University of Barishal

Project

Title

General Data Protection Regulation

Submitted to

Tania Islam

Assistant Professor

Computer science and engineering

University of Barishal

Submitted by

Name : **MD RABIUL HASAN**

Roll : 03

Batch : 47

Table of Contents

Executive Summary

The General Data Protection Regulation (GDPR), set to take effect in the European Union (EU) in May 2018, addresses modern challenges in personal data protection while aiming to harmonize regulations across the EU. While the GDPR promises to provide benefits for companies by ensuring uniformity in data protection measures and reducing legal complexity across member states, it also introduces new challenges. Many companies are unprepared for the changes and may be unaware of the regulation's strict requirements and enforcement mechanisms. Implementing the GDPR involves significant financial and human resources, along with employee training, making it essential for companies to receive adequate support during this transition. This study compared the existing Data Protection Directive 95/46/EC with the GDPR by systematically analysing the differences and exploring the practical implications for companies that rely on personal data for their services. The goal was to highlight key changes in the GDPR that would significantly impact these companies' data management and usage practices. A review, combined with a thematic analysis and synthesis of the regulation's changes, was conducted, identifying the most relevant aspects. The result of this analysis was a framework that outlined 12 critical areas of impact, along with guidance on how businesses could prepare for the new requirements, covering both business strategies and organizational and technical measures.

Introduction

If we accept the metaphor of data as the new oil, we would expect it to be handled with the utmost care. Every step, from extraction to disposal, would be meticulously planned and carried out by trained professionals. The extraction process would be regulated through permits, its usage carefully managed to prevent waste, its storage safeguarded, and its disposal conducted in an environmentally responsible way. Additionally, any negative impacts would be addressed, and the interests of all stakeholders would be taken into account(Hoofnagle et al., 2019a). Faithfully executes the implications of the oil metaphor, despite the metaphor's poor fit. The GDPR presumes that personal data are important, so much so that every aspect of interacting with data requires careful planning(Robinson et al., 2024a).

In this paper, we explain the GDPR approach to lawyers and academics, whether they are privacy and EU law specialists or not. We explain the GDPR's normative roots in multiple constitutional documents, detail its most important provisions, and tie these provisions to the short and medium-term strategic goals of the GDPR. We also highlight differences and similarities when comparing the GDPR to U.S. privacy law(Hoofnagle et al., 2019a). The European Parliament voted to adopt the General Data Protection Regulation (GDPR) in May 2016, and it will take effect in May 2018, replacing the Data Protection Directive 95/46/EC (DIR95). The GDPR aims to enhance the privacy protections of data subjects while simplifying compliance for organizations and companies through clearer rules, more defined requirements, and specific instructions for implementing its provisions. However, these new obligations introduce significant changes in how companies manage privacy protection. Any company handling the personal data of EU residents or monitoring their behaviour within the EU, regardless of its location, will be subject to the GDPR. This means that non-EU and international businesses must comply with both their own national laws and the GDPR. Since its adoption in 1995, DIR95 has served as the EU's primary legislative framework for personal data privacy(Tikkinen-Piri et al., 2018a). Governments, international organizations, and the private sector have united to advocate for the recognition of individual identity, supported by the European Digital Rights (EDRi) association, which includes both European and international members committed to EU digitalization efforts. The United Nations, through the ID2020 Alliance, also highlights the importance of recognizing digital identity as a fundamental human right, emphasizing that individuals should have control over their own digital identity. The objective is to ensure everyone has access to a reliable and sustainable form of legal digital identity. However, the use of biometric technology in digital identity

recognition has sparked ongoing debates about balancing security with the protection of fundamental rights and freedoms. One article reinforces this perspective, noting that the digitization of legal identity is based on human rights principles, such as Article 6 of the Universal Declaration of Human Rights and Article 16 of the International Covenant on Civil and Political Rights, which affirm the right to legal recognition for all. As a result, many countries are adopting policies to digitize and modernize their national identity systems, aiming to create a foundational registry for a digital identity ecosystem. A unique identifier can serve as proof of an individual's official digital existence, highlighting the need to legalize recognition techniques to establish identity in the digital realm(Bulgakova & Bulgakova, 2023).

