TECHNO LEGAL JURISPRUDENCE IN 21ST CENTURY

Gargey Yadav, LL.M Student, School Of Law, Galgotias University, Greater Noida, Uttar Pradesh

ABSTRACT

The author in this paper tries to explore the Techno Legal Jurisprudence in the context of Internet and Mobile, as it form the major interaction of humans with technology. The risk factors associated with this duo combination of mobile and internet are explored; and the author tries to suggest some reasonable changes that are required looking the risk factors.

Today, technology has become an important part of our daily life. In the morning from mobile alarm to watching entertainment shows in night, all are dependent on technology. The scope and ambit of technology has widened up with the advent of internet. No doubt, internet has served the world in becoming a globalized village.

But what if somebody is following you through your mobile phone or keeping an eye on your actions? What if someone is stealing your data? What are the risk factors associated with technology?

Law develops with the society. As the environment of society has developed, the whole society moved to the digital era. But lack of authority in the technology sector is like a state without law. Mobile with internet becomes the deadly combination and makes you the most vulnerable person. How is it a deadly combination? A mobile with an active internet connects the person to the whole world and this whole world follows the person from his pocket and that is most vulnerable part which makes this duo combination a deadly and risky one. So in today's time internet and mobile makes a major part of human interaction with technology.[1] Thus this paper also tries to explore the above said combination.

First let's consider the emerging risks in the field of internet and mobile.

- Internet
  - Websites
    - ❖ Social Networking Sites
      - Registration, Legality, Purpose
      - Fake Content(Message, News, Ids(Profile)[2],

[1] PTI, *Average time spent on smartphone up 25% to 6.9 hrs amid pandemic: Report* MINT (2020), https://www.livemint.com/technology/apps/average-time-spent-on-smartphone-up-25-to-6-9-hrs-amid-pandemic-report-11607859712125.html (last visited Jun 11, 2021).; Saumya Tewari, *Daily mobile internet consumption to touch 79 minutes by 2021: Study* LIVEMINT (2019), https://www.livemint.com/industry/media/daily-mobile-internet-consumption-to-touch-79-minutes-by-2021-study/amp-1560157007783.html (last visited Jun 11, 2021).

[2] Goswami, Manash. (2018). Fake News and Cyber Propaganda: A Study of Manipulation and Abuses on Social Media.

- Stealing Data (Personal Information, Message, Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)[3]
- Vulgar and Obscene Content
- No authority or complaint redressal forum

❖ News Portals

- Registration, Legality
- Fake Content(News),[4]
- Stealing Data (Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)
- Vulgar and Obscene Content

❖ Search Engines

- Registration, Legality
- Stealing Data (Personal Information, Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)
- Indexing fake content, pornography, illegal content, seditious content

❖ Online Shopping Sites

- Registration, Legality, Purpose
- Stealing Data (Personal Information, Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)
- Fake Reviews

❖ Online Banking Sites

[3] Sam Meredith, *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal* CNBC (2018), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html (last visited Jun 11, 2021).

[4] Yuthika Bhargava, *265 fake news websites in over 65 countries managed by Indian influence networks: study* THE HINDU (2019), https://www.thehindu.com/news/national/265-fake-news-websites-in-over-65-countries-managed-by-indian-influence-networks-study/article29967820.ece (last visited Jun 11, 2021).; *Breaking: Fake sites of 50 Indian News portals luring gullible readers - ET CIO* ETCIO (2021), https://cio.economictimes.indiatimes.com/news/digital-security/breaking-fake-sites-of-50-indian-news-portals-luring-gullible-readers/82321192 (last visited Jun 11, 2021).; *Bangladesh to take legal action against online portals spreading rumours, fake news- Information Minister*, DD News, http://ddnews.gov.in/international/bangladesh-take-legal-action-against-online-portals-spreading-rumours-fake-news (last visited Jun 11, 2021).

- Registration, Legality, Purpose
- Cyber attacks[5]
- Stealing Data (Personal Information, Message, Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)

❖ Entertainment Sites

- Censorship, Registration, Legality, Purpose
- Fake Content, Vulgar and Obscene Content
- Stealing Data (Personal Information, Message, Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)

➢ Mobile

- Applicatios
  - Registration, Legality, Purpose
  - Stealing Data (Personal Information, Message, Behaviour, Choices, Psychology, Day to day Activity, Location, Mobile stored data)[6]
- Biometrics

From the above mentioned fields, common risk factor can be taken out and those are:-

- Fake, Illegal, Vulgar and Obscene Content
- Data Stealing[7]

To curb this, some measures that can be adopted are:-

[5] ETCISO, *Beware of new malware that steal browser cookies, allow hackers remotely control your web activity - ET CISO* ETCISO.in (2020), https://ciso.economictimes.indiatimes.com/news/beware-of-new-malware-that-steal-browser-cookies-allow-hackers-remotely-control-your-web-activity/74632781 (last visited Jun 11, 2021).

[6] Devesh Arora, *These Android apps can hack into your banking apps* English (2021), https://www.indiatvnews.com/technology/apps-these-android-apps-can-hack-into-your-banking-apps-690567 (last visited Jun 11, 2021).; *Vulnerabilities found and fixed in banking apps: Cybersecurity researcher*, THE ECONOMIC TIMES, https://m.economictimes.com/industry/banking/finance/banking/vulnerabilities-found-and-fixed-in-banking-apps-cybersecurity-researcher/articleshow/75711417.cms (last visited Jun 11, 2021).; FE Online, *Cyber attack: 'Reasons for startups' data breaches go beyond lack of focus on securing apps, websites*' THE FINANCIAL EXPRESS (2021), https://www.financialexpress.com/industry/sme/cafe-sme/cyber-attack-reasons-for-startups-data-breaches-go-beyond-lack-of-focus-on-securing-apps-websites/2206518/ (last visited Jun 11, 2021).

