Digitization And Cyber Security as Necessities in Time of Pandemic

Adel Eltahar
Ph.D. Candidate

DOI: 10.29322/IJSRP.12.06.2022.p12649
http://dx.doi.org/10.29322/IJSRP.12.06.2022.p12649

Paper Received Date: 3rd June 2022
Paper Acceptance Date: 17th June 2022
Paper Publication Date: 20th June 2022

Abstract

Digital technology, not only the feature of the fourth industrial revolution, simultaneously transforms all social spheres, both life and business. The modern economy cannot imagine without reliance on e-platforms and a digitized business system. However, as we have already pointed out in this paper, any form of digital business carries a number of security threats with.

Keywords: *digitalization, digital platforms, cyber crimes, cyber security.*

Introduction

During the pandemic, there was a forced insulation of the population. The further form of social relations has fallen into its opposite: social distinguishing and locking. The consequences inevitably hit the economic sector drastically. The only possibility that has somewhat relieved the failure of the economic sector, was to direct the online platform.

Communications on digital platforms spilled into a significant number of social relations, including education, business, but also delivering food. The company that hit Lock Down quickly reoriented the digital lifestyle and business. Therefore, we must emphasize that digital platforms have been given a whole new dimension: they became a macroeconomic stabilizer during the pandemic time. If this alternative was not accepted for redirecting economic activities, the consequences of Lock Downs would be catastrophic for both global and national economies.

Of course, all this was not without dealing with different types of challenges. Users of digital technologies, especially digitally written populations, are aware of all risks and challenges that carry digital platforms with them. There is especially caution when it comes to online payment. These changes led to shock in a larger number of population, especially in the part that has never worked in this way before. But, each benefit of using digital platforms, at the same time, has its other side. Mass crossing on digital platforms led to facilitated data collection that is often called "digital prints". Users are thus past their will "scanned" with all their personal data, but also needs and interests. Here we now come to the issue we especially emphasize in this work, which refers to cyber security.

New ways to organize a business

Digital platforms are a modern form of business, they also turned out that they are very useful in globally crisis situations, but at the same time endangered the rights of individuals. The balance is not yet established and will still be a challenge for modern society, which is well-known that technology contributes to collecting social platform users, which they do not give consent, but often not even aware that their data is not They collect.

Given that the pandemic continues, research on digitalization contribution to mitigating its disastrous influence is negligible little, but those who have been published so far, indicate positive effects. Of course, the world is watched here with different platforms: a rich and poor world. Of course, they are the richest at the same time and best equipped, with the strongest digital structure, which makes it easier for them to switch to digital business. On a globally widespread move to digital platforms negatively affects this digital gap. There is also a non-interest in covering the population of the Internet, of 91% coverage in North America to 38% in Podsharish Africa. The benefits of digital infrastructure during the pandemic are not equally represented in all business sectors. As a good example, the distribution of food, but again most in richer countries. This situation inevitably led to the state aimed at which methods can be solved by the digital gap. In order to increase power of digitalization to alleviate the pandemic disorder, the digital infrastructure sector should review some basic sector of the premises maintained before Cavid-19:

- For governments, it is crucial to extract these difficult lessons and take measures in the telecommunications sector that enable private operators to provide universal access to quality digital infrastructure networks for all and support the development of digital economy.
- Governments should have a much broader, holistic view of investments in high speed network, given economic, social and environment / climate also uses investment costs. • The regulatory frameworks may need to be adjusted to stimulate investments to maintain a "reasonable" level of competition, transition from "puriste" on the "pragmatic" view of state aid regulations.
- The most important thing is for governments in market development markets to advance digital infrastructure regulation, especially related infrastructure.
- Rounded experts claimed that COVID-19 could be an opportunity to launch digital transformation in sectors that have not been promoted for decades before. Similar to SARS effect in China in 2003, which caused a huge growth of e-commerce, new production methods would appear. As a result, Cavid-19 could become a catalyst for adopting digitization in sectors in which he did not occur earlier, especially in more business-oriented applications "(Report of An Economic Experts Round-19 on Digital Infrastructure organized by ITU (2020) . International Telecommunication Union Place des Nations CH-1211 Geneva, Switzerland, p. 4-5).

The pandemic made a development jump in digital transformation, because society has become aware that the digital way of taking individual economic and social activities was possible only through digital platforms. "They were critical for telemedicine, distance work and online education, not only to maintain our social connections in times of physical distancing. We are also witnessing the growth of e-commerce in developing countries, with long-term implications "(Shamika, 2021).

The global economic debug requires uniformity of digital platforms to organize a uniform business. "In this context, the e-commerce group for all partners has been awarded forces in the outbreak of COD-19, with the aim of working together as the influence of the pandemic takes place in different regions of the world, which are barriers for countries and business. they faced when they tried to take advantage of digital solutions; What are the answers to the policy be taken; And - which is not least important - what we could do better to achieve synergy and improve global support to those countries that are least equipped to manage digital transformation to deal with pandemic and beyond. This study on the influence of COD-19 on e-commerce and digital trade is a joint effort and the first research oriented project undertaken within the Etrade for All "(Shamika, 2021).

