continue to ensure that information is protected, but will enable the Internet to continue to meet its potential as a means of sharing information.

XV-Results:

1. Enhanced Data Utilization: Mining IoT data enables organizations to maximize the value of the data collected by IoT devices. Through the extraction of meaningful insights, businesses can improve operational efficiency, predict maintenance needs, and make data-driven decisions.

2. Improved Decision-Making: With real-time data analysis from IoT systems, decision-making processes become faster and more informed. This leads to more accurate predictions, optimized operations, and enhanced productivity across various sectors such as healthcare, manufacturing, and transportation.

3. Predictive Maintenance: IoT mining allows industries to shift from reactive to predictive maintenance. By analyzing sensor data, organizations can identify issues before they become critical, reducing downtime and repair costs.

4. Increased Automation: Mining data from IoT devices facilitates the automation of processes. Smart systems can automatically adjust operations based on the insights

gained, reducing human intervention and enhancing efficiency.

5. Security and Privacy Concerns: While IoT mining presents significant benefits, it also raises concerns about data security and privacy. As more devices are connected, there is an increased risk of data breaches or misuse of sensitive information.

XVI-Recommendations:

1. Invest in Advanced Analytics: Organizations should invest in advanced data analytics tools and machine learning algorithms to effectively mine IoT data. These technologies will help extract valuable insights and improve overall decision-making processes.

2. Strengthen Data Security Protocols: As the amount of IoT data grows, it's crucial to implement robust security measures. This includes encryption, multi-factor authentication, and regular security audits to protect sensitive information from cyber threats.

3. Adopt Predictive Maintenance Practices: Businesses, particularly in manufacturing and industrial sectors, should adopt predictive maintenance strategies by leveraging IoT data. This will help reduce downtime, extend the lifespan of equipment, and minimize operational costs.

4. Automate Processes: Organizations should explore the potential of automating certain operations based on the insights gained from IoT data mining. Automation can lead to enhanced productivity and reduced operational errors.

5. Implement Privacy Regulations: To address privacy concerns, it is essential to implement clear privacy regulations that govern the collection, storage, and use of IoT data. These regulations should ensure that user data is handled responsibly and that individuals' privacy is protected.

6. Promote Collaboration Across Industries: To fully unlock the potential of IoT data mining, industries should foster collaboration between data scientists, engineers, and business leaders. This collaboration will help develop more comprehensive solutions and ensure the effective use of IoT data across sectors.

الهوامش

([1]) Valente, Fredy J., and Alfredo C. Neto. "Intelligent steel inventory tracking with IoT/RFID." In 2017 IEEE International Conference on RFID Technology & Application (RFID-TA), pp. 158-163. IEEE, 2017.

([2]) Farris, Ivan, Sara Pizzi, Massimo Merenda, Antonella Molinaro, Riccaro Carotenuto, and Antonio Iera. "6lo-RFID: A framework for full integration of smart UHF RFID tags into the internet of things." IEEE Network 31, no. 5 (2017): 66-73.

([3]) Yamin, Muhammad Mudassar, and Basel Katt. "Mobile device management (MDM) technologies, issues and challenges." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 143-147. 2019.

([4]) Kumar, A. Dinesh, and S. Smys. "An energy efficient and secure data forwarding scheme for wireless body sensor network." International Journal of Networking and Virtual Organisations 21, no. 2 (2019): 163-186.

([5]) Ylmaz, Ercan Nurcan, Bünyamin Ciylan, Serkan Gönen, Erhan Sindiren, and Gökçe Karacayılmaz. "Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect." In 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), pp. 81-85. IEEE, 2018.

([6]) Petkova, Bilyana. "Privacy as Europe's first Amendment." European Law Journal 25, no. 2 (2019): 140-154.

([7]) Lee, Hwansoo. "Home IoT resistance: Extended privacy and vulnerability perspective." Telematics and Informatics 49 (2020): 101377.

