Article

A NEW ORDER IN CYBERSPACE AWAITS US

*Dr. Pavan Duggal**

DOI 10.24833/2073-8420-2020-2-55-18-24

Introduction. *This paper represents the changes which has brought in new changed ground realities. Lot of new developments have started taking place, ever since the advent of coronavirus. The author is neither a soothsayer nor an astrologer who can adequately predict the coming future. However, at the time of writing, some broad trends are emerging on the horizon, which could impact the evolution of a new world order in cyberspace. These emerging trends are beginning to point in the direction of an irreversible change in cyberspace.*

Materials and methods. *The methodological basis of the study was made up of following general scientific and special methods of cognition of legal phenomena and processes in the field of Cyber law, Cybercrime & cybersecurity during corona virus age: a system-structural analysis method; method of synthesis of social and legal phenomena; comparative legal method; and formal logical method.*

The results of the study. *The analysis revealed that, the Cyberspace is full of so much of information and misinformation that people are clueless as to which information source they should rely upon and which they should not. In this pandemonium, that exist across the world, some broad new areas are emerging which are engaging the attention of numerous stakeholders.*

Discussion and conclusions. *In today's Coronavirus times, nothing can be predicted as absolute. However, if one keeps in mind the broad trends on the horizon, one could potentially be more well equipped to deal with challenges concerning the new cyber world order. The New Cyber World Order will be increasingly important for all digital and cyber stakeholders, as it will impact all our digital presence, digital activities and digital lives. The legal, policy and regulatory issues pertaining to New Cyber World Order will have to be appropriately considered and addressed by cyber stakeholders as New Cyber World Order takes root in the coming times.*

Introduction

As the world plunges into the Coronavirus crisis and as fear gloom and panic is reigning all around, a question that comes to everybody's mind is that whether there is any silver lining to the dark clouds above us.

Coronavirus has been the biggest and most significant public health emergency of our living times [15]. Number of confirmed deaths in

* **Dr. Pavan Duggal,** Advocate, Supreme Court of India. Chairman, International Commission on Cyber Security Law. President, Cyberlaws.Net
e-mail: pavan@pavanduggal.com
ORCID ID: 0000-0003-4782-1044

countries across the world continues to grow with each passing day. As on 7 June 2020, 05:30 GMT+5:30, there are confirmed cases 67,50,521 with 3,95,779 deaths in 216 countries, areas and territories.

The coronavirus age has brought in new changed ground realities. Lot of new developments have started taking place, ever since the advent of coronavirus. While there is no denying the fact that coronavirus is the largest pandemic in recent history, the fact remains that it is beginning to trigger off various responses from different stakeholders, apart from mere public health responses.

With more than billion people stranded in lockdown in their homes during national lockdowns, Internet has been the only saver for them. There is so much information, misinformation as also false and fabricated information that is going around concerning Coronavirus and COVID-19. Cyberspace is full of so much of information and misinformation that people are clueless as to which information source they should rely upon and which they should not.

In this pandemonium, that exist across the world, some broad new areas are emerging which are engaging the attention of numerous stakeholders.

The author is neither a soothsayer nor an astrologer who can adequately predict the coming future. However, at the time of writing, some broad trends are emerging on the horizon, which could impact the evolution of a new world order in cyberspace. These emerging trends are beginning to point in the direction of an irreversible change in cyberspace.

Study

New Cyber World Order

One new trend that is emerging on the horizon pertains to the newly emerging cyber world order.

In my recent book "New Cyber World Order Post Covid-19" [1], I have given a detailed analysis of how this newly emerging paradigm is going to impact all our lives in the coming times.

The new cyber world order refers to that new order or things in cyberspace that we will face once we conquer the Coronavirus infection and pandemic.

The four words in the phrase "New Cyber World Order" refer to a new world order in cyberspace scheme of things which would arise and be different from the prevailing scheme of things in the existing cyber world order. The said phrase refers to a dawn of a new era in the history of cyberspace, where unprecedented response mechanisms and steps, taken during the times of COVID-19 pandemic, are likely to have significant impact upon the future consolidation and growth of cyberspace as a paradigm. New Cyber World Order is likely to see remarkable changes in the emerging global situations concerning the Internet and its usage, which are likely to be substantially different from the existing situations and structures, prevailing at the time of writing.

Consolidation Of Sate Power

One of the most important elements visible today is that the world is seeing a tremendous consolidation of state power. Countries, through various governmental actions, are seeing more centralisation of power in their governments, under the garb of fighting the pandemic of COVID-19. It is correct that the pandemic like coronavirus requires the entire resources of the state. However, one is beginning to see some massive trends which will have a direct connection on cyberspace issues.

