2025 Volume: 01 Issue: 07 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-17

LEGAL STATUS AND LIABILITY OF DATA BROKERS AND THIRD-PARTY DATA PROCESSORS

S.V.Divya*[1], P.Venkadesh[2], M.Pandeeshwari[3], Selvakumaran.G[4]

[1,3,4]Department of CSE,V.S.B College of Engineering Technical Campus, Coimbatore.

[2]Department of IT, V.S.B College of Engineering Technical Campus, Coimbatore.

Article Received: 13 November 2025
Article Revised: 03 December 2025
Published on: 23 December 2025

***Corresponding Author: S.V.Divya**
Department of CSE,V.S.B College of Engineering Technical Campus, Coimbatore.

DOI: https://doi-doi.org/101555/ijrpa.2359

INTRODUCTION

In this modern era the data brokers are the one who plays important role in managing an individual's information along with the third-party data processors .The main routine of a data broker collects and sell the personal information of the individual without their knowledge, while third party processors are the one who manages the data on behalf of other organization. These data broker and data processors are only responsible for user information . They play an important role in data economy. Using this data economy many companies improves their financial support by selling individual's personal data, this process of data into money is known as data monetization. In India Cyber threads can be reduced by some restrictions such as DPDP Act, IT Act . The data ecosystem is very important in the data economy process because in the data ecosystem the data are produced. The trust level between the data processor and the data controller are maintained by data processing agreement (DPA). Based on these agreements the data are transferred across the boundaries to various countries and these processes is known as cross-body transaction.

Data Brokers and Third-Party data processors

Data brokers [1] are the data providers in which they collect the data from various digital platforms such as website, public records and social media. The data that are collected from these platforms may sell it to the other organizations without the individual's knowledge for their own profit. Third-Party data processors are the organization they handle the data on-behalf of another organization they don't have any rights to use the data, their only purpose is to store the data. Let us consider one example for the third-party data processors. AWS is the

one of the third party organization, it provides many services to other organization like server and database to store their data, if a company has to use the services of the AWS they need to sign a Data Processing Agreement to clarify the rules and regulations between the data transfer and they just verifies that it was under the law or not. These data party organization can also maintain a backup storage for the stored data. The comparison between the Data controller and the Data broker is depicted in Table.1.

Table.1: Comparison between Data Controller and Data Broker.

Data Controller	Data Broker
Data controllers are the decision makers that decides how and why the data is collected and how the data is used.	Data brokers purchases and sells the personal data without the individual's knowledge.
Data controllers has direct relationship with the individuals	Data brokers does not have any direct relationship with the individuals
The data controller collects the data and use the data to provide a service and it helps them to manage the business operations.	The data brokers can sell the data for their own financial profit.
Data controllers follow the rules according to the laws like GDPR, DPDP.	They do not follow any laws
Example: In this modern era educational institutions uses digital platform in various way in one such case is they stores the information of their students in a secured platform which was built by the third-party data processors. These third-party data processors only collect the data they don't have any rights to use the data.	**Example:** An organization sells the users information without the user's knowledge.

2.1 life Data

Cycle-Overview

The overview of the data life cycle which is shown in fig.1 reviews about how the data can be collected, monitored, shared and stored safely under the rules and regulation as per the law.

Figure. 1: Data lifecycle overview

1. **Data Collection:** The data controller uses the online platform to collect the personal information of the individual without their concern.
2. **Data Transfer to Controller:** These collected data stores in the different container based on the category, this category is divided by the data controller in what way the data is to be used.
3. **Data Sharing with Third-Party Processor:** The data controller can't able to manage the bunch of data, they want to store data in a secured place. So, they need a help of third-party data processor under certain conditions.
4. **Processing by Third-Party data processor:** The Third-Party data processor have rights to store and analyze data that they don't have the rights to decide in what purpose the data can be used. It should controll by the data controller.
5. **Complaints and Security Checks:** The data controller and third-party data processor have to follow the laws which was instructed by our Government. The uses some techniques to follow these laws such as encryption and decryption.
6. **Return of data or deletion:** The data controller uses the data as to their own wish after this process the data are deleted or returned.
7. **Monitoring by data controller:** The data controller monitors the uses of the data thus the

data is utilized in a right manner or not.

8. **User access:** Every individual has their rights to access the data and these data can also be accessed by our government officials.
9. **Final Disposal:** After the completion of the process the data is used for any other purpose is to be stored if not it will be deleted.

