

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

© 2021 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at submission@ijlmh.com.

A Study on Law Relating to Data Protection in India

B. MADHANA¹

ABSTRACT

This paper deals with the privacy issue in India faced by the people who use online as a means of communication, transaction, shopping etc., People with or without knowing tend to share their personal information in websites without even having knowledge whether the website is legally protected or not. When people share their data online fraudsters make this a platform to loot the personal information that are shared by the people. Privacy rights are enforced under the Indian Constitution and the Information Technology Act 2000, whereas the Indian Contract Act 1872, the Copyright Act 1957 and the Indian Penal Code 1860, protect property rights. An individual's right to privacy has evolved out of Article 21 of the Constitution and other constitutional provisions protecting fundamental rights.

Article 21 of the Constitution provides that no person shall be deprived of life or personal liberty except according to the procedure established by law. The Supreme Court of India has held in a number of cases that the right to privacy is implicit in the right to life and personal liberty guaranteed to Indian citizens. However, constitutional rights can normally be claimed only against the State or State owned enterprises and not against private individuals or establishments. The IT Act also prescribes penalties for hacking which is tampering with a computer's source code and any breach of confidentiality and privacy obligations by a person having powers under the IT Act. Under the IT Act a network service provider or an intermediary is liable for any known misuse of third party information or data or for not exercising due diligence to prevent the offence.

Keywords: Information Technology, Data Protection.

I. INTRODUCTION

India's business, data and knowledge process outsourcing industries have been growing significantly in the last few years. However various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. Unlike the US or the European Union, India does not have a data protection law. In the absence of specific

¹ Author is an Advocate at Madras High Court, India.

legislation, data protection in India is achieved through the enforcement of privacy and property rights. Privacy rights are enforced under the Indian Constitution and the Information Technology Act 2000, whereas the Indian Contract Act 1872, the Copyright Act 1957 and the Indian Penal Code 1860, protect property rights. An individual's right to privacy has evolved out of Article 21 of the Constitution and other constitutional provisions protecting fundamental rights. Article 21 of the Constitution provides that no person shall be deprived of life or personal liberty except according to the procedure established by law. The Supreme Court of India has held in a number of cases that the right to privacy is implicit in the right to life and personal liberty guaranteed to Indian citizens. However, constitutional rights can normally be claimed only against the State or State owned enterprises and not against private individuals or establishments.

The Information Technology Act, 2000 penalizes cyber contraventions section 43(a) to (h) and cyber offences (sections 65-74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers serious offences like tampering with computer source code, hacking with an intent to cause damage and breach of confidentiality and privacy all of which attract criminal prosecution. The IT Act also prescribes penalties for hacking which is tampering with a computer's source code and any breach of confidentiality and privacy obligations by a person having powers under the IT Act. Under the IT Act a network service provider or an intermediary is liable for any known misuse of third party information or data or for not exercising due diligence to prevent the offence. An intermediary is defined as anybody who receives, stores or transmits a particular electronic message on behalf of another person or who provides any service with respect to that message. Therefore, an Indian Business Process Outsourcing (BPO) company may be liable as a network service provider because it acts as a service provider and receives and transmits information or data. The IT Act covers offences and contraventions committed outside India as well irrespective of the offender's nationality as long as the computer system or network is located in India.

Data can be broadly classified into public data and personal data. Public data is that which is accessible to the public at large, such as, Court records, birth records, death records, basic company details. On the other hand, private data is personal to an individual/ organization and cannot freely be disseminated by anybody without the prior permission of the subject. It includes financial details, family details, browsing details, preferences, psychological characteristics, locations and travel history, behavior, abilities, photographs, aptitudes, and the like. It could also be a combination of these features or even inferences drawn from the refined

data. At the moment, India does not have a specific legislation enacted primarily for data protection. India's regulatory mechanism for data protection and privacy is the Information Technology Act, 2000 and its corresponding Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. In addition to this, personal data is also protected under Article 21 of the Indian Constitution which guarantees to every citizen, the Right to Privacy as a fundamental right¹. The Supreme Court has held in a number of cases that information about a person and the right to access that information by that person is also covered within the ambit of right to privacy².

