у законодавстві України, проблеми створення механізму їх належної та ефективної реалізації, а також розробити відповідні пропозиції.

UDC 355.451:004.7 (043.2)

Nageshwar Tigadi, Master,
Rajiv Gandhi University of Health Sciences, Bangalore,
Karnataka state, the Republic of India
Scientific Advisor: Myronets O.M., PhD in Law, Senior Lecturer

NEW CYBER POLICY IN INDIA

According to the Data Security Council of India, Indian is the second most cyber-attacked country in the world after the US. In the recent past, there has been a significant increase in cyber threats, and if the situation is not addressed, this could impact the GDP of the country, massively [1].

Indian telecom service providers offer the lowest data rates in the world. India is also the most populous country, with 1.3 billion people. More than half its population comprise youth below the age of 25 years. And smartphones are the primary source of Internet access for most Indians. With the availability of affordable data packs and falling smartphone prices, Indians are consuming more services (and data) on the Internet, through mobile apps, and of course, by watching a lot of videos! Digital payments and mobile wallets took off after the Government of India announced demonetization in 2016. All this makes Indian consumers prime targets for hackers who are out to steal user credentials (like credit card numbers and authentication details) and money from mobile wallets [2].

The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25) [3].

According to the Sixth Cyber Security India Summit 2020, the new policy is expected to be launched in the next two to three months and will address all the issues related to the cyber ecosystem, be it standardization, testing, auditing, and capacity development among others [1]. Proposed vision is to ensure a safe, secure, trusted, resilient and vibrant cyber space for our Nation’s prosperity [3].

A report from Symantec Corp. (now part of Broadcom) last year revealed that India is the second most cyberattacked country in the world, after the U.S. and China. This was widely reported in the media. Indian law, notably the Indian IT Act 2000, does not fully protect its citizens from new threat vectors like phishing, SIM jacking, ransomware, mobile payments fraud, bank fraud, malware attacks, social engineering, and DDoS attacks – all increasingly common these days. But the Indian government is expected to release a new

cybersecurity policy this year. India's Personal Data Protection Bill is also under review and is expected to be passed this year [2].

At the same time, as the investments in ICT infrastructure grow the vulnerability to damage by natural disasters or through attacks by insurgents/terrorists with objective to immobilize and paralyze day-to-day activities of the nation is becoming real. Such damage would cause short and long term setback to economy. We have many lessons from US initiative to secure our cyber system, while planning and implementing India's ICT infrastructure. Natural or insurgency/terrorist induced disaster increases pressure on available ICT systems exponentially to facilitate coordination between various agencies like fire brigade, medical services, police, media and civil administration. It is proposed that the existing and planned ICT infrastructure of the nation, both in public and private domain be analyzed by a group of experts under aegis of NDMA to suggest suitable operational arrangements to minimize their vulnerability to perceived attacks by inimical elements and natural disasters. This would entail rigorous technical analysis of current and emerging wireless and wired ICT systems. The expert group should find and recommend suitable mix of redundancies in the critical ICT systems supporting the governance structure of the nation. The focused analysis of the vulnerabilities and their protection, would lead to recommendations that would avoid duplication of effort and, therefore, economical at national level. The notion that disasters can be completely brought under control by technological and scientific capabilities alone would be too presumptuous. The most sacrosanct component in any such venture is participation from all stakeholders to ensure an appropriate solution for the welfare of humanity [4].

Pillars of Strategy We are examining various facets of cyber security under the following pillars: a. Secure (The National Cyberspace); b. Strengthen (Structures, People, Processes, Capabilities); c. Synergise (Resources including Cooperation and Collaboration) [3].

There is a renewed focus on cybersecurity practices in India, both from the government and the private sector. Many of the gaps existing in the current law (in terms of liability, penalty, reporting, disclosures, etc) are likely to be addressed in the new Personal Data Protection Bill 2019, which is expected to be passed in Parliament next year. The private sector is to intensify its engagement with the government in this area in view of the Digital India initiative, the increased volume of financial transactions online and the high level of reporting of cybersecurity attacks in India. The government is expected to develop a focused approach towards cybersecurity preparedness and awareness, including introducing its cybersecurity policy in 2020 [5].

Thus, the new cyber policy in India is still debatable in its details but it is accepted by the whole society as the need for the development of the whole country.

References

1. Amit Raja Naik. India To Launch National Cybersecurity Policy In The Next Three Months. URL: https://inc42.com/buzz/india-to-launch-national-cybersecurity-policy-in-the-next-three-months/ (date of access: 29.04.2020).
2. Brian Pereira. India to Get a New Cybersecurity Policy. URL: https://www.cisomag.com/india-cybersecurity-policy/ (date of access: 29.04.2020).
3. National Cyber Security Strategy 2020 (NCSS 2020). URL: https://ncss2020.nic.in/(date of access: 27.04.2020).
4. Chaturvedi M. M., Gupta M., Bhattacharya J. Cyber Security Infrastructure in India: A Study URL: https://www.researchgate.net/publication/228846974_Cyber_Security_Infrastructure_in_India_A_Study (date of access: 29.04.2020).
5. Aprajita Rana, Rohan Bagai. Cybersecurity in India. URL: https://www.lexology.com/library/detail.aspx?g=4cd0bdb1-da7d-4a04-bd9c-30881dd3eadf (date of access: 29.04.2020).

УДК 340(043.2)

Dr. Martín Beltrán Saucedo, Research professor,
Coordinator of the Master in Constitutional Law and Amparo,
Autonomous University of San Luis Potosí, Mexico,
Dr. Renfred Paisano, Teacher, Vice Dean Faculty of Legal and Social Sciences, Bluefields Indian & Caribbean University Bilwi Campus,
Puerto Cabezas,
Autonomous Region of the North Caribbean Coast, Nicaragua,
Doctor in Labor Law from the Paulo Freire University
of Managua, Nicaragua

ПРАВА ЧЕЛОВЕКА И ПРАВА РАБОТНИКОВ ДАЙВЕРОВ В АВТОНОМНОМ РАЙОНЕ СЕВЕРНОЙ ЧАСТИ КАРИБСКОГО ПОБЕРЕЖЬЯ НИКАРАГУА

Качество жизни в дайвинге на северном побережье Карибского моря в Никарагуа тесно связано с трудовыми правами человека и социальными правами. Однако понятие потребностей очень ограничено, и предлагается сделать шаг к концепции прав. Говорит Эрнандес, Х. (2007: с. 16). это (...). «Потребности не создают обязательств для государств». Права делают и делают это на основе человеческого достоинства. По этой причине они имеют политическую и юридическую ценность, которой нет с точки зрения потребностей. Они позволяют жить достойно, могут быть востребованы правительством и подразумевают обязанность правительства соблюдать его.

Такие авторы, как Фольгадо и Элио Гальего, обращают внимание на видение субъективного права как факультета или «протестов», то есть как силы, которую можно требовать. «Конкретный индивид» не соответствует