Background

The implementation of the General Data Protection Regulation (GDPR) will affect data science in Europe, with specific concerns raised about consent requirements that could significantly limit medical data research(Rumbold & Pierscionek, 2017). The GDPR was introduced to replace the 1995 Data Protection Directive that had been used by various European countries. With the rise of the internet, the EU Parliament recognized the need for a new regulation that better suited a more connected world where data plays a central role. The GDPR was designed to address modern technologies and data practices(Yanamala & Suryadevara, 2024). In addition Unlike the 1995 law, which allowed each country to customize its privacy regulations, creating challenges for businesses operating across borders, the GDPR simplifies this by providing a single set of rules for all EU member states. This makes it easier for businesses to operate across the EU by adhering to one uniform standard. Moreover The GDPR came into force on May 25, 2018, and has since been the benchmark for privacy laws. It has also seen updates, including significant changes in 2021. One major update was the removal of the Privacy Shield, which previously facilitated business between U.S. companies and EU citizens. Another important change was the introduction of stricter cookie consent rules, preventing companies from denying access to content if users don't agree to cookies(Kohl, 2023).

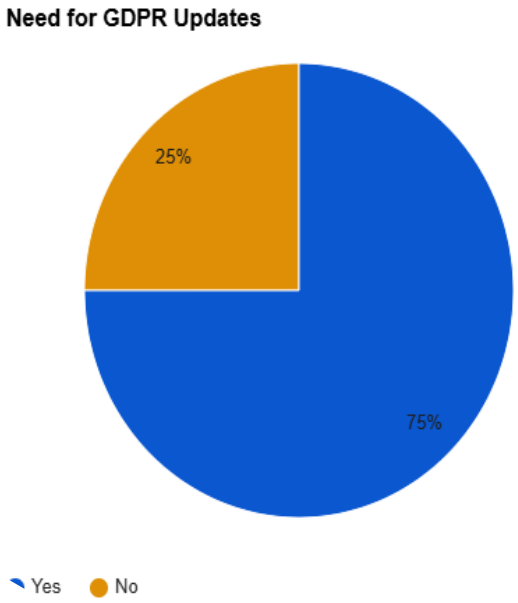
The UK's version of GDPR, created after Brexit, is based on the EU regulation and is enforced through the UK's Information Commissioner's Office (ICO) under the 2018 Data Protection Act. Companies dealing with both EU and UK customers must comply with both sets of data protection laws(Bloxberg, 2022).