States are increasingly getting more and more powerful, by means of coming up with new legislations, legal provisions and connected measures. These provisions are often being made by governments, under the garb of outdated epidemic laws, in order to gain upon themselves, more power to legislate, to take appropriate actions and to influence peoples' lives and their day-to-day activities.

When one peruses through various legislative and policy measures adopted by different countries during Coronavirus age, almost all of them have been motivated by the singular need to fight COVID-19 pandemic. However, under the garb of the same, such legislative measures and policies are increasingly aiming to centralize lot of powers in the hands of the states. Consequently, states are likely to take upon themselves lot of powers and jurisdictions, which under normal circumstances, states would not have been done or if they would have tried to do so, there would have been a lot of public outcry.

Such approaches could have prejudicial impact upon the growth of cyberspace issues during and post COVID-19.

Based on the existing trends, there is no denying the fact that cyberspace is going to be massively impacted with the advent of New Cyber World Order. The New Cyber World Order is likely to have significant impact upon the enjoyment of digital and cyber liberties and rights.

Further, New Cyber World Order could potentially see the emergence of much more powerful nation states which are likely to further impact the future growth of cyberspace.

The dawn of New Cyber World Order is likely to enable cyberspace to enter into a new era. This era will have its own distinct challenges and opportunities and would potentially even aim to redefine some of the existing concepts that the world has currently known [17].

COVID-19 Tracing Apps

One of the most significant aspects in this regard pertains to massive increase in Governmental power, with governments around the world, coming up with their COVID-19 tracing apps [16]. These are apps which have been prepared by different Governmental agencies across the world for the purposes of assisting the tracking of COVID-19.

Citizens across the world are either being encouraged or mandated to download these COVID-19 tracing apps. These apps, on a cumulative basis, are constantly collecting sensitive personal data, including medical and health related data of individuals. This data is increasingly being accessed by state agencies, as per the applicable norms across different countries, for constantly evolving new strategies to fight against COVID-19. It is pertinent to note that different countries have in place different national cyber laws which have laid down the foundations concerning electronic data, its protection, security and preservation.

Some countries also have dedicated data protection laws. These COVID-19 apps in different parts of the world are seeking to collect data as part of legitimate governmental responses, to go ahead and fight against COVID-19. In number of jurisdictions, there is no end date for such COVID-19 tracing apps. The effect of this is that these COVID-19 apps are likely to continue even after fight against COVID-19 comes to an end.

Fears About Increasing Interception

Hence, there are legitimate fears being stipulated in different parts of the world that COVID-19 related data, being collected by these apps, could be misused for the purposes of surveillance, monitoring and tracing of people [18].

These COVID-19 apps and the data that they are collecting, do provide the possibility to the government to have ability to carry out more surveillance. This ability can be used to constrain democratic freedoms. It creates an underlying vulnerability for civilization as critical infrastructure and many public services become reliant on a digital network that can easily be attacked from any corner of the globe [2].

Hence, it is possible that the collected medical data could be potentially used for the purposes of tracking people. This raise large number of legal issues inasmuch as the same could have direct impact upon the enjoyment of civil liberties and digital freedoms.

Countries are invariably invoking a mixture of both existing laws and also of new legal frameworks, for the purposes of addressing Coronavirus pandemic and have further been focusing on coming up with provisions, granting extensive powers to the Government to do acts in their judgment for fighting the Coronavirus pandemic. While the noble objections of fighting pandemic are indeed laudable, experts are worried about continuation of such powers granted to the Government, once the fight against pandemic comes to a close.

Consequently, it is expected that Cyberlaw is likely to have an impacted role in the perpetuation and continued maintenance of New Cyber World Order. Lot of new secondary legislations, rules, guidelines and regulations are being pushed in many countries, whether under the ambit of their national cyber legal frameworks or within the ambit of their national epidemic laws or national disaster management laws. These rules and regulations are increasingly expanding the ambit and scope of state power in the wake of pandemic and represent a rising trend of increasing intrusiveness, with which state powers could potentially be used for curtailment of digital or cyber liberties and rights.

Internet provides massive source of regulating and impacting the thinking and psyche of internet users. Further, internet users are continuing to grow with each passing day. As per the figures of the International Telecommunications Union (ITU), more and more people are coming on the digital bandwagon.

