INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

ISSN: 2582-7677

EVALUATING EXISTING CYBER CRIME POLICIES: DO THEY SUFFICE IN TODAY'S WORLD?

RANI SUPRIYA

Law College Dehradun

Introduction

Due to social distancing conventions and countrywide lockdowns, the COVID-19 pandemic has inevitably resulted in an increase in the usage of digital technology. People throughout the world have adapted to the changing work culture and lifestyle. A world without the internet is now unthinkable. The internet, which connects billions of people across the world, is a key component of the modern information society. There were 4.66 billion active internet users globally in January 2021, accounting for 59.5 percent of the global population.

In recent years, cyber crimes have increased due to the worldwide pandemic and growing digitalization. According to experts speaking at Pursuit 2021, an event on cybersecurity hosted by the Internet and Mobile Association of India, the number of breaches in India surged by 2000% during the epidemic (IMAI). Dr.Gulshan Rai, India's first Cybersecurity Coordinator and Distinguished Fellow at the Observer Research Foundation (ORF), has cautioned that a rise in cybercrime or "cyberwar" has started to affect the business as well. Meanwhile, the National Cyber Crime Reporting Portal of the Ministry of Home Affairs claimed to have received over four lakh cyber threat reports in less than a year. Financial fraud accounts for around half of the instances. According to a recent analysis by global VPN service provider Nord VPN, India ranked 19th out of 21 nations in the National Privacy Test, indicating that it is at the bottom of a worldwide tally of countries with strong online security practices and cyber hygiene[1].

Statutes on cybercrime

[1] Statista. (2021, September 10). *Worldwide digital population as of January 2021.*

ISSN: 2582-7677

Many sovereign countries across the globe have laws in place for preventing, monitoring, criminalizing, investigating, and punishing cybercrime, and are working to establish legislation to address the threat posed by cybercrime:

In 1997, the G8 released a Ministers' Communiqué outlining an action plan and principles to combat cybercrime and protect data and systems from unauthorized access. It also stated that all law enforcement personnel must be trained and equipped to deal with cybercrime and that all member countries must have a point of contact available 24 hours a day, seven days a week.

In 1990, the United Nations (UN) General Assembly passed a resolution on computer crime law. It also passed a resolution in 2000 to combat illegal misuse of information technology, and a second resolution in 2002 to oppose criminal misuse of information technology.

The International Telecommunication Union (ITU), which is responsible for telecommunications and cyber security issues at the United Nations, issued the Geneva Declaration of Principles and Plan of Action in 2003, highlighting the importance of measures in the fight against cybercrime, and in 2005, the Tunis Commitment and Tunis Agenda for the Information Society[2].

In 2001, the Council of Europe (CoE), which has 47 European member states, took the initiative by establishing the first International Convention on Cybercrime (Budapest Convention), which was developed in collaboration with the United States, Canada, and Japan and signed by 46 member states but ratified by only 25. The Convention, also known as the Budapest Convention, wsthe first international convention addressing crimes perpetrated over the Internet and other computer networks, focusing on copyright infringements, computer-related fraud, child pornography, and network security violations. It also includes a number of authorities and processes, such as computer network search and interception.

The Asia-Pacific Economic Cooperation (APEC) published the Cyber Security Strategy in August 2002, which is included in the Shanghai Declaration, as part of regional attempts to

[2] CXOtoday News Desk. (2021, July 19). *2000% Increase in Cyber Security Breaches during Covid-19 Pandemic*.

ISSN: 2582-7677

stop the tide of cybercrime. The aforementioned Cyber security plan focuses on six critical areas for member economies to collaborate on: legal changes, information exchange and cooperation initiatives, security and technological guidelines, public awareness, training and education, and wireless security, to name a few.

In 2002, the Organization for Economic Co-operation and Development (OECD) issued "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," which included 34 nations.

In 2002, the Commonwealth Nations submitted a model law written in line with the Convention on Cybercrime (International Telecommunication Union, 2009), which establishes a legal framework for harmonizing legislation throughout the Commonwealth and facilitating international collaboration.

The Economic Community of West African Nations (ECOWAS), which consists of fifteen member states, enacted the Directive on Combating Cybercrime in ECOWAS in 2009, which establishes a legal framework for member states that encompasses both substantive and procedural criminal law.

World and cybersecurity

The United States Of America

In terms of cybercrime, the United States leads the globe. It has been the world's most impacted country in terms of internet-related crimes, accounting for 23% of global cybercrime. It is, nevertheless, the country with the most stringent cyber regulations. Approximately 60% of cyber cases result in convictions and jail terms. The Computer Fraud and Abuse Act, enacted in 1984, was the first effective statute against such offences (CFAA). The statute, however, did not include a provision for harmful code that was used to intentionally harm equipment. Viruses, to put it another way[3].

The National Information Infrastructure Protection Statute (NIIA) was proposed to strengthen the act. It was repealed as the earlier espionage rules made it unlawful to access computer data without permission. Beyond these regulations, the United States has created rigorous

[3] Ajayi, E. F. G. (2016). *Challenges to enforcement of cyber-crimes laws and policy.*

ISSN: 2582-7677

definitions and penalties for cybercrime. In cyberbullying, punishments range from expulsion to criminal misdemeanour to felony. Identity theft carries a punishment of 15 years in jail and penalties. Hacking and computer property damage carry a penalty of six to twenty years in jail. The United States has a stranglehold on cyber legislation.

The United Arab Emirates

Among the Middle Eastern countries, the UAE has the most extensive and effective cybercrime legislation. The UAE is only exposed to 5% of the world's cyber dangers. However, being the Gulf Region's financial hub, it has robust rules in place to safeguard its companies from assaults.

Each violation, as well as the penalty connected with it, has been precisely specified by the country. For the basic offence of internet stalking and harassment, the maximum penalty is two years in jail or a fine of 250-000-500,000 AED (Arab Emirates Dirham). Forgery can result in a sentence of up to two years in jail and a fine of up to two million AED. For cyber terrorism, he was sentenced to life in jail. For any cyber danger, the UAE has clear and strict regulations in place.

Kingdom Of Saudi Arabia

In comparison to the rest of the globe, Saudi Arabia has a low rate of cybercrime. These offences, on the other hand, have gradually increased over time. Pornography accounts for 76% of this, costing the country around 6.5 million dollars in 2016. While the Kingdom of Saudi Arabia has some laws in existence, most other cyber incidents, such as cyber bullying, piracy, and signature fabrication, remain undefined.

Hacking, unauthorized data access, pornography, denial of service, and cyber terrorism are the only regulations in force. For cyber terrorism, the penalties range from a year in prison and a fine of 100,000 Riyals to a maximum of 10 years in prison and a fine of 5,000,000 Riyals.

China

In terms of cyber regulations, China has traditionally set the standard. While the Chinese government's regulations may look authoritarian to outsiders, they are vital forthe country's survival. The State Council formalized the 'Computer Information Network and Internet

ISSN: 2582-7677

Security, Protection, and Management Regulations' in 1997, which recognized and punished cybercrime. Acts like hacking, destroying data, or developing and spreading computer viruses are punishable by a minimum of three years in jail. In more serious situations involving sensitive data, the punishment is raised dramatically[4].

The Chinese government has complete and total control over the internet within its boundaries. As a result, China has blocked several of the world's most popular websites. Take Google, for example. While this may seem absurd to us, it has proven to be advantageous to China's domestic e-commerce and digital businesses.

The Cybersecurity Law, which took effect in June, is the most recent addition to China's legal framework. All international firms must keep their vital data of use within the country, according to the legislation. In addition, the government will be able to perform checks on the company's networks and data.

India and cybersecurity

To prevent such crimes and speed up investigations, the central government has made efforts to raise awareness about cybercrime, issue alerts/advisories, develop capacity/train law enforcement personnel/prosecutors/judicial officials, improve cyber forensics capabilities, and so on. Complainants can make complaints against Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries, or sexually explicit information using the government's online cybercrime reporting site, www.cybercrime.gov.in. The Indian Cyber Crime Coordination Centre (I4C) has been established by the Central Government to address matters connected to cybercrime in the country in a comprehensive and coordinated way. .According to the Indian Constitution, 'Police' and 'Public Order' are state subjects. Through their law enforcement apparatus, states/UTs are largely responsible for the prevention, detection, investigation, and punishment of crimes. Law enforcement agencies take legal action against cybercriminals in accordance with the law.

Policies enacted by the Indian government to enhance the country's cyber security include:

[4] Nazir, S. (2017, July 24). *Cyber Laws: What Have Different Countries Done To Prevent Cyber Crime*

ISSN: 2582-7677

The Information Technology Act of 2000 is now the country's principal statute for dealing with cybercrime and digital trade. The Act was initially drafted in 2000, then amended in 2008, and finally implemented a year later. The Information Technology (Amendment) Bill of 2008 made changes to a number of provisions pertaining to digital data, electronic devices, and cybercrime[5].

Sections 43 (data protection), section 66 (hacking), section 66A (measures against sending offensive messages), section 66B (punishment for illegally possessing stolen computer resources or communication devices), section 67 (protection against unauthorised access to data), 69 (cyberterrorism), section 70 (securing access or attempting to secure access to a protected system), and section 72 (privacy and confidentiality) of the Information Technology Amendment Act of 2008, among others, govern cybersecurity.

The government has adopted a framework to improve cyber security in India, with the National Security Council Secretariat serving as the main institution.

The National Cyber Security Policy of 2013 was created to ensure that India's residents and companies have access to a safe and resilient cyberspace. The policy, according to the Ministry of Electronics and Information Technology, aims to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities, and minimise the damage caused by cyber incidents by combining institutional structures, people, processes, technology, and cooperation.

The National Technical Research Organization is the primary organisation in charge of safeguarding national critical infrastructure and responding to all cybersecurity events in the country's key sectors.

In addition, the Indian Computer Emergency Response Team (CERT-In) is in charge of incident response, which includes cybersecurity analyses, predictions, and warnings.

The Ministry of Home Affairs (MHA) has issued advisories to states and union territories in the nation on how to combat cybercrime, which are published on the Ministry's website.

[5] *Cyber Crime And Policies To Address Security Concerns* – Groups Master. (2021). Groups Master. Retrieved October 19, 2021

ISSN: 2582-7677

The Cybercrime Prevention against Women and Children Scheme is being implemented by the Ministry of Home Affairs with the goal to prevent and reduce cybercrime against women and children. This plan would enact tighter regulations and rules, as well as run programmes to raise knowledge about cyber dangers and how to deal with them[6].

Conclusion

The efforts made through legislations at regional, national and international, levels were discussed; without prejudice to the effectiveness of the existing laws in place to combat cybercrime.

The lack of a global consensus on the types of conduct that constitute a cybercrime; the lack of a global consensus on the legal definition of criminal conduct; the inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to computerised data; the lack of uniformity between national procedural laws concerning cybercrime investigations; and the lack of extradition are Challenges to framing and enforcing laws related to Cybercrimes.

Experts think that combining AI-based cybersecurity solutions with trained humans will be the most effective method to deal with the increasing threat scenario. Developing and least developed nations must think and act quickly, else, there will be a significant digital divide between developed and developing countries. Through education and training, the government should begin by assisting its citizens in becoming more aware of the security problems surrounding information technology. Cultural differences and selfish gain have no place in this world. Adopting proper legislation and enforcing cyber laws, as well as a strong institutional structure and worldwide collaboration, are all essential for cyber security. An R&D department, for example, would almost certainly encourage innovation, making everything seem conceivable

[6] https://www.statista.com/statistics/617136/digital-population-worldwide/