2.2 Challenges

- The data brokers [2-3] work in a place where the people in that place where has no sufficient awareness about cybercrime laws.
- The data should be kept safe otherwise it leads to misusage of data.
- The data controller should maintain strict contract to third-party data processor otherwise there leads to unauthorizing access of the data.
- There are various laws to protect the data but the laws are may differ based on the country in a way that legal in some countries and illegal in another countries.
- The user doesn't have trust on the data controller because the user doesn't know that their can be accessed by anyone.
- If they misuse the data it leads them to come under severe punishments and big fines.

Data Economy

In this technical world, data is considered extremely valuable. Using these data one can do anything as they want and these data is collected and traded by some companies for their own benefits this system is known as data economy. It leads to data monetization.

Values of data economy:

- **Personalization:** Most of the e-commerce websites collect the data to provide personalized experience to the consumers.
- **Innovation:** Having a lots of data access helps to improve artificial intelligence, machine learning and smart technology like google voice assistant.
- **Economic growth:** Using the data some of the company follows some strategy to improve their economic growth such as, using these data they can understand the needs of the consumers based on the consumer needs they increases their stock values for their profit.
- **Efficiency:** Business uses current data to make better decisions that improves their efficiency of the company.

Risk of data economy

- Privacy invasion: Somebody is looking at our personal data without our permission.
- Security threats: Hackers try to access our personal data a financial data without our permission.
- Lack of transparency: An individual doesn't know what way that their data have been used.

Data Monetization

Companies earn money using our personal data. In this modern world we want to use various apps for our daily life, if we want to access the app, we have to accept the terms and conditions of that app. By accepting those terms and condition we have accepted all their requests. Because, of our acceptance the application can access our mobile's camera and it can detect were we are. What are all the information collected by the application are the investment of the business. Using that information, they can predict our daily needs and our wishes and it helps them to make it profit in the short duration of time. This is called data monetization. In simple words data monetization is the process of making money from collected information or data in different ways.

Responsibility of data controller

The main responsibility of the data controller is to prevent the data from the unauthorized access. They are the one who need to secure the data from the others without their knowledge we can't able to access the data. If we breach the law of the data controller then we will punish as per the law.

The data controller uses the secured platform to store the collected data in the secured platform. These secured platforms organized by the third-party company. These third-party organization has right to store the data their responsibility of the third-party data processor is to keep the data safe and secure, if they fail in their responsibility they can punish as per the law.

Challenges

- When different companies are using the same data source, if error is made it is very difficult to find who makes such error.
- An individual doesn't know what way that their data have been used.
- It makes data tracking difficult.

- There are various laws to protect the data but the laws are may differ based on the country in a way that legal in some countries and illegal in another countries.
- If anyone breached that law , we must need sufficient time to find who had made that mistake because of long duration of the time it makes difficult to track.

Cyber-Crime Laws

To avoid illegal activities through internet most of the Government introduce laws to reduce the rate of the cybercrimes. These cybercrimes can be cause by an individual or a group of people we have to take it serious otherwise it leads to serious consequences.Some of the laws are:

- Information Technology Act (2000) – India
- Information law and Criminal Code - Russia
- Computer Fraud and Abuse Act (CFAA) – United States
- Data protection Act (2018) – United Kingdom

Based on the above laws, the following activities are punishable,

- Hacking
- Identity theft
- Spreading Unwanted information

4.1 Difference between Legal and Ethical Responsibilities: The differences between the Legal and ethical responsibilities is shown in Table.2.

Table.2: Comparison between Legal and Ethical responsibilities.

Legal Responsibilities	Ethical Responsibilities
The legal responsibilities are based on some rules and regulations.	Our activities should be truthful to our heart and these activities should accepted by our norms.
These laws are designed by our government and the government officials.	These norms are decided by ourselves.
If we break the rules then we will punish by penalties and imprisonment.	If we break our norms then it makes us like dishonest person. It will damage our reputation.
Eg; Identity theft.	Eg: Tracking users' information without their information it may be legal and unethical.
It saves us from legal compliances.	It is used to promote our honesty and out responsibility.