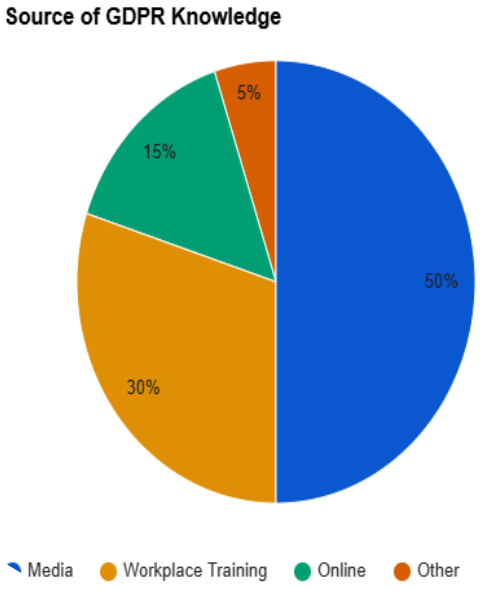
Research Questions

Question	Response Categories
Are you aware of the GDPR?	Yes: 70%, No: 30%
How did you first learn about GDPR?	Media: 50%, Workplace Training: 30%, Online: 15%, Other: 5%
Do you know your rights under GDPR?	Yes: 60%, No: 40%
Have you ever exercised your GDPR rights?	Yes: 40%, No: 60%
How satisfied were you with the response?	Very Satisfied: 20%, Satisfied: 50%, Neutral: 20%, Dissatisfied: 10%
Does your organization comply with GDPR?	Fully: 50%, Partially: 30%, Not at All: 20%
Has your organization conducted GDPR-specific training?	Yes: 80%, No: 20%
What was the biggest challenge in achieving GDPR compliance?	Cost: 35%, Complexity: 40%, Lack of Expertise: 20%, Other: 5%
Has your organization experienced a data breach?	Yes: 25%, No: 75%
Was the breach reported to relevant authorities?	Yes: 80%, No: 20%
Are you aware of GDPR fines in your industry?	Yes: 40%, No: 60%
Do you think GDPR enforcement is strict enough?	Yes: 55%, No: 45%

Question	Response Categories
Has GDPR improved data privacy for individuals?	Yes: 65%, No: 35%
How effective is GDPR in preventing data breaches?	Very Effective: 15%, Effective: 45%, Neutral: 25%, Ineffective: 10%, Very Ineffective: 5%
Should GDPR regulations be updated?	Yes: 75%, No: 25%

Visual Presentation





Features

Data Subject Rights The data subject has the right to request confirmation from the controller about whether their personal data is being processed. If so, they are entitled to access the data and receive the following information. The data subject must be informed about the specific purposes for which their personal data is being processed, as well as the types of personal data involved. They should also be made aware of the recipients, or categories of recipients, who will receive their data, including any transfers to third countries or international organizations. If possible, the expected duration of data retention should be disclosed, or, if unknown, the criteria used to determine this period. Additionally, data subjects have the right to request the rectification or deletion of their personal data, restrict its processing, or object to its processing. They also have the right to file a complaint with a supervisory authority. If the data was not collected directly from the data subject, information regarding the source of the data must also be provided.t("Art. 15 GDPR – Right of Access by the Data Subject," n.d.).In addition Explicit consent is a form of consent that requires a clear and specific agreement from the data subject for the processing of their personal data. It must be given freely and clearly, typically through a written or oral statement, including electronic forms. This type of consent is particularly important for handling sensitive personal data or situations that have a significant impact on the individual. Under GDPR, explicit consent ensures that individuals fully understand and agree to how their personal data will be used. It is crucial for processing sensitive information, ensuring transparency, and safeguarding individual rights in the digital era. To obtain explicit consent, organizations should provide a clear, simple, and accessible form that explains the purpose of data collection and usage. The form should require an active, deliberate action, such as ticking a box or signing a document, without any pre-ticked boxes or assumptions of consent(Sullivan, 2024).Moreover Data protection law has become a significant safeguard against online privacy violations, yet its place within the broader scope of privacy law remains somewhat awkward. Unlike traditional privacy law, which focuses on protecting "private" information, data protection law centres around "personal" information. This distinction creates a fundamental difference, as data protection law also addresses public personal information or information that has been made public through disclosure. Drawing on James Whitman's comparative study of privacy, this article suggests that data protection law is not an outlier within privacy law, but rather a reflection of the Continental European approach to privacy. Its uniqueness lies not in its technical aspects, but in its strong embrace of privacy in public spaces—an idea that contrasts with the Anglo-American conception of privacy(Sarabdeen &