([8]) Petkova, Bilyana. "Privacy as Europe's first Amendment." European Law Journal 25, no. 2 (2019): 140-154.

([9]) Thomopoulos, Stelios CA. "Risk-based security: from theory to practice." In Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, vol. 11756, p. 117560M. International Society for Optics and Photonics, 2021.

([10]) Levin, Avner, and Mary Jo Nicholson. "Privacy law in the United States, the EU and Canada: the allure of the middle ground." U. Ottawa L. & Tech. J. 2 (2005): 357.

([11]) Russell, Andrew L. "Ideological and Policy Origins of the Internet, 1957-1969." arXiv preprint cs/0109056 (2001).

([12]) Kita, Chigusa Ishikawa. "JCR Licklider's Vision for the IPTO." IEEE Annals of the History of Computing 25, no. 3 (2003): 62-77.

([13]) Paloque-Bergès, Camille, and Valérie Schafer. "Arpanet (1969–2019)." Internet Histories 3, no. 1 (2019): 1-14.

([14]) Ahsan, Muhammad, Mazhar Javed Awan, Awais Yasin, Saeed Ali Bahaj, and Hafiz Muhammad Faisal Shehzad. "Performace Evaluation of TCP Cubic, Compound TCP and NewReno under Windows 20H1, via 802.11 n Link to LTE Core Network." Annals of the Romanian Society for Cell Biology 25, no. 6 (2021): 5357-5369.

([15]) Radu, Roxana. Negotiating internet governance. Oxford University Press, 2019.

([16]) Smyrnaios, Nikos. Internet oligopoly: The corporate takeover of our digital world. Emerald Group Publishing, 2018.

([17]) Ibid.

([18]) Tzafestas, Spyros G. "Ethics and law in the internet of things world." Smart cities 1, no. 1 (2018): 98-120.

([19]) U.S. Congress, Health Insurance Portability and Accountability Act, 1996

([20]) Choi, Young B., Kathleen E. Capitan, Joshua S. Krause, and Meredith M. Streeper. "Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules." Journal of medical systems 30, no. 1 (2006): 57-64.

([21]) Kibbe, David C. "Ten steps to HIPAA security compliance." Family practice management 12, no. 4 (2005): 43.

([22]) Raul, Alan Charles. "Privacy & Security." (2010).

([23]) U.S. Congress, Gramm-Leach Bliley Act, 1999

([24]) Russo, Kathryn F. "Regulation of Companies' Data Security Practices under the Federal Trade Commission Act and California Unfair Competition Law."

([25]) Fuller, Caleb S. "Privacy law as price control." European Journal of Law and Economics 45, no. 2 (2018): 225-250.

([26]) U.S. Congress, Patriot Act, 2001

([27]) Ibid., s. 204

([28]) Ibid., s. 210

([29]) Ibid., s.211

([30]) Ibid., s. 215

([31]) Ibid., s. 216

([32]) Ibid., s. 314

([33]) Ibid., s. 319(b)

([34]) Ibid., s. 326

([35]) Ibid., s. 505

([36]) Richardson, Brittlin M. "Big Brother is Watching You: Establishing the Constitutionality of the Post-9/11 USA Patriot Act." (2020).

([37]) Twomey, William. "A History of Privacy Rights in America: From the Fourth Amendment to the Patriot Act." In Colloquium: The Political Science Journal of Boston College. 2018.

([38]) Alsultanny, Yas. "Evaluating the effect of studying computer ethics and computer ethics rules and regulations on computer ethics at work." Cloud Computing and Data Science (2020): 21-30.

([39]) U.S. Congress, Sarbanes-Oxley Act, 2002

([40]) Gupta, Parveen P., and Nandkumar Nayar. "Information content of control deficiency disclosures under the Sarbanes–Oxley Act: An empirical investigation." International Journal of Disclosure and Governance 4, no. 1 (2007): 3-23.

([41]) Ibid., s. 404

([42]) U.S. Congress, Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003

([43]) Mishan, James. "Salcedo v. Hanna." NYLS Law Review 65, no. 2 (2020): 277-289.