4.2 Handling Personal data in Honest way

The manner of handling the individual's private information with respect and honest. It means that the individual should know that how their data are used i.e, data transparency, the

usage of data is very clear and should not lie about it. And should not take more data than required, don't use unwantedly. Companies must keep the data safely from the hackers. Every individual has rights to see, how their data will delete, change and used. Then they should know where and when their data should used and handled in an honest way, it helps to protect our data properly and stop the purpose of data misuse. It's not about just following the rules the main here is about doing the right thing. The above concept is the idea of handling personal data in honest way. In short,

- Ask permission before taking or using the common individual's data.
- Be honest about why should you use their data.
- Don't misuse the data without the individual's knowledge.
- Allow the individual to view, update or delete their data if they need.

4.3 Challenges faced by the current technology with traditional laws

- Most of the laws didn't explain how to handle modern technologies.
- The process of changes in technology goes fast but, the updating laws regarding to that is very slow.
- In some cases, old laws may not protect personal data securely.
- The modern technology is common, but the laws according to that is different in countries.
- It's very difficult to know who is responsible when the data is theft.

Definition of Cross-Border Data Transfer

Now let us discuss about cross border data transfer. The cross border data is the process of sending personal and professional information from one country to another country. This is important because if we want your website service all over the world then we can use it

5.1 Requirement of following laws

There are many laws to secure our data from unauthorized users some of the laws are GDPR [4], DPDP. There are more differences in these laws one differs from one another. The differences are,

- In the GDPR act the data can be sent to other countries which was approved by the European government and they have high data production .But in DPDP the Indian government will release a list of countries they will share their data with if we share the data with other countries then it will be punished under the law.

- Based on the GDPR act the agreement must be signed between the sender and the receiver But in the DPDP act the companies have to ensure that the data is processed based on the law in the secured manner.
- The GDPR act only focuses on the fundamental rights but the DPDP act focuses on both rights and the new innovations.

5.2 Punishment for not following laws

Based on the GDPR [5-6] act if we violate the act then we have to face a huge fine that is 4 percent of your annual income this act doesn't care about your annual income. This penalty depends on your actions and what you have performed. If the action is big then the company must face big consequences. For example: if a company sends our data to other countries without necessary safety measures then they will face a huge fine.

Based on the DPDP act if we violate the act then we have to pay a penalty up to 250Crore for single action and this penalty was decided by the Data production board of India. If the company fails to protect the individual's data then they will be punished under the law. For example: if the company shares an individual's data to another company without the approval of the board then they need to face the consequences.

5.3 Challenges

- Every country has their own rules to protect their data that means action is legal or illegal is based on the country.
- Every company should get permission from the individuals before they send their data to another country.
- Some countries don't have enough security measures to ensure the security of the data may be accessed by the unauthorized users in other words Hackers.
- Companies must make sure that the data remains the same it is not changed or stolen before the transaction to other countries.
- This transaction is based on the contracts and agreements between two companies or countries.
- If the companies violate the law then they will be punished under the law the actions are putting fine and it leads to ban.
- In some case the Data transfer can be delayed by the government because of the political issues or for legal reasons.

5.4 Case studies

1. Meta (Facebook) GDPR ACT:

Issue happened:Facebook sent the information of the European users to the USA for the storage purposes and processing.

Problems:The European government said that the US doesn't have enough security to secure the information of the European users this case came under the GDPR act.

Result:In the year of 2023 the Meta paid a penalty amount of 1.2 billion dollars which was the highest penalty which was paid ever and they stopped the data transfer between Europe and the US

Percussions: Every company should maintain the strong agreement between sending and receiving countries if meta does it right then they can easily avoid that penalty.

2. Google Analytics (Banned in some European countries)

Issue happened:Some of the European countries says that using the Google Analytics was against the GDPR act[7-8].

Problems: When the people visited the websites using Google Analytics their data was sent to the USA and they have accepted by the US officials.

Result:Data protection board ordered the website owner to stop using Google Analytics and insist to improve the security features.

Percussions: Every simple tool must be examined because a tool can transfer data to away borders.

II. How Laws Assign Legal Responsibilities

The laws [9] find out who is responsible by seeing what each person did. For example, data controller is the only responsible for taking decision for how and when the data should use, so the data controllers having more responsibilities than the data processors. Many people are the part of the mass systems like Technology and HealthCare, the law checks the for the person who took the important decision. This way, laws aim to ensure fairness and accountability.