(A) Objective of Study

The objectives of the study are as follows:

- to analyze the data protection policies in India
- to study about the legislations which governs the data privacy and the maintenance of secrecy in data protection.
- to analyze whether people are aware of data protection
- to know about the frequently faced issues by the users

(B) Hypothesis of Study

The usage of internet is more in Urban group³ than the Rural group⁴ and the data is shared online by the Urban group which leads to online crime and data theft.

(C) Review of Literature

Gerardus Blokdyk (2019) in his book named 'Data Privacy a complete Guide' states about the scope and the resources needed for data protection and he also states about the diagnose data privacy project, initiatives, organizations and to also implement evidence based practice strategies and to integrate recent advances in Data privacy.

Raj Rathour in his book named Data Privacy Law and Compliance guidebook intends to provide data privacy professionals with an over view of the fundamentals of data privacy law and to serve as a quick reference for the other data privacy concerns. It mainly focuses on the technical aspects of data privacy and also data breach.

Maja Brkan in his book Courts, Privacy and Data Protection in Digital Environment in the year 2017 reveals the significant role Courts play in the protection of privacy and personal data

² Personal data protection Laws in India, by RK Dewan & Co. , <https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d>

³ People living in Urban areas

⁴ People living in Rural areas

within the new technological environment.

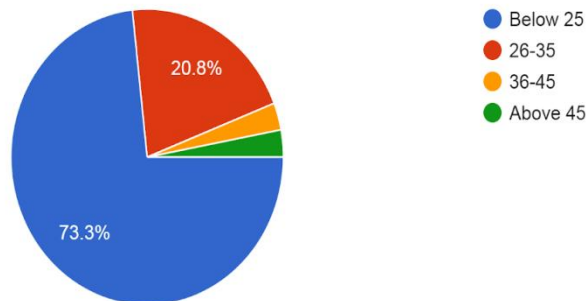
Navi in his book Personal Data Protection Act of India (PDPA 2020) captures the complexities involved in creating a law that tries to protect the human right of privacy with controls on the processing technology without adversely affecting the value of personal data to businesses as a productive asset. The book provides a good foundation to all stakeholders on how to understand and practice data protection and also throws some useful tips of using technology as a tool of data protection.

Anghrija Chakraborty, Ashima Obhan, Amar K Sundram in their book named data Protection Laws Demystified addresses the issues of privacy and protection of personal data as well as client confidential data, especially brought to the fore by the European Union (EU) General Data Protection Regulation, the new draft of the Indian Data Protection Bill 2018 submitted by the Justice B. N. Srikrishna Committee on personal data protection in India, and other major privacy and personal data protection related legislative developments worldwide.

II. RESPONSES

Age

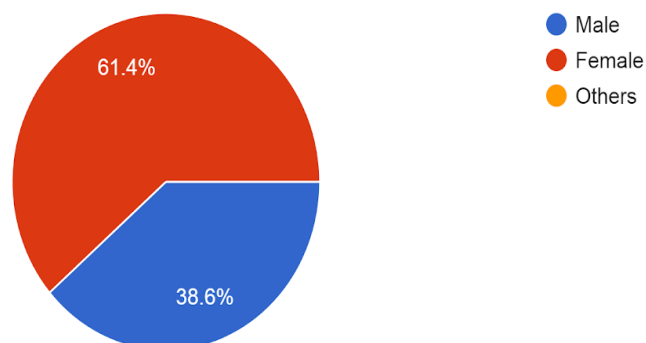
101 responses



The age group below 25 shows the maximum of 73.3%, which clearly shows that the internet is used majorly by youngsters.

Gender

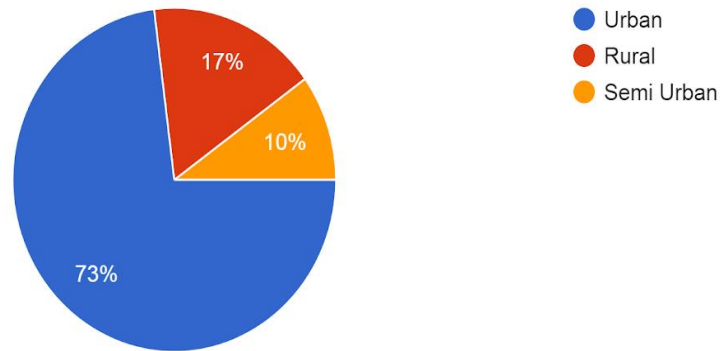
101 responses



Out of 101 responses, 39 individuals are male and 62 individuals are female respondents respectively.