International cooperation in the field of cyber security

The natural independent character of the network and information infrastructure and its growing importance for the economy, public safety and our society do note control and combat potential threats to the demanding and critical challenge for both companies and companies.[1] Many works of cybercrime include a transnational dimension, engaging the issue of transnational investigations, sovereignty, jurisdiction, extertoritorial evidence and conditions for international cooperation. [2] The issues of cooperation are of the utmost importance for any effective regulation of globalized networked technologies. The best international practice and international cooperation, it is more obvious in the field of cybercrime, perhaps partly due to almost universality of the essential provisions of the Budapest Convention. [3]

It is often said that cyber crime knows borders, which means that criminals can easily commit crimes through national borders using internet and related electronic communications. This observation is contrary to traditional restrictions facing law enforcement agencies and judicial systems, which remain stubbornly by geographical, prosecutorial and court powers, because the cyber crime knows borders, but the criminal law remains substantially territorial character.[4]

Despite the fact that many attacks are performed in several jurisdictions and that they often come from foreign countries, the current international law does not recognize the nations as obligatory to help in the investigation of cyber attacks that allegedly originated in their jurisdiction. As a result, nations trying to develop and implement Cyber security measures often do not have international support from nations from which a certain cyber attack was likely to be created. Even when the victim provides cooperation by the state in accordance with, for example, a contract of mutual legal aid (beating), evidence requirements often takes several months to comply, if they are met at all. Since evidence of cyber attacks can be quickly removed, current international agreements such as the smaller co-operation between law enforcement bodies are being able to be effective.[5]

No national state can reach adequate cyber security itself, so international coordination and cooperation must be part of the answer to this problem.[6] The current international cooperation does not take into account the specifics of electronic evidence and the global nature of cybercrime. This is especially true for cooperation in investigative actions. Lack of common approach, including current instruments of multilateral cybercrime, means that acknowledgments, such as accelerating data outside those countries with international obligations to provide such an facility and to make it available on request, may not be easily met. Globally, differences in the extent of cooperation provisions, the lack of an obligation to respond time, more non-formal law enforcement and variations in protective cooperation measures, represent significant challenges for effective international cooperation related to electronic evidence in criminal matters.[7] Moreover, sovereignty and other issues represent countries with inherently opposed political goals and cultural conflicts, including the need to balance different interests and rights, and are difficult to develop rapidly developing the structure of any agreement.[8] Despite the challenges, in recent years, there has been significant success in law enforcement. Some of them included a high degree of international cooperation in law enforcement, with the help of modernized understanding of the legal competence and use of cross-border mechanisms such as mutual legal

[1] Kremer Jan-Frederik & Müller Benedikt (2014). Cyberspace and International Relations: Theory, Prospects and Challenges. Springer .

[2] Sandage, John et al. eds. (2013). Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime).

[3] Satola David & Judy Henry (2011). *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW.

[4] Urbas Gregor (2012) *Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement*, JOURNAL OF INTERNET LAW, Vol. 16, Issue 1: 7-17

[5] Stahl, William M. "*The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*." Georgia Journal of International and Comparative Law. Vol. 40. (2011): 247-274.

[6] Satola David & Judy Henry (2011). *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW.

[7] Sandage, John et al. eds. (2013). Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime).

[8] Satola David & Judy Henry (2011). *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW.

assistance and extradition.[9] Since the powers of law generally do not exceed the national borders, for example, permitting police from one country to travel and investigate crimes in another, without permitting this second, cross-border investigation depends on cooperation at the level of the National Agency or even a local official. Cooperation can take place with minimal formalities, through temporary contacts between officials or through the established communication channels such as 24/7 contact points for law enforcement, as provided by the Council of Europe Convention on cybercrime.[10]

Due to the unstable nature of electronic evidence, international cooperation in criminal matters in the field of cybercrime requires timely answers and the possibility of requiring specialized investigative actions, such as computer data conservation. The time to respond to formal mechanisms, currently being used, are several months, and for extradition requirements and for mutual legal aid, which is a time frame that is a challenge for collecting unstable electronic evidence. Initiatives and innovations for informal cooperation and to facilitate formal cooperation, such as networks 24/7, offer an important potential for faster response time. Formal and informal ways of cooperation are designed to manage the process of giving the agreement of the State for the implementation of foreign law enforcement issuing laws that affect the sovereignty of the state.