6.1 Importance of Securing Data in Companies

There are some security strategies helps companies to secure our data from unauthorized access and it should under the law. One such strategy is risk mitigation strategy, based on this strategy they have using strong password to secure our data and they used for some other purpose also like updating software etc,. They also creates awareness to their workers about

this strategy to and ensure that all should follow to secure all the data to reduce risk.

III. Representative for Data Management

We can't find out the responsible one for the data management because data management includes various steps they are, data storing, processing and sharing. Based on these functions there are multiple peoples working on it. They are,

- Data Controllers
- Data Processors
- Third-Party data processor
- Insiders
- Without knowing the laws

7.1 Data Ecosystem:

Data ecosystem is an environment which consists of various organizations they can perform different functions like storing, sharing, processing. These processes are depending on one another.

7.2 Relationship between data economy and data ecosystem

The data ecosystem is the which is more important for the data economy because in the data economy the data are sell or bought by someone for financial support but data are formed by data ecosystem without data, they can't run data economy. Let us consider data ecosystem as an agriculture land. Here the data are cultivated crops and the selling or trading area is known as data economy. In simple words without data ecosystem data economy can't able to run.

7.3 Life cycle of data ecosystem

The life cycle of the data ecosystem as shown in fig.2 shows how one another depends on each other that is based on the data usage. There includes, data collection, data storage, processing of the data, data sharing [10-11] , data use and the disposal of the data.

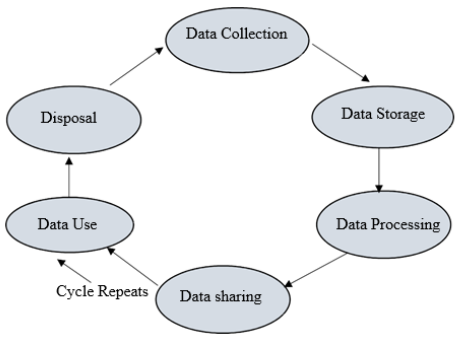

Figure. 2: Lifecycle of Data ecosystem.

Data Collection: Data collection is the process of collecting the data from online platforms such as, Flipkart, Amazon, Instagram, Facebook, etc,

Data Storage: The next process of data collection is data storage; in this process the collected data are stored in a secured place that the stored data can't accessed by unauthorized process.

Data Processing: Data processing is nothing but the changing the data into meaningful information which helps the organization to get more information about the data. Data process consists of various operations such as data collection, data storage, data transformation, data analysis and data retrieval.

Data Sharing: Data sharing is nothing but sharing the collected data from one to another under the cyber-crime laws, we can also share the data over the boundaries but as per the rules and regulations of cyber-crime laws.

Data Use: Data use is nothing, using the collected data as their wish, using the collected data they can know what the individuals like to do.

Disposal: After the fetching all the information from the data. The data can be used as needed, and it will be disposed of properly when it is no longer required.

7.4 Case Studies

7.4.1. Equifax System (USA, 2017)

Issue Happened: The Equifax systems were hacked by unauthorized users because the company doesn't rectify the problem in their software which was already known to them.

Problems: The data of 147 Million people has been stolen, these data include many information-like passwords, date of birth. The company doesn't expose the problem to the consumers that the security was not good as they think.

Result: The company had paid the penalty of 700 Million Dollars for their insecurity of data and also, they lost their fame. After seeing the fall of this company other companies planned to improve their security level to overcome the penalty.

7.4.2. Facebook–Cambridge Analytica (UK/USA, 2018)

Issue Happened: Facebook allows a third-party app to collect the information of Facebook users without the users' concern and they use it for political acts.

Problems: The Facebook users doesn't know that their data has been shared the Facebook doesn't know in what way the data has used and it makes high controversy for their trust.

Result: Because of this case it peoples and law makers are have awareness about data ethics and concern. It makes lots of changes in privacy policy. The Facebook has paid $500,000 in

UK.

7.4.3. Yahoo Breach (USA, 2013–2014)

Issue Happened: Over 3 Billion accounts have been hacked by hacker and the data have stolen. It was the biggest data breach ever happened in the world.

Problem: Problem: The security features of yahoo was very weak they don't inform the users that their data have stolen. The company was not active about this data breach.

Result: Yahoo paid 117.5 Million Dollars as legal settlements and the share value of the Yahoo has been dropped up to 350 Million dollars. Then it was hand-over to Verizon, this incident is the great example for miscommunication of consumer and producer.