[7] *Ibid.4*

- Registration and Licensing of Websites and Application
- Data Protection

Above functions can be performed by:-

- Burden of Responsibility on State
- Burden of Accountability on Developer

Burden of Responsibility on State

The authority of State is duty bound to protect its citizens, and has to put a check upon all the activities through security raids, and better to grant affiliation and approval.

A review mechanism by the State on websites, mobile applications is needed. The State cannot run away from its duty and it is the main responsibility of state to protect its citizens as a whole.

- **Registration and Licensing of Websites and Application**

First step in developing this jurisprudence is to recognise. The recognition should not be societal but legal. That is to say that before coming into societal existence, websites, mobile apps need to be registered with their clear purpose. This can help in allowing registered ones and not the others. Access should given only to licensed and registered ones and not to others.

This is a kind of scrutiny that is require to prevent unethical website and application from operating, like of porns, fake content websites, fake news websites.

It will be clearer if OverTheTop(hereinafter as OTT) platforms and news portals are taken into consideration. There is obscene, vulgar content on OTT platforms and there is no censorship or authority to look over it. Thus are running without certification, censorship or regulation. The same is happening in the case of news media or blogs, as there is no registration process, even many times blogs are acting or portraying themselves as news media portals.

These things are need to be regulated, as they have a societal impact. Fake news, obscene content should not be entertain in order to prevent society. Some prevalent platforms are

Youtube, Netflix, Amazon Prime etc.

- **Data Protection**

The second step is to protect data. This is of very importance, as every person is generating data and this data is to be protected. Few question will give direction to this topic.

1) Where data is generated?
2) Where data is stored?

If both place where data is generated and where it is stored are not same, then it is a matter of concern and even has been raised. As it raise a suspicion that the data stored in some other place may be exploited against the State where it was generated and also hamper the sovereignty of State.

The data generated comprises of pattern of behaviour, personal information, choices, which is something more vulnerable and should be prevented from exploitation and even to prevent data, "right to forgotten" should be given to users, so that their preference are not stored.

The another type of data generated is biometrics, face recognition, the privacy of the people, all these are also at stake. If this personal detail is leaked, or exploited by mobile, laptops companies, then it will be a direct encroachment on the individuality of a person.

Or if take in account that all the data a person is storing i.e. personal details, photos, documents are monitored /stored by some website, application and the person is unaware of it, then his all privacy is at the stake. As the very concept of privacy is also acknowledged by UN.[8]

In this way a kind of insecurity is there and at the same time no awareness, regarding these issues, and in Welfare State there is no space for insecurity.

A committee was setup under the chairmanship of Justice.B.N.Krishna for Data Protection in

[8] *Universal Declaration of Human Rights*, United Nations, https://www.un.org/en/about-us/universal-declaration-of-human-rights (last visited Jun 11, 2021).

India.[9] Several other countries like ARGENTINA, AUSTRALIA, BRAZIL, CANADA, FRANCE, GERMANY, RUSSIA, UNITED KINGDOM, UNITED STATES etc have brought legislation to protect data.[10] This new jurisprudence is still developing, as and when required.

Burden of Accountability on Developers

As the State has some responsibility, so the developers have i.e. accountability on their part. They have to be fair and transparent, to their users regarding their policy towards user's data. Their policy and purpose should also be clear regarding their establishment. From developers side there should be no stealing and selling of user's data, and this can only be done when burden is imputed on them. On the safer side they should also maintain such type of security checkpoints so that the user will not face any cyber attack.

The owners of platform should be alert on the activity going on their platform. Security Audit should be regularly taken into account by the developers.[11]

Conclusion

Internet and mobile has become a world of without limits. Thus to fence the boundaries the burden of accountability on developers and burden of responsibility on State should be imputed. Thus there will be a fair balance.

There should be an authority under whose jurisdiction all the wrongs can be complained and solved easily, otherwise in cyber world there will be lawlessness. Grievance redressal forum to respond to the grievances of people should be there on the part of State and Developers.

---

[9] *Clear method for data collection must, says BN Srikrishna*, HINDUSTAN TIMES (2020), https://www.hindustantimes.com/india-news/clear-method-for-data-collection-must-bn-srikrishna/story-sIgkJwWdapfVdm8hdLllIN.html (last visited Jun 11, 2021).

[10] i-Sight Software, *A Practical Guide to Data Privacy Laws by Country* I-SIGHT, https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/#:~:text=Some%20countries%20have%20sectoral%20coverage,to%20provincial%20or%20sectoral%20regulations (last visited Jun 11, 2021).

[11] FE Online, *Cyber attack: 'Reasons for startups' data breaches go beyond lack of focus on securing apps, websites*' THE FINANCIAL EXPRESS (2021), https://www.financialexpress.com/industry/sme/cafe-sme/cyber-attack-reasons-for-startups-data-breaches-go-beyond-lack-of-focus-on-securing-apps-websites/2206518/ (last visited Jun 11, 2021).