Mohamed Ishak, 2024).Although these two privacy traditions have intersected in various legal systems, the article explores their continuing influence and tension within three modern privacy frameworks. It examines the right to be forgotten, a prime example of privacy in public, particularly in cases involving spent criminal convictions. The article evaluates how three legal bodies approach such claims: first, the Court of Justice of the European Union, which is the key authority on the General Data Protection Regulation (GDPR); second, the U.S. judiciary, with its dedication to the First and Fourth Amendments; and third, the European Court of Human Rights, which balances Anglo-American and Continental European privacy principles under Article 8 of the European Convention on Human Rights(Seun Solomon Bakare et al., 2024).The jurisprudence of the European Court of Human Rights, in particular, underscores the challenges of blending these two privacy traditions, or combining data protection with traditional privacy law. However, these tensions also reveal valuable insights and potential opportunities for navigating privacy concerns in modern legal contexts(Kohl, 2023).Furthermore Data Breach Notifications In the event of a security breach involving personal data, the data controller is required to notify the supervisory authority within 72 hours. The supervisory authority refers to the public body designated by the EU member state to enforce GDPR regulations. If the notification is not made within the 72-hour window, the data controller must explain the reason for the delay. The breach notification must provide at least the following details: the nature of the breach, the types and number of personal data subjects affected, and the number of data records potentially compromised. The organization responsible for the data must also outline any potential consequences of the breach and explain the actions being taken to mitigate its impact. Notifications must be communicated directly to the affected individuals, rather than through a general public announcement. Additionally, the data controller must record the breach and the steps taken to address it, and submit this documentation to the supervisory authority for verification(Robinson et al., 2024a).In addition too A Data Protection Officer (DPO) plays a crucial role in ensuring that an organization complies with data protection laws and regulations. Their responsibilities include implementing appropriate measures to safeguard personal data, educating staff on best practices, and addressing any concerns or complaints related to data protection. The DPO also oversees the organization's data protection policies through regular monitoring and provides guidance to employees on related matters. In certain instances, the DPO may conduct Data Protection Impact Assessments (DPIAs) and engage with regulatory authorities to ensure compliance with data protection standards(Expert, 2022).Moreover The GDPR sets a framework for maximum fines, allowing penalties of up to €20 million or 4% of a company's

global annual revenue, whichever is greater. In some cases, the fine may be reduced to €10 million or 2% of revenue, as specified in Article 83(4) of the GDPR. Additionally, individual EU member states can impose their own fines for violations not addressed in Article 83, under the GDPR's flexibility clause. The largest fine to date was imposed on Meta in 2023, amounting to $1.3 billion, for breaching GDPR rules regarding data transfers(Husain, 2024).

Functionality

The GDPR aims to safeguard individuals and the personal data associated with them, ensuring that organizations handle such data responsibly. It requires that personal data be securely maintained, protecting it from "unauthorized or unlawful processing" as well as from accidental loss, destruction, or damage(Tikkinen-Piri et al., 2018a).Moreover The GDPR also specifies that data collection must serve a specific and legitimate purpose and should not be used for any other reason beyond that. Additionally, the regulation limits the amount of data collected, stating that it should be restricted to what is necessary for its intended purpose. Organizations are further required to ensure that the data collected is accurate and updated as needed(Robinson et al., 2024b).

Applications

The General Data Protection Regulation (GDPR) is an EU regulation (Regulation (EU) 2016/679) that was enacted on April 27, 2016. It focuses on protecting individuals' personal data and ensuring its free movement across the EU.The GDPR applies to the processing of personal data by or on behalf of a data controller. Personal data refers to any information that can identify an individual, either directly or indirectly. This includes identifiers such as names, identification numbers, location data, online identifiers, and data related to a person's physical, physiological, genetic, mental, economic, cultural, or social identity(De Hert & Papakonstantinou, 2016).In addition The data controller is responsible for ensuring that personal data is processed in accordance with GDPR guidelines. The key principles for handling personal data include lawfulness, fairness, and transparency, meaning that data must be processed legally, fairly, and in a transparent manner. Additionally, data should only be collected for specific, legitimate purposes (purpose limitation) and should not be used in ways that deviate from those purposes. Data minimization ensures that only relevant and necessary data is collected for the intended purpose, while accuracy requires that data be kept up to date, with inaccuracies corrected or erased as needed. Data should not be retained in a form that allows for the identification of individuals for longer than necessary (storage limitation), and it must be protected from unauthorized processing, loss, or damage through appropriate security measures (integrity and confidentiality). Lastly, the principle of accountability requires the data controller to demonstrate compliance with these principles. Data controllers must also justify the processing of personal data under one of the following conditions: the individual has given explicit consent for specific purposes; the processing is necessary for fulfilling a contract; it is required to meet a legal obligation; it is necessary to protect someone's vital interests; it is needed for tasks carried out in the public interest or in the exercise of official authority; or it is necessary for legitimate interests, provided these do not override the individual's rights and freedoms, especially in the case of children.(BIBM, 2021).

