DE JURE NEXUS LAW JOURNAL

Author:

Huzaifa Hasan

Symbiosis Law School, Noida

1st Year, BBA LL.B.

SUSTAINABLE DEVELOPMENT GOALS AND CYBER SECURITY CHALLENGES

Abstract

The fast-paced change in the wake of technological development in all the sectors of the economy from using the traditional outlived things to the whole ICT gadgets, has given a rise to the concerns of cyber security. Where the whole world is digitally dependent, it is the requirement to build CCB and to address all the trials that are entailed with the technological advancement and digitalization and their relationship with the sustainable development goals.

United Nations have relentlessly been enshrining the different sustainable development goals and the dependency of these goals on digitalization, and this is a time now to address all the challenges that cybersecurity encounters while maintaining cyber hygiene, smooth functioning of the transactions and cutting down all kind of cybercrimes and cyber terrorism. This research is an attempt to acknowledge and shed a light on the nascent literature on cyber security and its connection with sustainable development goals.

Keywords: *ICT, digitally dependent, digitalization, SGD, cyber hygiene, cyber terrorism, and cyber security.*

Introduction

With the fostering interdependencies between the different departments of economy, a rise to inter-organizational structure follows, where the cyber security and sustainable development hold a tremendous concern. Due to the advent of digitalization, there has been a sheer surge in the dilemmas and the challenges of cybersecurity and its relationship with the sustainable development. It is a question of wider import that how in the wake of digitalization new connections and disconnections between different countries take place and what role does digitalization play for the Sustainable Development Goals framework laid down by the United Nations? Therefore, this article is an attempt to answer all such questions which comes forward in our mind in the first place and are worth pondering upon.

Sustainable Development Goals and Their Relationship with Cyber Security

Among the abundant number of sustainable development goals and the targets set by United Nations, various of them are directly and indirectly dependent on digitalization. For instance, the water pipelines and the water management systems are backed by the digital devices, their inflow and outflow depend on one trigger or a button and if they are not regulated with best cyber security, it'll surely exacerbate the situation.

The first SDG that is greatly reiterated by the United Nations which is to reduce poverty can be attained by the help of cyber security. People's ability to access information through the Internet is critical to ending poverty. As a result, it's possible that it'll be disrupted by flaws in, and attacks on, data administrations and the organizations that people utilize to interact with them.[1] Also, the access to digital arena and digitalization will increase the working efficiency of the people and will boost the income of the workers thereby, increasing the innovative capacity and cutting down the cost of initial investments (SDG 8 and 9). The health sector and the utmost health of all the individuals can be assured with the help of digitalisation and can lead to the attainment of 8th goal of sustainable development. Furthermore, quality education and access of education to all the

[1] Morgus, R., 2018. Securing Digital Dividends. [online] New America. Available at: <https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/appendix-the-sdgs-and-cybersecurity/> [Accessed 10 February 2022].

refugees and children below the age of 18 and people who are behind the curve of education is lacking. The linguistic barriers are the soundest reasons for the dearth of vocationalization of education, also at times, the discrimination in the newly established education system in certain schools give rise to lost generation.[2] All these barriers can efficiently be met by the overarching technological landscape and with the advent of digitalisation where internet access is easy for all (SDG 4). Besides, as water and energy supplies (SDGs 6 and 7) become more digitalized, the ability to protect the basic indispensable data framework, which is frequently as open private organizations, turns out to be progressively significant for access reliability and quality.[3] Additionally, justice and peace will efficiently be driven and delivered if an organised access to the information is provided to the general public. Also, scrutinization will be promoted more with the help of dissemination and access of information among the people, consequences of which will promote greater peace, justice, and strong institutions (SDG 16). A responsible use of internet is the utmost requirement and all the countries in the world need to assure that digitalisation is not being used to oppress, suppress, and survey the domestically ran organisations but the free-fair AND open internet is provided to all.

Challenges and Digital Risks Faced By Cyber-Security

While the benefits from the internet are confirmed from the various research and its role in creating a bigger and productive socio-economic landscape, there are numerous hurdles that are to be dealt with before most of the people can enjoy the extensive use of internet in all the countries. The countries which suffer from the lack of development, poverty and poor governance may become a safe heaven for the cyber criminals and they can become a whole new breeding ground for all the cybersecurity vulnerabilities and challenges. Therefore, it is evident that a whole new dimension of social vulnerability follows in the wake of development opportunities offered by the digital revolution.[4]

[2] Drc.ngo. 2022. *UN Sustainable Development Goals*. [online] Available at: <https://drc.ngo/about-us/who-we-are/un-sdgs/?gclid=Cj0KCQiAr5iQBhCsARIsAPcwRON7CF-k0fm_4EWz0cYQz-M_rOJtwv9XcsFRpLRuP-EUXVz1nR9lmJsaAr60EALw_wcB> [Accessed 11 February 2022].

[3] Data.europa.eu. 2015. Riding the digital wave : the impact of cyber capacity building on human development.. [online] Available at: <https://data.europa.eu/doi/10.2815/43396> [Accessed 10 February 2022].

[4] Schia, N. and Willers, J., 2020. *Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries. Industry, Innovation and Infrastructure*, [online] pp.1-10. Available at: <https://www.researchgate.net/publication/347920471_Digital_Vulnerabilities_and_the_Sustainable_Development_Goals_in_Developing_Countries> [Accessed 10 February 2022].

As relative late connectors of technological advances, developing nations participate in "**mechanical jumping**," or "**Technological Leapfrogging**" which thusly is interlinked with the gamble of new and phenomenal societal vulnerabilities. Although, the amount of tribulations and ordeals that global south face in the wake of digitalization are comparatively much higher than the global north, donor and well developed nations. It is because the developing countries hold much potential to work towards the digitalization in a rapid face and their concern is generally towards the universalization of internet but they dearth the regulatory and managing capacity for the services they cater. "*Cyber Security Capacity Building (CCB) seems set to play an increasingly important role in future foreign policy considerations and government programs."*[5]

Digitalisation is not a mere linking with the cyber landscape but is more like a phenomenon of connecting and disconnecting with the world. Most of the cases are those where the whole county is reliant on either a single or very few **Internet Exchange Point** to connect globally, the problem that relatively arises with such a model is that, it is quite disruptive and vulnerable as all the governmental data travel across only one exchange point and one cyber-attack will cause everything go on toss. Many developing countries are relying on the wireless connections and there is no or very less framing of fixed line cables under the ground which directly hinders the speed of the internet and its stability, along with that it is quite expensive. In a conclusion by the World Bank, it is stated that most of the developing countries are stuck with a cheap and second-class internet facility which fails to provide an encrypted and safe surfing environment to its users and businesses.[6] A security risk can also be instigated by slow internet, for instance, the mitigation of **DDOS (Distributed Denial of Service)** attacks is quite difficult and Myanmar is the live example of what occurred in 2010.

Another challenge has been an overall absence of implementers which can be followed back both to a worldwide deficiency of digital specialists and to an absence of financing open doors. Cyber criminals deliberately operate in the nations which have extremely less legislations in the areas of cyber security to avoid their malicious transactions and arbitrage, often operating with impunity.

[5] Schia, N., 2016. *Teach a person how to surf: Cyber security as development assistance*. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/299655657_Teach_a_person_how_to_surf_Cyber_security_as_development_assistance> [Accessed 11 February 2022].

[6] World Bank Group. 2016. *World Development Report 2016: Digital Dividends*. [online] Available at: <https://openknowledge.worldbank.org/handle/10986/23347> [Accessed 11 February 2022].

Indian Legislation on Cyber Security and Information Technology Act

The IT Act was initially passed to give lawful acknowledgment to online business and approvals for computer abuse. In any case, it had no express arrangements regarding information security. Moreover, the hackers could be penalized but there were no provisions for the organisations that keep the data of public at large. But due to the immense rise in the cybercrimes and unhygienic cyber practices, there are two provisions incorporated in ***IT (Amendment) Act 2008*** to provide remedy to people who suffer or likely to suffer from their personal data not being adequately used.[7]

Also, the government timely formulate the new rules under the sections of IT Act to broaden the scope of privacy of data and regulations which reduces the cybercrimes. The IT Rules are statutory laws and most recently in April 2011 four rules were notified under section **43A of IT Act** to increase the confidence of people regarding their privacy. **Government has set up different relevant tribunals and compliance regulators such as CERT-IN (Indian Computer Emergency Response Team)** and **CRAT (Cyber Regulations Appellate Tribunal)** to curtail all kinds of cyber incidents at the time when they occur.[8] The data protection can also be ensured with the help of additional legislation to the above legislation such as authorization of property privileges in view of the Copyright Act (1957), Telegraph Act 1885 in relation to all kinds of telegraph activities along with many other legislations.