([44]) De Bruyn, Warren J., Catherine D. Clark, Mary Senstad, Natalie Toms, and Aaron W. Harrison. "Biological degradation of ethanol in Southern California coastal seawater." Marine Chemistry 218 (2020): 103703.

([45]) Ibid.

([46]) U.S. Congress, Personal Data Privacy and Security Act, 2005

([47]) Park, Sangchul. "Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records." International Review of Law and Economics 58 (2019): 132-145.

([48]) Milne, George R., George Pettinico, Fatima M. Hajjat, and Ereni Markos. "Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing." Journal of Consumer Affairs 51, no. 1 (2017): 133-161.

([49]) U.S. Congress, The Financial Data Protection Act, 2005

([50]) E.U. Senate, General Data Protection Regulation, 2016

([51]) Ibid.

([52]) Tesfay, Welderufael B., Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. "PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy

evaluation." In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, pp. 15-21. 2018.

([53]) Gilman, Michele E. "Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice." Ariz. St. LJ 52 (2020): 368.

([54]) Barrett, Catherine. "Emerging Trends from the First Year of EU GDPR Enforcement." Scitech Lawyer 16, no. 3 (2020): 22-35.

([55]) Tesfay, Welderufael B., Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. "PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation." In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, pp. 15-21. 2018.

Bibliography

1) Ahsan, Muhammad, Mazhar Javed Awan, Awais Yasin, Saeed Ali Bahaj, and Hafiz Muhammad Faisal Shehzad. "Performace Evaluation of TCP Cubic, Compound TCP and NewReno, Under Windows 20H1, via 802.11 n Link to LTE Core Network." Annals of the Romanian Society for Cell Biology 25, no. 6 (2021): 5357-5369.
2) Alsultanny, Yas. "Evaluating the effect of studying computer ethics and computer ethics rules and regulations on computer ethics at work." Cloud Computing and Data Science (2020): 21-30.
3) Barrett, Catherine. "Emerging Trends from the First Year of EU GDPR Enforcement." Scitech Lawyer 16, no. 3 (2020): 22-35.
4) Choi, Young B., Kathleen E. Capitan, Joshua S. Krause, and Meredith M. Streeper. "Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules." Journal of medical systems 30, no. 1 (2006): 57-64.
5) De Bruyn, Warren J., Catherine D. Clark, Mary Senstad, Natalie Toms, and Aaron W. Harrison. "Biological degradation of ethanol in Southern California coastal seawater." Marine Chemistry 218 (2020): 103703.
6) E.U. Senate, General Data Protection Regulation, 2016
7) Farris, Ivan, Sara Pizzi, Massimo Merenda, Antonella Molinaro, Riccaro Carotenuto, and Antonio Iera. "6lo-RFID: A framework for full integration of smart UHF RFID tags into the internet of things." IEEE Network 31, no. 5 (2017): 66-73.
8) Fuller, Caleb S. "Privacy law as price control." European Journal of Law and Economics 45, no. 2 (2018): 225-250.
9) Gilman, Michele E. "Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice." Ariz. St. LJ 52 (2020): 368.
10) Gupta, Parveen P., and Nandkumar Nayar. "Information content of control deficiency disclosures under the Sarbanes–Oxley Act: An empirical investigation."