However, more and more investigators, consciously or unconsciously access extertoritorial data during evidence collection, without the consent of the state in which the data is physically found. This situation arises, especially, due to cloud computing technologies (cloud) involving storage data in multiple data centers in different geographical locations. "Location" of data, although technically known, is becoming all artificial, to that measure that even traditional requirements for mutual legal assistance will often be sent to the country, which is the headquarters of service providers, not the country in which the data center is physically located. Investigators for law enforcement may, occasionally, receive data from extertoritorial service providers through an informal direct request, although service providers usually require appropriate legal proceedings.[11]

Among countries such as Australia, New Zealand, Canada, United States and many European countries have been established in sufficient contacts during years to enable very effective cooperation. With countries in Eastern Europe or developing countries, new relations have been established. For example, in the last decade, the US Ministry of Justice (DOJ), especially through its computer crime and intellectual property (CCIPS), has successfully encouraged cooperation agencies in Belarus, Bulgaria, Estonia, Poland, Romania and Ukraine, as their traditional partners, in order to distract the International Group for Cyber Crime and bringing their members to justice.[12]

In the most sophisticated, law enforcement agencies in several countries are able to share operational information and coordinate key shares in real time, so that the executions of the search and arrests occur at the same time at different locations around the world. It is clear that this is important to ensure that all members, globally scattered groups can be arrested before they have the opportunity to escape or destroy evidence. Significant internationally coordinated actions against international groups for the exploitation of children and global copyright protection groups have been reported.[13]

Private, governmental and non-governmental sectors, based on national and international efforts, take steps to increase the safety of its products, services and networks. These efforts include, for example, the work of international bodies for standards, which range from the International Telecommunications (ITU), based on contracts to non-governmental, but very

[9] Urbas Gregor (2012) *Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement*, JOURNAL OF INTERNET LAW, Vol. 16, Issue 1: 7-17

[10] Ibid

[11] Urbas Gregor (2012) *Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement*, JOURNAL OF INTERNET LAW, Vol. 16, Issue 1: 7-17

[12] Ibid

[13] Ibid

influential and essential bodies, such as Internet Engineering Working Group (IETF). Important issues for consideration include the role of standards and role in government development.[14]

Cyber security is the problem of the twenty-first century that requires answers. However, in the legal sphere, many concepts developed in analogue ERI simply cannot be applied in a digital era, or cause difficulties when applied. For example, the lack of consensus on basic and related matters of competence and sovereignty makes it difficult for an effective transition of borders to resolve international incidents of cyber security. The National State may consider that its sovereignty has been violated, if another national state can perform "jurisdiction" within its borders. However, national states may consider that their sovereignty has improved, if a joint arrangement gets jurisdiction in the territories of each other. In order for the rule of law prevalents, the inherent cross-border nature of cyber space seems to require such agreements in order to mutually expand competencies.[15]

Cyber security and cybercrime-based access to contracts

The international community has a clear interest in the development of a comprehensive, multilateral use of Internet in every aspect of everyday life has created almost non-residential advantages and because the conceptual basis of existing legal frameworks are not easily adaptable threats that appear in cyber Space.[16]

There is no comprehensive international legal framework dealing with cyber security. International efforts to solve this issue are a narrow scale, focusing primarily on data privacy and human rights, to the expense efforts to define and differ different levels of cyber aggression and are a different level of international approach to deal with challenges. In the absence of codified law, nations trying to implement its cyber security regimes, against foreign perpetrators, they made them mainly according to international law regulating military use of force and domestic criminal law. Existing international agreements on cyber security are a narrow range, focus on criminal activities in cyberspace and fail in an adequate way to consider cyberspace as a platform for terrorism and military action.[17]

These shortcomings can be partly due to the nature of cyber aggression, which in question the conceptual categories we have used so far to avoid chaos and maintain order in our societies and our lives. Without a comprehensive international definition, the species of cyber aggression, the nation will continue to face the challenges in assessing the laws of their response to a given attack. Also, since there is no international body to investigate and prosecute the criminal aggression without restrictions on the site, nations resort to legal systems based on the principle of territorial competencies in creating answers to cyber attacks. Efforts of the nation are hampered by the fact that international law does not recognize any obligation to help other countries in the investigation of cyber aggression without explicit agreement between the parties. Definitely, lacking a comprehensive international agreement on some or all aspects of cyber security issues.

Conclusion

Any attempt to achieve an international consensus on cyber security will probably reveal a number of concerns, which arise from different visions of national security, on the role of internet, human rights and economic policy. Some see cyber security as the core of state security, which leads to emphasis on the possibilities of monitoring and attribution of transmission

[14] Satola David & Judy Henry (2011). *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW.

[15] Ibid

[16] Stahl, William M. "*The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*." Georgia Journal of International and Comparative Law. Vol. 40. (2011): 247-274.

[17] Stahl, William M. "*The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*." Georgia Journal of International and Comparative Law. Vol. 40. (2011): 247-274.

and blocking any undesirable content. Others believe that internet management (including safety on the Internet) includes integration and balancing of interest, including not only national security, but also human rights and economic and development interests associated with a lively, innovative and competitive ICT sector. These different perspectives are manifested in many areas, including, for example, an increasing debate on the issue of attribution. [18]

Although no significant shifts have been noticed in the last decade in the declaration of agreements on cyber security, the proclamation of international and regional instruments aimed at combating cybercrime were more successful. This includes binding and non-binding instruments. Five groups of international or regional instruments can be identified, consisting of instruments developed in context or inspired:

- Council of Europe or the European Union,
- Community of Independent States or Shanghai Cooperation,
- Intergovernmental African organization,
- The League of Arab States, and
- the United Nations.

[18] Satola David & Judy Henry (2011). *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW.