



SIGNIFICANCE OF REGULATION FOR ENHANCING ONLINE ACTIVITY

Naeem Allah Rakha

Master of Business Law, Tashkent State University of Law Tashkent, Uzbekistan
Chaudharynaeem133@gmail.com

Abstract

Technologies somehow made this world a small village. A website gives access to everyone globally, regardless of state boundaries, who has internet facilities. In these circumstances, the question arises whether regulations are developing in the same manner as technologies? Are local or international laws regulating the transactions done in several countries. This article aims to discuss the role and contribution of regulations to promote business activity done on the internet in several states. There has been progress over time to regulate unlawful activities, but there is still a need to secure data, trade, IPOs, cyber security, online payment, and cultural norms to promote it business-friendly.

Keywords: Cyber law, Fintech, Internet Governance, WIPO, GDPR, ICPEN.

Introduction

With the transformational development in information technology, especially the widespread use of mobile technologies, there are growing business and sustainable development. The important element of the technologies to integrate into the particular aspect of the activity is potential benefits. It offers market access and improved efficiency as well as lower transactional cost.

This is foremost for the countries to enact a framework for the user and government themselves to get the advantages of opportunities from new technology. An illegal activity like online fraud, misuse of data, not only for the common user but large enterprises also affect in the same way. All unlawful activity must be prevented by making regulations at national and international levels for enhancing online business. International Organizations are providing the framework for cyber laws. with best practices concerning cyber laws and regulation as well as using recommendations on the way of enabling regulatory framework would protect the consumer and increase the benefits of new technology.

Fintech

The business of technology increases day by day. You are just one click away from getting the advantages of technology. It has entered almost every aspect of life. It





provides global access 24 hours a day 7 days a week, as well as it also improved client services, less transportation, increased professionalism, less paper waste, and allows you to handle your work from anywhere in the world.

In the present day, customers give preference to getting services online instead of visiting personally. That is a reason, you can do anything online that you want to do, from running an online shop to managing your finances, such as online payments. There are a lot of tools available to facilitate you to do online activities. Their numbers and features are increasing. The growth of fintech is surprisingly very high. On the other hand, there is also a high risk. There is a variety of computer viruses, scams, data theft, loss of, or damages to devices, etc.

In the smooth development and to take adequate benefits from the new technology. We need to shape up our laws and regulations as technology develops.

Legal Obligations

A protective legal environment is necessary to build trust and secure online activities among enterprises, individuals, and public authorities. States need to have adequate legislation in place as well as whether such regulation is implemented and enforced considerably. Implementing these regulations would increase the confidence of users. In the digital market, data is more costly than anything else. Every day, an extensive amount of data is transmitted, stored, and collected online. That's why, protection of it, is a big concern to states, enterprises, and individuals, too.

The surge in cloud computing services across the globe and growing data breaches emphasize the requirement of rule of law in cyberspace. It is very easy to commit a cybercrime even without moving a single step. Cybercriminals take their route to communication through local telephone, long-distance carriers, internet service providers, wireless and satellite networks and may go through different computers in several countries before attacking particular objectives.

States have the laws to regulate the conduct of online activity but still, need to improve regulation for unlawful actions done in different jurisdictions. Data protection principles must be observed while using personal data. It should make sure that all information must be utilized fairly, lawfully, and transparently. Those who collect and store the personal information and contact information of their users. It should be necessary for them to make their users aware of what they are storing. They must also distinctly describe how they will use your information.

Individuals face a lot of issues due to lack of capacity, but enterprises who assume that they have resources also face serious issues such as intellectual property. Using many promotional Emails and SMS is an inconvenient nuisance. Precautionary measures





for the protection of culture and norms must be considered while using online activities within and among communities.

Things cannot be limited in their boundaries. Modern technology has gone beyond local jurisdiction. Therefore, the security of devices and networks from information disclosure, theft, or damage to hardware, software, and electronic data as well as misuse can only be protected by following international laws. Regulation should be enacted with the aim of reducing the risk of online breaches. Digital Law is the idea to control and govern the Information in the modern technology era by International Organization to enhance online activities.

Misuse of Technology

The use of technology in the wrong way is not limited. Let's consider some specific cases. In 1994, a group of criminals belonging from different continents, led by a young computer programmer in St. Petersburg. They hacked the electronic systems of major banks in the United States of America and stole money secretly. No mask, no gun, no fear of police arrival. It was a modern robbery done by using technology. A total of \$400,000/- was missing from accounts of corporate clients.

Similarly, a cyber ring infected 4 million computers in more than 100 countries by using a malware called DNSChanger. These computers belonged to individuals, enterprises, and Government agencies such as NASA. They manipulated internet advertisements and were able to generate at least \$14 million.

Authorities in Russia say the Revel, a group involved in Internet attacks and ransomware, has been eliminated. The United States has announced a reward of up to 10 million for information leading to the capture of gang members following ransomware (online) attacks. The arrests are a milestone in cybercrime and cyber relations between the two States.

Governance

Users are at high risk during online activities from deception and fraud. Therefore, Laws, Policies, and Regulations may protect rights, limit unlawful conduct, and help to create trust. States try to control illegal activities in their jurisdiction through local laws and regulations, but the problem is when it has been done outside the jurisdiction. To consider these elements, the Budapest Convention on Cybercrime came into existence in 2001. It provides for criminalization of conduct ranging from illegal access to fraud, procedural law tools to investigate cybercrimes, and efficient international cooperation.





