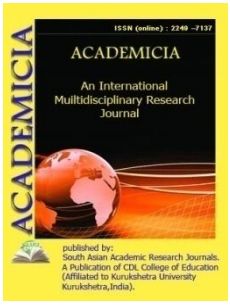
ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)



DOI: 10.5958/2249-7137.2021.01746.8

THE IMPACT OF GOVERNMENT REGULATION AND SURVEILLANCE OF INFORMATION COMMUNICATION TECHNOLOGIES

Gofurov Mansurjon Ravshanbekovich*

*Assistant of Business Department,
Kokand University, UZBEKISTAN.
Email id: gofurovmansurbek@gmail.com

ABSTRACT

As human lives transition online, so do human rights. The main challenge for the world and other actors is to transition all human rights to the digital sphere. This paper argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. This article provides an overview of countries and companies that pose risks to human rights in the digital sphere and development of information communication technologies. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere.

KEYWORDS: *ICT, Internet, Facebook, Human Rights, Companies, E-Mail, Countries Of The World, Digital Sphere, Digital Economy, E-Government.*

INTRODUCTION

As human lives transition online, so do human rights. While human rights were developed at a time before the accelerated dynamics of digitization, their value to protect every individual remains the same. In order to fully enjoy their safeguards, our understandings, frameworks, the roles of different actors and tools to protect and promote human rights, these need to be refined, clarified, revised and updated. This report hopes to contribute to a better understanding of human rights in the digital age. The key word is 'transition': human rights protections need to be effectively enforced in the digital sphere. Only then, will the affirmation "the same rights that people have offline must also be protected online" be truly meaningful. Developments in information and communication technology (ICT) have not only transformed economic, political and social life, they have also altered lives of almost every single individual in the world. Whether we like it or not, our lives are all irrevocably influenced by this transition. Whenever

civil unrest and protests occur around the world, the Internet, mobile phones, and social media are invariably blamed or praised for enabling these popular expressions of discontent. Such events encourage us to think of the Internet and the Web as an extraordinary technology unleashing torrent of human creativity, innovation, expression, popular rebellion, and sometimes, even democracy. How ironic then that the same Internet has also spawned an explosion in government control and surveillance. Totalitarian dictators of the mid twentieth century would have given their eyeteeth for a technology such as this, that can track what millions of people do, say, think, and search for in billions of e-mails, searches, blogs, and Facebook posts every day. In the early years of the Internet and the Web, many people assumed that because the Internet is so widely dispersed, it must be difficult to control or monitor. But the reality is quite different. Just about all governments assert some kind of control and surveillance over Internet content and messages, and in many nations, this control and surveil- lance is very extensive. While the Internet is a decentralized network, Internet traffic in all countries runs through large fiber optic trunk lines that are controlled by national authorities or private firms. In China, for instance, there are three such lines, and China requires the companies that own these lines to configure their routers for both internal and external service requests. When a request originates in China for a web page in Chicago, Chinese routers examine the request to see if the site is on a blacklist, and then examine words in the requested web page to see if it contains blacklisted terms. The system is often referred to as “The Great Firewall of China” (but formally by China as the “Golden Shield”) and was implemented with the assistance of a number of U.S. technology firms such as Cisco (the largest manufacturer of routers in the world), Juniper Networks, and Blue Coat (which provides deep packet inspection software), among others.