By 2030, 6 Billion people will be online. Going forward, markets to see the fastest growth in Internet users, will be predominantly low-income, late-adoption societies in Africa and Asia. Mobile will be the most significant segment in driving Internet penetration, with lower data tariffs and cheaper smartphones key to uptake [1].

A perusal of the emerging trends clearly shows that there are visible signs on the horizon to point towards the evolution of the powerful and totalitarian state power.

Health Data And Challenges

Further, huge volumes of collected COVID-19 related health data are being stored in different locations which are potentially being targeted by cyber criminals. Hence, this COVID-19 related medical data presents immense cyber security challenges as its breach could potentially expose not just governments but also their citizens to potential legal consequences.

Already, the COVID-19 age has been seeing a massive increase in cyber security breaches.

Rise In Malicious Domain Name Registrations

Cybercriminals are increasingly coming up with customized, new and innovative approaches to target innocent Internet users. Using deception to win over the trust of the people in these hard times, appears to be the prevailing mantra for cybercriminals.

We are also seeing the emergence and increased use of malicious domain names. The year 2020 has seen massive increased in registration of domain names which either have connection or association with COVID-19 or coronavirus.

There are a considerable number of registered domains on the Internet that contain the terms: «coronavirus», «corona-virus», «COVID19» and «COVID-19». While some are legitimate websites, cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware [4].

Increasing Cybercrime

No wonder, phishing has become one of the most significant prominent cybercriminal activity in the global scenario. Instances of phishing are continuing to keep on increasing.

Phishing is a cybercrime [19] in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords [5].

Phishing often is aimed at building on the fear or panic element on the targeted victims.

As per Forbes [6], it has been pointed out that scammers can piggy ride on legitimate email addresses and services by uploading files to Dropbox and One Drive and then using the share function to send links to potential victims often aimed for winning the trust of people and making them victim of phishing.

Further, cyber criminals are increasingly using identity theft, fraud and malware as potent weapons in their ammunition bags to target innocent users.

Further, in these times, ransomware has increasingly become the preferred computer contaminant for cyber criminals.

The ransomware can enter their systems through emails containing infected links or attachments, compromised employee credentials, or by exploiting a vulnerability in the system [7].

New kinds of cybercrimes are emerging in the coronavirus age. Increasing cybercrimes across the world is now a documented fact and has been well pointed out by various public figures and personalities.

The advent of Work From Home during COVID-19 times has further facilitated the growth of cybercrimes. Given the fact that national lockdowns have been announced, remote working was thrust on various stakeholders.

Remote Working Becomes the New Normal Companies forced to embrace remote working are likely to find their employees questioning why they need to return to the office at all once the crisis is over [8].

At the same time, cybercrime is specifically being targeted at Work From Home sector. It has been reported that almost half of UK employees working from home during the coronavirus pandemic have been the victim of cybercrime, according to a new survey. Some 42% of people working remotely due to the coronavirus pandemic have received suspicious emails and 18% have tackled a security breach since lockdown began, according to the research by cybersecurity firm SentryBay [9].

Increasing Cyber Security Breaches

Given the lack of attention to cyber security at Work From Home, we have seen massive increase of cyber security targeting Work From Home ecosystem.

Hackers are actively targeting companies that launched a work-from-home policy in response to the COVID-19 outbreak by exploiting outdated virtual private networks, a lack of multi-factor authentication, and insecure at-home servers [10].

The recent worldwide assault on computer users and the internet involving worms, ransomware, malware and digital currencies, illustrates the complexities of the new threats in cyber space. The scale of the incidents came as a surprise to organisations of all sizes and industries, as well as the average computer user [11].

Further, cyber security breaches have become far more vicious during the coronavirus times. Cyber criminals are increasingly targeting hospitals, medical testing labs and other health related infrastructure to cause the maximum damage. Even, critical information infrastructure is being increasingly targeted as their cyber security is being breached for causing greater harm to the greater numbers.

Both cybercrimes and cyber security breaches are expected to massively increase with the passage of time while the world fights the coronavirus pandemic. Both cybercrimes and cyber security breaches are likely to herald in a New Cyber World Order where ground realities would be completely different. As digital users, we have to be prepare for far more cyber criminal instances and cyber security breaches, being an integral part of our day-to-day existence.

Cyber Norms

Cyber ecosystem, both pre and during COVID-19 times, has also seen focus on cyber norms. As a result, a new ecosystem of "cyber norm" processes has emerged in diverse fora and formats. United Nations (UN) groups (for example, the Group of Governmental Experts [GGE] and the Open-Ended Working Group [OEWG]), expert commissions (for example, the Global Commission on the Stability of Cyberspace), industry coalitions (for example, the Tech Accord, the Charter of Trust), and multistakeholder collectives (for example, the Paris Call for Trust and Security in Cyberspace) all purport to identify or operationalize various normative standards of behavior for states and/or other stakeholders in cyberspace [12].

Need To Keep Data & Cyberspace Safe

No wonder during COVID-19 times, various governmental agencies across the world have advised stakeholders to keep health data of individuals confidential.

In the United States, the Centers for Disease Control and Prevention ("CDC") and the US Equal Employment Opportunity Commission ("EEOC") have advised employers to keep certain personal health data confidential, and most companies have made commitments to their employees, customers, and/or users about keeping their personal health data confidential [13].

On March 13, 2020, and March 17, 2020, the German Conference of Federal and State Data Protection Authorities ("DSK") and several state-level DPAs published COVID-19 guidance on the collection and processing of health data, respectively [13].

The applicability of existing data protection legal regimes in the context of health data of COVID-19 have yet to be fully tested.

Contrasting with these are developments in China where a new law concerning encryption has been rolled out.

In the United States, there have been calls for increasing the cyber defence forces. The U.S. Cyberspace Solarium Commission, a bipartisan organization created in 2019 to develop a multipronged U.S. cyber strategy, will recommend the Department of Defense add more cyberwarriors to its forces [14].

While different countries across the world are taking steps to beef up their cyber security legal regimes, one find that there are other process taking place in other countries to protect and preserve cyber security. Different draft legislations have been introduced in different countries to protect and preserve cyber security.

Migration To The Dark Net

We are likely to see massive changes in legal approaches to superficial net and darknet. As governments across the world are increasingly emerging more stronger, they could increasingly be movements of people from superficial net to darknet, both for legitimate and illegitimate purposes.

Globalization And National Interests

Further as national interest becomes more paramount, the concept of globalization is likely to take a back seat. More and more countries are likely to move in the direction of data localization to have more control on data of their citizens. Increasingly, countries are connecting the power of data to the issue of protection of their cyber security. We are likely to see the emergence and strengthening of the concept of cyber sovereignty [20], as countries are coming up with new innovative mechanisms to expand the protection and preservation of their sovereign interests in cyberspace.

Conclusion

All said and done, the new cyber world order promises to transform we are accessing the internet. The quickly we are able to prepare about the forthcoming developments of cyberspace, the better it is. In today's Coronavirus times, nothing can be predicted as absolute. However, if one keeps in mind the broad trends on the horizon, one could potentially be more well equipped to deal with challenges concerning the new cyber world order.

It is a New Cyber World Order that COVID-19 is throwing up and it is likely to be consolidated, post eradication of COVID-19. The New Cyber World Order will be increasingly important for all digital and cyber stakeholders, as it will impact all our digital presence, digital activities and digital lives. The legal, policy and regulatory issues pertaining to New Cyber World Order will have to be appropriately considered and addressed by cyber stakeholders as

New Cyber World Order takes root in the coming times.

We have to be quickly prepare for this newly emerging New Cyber World Order. Cyberlaw jurisprudence is likely to substantially evolve in this regard. However, there will be need for coming up with appropriate checks and balances to ensure that the evolving New Cyber World Order is most reasonable, fair and balanced.

There will be need for coming up with harmonized holistic approaches for the purposes of harmonizing both the interest of nation states as also their citizens, as the New World Order in Cyberspace awaits us after the end of fight against COVID-19.

The New Cyber World Order has already emerged and is continuously evolving itself. It will be interesting to see how legal, policy and regulatory issues pertaining to New Cyber World Order are going to be appropriately addressed by stakeholders at the international, regional and national levels. All approaches concerning the New Cyber World Order, evolving during and after the COVID-19 era, have to ensure the basic principle that humanity needs to use the Internet as its biggest instrument for social upliftment, benevolence and further evolution.

Lot of current developments that are happening in COVID-19 times will substantially contribute in the solidification and further evolution of the New Cyber World Order impacting cyberspace and the Internet at large. This is a very interesting area to watch for all stakeholders who are interested in knowing how New Cyber World Order further develops and evolves with the passage of time.

References:

1. Duggal, Pavan. New cyber world order post COVID-19. eBook: Amazon.in: Kindle Store. URL: https://www.amazon.in.
2. Cyberspace and the World Order. URL: https://carnegieeurope.eu.
3. Statista - The Statistics Portal. URL: https://www.statista.com.
4. The new world order of cyber threats. URL: https://www.aon.com.au.
5. KnowBe4. Phishing. What Is Phishing? URL: https://www.phishing.org.
6. Stu Sjouwerman, 2020. Council Post: Bad Guy Tactics: How To Root Out Phishing Attempts. *Forbes*.
7. COVID-19 cyberthreats. URL: https://www.interpol.int.
8. Turner D. What Does the Covid-19 Outbreak Mean for Cybersecurity? URL: https://www.deep-secure.com.
9. Canter L. Coronavirus: Half of remote workers "victims of cybercrime". URL: https://in.news.yahoo.com.
10. Privacy and Cybersecurity Issues Related to COVID-19. URL: https://www.gibsondunn.com.
11. The new world order of cyber threats. URL: https://www.aon.com.au.
12. Ruhl C., Ruhl C. Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. URL: https://carnegieendowment.org.
13. Privacy and cybersecurity issues related to COVID- 19. 2020.
14. Pomerleau M. Congressional commission wants more cyberwarriors for the military. URL: https://www.defensenews.com.
15. World Health Organization., COVID-19 strategy update. 14 April, 2020.
16. Fida H., 2020. COVID-19 Tracing App, Respect my Privacy? Part 1. How does it work?
17. Check point. Coronavirus the day after, secure your everything. 2020.
18. Philip A., 2020. Lawful Interception of the Internet.
19. Gharibi W. Some Recommended Protection Technologies for Cyber Crime Based on Social Engineering Techniques -Phishing.
20. Yeli H. A Three-Perspective Theory of Cyber Sovereignty. PRISM. Vol. 7. № 2.

НАС ОЖИДАЕТ НОВЫЙ ПОРЯДОК В КИБЕРПРОСТРАНСТВЕ

Введение. *В данной работе представлены изменения, на основании которых были введены новые реалии измененной нормативно-правовой базы. Многие изменения начали осуществляться с самого момента наступления пандемии коронавируса. Автор работы не позиционирует себя в качестве провидца или астролога, который может с достаточной степенью точности предсказать будущее. Однако на момент написания работы начался процесс формирования коренных формообразующих изменений, которые могут повлиять на развитие нового мирового порядка в киберпространстве. Данные формообразующие изменения начинают подавать признаки необратимого по своему характеру преобразования киберпространства.*

Материалы и методы. *В методологическую основу исследования вошли следующие общенаучные и специальные методы познания правовых явлений и процессов в области кибернетического законодательства, а также в области киберпреступности и кибербезопасности, применяемые в эпоху коронавируса: системно-структурный метод; метод синтеза социально-правовых явлений; сравнительно-правовой метод; а также формальный логический метод.*

Результаты исследования. *В ходе анализа было выявлено, что киберпространство настолько сильно заполнено информацией и дезинформацией, что люди теряются в догадках: каким источникам информации им следует доверять, а каким нет. В сложившейся во всем мире неразберихе начинают формироваться новые области, привлекающие к себе внимание многочисленных заинтересованных сторон.*

Обсуждение и выводы. *В существующих условиях коронавируса невозможно ничего предсказать с абсолютной степенью точности. Однако если учитывать сформировавшиеся коренные формообразующие изменения можно приобрести больше возможностей по урегулированию актуальных вопросов, связанных с новым мировым порядком в киберпространстве. Новый мировой порядок становится более значимым для всех заинтересованных субъектов сферы цифровых технологий и киберпространства, поскольку он будет оказывать влияние на все наше присутствие, все виды деятельности и виды времяпрепровождения в сфере цифровых технологий. Правовые, организационные и нормативные вопросы, относящиеся к Новому мировому порядку в киберпространстве, должны быть соответствующим образом приняты к рассмотрению и урегулированы заинтересованными субъектами кибернетической деятельности, поскольку Новый мировой порядок в киберпространстве будет учрежден в самое ближайшее время.*

Д-р Паван Дуггал,
Адвокат, Верховный суд Индии.
Председатель Международной комиссии
по вопросам законодательства в области
кибербезопасности. Президент сети
кибернетической нормативно-правовой
базы Cyberlaws.Net.

Ключевые слова:
Новый мировой порядок в киберпространстве, коронавирус, киберпространство, кибернетическое законодательство, киберпреступность и кибербезопасность, информация, дезинформация, субъекты кибернетической деятельности

Keywords:
New Cyber World Order, Coronavirus, Cyberspace, Cyber law, Cybercrime, cybersecurity, information, misinformation, cyber stakeholders