7.5 Risks in the Data Chain: Third Parties and Shared Responsibility

Process of Risk management as shown in fig.3 includes four process namely, introduction of organizational standards, third-party risk evaluation forms, execute external evaluation, processing.

Figure. 3: Risk Management Process.

7.5.1 ***Introduction of Organizational Standards:*** Organization standard are the rules and regulations that the company want to follow to reduce the risk from the cybercrimes by following the law, they can ensure the safety of the data and it built the trust between user

and the organization.

7.5.2 ***Third-Party risk evaluation forms:*** The third-party risk evaluation form is used to find our suitable client who agrees our rules and norms in data sharing as well as data storage and security using these forms, we can also create a trust wall between client and our organization.

7.5.3 ***Execute an external evaluation:*** They helps to find the genuine client by verifying the company's information such as certificates like ISO and their reputation and the trust among the public about the company. It gives some suggestion about the company.

7.5.4 ***Process the reviews:*** After the completion of external evaluation it gives some suggestion that are verified by the user and then they finds an genuine client by processing the above reviews given by the external evaluators.

Role of Data Processing Agreement

Data processing agreement is nothing but a legal agreement between data controller and data processor, it ensures the security of the data. The data controller and the data processor follow the terms and conditions that mentioned in the agreement both should follow the agreement without any deviation.

8.1 Importance of Data Processing Agreement

Based on this agreement all information are kept safe. Before the cross-border transactions, the sender and receiver must sign a DPA contract between them which was mentioned in the norms of the law.These agreements clearly show who is responsible for the data and how the data is to be handled.This agreement reduces the sharing of data between one company to another company for unwanted reasons.Based on these transactions there was belief between send and the receiver which makes it safe and secure.

IV. Advantages and Disadvantages of Key Players of Data-Ecosystem

9.1 Data Brokers : The advantages are discussed below:

- Making advertisements by focusing common peoples to understand about them.
- People can see that they what actually interested in, like products etc.,
- To approve loans and policies the companies like bank insurance companies are using brokered data to check out the risks quickly.
- The data that have collected by the data brokers can be used in market research, public trends and business planning.
- They can access useful customer data without they asset it as their own.

Disadvantages of Data Brokers

- The people don't know that how their data are used after the collection.
- Data collected by the data brokers may be used without the person's knowledge.
- It is difficult to say that how our data are used after collecting.
- If someone broke the data broker's system the large amount of data of the individuals can be leaked
- It causes trouble to the data brokers when the individual's data leaked out.

9.2 Third-Party Data Processors Advantages

- Companies spend less money to hire the people they handle instead of handling their own data.
- They use modern tools and they have more experienced teams to protect the data in the right way.
- Easy to handle large amount of data without adding new tools.
- They don't have to worry about the other things they can focus on their main work.
- Their systems and technology may be more advanced what's available inside the company.

Disadvantages

- If the protection is didn't strong, the data may be get hacked or leaked.
- Third-Party data processors can't able to always manage the data once it was handover.
- If the processors don't follow the data protection laws, the company hired them also get in trouble.
- If the contracts and the updates between the company and the third-party data processor is not clear it will lead to unexpected issues.
- If the third-party data processors are not clearly monitored, they may be misuse the data for their personal financial profits.

9.3 Cross Border Data Transfer Advantages

- This helps the company to work across the boundaries it helps them to improve their company worldwide.
- Using this technique people can work together with different people in different locations it leads to the birth of new innovations.
- Companies can use cloud storage to store their data it makes it very efficient.

- This technique is used to improve the economic value of your company in the short duration of time
- It helps companies to provide services like online shopping in online platforms it doesn't matter where they are.

Disadvantages

- It may be weak in security of data storage
- Different countries have different laws for cyber security which makes us confused.
- Data may be hacked by unauthorized users while being sent across boundaries.
- We may lose control of the data once it goes out of our country.
- It provides an unsecured feeling to the common man they don't have any knowledge about it.

9.4 Cyber-Crime : The advantages and disadvantages of cyber crime acts like GDPR, DPDP are discussed below:

Advantage

- It makes the data safe and secure.
- Using these laws, a common man can question a company about their own data the company needs to answer them based on the law.
- Every company should follow these rules without any fail.
- Because of this act the interaction between the company and the common man gets increased.
- Based on these laws the company should get permission from the respective people whose data he wants to sell.

Disadvantage

- This is very expensive.
- These laws are difficult to understand.
- These laws may slow down the new innovations because of the safety of the company.
- It is very difficult for the government to find that all the companies are following laws are not.
- Companies in different locations may face many problems than local companies.

V. CONCLUSION

The above paper explores the role of data broker, data controller and data processors and it shows what are the differences between data controller and data brokers. It gives elaborate information about the life of the data and the challenges faced in the data life cycle. It briefly explains about the data economics and its values and what are all the risks faced in the data ecosystem and the way of using data economics and it shows the relationship between data ecosystem and data economy. It clearly explains the responsibility of the data controller and the challenges faced by the data controller. By this paper we can get knowledge about the Cyber-Crime laws like (DPDP act). It differentiates how legal responsibility differs from ethical responsibility and the way of using the data and what are all the challenges faced while using the data. It tells what cross border data transfer is and its importance and the challenges faced while using this technique. We can understand this paper while we see the case studies. It shows the definition of data ecosystem and the relationship between data economy and data ecosystem and the life cycle of the data ecosystem. The role of data processing agreement in the data protection process and its importance and it explains the advantages and disadvantages of key players of the data ecosystem and Cyber-Crime acts. This paper offers a clear idea about the data ecosystem and technologies used for data protection and the laws to secure it.

REFERENCES

1. C.-L. Yeh, “Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers,” *Telecommunications Policy*, vol. 42, no. 4, pp. 282–292, 2018, doi: 10.1016/j.telpol.2017.12.001.
2. U. Reviglio, “The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview,” *Internet Policy Review*, vol. 11, no. 3, 2022, doi: 10.14763/2022.3.1670.
3. Ruschemeier, “Data Brokers and European Digital Legislation,” *European Data Protection Law Review*, vol. 9, no. 1, 2023, doi: 10.21552/edpl/2023/1/7.
4. T. Urban, D. Tatang, M. Degeling, T. Holz, and N. Pohlmann, “Measuring the Impact of the GDPR on Data Sharing in Ad Networks,” in *Proc. 15th ACM Asia Conf. on Computer and Communications Security (ASIA CCS ’20)*, 2020, pp. 222–235, doi: 10.1145/3320269.3372194
5. J. Menezes Cordeiro, “Civil Liability for Processing of Personal Data in the GDPR,” *European Data Protection Law Review*, vol. 5, no. 4, 2019, pp. 538–552, doi:

10.21552/edpl/2019/4/7

6. P. T. J. Wolters, "The security of personal data under the GDPR: A harmonized duty or a shared responsibility?," *International Data Privacy Law*, vol. 7, no. 3, pp. 165–178, 2017, doi: 10.1093/idpl/ipx008
7. R. Becker, A. Thorogood, J. Bovenberg, C. Mitchell, and A. Hall, "Applying GDPR roles and responsibilities to scientific data sharing," *International Data Privacy Law*, vol. 12, no. 3, pp. 207–219, 2022, doi: 10.1093/idpl/ipac011.
8. P. W. J. van Beek and R. Akkermans, "Between the Data Act and the GDPR: Attributing responsibility for personal data protection," Yearbook of Antitrust and Regulatory Studies, vol. 17, no. 29, pp. 87–106, 2024, doi: 10.7172/1689-9024.YARS.2024.17.29.4.
9. T. Herbrich and E. Niekrenz, "Privacy Litigation Against Real-Time Bidding—Data-driven online marketing: Enforcing the GDPR by protecting the rights of individuals under civil law," Computer Law Review International, vol. 22, no. 5, pp. 129–141, 2021, doi: 10.9785/cri-2021-220502.
10. Napieralski, "Between the Data Act and the GDPR: Attributing Responsibility for Data Sharing," Yearbook of Antitrust and Regulatory Studies, vol. 17, no. 29, pp. 127– 146, Jan. 2024, doi: 10.7172/1689-9024.YARS.2024.17.29.4.
11. Giannopoulou and V. Ferrari, "Distributed Data Protection and Liability on Blockchains," in Internet Science – INSCI 2018, S. Bodrunova, et al., Eds., Lecture Notes in Computer Science, vol. 11551, Cham, Switzerland: Springer, Apr. 2019, pp. 195–208, doi: 10.1007/978-3-030-17705-8_17.