Challenges

In just a year, the European Union's General Data Protection Regulation (GDPR), designed to enhance data protection for individuals, will come into effect. This regulation will impact all companies, both within and outside Europe, that handle personal data of European citizens. A major concern for these companies is how to track and manage all the necessary data to uphold the new consumer rights under GDPR. For example, they need to handle data related to "The Right to be Forgotten" and ensure proper consent for marketing activities. This blog post explores the four biggest challenges related to personal data under GDPR and provides solutions for addressing them(Tikkinen-Piri et al., 2018b).In addition Identity Resolution To manage consents, correct or delete personal data, and inform individuals about their data and its usage, companies must accurately identify each individual. This involves identity resolution—a process of consolidating disparate data sets and databases into a single, up-to-date profile for each person. For example, if Ana Maria has multiple profiles across different systems, these duplicates need to be merged into one comprehensive profile. This task can be challenging, as many companies struggle with scattered systems and incomplete or duplicated customer data. A recent Royal Mail Data Services study found that over half of businesses have missing, outdated, or incomplete customer data. The study highlighted that 63.3% of UK businesses reported outdated information, 62.8% had incomplete data, and 60.1% had minimal data for some customers. Without accurate identification of customer profiles, providing a complete overview of personal data becomes difficult(Yanamala & Suryadevara, 2024).Moreover Consent Overview Under GDPR, organizations must adopt a more stringent consent protocol for storing and using personal data. Consent must be specific to each purpose, such as newsletter subscriptions, online purchase histories, or campaign cookies. Companies need to track and link each profile to the various processes and services for which consent has been given. This requires maintaining a clear overview of all the consents granted by each individual(Oluwatosin Reis et al., 2024).In addition to Identify Associated Data Business processes mentioned in #2 require specific data. For example, sending a newsletter needs a name and email address, while personalized marketing might require additional details like gender, nationality, age, preferences, and social media handles. It’s crucial to identify which data categories correspond to each processing purpose and ensure these are linked correctly. This process helps document how data is used and provides necessary information for compliance with authorities(Oluwatoyin Ajoke Fayayola et al., 2024).Apart from this Data Governance Establishing a data governance framework is essential for managing data flow

effectively. This includes determining how long data remains valid and setting up validity periods, such as updating addresses every two years. GDPR mandates that data should only be kept as long as necessary for its intended purpose. Additionally, controlling access to data is crucial; only those who need it for their roles should have access. For instance, social media handles might be relevant only to marketing teams, not the financial department. Companies must define their data policies clearly, deciding what constitutes contact data and implementing the appropriate rules for data access and retention(Nielsen, 2024).

Conclusion

This paper explores the normative foundations, characteristics, and strategic approach of the European Union's General Data Protection Regulation (GDPR). It traces the origins of the GDPR, outlines its approach and provisions, and anticipates its short- and medium-term effects. The GDPR is seen as an evolution of the 1995 Data Protection Directive, maintaining its core principles, akin to the Fair Information Principles. Nonetheless, the GDPR introduces notable changes. It establishes a detailed and protective regulatory framework for personal data, prompting companies to reconsider their data practices and take privacy more seriously. The GDPR also requires companies to assess their service providers' compliance and elevates the role of privacy officials within organizations. Additionally, it is critical of the concept of 'informed consent,' indicating that in some cases, organizations cannot rely solely on consent. The GDPR emphasizes the need for accurate data and grants individuals the right to access and correct their data. In the private sector, we anticipate that relationships directly with individuals will gain importance over third-party relationships. There may also be ongoing disputes between Data Protection Authorities and large tech companies regarding GDPR interpretations. One significant drawback of the GDPR is its complexity, with 99 detailed provisions. Whether the GDPR will effectively enhance fairness and respect for fundamental rights can only be judged after it has been in effect for a while. As with consumer protection or environmental laws, data protection rules will need continuous updates to keep pace with evolving circumstances. In summary, the GDPR represents a significant shift in privacy law and is expected to have a global impact on policy.