Main body. Over the past several years, China has strengthened and extended its regulation of the Internet in the name of social stability. In June 2017, a new comprehensive statute governing cyber security went into effect in China. The law requires that data relating to Chinese citizens must be stored on Chinese servers and that firms must submit to a security review before moving data out of China. The law makes unauthorized collection of such data a criminal offense. Other legislation provides that web users may be jailed for up to three years if they post defamatory rumors that are read by more than 5,000 people. China has also issued rules to restrict the dissemination of political news and opinions on messaging applications such as We Chat and WhatsApp, and in July 2017, began using image filtering technology that enables it to erase images sent on those apps in mid-transmission, before they are ever received. Users are required to post political opinions and news only to state-authorized media outlets and are required to use their own names when establishing accounts. In 2016, China issued new rules barring foreign companies or their affiliates from publishing online content without government approval. It also began to subject online programs to the same censorship regulations as regular TV shows. It also said it would punish websites that publish unverified social media content as news, and ordered several of the most popular Chinese portals, such as Sinu, Sohu, and Net Ease, to cease original news reporting. While China is often criticized for its extensive Internet controls, other countries are not far behind. Iran’s Internet surveillance of its citizens is considered by security experts to be one of the world’s most sophisticated mechanisms for controlling and censoring the Internet, allowing it to examine the content of individual online communications on a massive scale. The Iranian system goes beyond merely preventing access to specific sites such as Google, Twitter, and Facebook and reportedly also utilizes deep packet inspection. Deep packet inspection allows

governments to read messages, alter their contents for disinformation purposes, and identify senders and recipients. It is accomplished by installing computers in the line between users and ISPs, opening up every digitized packet, inspecting for keywords and images, reconstructing the message, and sending it on. This is done for all Internet traffic including Skype, Facebook, e-mail, tweets, and messages sent to proxy servers. In 2016, Iran completed the first stage of establishing an isolated, domestic version of the Internet that it calls The National Information Network, one that purportedly is faster and less costly, but which controls what users can and cannot see and subjects its users to even more heightened surveillance. In February 2017, it launched the second phase of the Network.

In Russia, the government may close websites without a court decision if the General Prosecutor's office declares the material on a site to be "extremist." Russia also regulates the blogosphere, requiring bloggers with more than 3,000 daily readers to register their real names and contact information with Russia's communications regulator. Russia also has a law similar to China's requiring Inter- net companies to store their data on Russian soil, which allows the government to control it and limit access, and in July 2016, passed additional laws that provide for mandatory data retention by ISPs and telecommunications providers for between 6 months and three years, require those companies to provide access to all such data without a warrant, and also require a government backdoor that will enable it to access all encrypted communications.

In July 2017, Russia enacted a law banning the use of virtual private networks (VPNs) and anonymizers, tools that can be used to establish a secure and anonymous connection to the Internet. Turkey is another country that has increasingly attempted to control and censor Internet content. These efforts have increased after the terrorist attack on Istanbul's Ataturk Airport and the failed coup against President Recep TayyipErdogan. In April 2017, the Turkish government blocked access to Wikipedia after it refused to remove various statements that the government found objectionable. But it is not just totalitarian nations that have sought to regulate and surveil the Internet. Both Europe and the United States have, at various times, also taken steps to control access to certain websites, censor web content, and engage in extensive surveillance of communications. For instance, Great Britain has a list of blocked sites, as do Germany, France, and Australia. The United States and European countries generally ban the sale, distribution, and possession of online child pornography. France, Germany, and Austria all bar the online sale of Nazi memorabilia. Even in South Korea, one of the world's most wired countries, there are restrictions on content that is deemed subversive and harmful to the public order. In response to terrorism threats and other crimes, European governments and the U.S. government also perform deep packet inspection on e-mail and text communications of terrorist suspects. This surveillance is not limited to cross-border international data flows and includes large-scale domestic surveillance and analysis of routine e-mail, tweets, and other messages. In 2013, National Security Agency (NSA) contractor Edward Snowden made headlines by leaking classified NSA documents shedding light on the NSA's PRISM program, which allowed the agency access to the servers of major Internet companies such as Facebook, Google, Apple, Microsoft, and many others. Additionally, the documents revealed the existence of the NSA's XKeyscore program, which allows analysts to search databases of e-mails, ats, and browsing histories of individual citizens without any authorization. Warrants, court clearance, or other forms of legal documentation are not required for analysts to use the technology. Snowden's documents also showed spy agencies were tapping data from smartphone apps and that the NSA was tapping the