Also, the *data protection* has not been defined in IT Act but is defined in the ***Personal Data Protection Bill 2019*** is relied upon to pass into regulation inside the following year, turning into India's first and most extensive cross-sectoral data protection regulation.

Other Countries' Outlook and Standpoint

The Budapest Convention on Cybercrime lays out a structure for orchestrating public regulation to guarantee that cybercriminals don't work without risk of punishment. National Cyber Security

[7] Subramaniam, A. and Das, S., 2021. *The Privacy, Data Protection and Cybersecurity Law Review*. [online] Thelawreviews.co.uk. Available at: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and cybersecurity-law review/india#:~:text=The%20Information%20Technology%20Act%20(2000)%20(the%20IT%20Act),)%2C%20which%20attract%20criminal%20action.> [Accessed 11 February 2022].

[8] Subramaniam, A. and Das, S., 2021. *The Privacy, Data Protection and Cybersecurity Law Review*. [online] Thelawreviews.co.uk. Available at: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and cybersecurity-law review/india#:~:text=The%20Information%20Technology%20Act%20(2000)%20(the%20IT%20Act),)%2C%20which%20attract%20criminal%20action.> [Accessed 11 February 2022].

of United States of America guarantees the security of the internet and American network along with many objectives such as guarding the country by safeguarding networks, frameworks, capacities, and information also by sustaining a protected, flourishing computerized economy and cultivating solid homegrown development.[9]

At the highest point of the positioning for most digital secure nations, Denmark got a generally digital wellbeing score of 8.91, excelling on the Cybersecurity Exposure Index, where it scored simply 0.117. Germany had a digital security score of 8.76, while the US scored 8.73. Norway, the United Kingdom, Canada, Sweden, Australia, Japan, and the Netherlands were among the top ten most secure nations, in order of rating.[10]

Other countries which cater internet access without any data protection and security have a lack of regulated legislation and they are very vulnerable to threats and are successful breeding grounds for most of the cybercrimes due to this dearth of expressed legislation and formulated rules and regulations.

Conclusion and Suggestions

This article has been written on the extant literature on cyber security and its sheer connections and disconnections with the United Nations sustainable development goals. A mammoth of social dearth and vulnerabilities are being emerged in the wake of universalisation of digitalisation. With the help of this existent literature, this article has made an attempt to shed a light on the relationship between digitalisation, cyber security and economic growth. It is nebulous and viable by the study that the regulatory capacity of the developing nations is not compatible with the hitherto emerge of digitalisation that follows in the wake of technological advancement.

The global north which comprises of the many developed nations have focused simultaneously on the cyber security with the growing trends of digitalisation to make their economy fit in all the spheres of sustainable development goals. Developing nations, on the other hand, have been sluggish to join the convention and mostly lack the required law enforcement power to implement

[9] Trumpwhitehouse.archives.gov. 2018. *NATIONAL CYBER STRATEGY*. [online] Available at: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> [Accessed 11 February 2022].

[10] Sharma, S., 2021. *Which countries are most (and least) at risk for cybercrime?*. [online] ARN. Available at: <https://www.arnnet.com.au/article/693057/which-countries-most-least-risk-cyber-crime/#:~:text=At%20the%20top%20of%20the,while%20the%20US%20scored%208.73.> [Accessed 11 February 2022].

it. Cybersecurity has different characteristics coupled with different challenges such as global politics, security politics and SDGs. The capacity building in cybersecurity is a new trend and has yet not been admitted in SDGs and nor in many big reports. It requires the same concern as it gets while the technological advances are introduced. **Therefore, SDGs can continue to come up with other plans but this time they should be inclusive of the cybersecurity capacity building approach and a smooth economy entangling the most of cyber unhygienic crimes and hence curtailing challenges entailed with it.**