The World Intellectual Property Organization also called "WIPO" is the specialized agency of the United Nations. It is designed to promote the worldwide protection of intellectual property rights. It includes both industrial properties such as inventions, trademarks, and designs, as well as copyright materials such as literary, musical, photographic, and other artistic works. WIPO Lex is a global database that provides free-of-charge access to legal information on intellectual property, including intellectual property laws and regulations.

A remarkable work done by European Union is the General Data Protection Regulation. It is also called "GDRP". It is substantial privacy, and security law, imposing obligations onto enterprises, whenever they collect data related to the peoples of Europe. The GDPR charges punitive fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. This regulation was enforced on May 25, 2018.

The International Consumer Protection Enforcement Network (ICPEN) is an organization consisting of more than 70 countries. ICPEN provides a forum for fair trade law enforcement and consumer protection activities. It aims to enable its members to have a greater impact on their consumer laws and regulations in the international context.

The Payment Card Industry Security Standards Council (PCI-SSC) is a global forum of security standards for account data protection. This Council consists of American Express, Discover, JCB International, Mastercard, UnionPay, and Visa Inc, and is led by a policy-setting Executive Committee composed of representatives. A role is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

Challenges

To enactment of international cyber law has itself a lot of issues. Among them is territorial jurisdiction. A manufacturer of defective products in Taiwan selling them through a Canadian website to Brazil can only be sued in their local court and who will go to Taipei City to enforce warranty requirements required by law in Brasilia? Another important hurdle to enforcing international cyber law is the political sovereignty of states. States themselves use this technology for taking revenge from other States. Lack of professional training and fewer resources like problems are there for abandoning international regulations.





Conclusion

There has been remarkable progress in the cyber laws and regulations, and relatively increase harmonization in many States, but there is still a need to align laws with leading international legal instruments to favor cross-border activities. The technology has raised legal challenges. It would be necessary for the States to address it with international cooperation. Furthermore, States need to adopt basic regulations in legal areas where they do not exist. In doing so, it will also need to ensure the enforcement of laws. The next great challenge awaits them both domestically and internationally.

References

1. Castellucci, V. (2022). Digital Business 2021 | Laws and Regulations | USA | ICLG. International Comparative Legal Guides International Business Reports. Retrieved 17 January 2022, from <https://iclg.com/practice-areas/digital-business-laws-and-regulations/usa>.
2. Estay, B., 2022. 10 Online Business Laws You Need to Know for Ecommerce [2020]. [online] The BigCommerce Blog. Available at: <<https://www.bigcommerce.com/blog/online-business-laws/#undefined>> [AcUnctad.org. (2022). Retrieved cessed 17 January 2022].
3. Wolford, B. (2022). What is GDPR, the EU's new data protection law? - GDPR.eu. GDPR.eu. Retrieved 17 January 2022, from <https://gdpr.eu/what-is-gdpr/>.
4. 17 January 2022, from https://unctad.org/system/files/official-document/ciiem5d2_en.pdf.
5. Laws Pertaining to Commerce on the Internet | Stimmel Law. Stimmel-law.com. (2022). Retrieved 17 January 2022, from <https://www.stimmel-law.com/en/articles/laws-pertaining-commerce-internet>.
6. Legal obligations for online business | Business Queensland. Business.qld.gov.au. (2022). Retrieved 17 January 2022, from <https://www.business.qld.gov.au/starting-business/internet-start-ups/online-basics/legal-obligations>.
7. Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. Pcisecuritystandards.org. (2022). Retrieved 17 January 2022, from https://www.pcisecuritystandards.org/about_us/.
8. Oecd.org. (2022). Retrieved 17 January 2022, from <https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf>.





9. International Cyber Ring That Infected Millions of Computers Dismantled | Federal Bureau of Investigation. Federal Bureau of Investigation. (2022). Retrieved 17 January 2022, from <https://www.fbi.gov/news/stories/international-cyber-ring-that-infected-millions-of-computers-dismantled>.
10. The Budapest Convention on Cybercrime: a framework for capacity building – Global Forum on Cyber Expertise. Thegfce.org. (2022). Retrieved 17 January 2022, from <https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/>.
11. Tidy, J. (2022). REvil ransomware gang arrested in Russia. BBC News. Retrieved 17 January 2022, from <https://www.bbc.com/news/technology-59998925>.

About the Author:



Naeem is a lawyer by profession and was born in Karachi, Pakistan. He received his LLB. degree from Bahria University, Islamabad, Pakistan. and is now studying for an LLM in Business Law at Tashkent State University of Law, Tashkent, Uzbekistan. He is also working on their doctoral research proposal.

He has been working as a lawyer since 2019 to advise clients on their rights, responsibilities, and duties under the law. The primary focus is to draft legal documents and represent clients in court. He also works for his corporate clients in their legal matters to provide legal assistance, assess contracts, partnerships, and negotiate deals as well as provide arbitration.

Mr. Naeem was president of the Law Moot Society while studying at Bahria University. He is a member of the Punjab Bar Council in Lahore, Pakistan. He is also a member of the Australia New Zealand International Law Society.