References

Art. 15 GDPR – Right of access by the data subject. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved September 12, 2024, from https://gdpr-info.eu/art-15-gdpr/

BIBM. (2021). Rules for the application of the GDPR (General Data Protection Regulation) in BIBM. *BIBM*. https://bibm.eu/about/gdpr-compliance/

Bloxberg, D. (2022, August 1). A Brief History of the GDPR | Inspired eLearning Blog. *Inspired eLearning*. https://inspiredelearning.com/blog/a-brief-history-of-the-gdpr/

Bulgakova, D., & Bulgakova, V. (2023). The Compliance of Facial Processing in France with the Article 9 Paragraph 2 (a) (g) of (EU) General Data Protection Regulation. *NaUKMA Research Papers. Law*, *11*, 64–76. https://doi.org/10.18523/2617-2607.2023.11.64-76

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

Expert, P. (2022, December 16). *The main responsibilities of the data protection officer (DPO)*. Pandectes. https://pandectes.io/blog/the-main-responsibilities-of-the-data-protection-officer-dpo/

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Husain. (2024). *52 Biggest GDPR Fines and Penalties (2018—2024)*. https://www.enzuzo.com/blog/biggest-gdpr-fines

Kohl, U. (2023). THE RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW AND TWO WESTERN CULTURES OF PRIVACY. *International & Comparative Law Quarterly*, *72*(3), 737–769. https://doi.org/10.1017/S0020589323000258

Nielsen, M. S. (2024). *4 Major GDPR Challenges and How to Solve Them ➤*. https://www.stibosystems.com/blog/the-four-biggest-personal-data-challenges-of-the-general-data-protection-regulation

Oluwatosin Reis, Nkechi Emmanuella Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, & Temitayo Oluwaseun Abrahams. (2024). PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT. *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88. https://doi.org/10.51594/ijarss.v6i1.733

Oluwatoyin Ajoke Fayayola, Oluwabukunmi Latifat Olorunfemi, & Philip Olaseni Shoetan. (2024). DATA PRIVACY AND SECURITY IN IT: A REVIEW OF TECHNIQUES AND CHALLENGES. *Computer Science & IT Research Journal*, *5*(3), 606–615. https://doi.org/10.51594/csitrj.v5i3.909

Robinson et al.,. (2024a). *What is GDPR (General Data Protection Regulation)? Compliance and Conditions Explained*. WhatIs. https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

Robinson et al.,. (2024b). *What is GDPR (General Data Protection Regulation)? Compliance and Conditions Explained*. WhatIs. https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

Rumbold, J. M. M., & Pierscionek, B. (2017). The Effect of the General Data Protection Regulation on Medical Research. *Journal of Medical Internet Research*, *19*(2), e47. https://doi.org/10.2196/jmir.7108

Sarabdeen, J., & Mohamed Ishak, M. M. (2024). A comparative analysis: Health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). *International Journal of Law and Management*. https://doi.org/10.1108/IJLMA-01-2024-0025

Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, & Nkechi Emmanuella Eneh. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. *Computer Science & IT Research Journal*, *5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

Sullivan. (2024). *A Guide to Collecting Explicit Consent Under GDPR*. Transcend. https://transcend.io/blog/explicit-consent

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018a). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018b). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Yanamala, A. K. Y., & Suryadevara, S. (2024). *Navigating Data Protection Challenges in the Era of Artificial Intelligence: A Comprehensive Review*. *15*(01).