flow of personal user information between Google and Yahoo. The NSA claimed that the program was only used to monitor foreign intelligence targets and that the information it collects has assisted in apprehending terrorists. The FBI also has an Internet surveillance unit, the National Domestic Communications Assistance Center. The NDCAC's mission is to assist in the development of new surveillance technologies that will allow authorities to increase the interception of Internet, wireless, and VoIP communications. Many European powers have also moved ahead with plans to fortify their online surveillance. In response to multiple terrorist attacks, France has passed rules that force ISPs to maintain browsing data, as well as additional provisions for surveillance of phone calls, e-mails, and all mobile phone communications. The Investigatory Powers Act 2016 gives the British government some of the world's strongest powers to conduct online surveillance, including the bulk interception of overseas-related communications, and after further terrorist attacks in 2017, some British politicians are pushing for even stronger measures. In Germany, the Communications Intelligence Gathering Act authorizes Germany's Federal Intelligence Service to gather and process communications of foreign nationals, including communications flowing through Internet Exchange Points (IXPs) located within Germany.

CONCLUSION

However, in the United States, efforts are underway to curb domestic and international counter-terrorist agencies like the NSA from con- ducting dragnet surveillance of the entire American population, strengthen court oversight of surveil- lance, limit surveillance to specific individuals, and ease disclosure rules for Internet firms who receive requests from government agencies. In 2015, Congress passed the USA Freedom Act, which limits the bulk collection of Americans' phone records. However, equally concerted efforts are underway to expand these types of spying powers. Forinstance, the Obama administration expanded the NSA's ability to perform warrantless wiretaps on suspected malicious hackers, allowing them to monitor international Internet traffic from these suspects as well as domestic traffic. Concerns about the use of the Internet and other methods of encrypted communications by the Islamic State to recruit new members and engage in terrorism have further heightened the tension.

REFERENCES:

1. K. C. Laudon, C. G. Traver. E-COMMERCE: business, technology, society. Pearson – 2018.
2. Hoffmann, K., The EU in Central Asia: successful good governance promotion? Third World Quarterly, 2010.
3. HRW, Hungary. Human Rights Watch, 2014. Retrieved January 06, 2015, from http://www.hrw.org/europecentral-asia/hungary
4. LaFrance, A., Where Design Choices and Civil Rights Overlap - The Atlantic. The Atlantic, 2015. Retrieved January 14, 2015, from http://www.theatlantic.com/technology/archive/2015/01/where- design-choices-and-civil-rights-overlap/384142/
5. Mulaydinov, F. (2021). Digital Economy Is A Guarantee Of Government And Society Development. *IlkogretimOnline*, *20*(3), 1474-1479.
6. Butaboyev, M., Urinov, A., Mulaydinov, F., &Tojimatov, I. Digital economy.

7. Farkhod, M. (2020). Econometric Modelling of the Innovation Process in Uzbekistan. *InternationalJournalofPsychosocialRehabilitation*, *24*(02).

8. TURSUN, S., TUYCHIEVICH, B. M., & MUROTOVICH, M. F. Effects of the Global Crisis on the Economy of Uzbekistan During the CoronovirusPandemidia and Measures to Ease IT. *JournalNX*, *6*(05), 277-280.

9. Solidjonov, D. Z. (2021). The Impact Of Social Media On Education: Advantage And Disadvantage. *Экономика и социум*, (3-1), 284-288.

10. Solidjonov, d. z. o. (2021). the impact of the development of internet technologies on education at pandemic time in uzbekistan. in *студент года 2021* (pp. 108-110).

11. Abboud, L., &Maushagen, P., Germany wants a German Internet as spying scandal rankles, Reuters, 2013. Retrieved March 05, 2015, from http://www.reuters.com/article/2013/10/25/us-usa-spying- germany-idUSBRE99O09S20131025

12. Arce, N., Cyber Attack Bigger Threat Than ISIS, Says U.S. Spy Chief. Tech Times, 2015. Retrieved March 06, 2015, from http://www.techtimes.com/articles/35965/20150227/cyber-attack-bigger- threat-than-isis-says-u-s-spy-chief.htm

13. Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J., After Snowden: Rethinking the Impact of Surveillance. International Political Sociology, 8(2), 121–144. doi:10.1111/ips.12048, 2014.