Geographical location

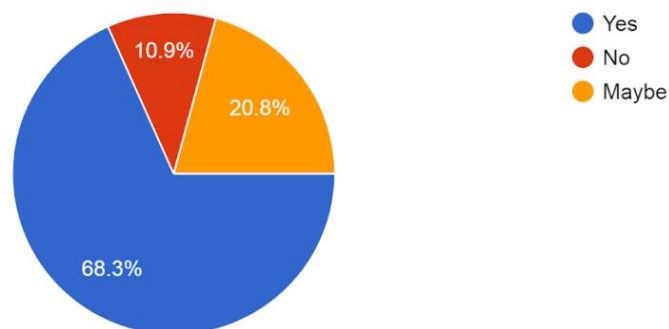
100 responses



Out of 100 responses, 73% are from urban location, 17% are from rural location and 10% are from semi urban location. Therefore the maximum respondents are from metropolitan cities and people in urban locality are more prone to the use of internet. Since they are more prone to the use of internet the online crimes in the urban areas keeps developing do to the lack of data protection.

Do you think using the Internet for shopping and banking would make your life easier?

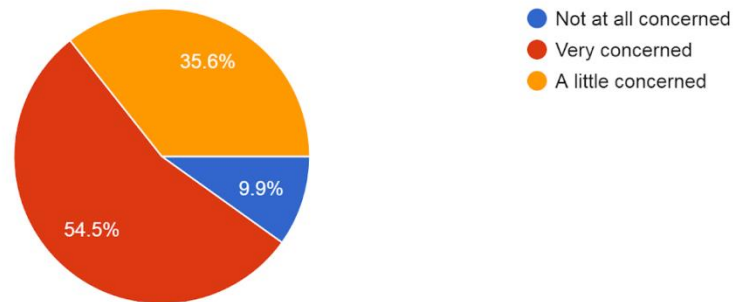
101 responses



Here the individuals who thinks that using internet for shopping and banking purpose makes their life easier are 68.3% (69 respondents), the individuals who are against the use of internet for shopping and banking purposes are 20.8% (21 respondents). Thus, it is proved that people wants to lead a easier life and so they use online shopping and banking.

How concerned are you about security for sharing the data online?

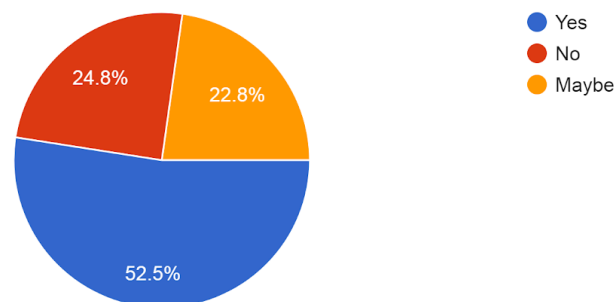
101 responses



The individuals out of 101 responses got a majority of 54.5% as they are very concerned about the security for sharing the data online and 35.6% respondents are little concerned about the security for sharing data online and 9.9% respondents are not at all concerned about the security while sharing data online. Thus people are always very much concerned about the safety and security when they share any data online.

Do you prefer online shopping?

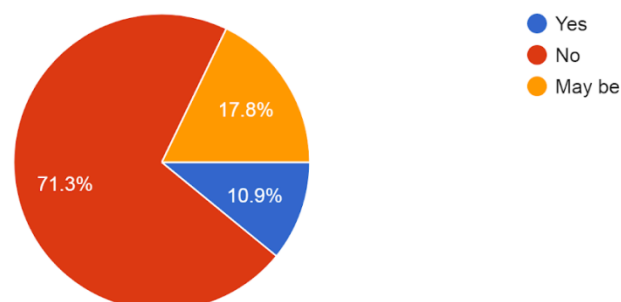
101 responses



Here the out of 101 responses, the maximum 52.5% (53 respondents) prefer online shopping, 24.8% (28 respondents) do not prefer online shopping. Hence in this present generation due to the vast development in technology people prefer online shopping.