International Journal of Disclosure and Governance 4, no. 1 (2007): 3-23.
11) Kibbe, David C. "Ten steps to HIPAA security compliance." Family practice management 12, no. 4 (2005): 43.
12) Kita, Chigusa Ishikawa. "JCR Licklider's Vision for the IPTO." IEEE Annals of the History of Computing 25, no. 3 (2003): 62-77.
13) Kumar, A. Dinesh, and S. Smys. "An energy efficient and secure data forwarding scheme for wireless body sensor network." International Journal of Networking and Virtual Organisations 21, no. 2 (2019): 163-186.
14) Lee, Hwansoo. "Home IoT resistance: Extended privacy and vulnerability perspective." Telematics and Informatics 49 (2020): 101377.
15) Levin, Avner, and Mary Jo Nicholson. "Privacy law in the United States, the EU and Canada: the allure of the middle ground." U. Ottawa L. & Tech. J. 2 (2005): 357.
16) McKelvey, Fenwick, and Kevin Driscoll. "ARPANET and its boundary devices: modems, IMPs, and the inter-structuralism of infrastructures." Internet Histories 3, no. 1 (2019): 31-50.
17) Milne, George R., George Pettinico, Fatima M. Hajjat, and Ereni Markos. "Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing." Journal of Consumer Affairs 51, no. 1 (2017): 133-161.
18) Mishan, James. "Salcedo v. Hanna." NYLS Law Review 65, no. 2 (2020): 277-289.
19) Paloque-Bergès, Camille, and Valérie Schafer. "Arpanet (1969–2019)." Internet Histories 3, no. 1 (2019): 1-14.
20) Park, Sangchul. "Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records." International Review of Law and Economics 58 (2019): 132-145.
21) Petkova, Bilyana. "Privacy as Europe's first Amendment." European Law Journal 25, no. 2 (2019): 140-154.
22) Petkova, Bilyana. "Privacy as Europe's first Amendment." European Law Journal 25, no. 2 (2019): 140-154.
23) Radu, Roxana. Negotiating internet governance. Oxford University Press, 2019.
24) Raul, Alan Charles. "Privacy & Security." (2010).
25) Richardson, Brittlin M. "Big Brother is Watching You: Establishing the Constitutionality of the Post-9/11 USA Patriot Act." (2020).
26) Russell, Andrew L. "Ideological and Policy Origins of the Internet, 1957-1969." arXiv preprint cs/0109056 (2001).
27) Russo, Kathryn F. "Regulation of Companies' Data Security Practices under

the Federal Trade Commission Act and California Unfair Competition Law."
28) Smyrnaios, Nikos. Internet oligopoly: The corporate takeover of our digital world. Emerald Group Publishing, 2018.
29) Tesfay, Welderufael B., Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. "PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation." In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, pp. 15-21. 2018.
30) Tesfay, Welderufael B., Peter Hofmann, Toru Nakamura, Shinsaku Kiyomoto, and Jetzabel Serna. "PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation." In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, pp. 15-21. 2018.
31) Thomopoulos, Stelios CA. "Risk-based security: from theory to practice." In Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, vol. 11756, p. 117560M. International Society for Optics and Photonics, 2021.
32) Twomey, William. "A History of Privacy Rights in America: From the Fourth Amendment to the Patriot Act." In Colloquium: The Political Science Journal of Boston College. 2018.
33) Tzafestas, Spyros G. "Ethics and law in the internet of things world." Smart cities 1, no. 1 (2018): 98-120.
34) U.S. Congress, Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003
35) U.S. Congress, Gramm-Leach Bliley Act, 1999
36) U.S. Congress, Health Insurance Portability and Accountability Act, 1996
37) U.S. Congress, Patriot Act, 2001
38) U.S. Congress, Personal Data Privacy and Security Act, 2005
39) U.S. Congress, Sarbanes-Oxley Act, 2002
40) U.S. Congress, The Financial Data Protection Act, 2005
41) Valente, Fredy J., and Alfredo C. Neto. "Intelligent steel inventory tracking with IoT/RFID." In 2017 IEEE International Conference on RFID Technology & Application (RFID-TA), pp. 158-163. IEEE, 2017.
42) Yamin, Muhammad Mudassar, and Basel Katt. "Mobile device management (MDM) technologies, issues and challenges." In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 143-147. 2019.
43) Ylmaz, Ercan Nurcan, Bünyamin Ciylan, Serkan Gönen, Erhan Sindiren, and Gökçe Karacayılmaz. "Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect." In 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), pp. 81-85. IEEE, 2018.