Do you share personal information with your family or friends?(Example: Password, CVV, ATM PIN etc)

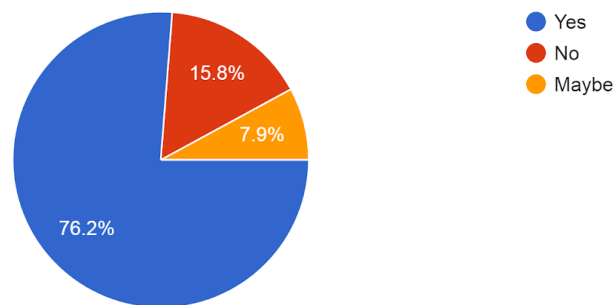
101 responses



When it comes to sharing of personal information like CVV, ATM pin, with friends and family 71.3% (73 respondents) do not share any of the personal information, 10.9% (11 respondents) share their personal information with friends and family, and 17.8% (18 respondents) may or may not share the personal information with regard to the situation. Hence the maximum respondents do not share CVV, ATM pins with friends and family.

Will you report if there is a security breach in any of your online account?

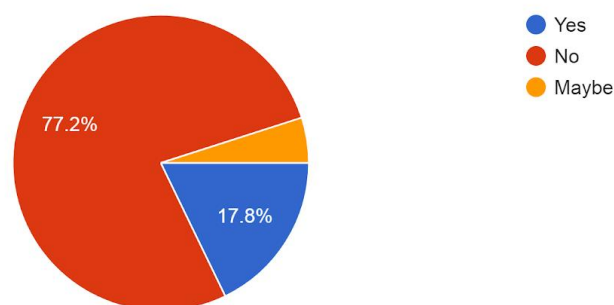
101 responses



Here 76.2% (77 respondents) states that they will report if there is any security breach in any online account. 15.8% (16 respondents) states that they would not report in case of any security breach in any online account. Hence the maximum people are aware of the security breach while using online account.

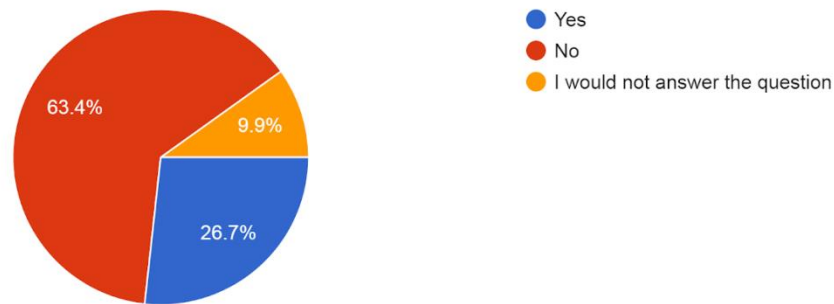
Have you ever come across any unauthorized money transaction online?

101 responses



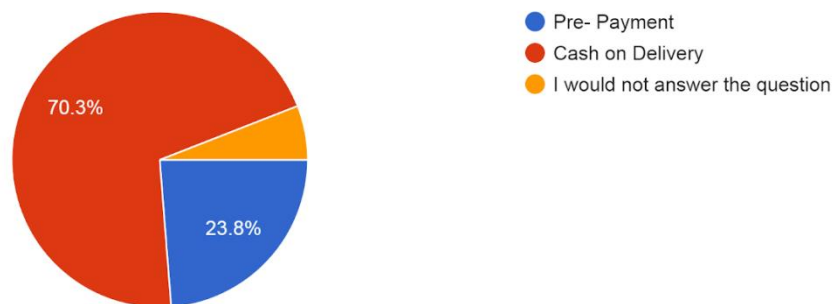
In the above figure, 77.2% of individuals have not come across any unauthorized money transactions online and only 17.8% of individuals have come across unauthorized money transaction online. Thus it is clear that there are only rare cases on unauthorized money transactions online.

Do you have your card details saved on any online website?
101 responses



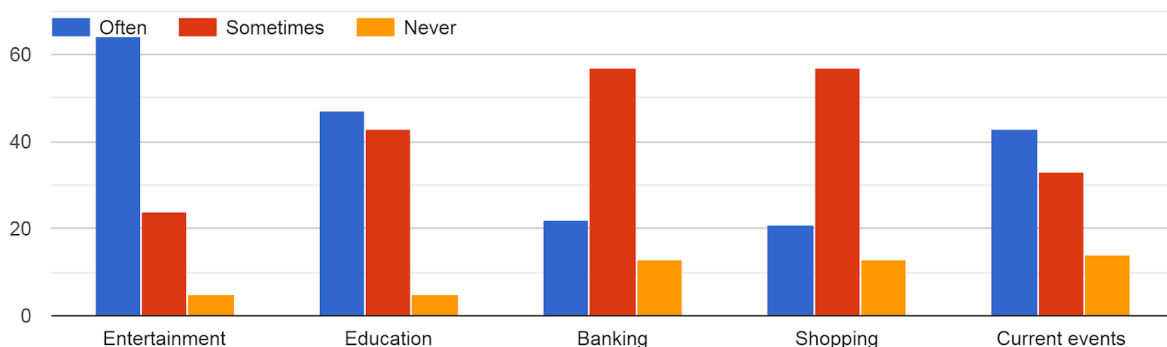
Here 26.7% individuals have saved the card details on online websites and 63.4% individuals have not saved the card details on online websites. Hence people are aware of their data protection and so they do not save any of their card details online.

Do you prefer pre-payment or cash on delivery while shopping online?
101 responses



Here out of 101 responses, 70.3% individuals prefer cash on delivery while shopping online and 2.8% individuals prefer pre payment while online shopping. Thus the maximum respondents prefer cash on delivery in order to avoid online transactions.

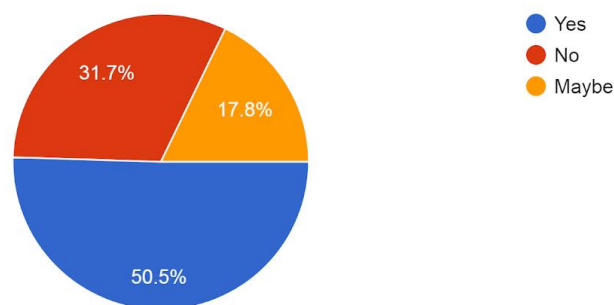
How often do you use Internet for the following purposes?



In the above figure it clearly denotes that people use internet often for entertainment purpose. Internet is very essential in the present era for day today life. People also use internet sometimes for banking and shopping purposes. So it is very clear that the respondents use internet to the maximum for entertainment and next for banking and shopping purpose, whereas the use of internet is very less in case of education purposes and also for the current affairs.

Have you been asked to provide personal information at websites you visit?

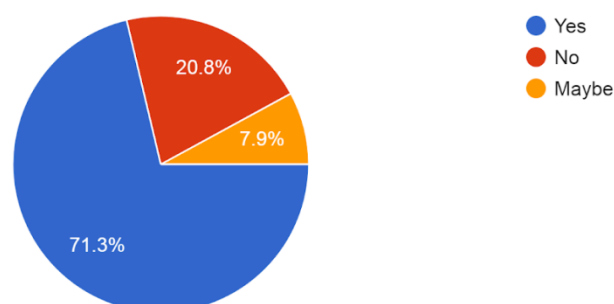
101 responses



Here out of 101 responses, 50.5% (51 respondents) answered that they had been asked to provide personal information at websites they visit, and 31.7% (33 respondents) answered that they have not been asked to provide any personal information at websites they visit. Hence it is proved that most of the websites ask the users there personal information in order to access websites.

Do you consider sites recording your Internet activity with/without your knowledge to be a violation of privacy?

101 responses

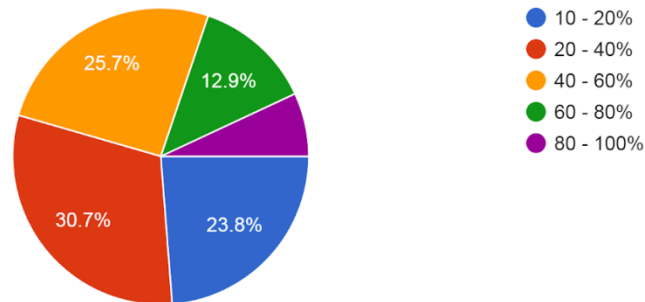


In the above figure it clearly states that 71.3% (72 respondents) state that the sites recording internet activities with or without the knowledge as violation of privacy. 20.8% (21 respondents) state that the sites that are recording the internet activities with or without knowledge is not a violation of privacy. The maximum respondents consider that recording the

internet activities as violation of privacy.

If it is must to provide the personal details on the website, what will be the percentage you would provide false information?

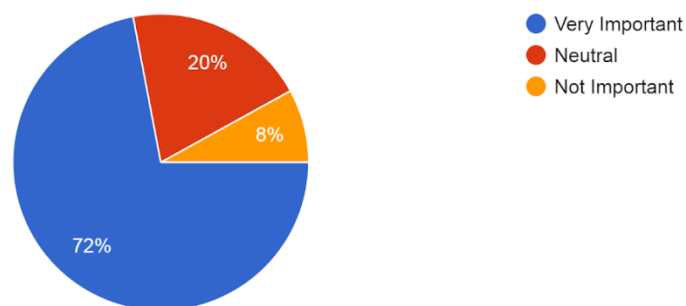
101 responses



Here out of 101 responses, 30.7% (31 respondents) chose to provide 20-40% false information in the websites asking personal details, 25.7% (26 respondents) chose to provide 40- 60% false information in the websites asking personal details, 23.8% (24 respondents) chose to provide 10-20% false information and 12.9% (13 respondents) chose to provide 60-80% false information in the websites asking personal information.

According to you how important is one's consent necessary when the web sites sell or share your personal details with others?

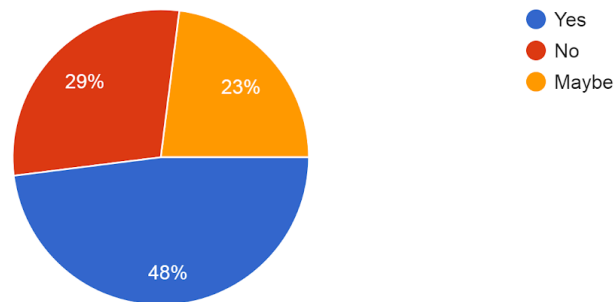
100 responses



One's consent is very necessary when the websites sell or share the personal details with others and 72% (72 respondents) have agreed and answered that it is very important, 20% (20 respondents) are neutral and 8% (8 respondents) state that one's consent is not necessary when the web sites sell or share their personal details with others. Hence it is proved that the maximum respondents chose that one's consent is very much important in case of sharing any personal details with others in order to avoid online offences and also to protect the data.

Have you been asked to provide personal information at websites you visit?

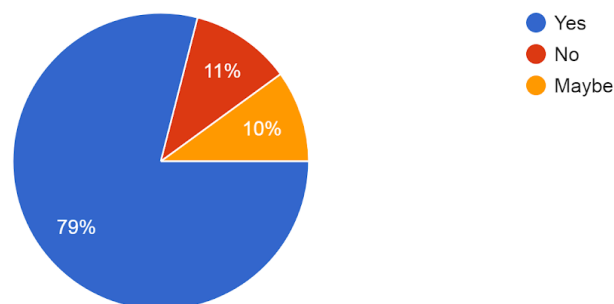
100 responses



Here in the above figure, 48% (48 respondents) were asked to provide personal information at websites they visit, 29% respondents have not been asked for any information at websites they visited and 23% respondents states that may be they have been asked to provide their personal information in web sites they visit. The maximum states that the websites always ask for personal information in order to access their websites.

Do you suggest that there should be an update in law and amendments to avoid Data theft and cyber crime?

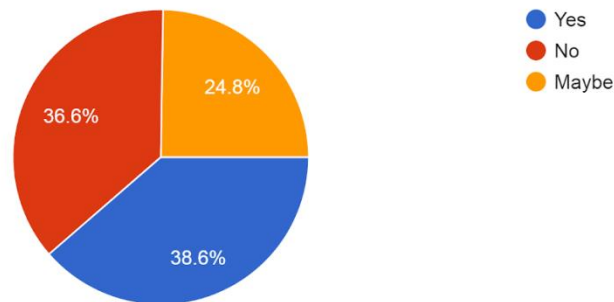
100 responses



Here 79 respondents states that there should be an update in the law and amendments have to be made in order to avoid data theft and cyber crime, 11 respondents state that it is not necessary for any amendments with regard to the laws relating to data theft and cyber crime and 10 respondents state there may be amendments brought in according to the present era. Thus it is proved that the maximum respondents suggest that there should be an amendment in law relating to cyber crime and data theft considering the development in technology, because as the technology keeps developing the crime rates also keeps increases. Hence amendments on laws is necessary.

Will you suggest you friends, relatives etc to prefer Online method rather than traditional method?

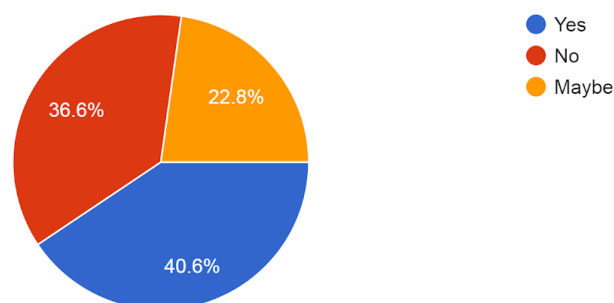
101 responses



Online method and traditional method has its own advantages and disadvantages. Out of 101 responses, 38.6% (39 respondents) states that they would suggest online method to their friends and relatives rather than traditional method, 36.6% (37 respondents) states that they would suggest traditional method rather than online method and 24.8% (25 respondents) states that they may suggest the online method rather than the traditional method. Though technology keeps developing, people still use the traditional method and only the youngsters and the educated people tend to use the online method.

Do you know any legal aspects related to data protection?

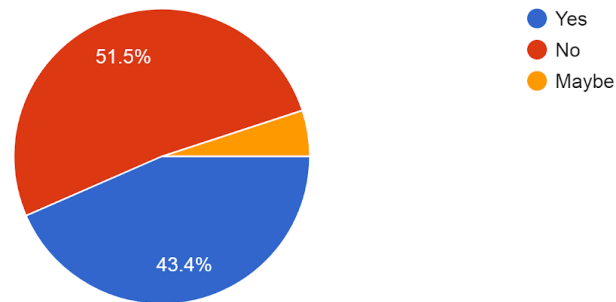
101 responses



Here out of 101 responses, 40.6% (41 respondents) states that they are aware of the legal aspects related to data protection, 36.6% (37 respondents) states that they are not aware of the legal aspects related to data protection and 22.8% (23 respondents) states that they are not sure about the legal aspects relating to data protection. people having legal knowledge would have some idea on the legal aspects on data protection apart from that the common man should also have some knowledge with regard to data protection.

Have you ever given online complaint?

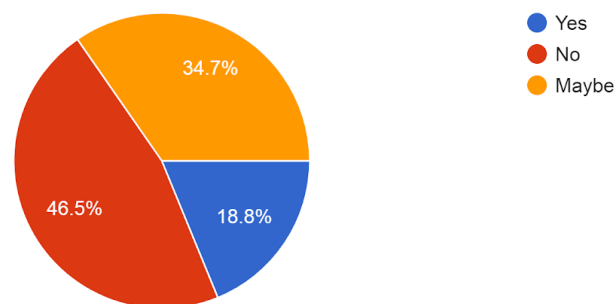
99 responses



Here in the above figure, it states that 43.4% (44 respondents) have given online complaint and 51.5% (52 respondents) have not given online complaint. Hence the maximum has not given any online complaints.

Do you agree the present legislation relating to data protection is effective?

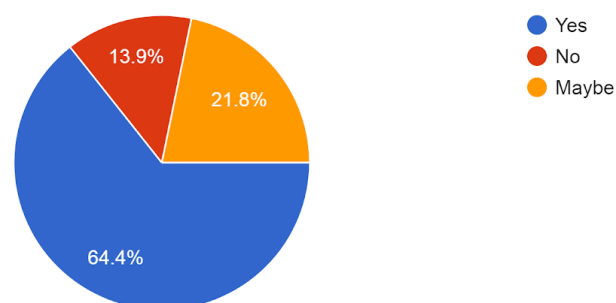
101 responses



Out of 101 responses, only 18.8% (19 respondents) agree that the present legislation relating to data protection is effective, 46.5% (47 respondents) states that the present legislation relating to data protection is not effective and 34.7% (35 respondents) states that there may be an effective legislation relating to data protection. The maximum number of respondents states that the present legislation relating to data protection is not effective.

Does data privacy increase the percentage of online users?

101 responses



Here from the above figure, 64.4% (65 respondents) agree that data privacy increase the percentage of online users, 13.9% (14 respondents) states that data privacy does not increase the percentage of online users and 21.8% (22 respondents) states that there may be a chance that the data privacy increases the percentage of online users.

III. RESULT – CONTINGENCY TABLE

| Area and Assessment | Higher Assessment | Lower Assessment | Total |
|---------------------|-------------------|------------------|-------|
| Urban | 32 | 26 | 58 |
| Rural | 25 | 17 | 42 |
| Total | 57 | 43 | 100 |

IV. CONCLUSION

Hence it can be concluded that :

- 73% of the population from the Urban areas are more prone to the use of internet than the people in Rural areas.
- The Respondents also said that they have been asked about their personal information in the websites they visit.
- Out of all the responses, it is very clear that people nowadays wanted everything to be online which is easier and time saving. All the citizens are becoming netizens due to the vast use of internet in our day today life.

Therefore it can be assumed that the people in urban areas were more prone to the use of internet when compared to the people living in the rural areas. Since the use of internet keeps increasing day by day, the crimes relating to online also keeps increasing. So it is very essential to protect our data in order to avoid online crimes. However various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. Health data comprises of a variety of information such as a patient's age, contact information, pathological reports, digital health records, medical history. It has immense value in the healthcare and pharmaceutical sector. People use fitness apps, gadgets like Fibits, etc. Some of us may have searched health information online or signed up for a free diagnostic check-up or may have claimed health insurance. Each time when we do any of these, we share our sensitive data related to our health with various entities.

The IT Rules only protect a limited set of information like physical, physiological and mental health conditions; sexual orientation; medical records, and history, and hence a major part of health data is left uncovered. The compliances under the IT Rules are also limited to obtaining consent before the collection or transfer of private data or publishing a privacy policy. The survey was conducted in small geographical dispersion; hence the results obtained are indicative and not exhaustive. It can be further explored at a wider level.

After a through study and calculation in Knowledge, Involment and Assessment, it is found that there is good knowledge from people belonging to urban areas when compared to the people of rural areas. In case of involvement it is found that there is poor involvement in rural areas when compared with urban. Finally normal response has been obtained from both rural and urban in the case of assessment.

Thus from the study, it is apparent that there is more awareness among the people belonging to urban region and steps have to be taken in order to create awareness among the people living in rural region. Such a step may definitely help the public to make a move in its way and also to use the proper use of internet and also for data protection. The spread of the awareness alone is not a remedy but still reformative steps must be taken by the authorities in order to regulate implementation.

V. BIBLIOGRAPHY**(A) Primary Source**

- The personal Data Protection Bill, 2018
- The Information Technology Act, 2000

(B) Secondary Source

- Will India's proposed Data protection Law protect privacy and Promote growth?, by Aniruth Burman, March 2020.
- A pragmatic approach to Data Protection, by Suyash Rai.

(C) Webliography

- <https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d>
- https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
- <http://www.legalserviceindia.com/article/1406-Does-India-have-a-Data-Protection-law.html>
- <https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html>.
- <https://www.linklaters.com/en/insights/data-protected/data-protected---india>.
