UDC 343.236:001.102:667(043.2)

Andoh Ernest Nyame Yie, Master student,
the University of Salford, Salford, Manchester,
the United Kingdom of Great Britain and Northern Ireland
Scientific advisor: Myronets O.M., Senior Lecturer

THEORETICAL AND LEGAL ASPECTS OF CYBERCRIMES IN GHANA

In Ghana illegal actions in the informational sphere are called “sakawa”. They may have different types and their investigation is still very important and relevant to improve security in this country and sufficient protection of human rights and freedoms.

Ghana has had a number of websites defaced by hackers in recent times. The most recent one being Ghana’s official web portal. Very important websites like the website of National Communication Authority, the National Information Technology Agency (NITA) and the website of the vice president of Ghana have all being defaced in recent past. These attacks have indented the national image of Ghana and indicated a security weakness of our cyber infrastructure and space [1, p. 9].

As Jason Warner admitted, internet criminality has recently surfaced as a real concern for law enforcement officials in Ghana, and by proxy, members of the global community at large. Its victims range from Europeans to Ghanaians to U.S. citizens, yet relatively scant attention has been given to gaining an understanding of the ground-level realities underpinning these processes. This article has sought, in its own modest way, to broach the topic in ways that have heretofore been unexamined. It began by giving a standard, top-down overview of the contemporary incarnations of Ghanaian cybercrime, before moving on to investigate three more complex, yet understudied, grassroots realities that must be understood if Internet criminality is to be mitigated [2, p. 747].

A deduction from the above is that the four major forms of cybercrime are hacking, credit card fraud, software piracy and cyber identity theft. 40 (20.0%) of the respondents indicated that hacking is a form of hacking, 36 (18.0%) associated theirs to credit card fraud, 30 (15.0%) also associated theirs to software piracy, 22 (11.0%) related their reason to cyber identity theft, 11 (5.5%) also related their forms to cloning of website or phishing. Again, 20 (10.0%) indicated pornography as a form of cybercrime, 15 (7.5%) associated theirs to sweet heart swindle (social network), 10 (5.0%) stated cyber defamation as a form and 9 (4.5%) also associated their reason to the malicious program or virus dissemination. The remaining 7 (3.5%) indicated cyber stalking as a form of cybercrime [3].

Cyber crime is common to both developed and developing countries. Its impact appears to be worse in developing countries where the technology and

law enforcement expertise is inadequate. This shared challenge tends to be reflected in Ghana. The limited options for the Police, legal and financial institutions to address cyber crime call for a multi-stakeholder analysis at the national-level. Concerning practice and policy implications, the research provides the basis for a concerted effort on the part of individual citizens and corporate bodies, to report cyber crime cases and demand that government put in place laws, policies and technologies to curb cyber crime. As with other forms of ICTs, since these laws are critical, there is the need to gain political support. This could be from the government, or political parties, interest groups, private sector advocates, thus key stakeholders who can push for these legislation and rules. The government should empower the Police force by providing the needed training and technical resources required to discharge their duties effectively. Internet service providers operating in the country should also be mandated to report suspicious traffic going through their networks. Since cybercrime is a global problem, the need also arise for law enforcement agents in Ghana to collaborate in the area of information sharing, infrastructure and personnel with other African Countries and major international security agencies such as the Federal Bureau of Investigation and INTERPOL to crack-down on cyber criminals [4, p. 96].

According to Kwaku Anhwere Barfi Mr., Paul Nyagorme Dr., Nash Yeboah Mr., it is recommended that 1) curriculum in the Senior High Schools should include courses on cybercrime, cyber management and its prevention in both tertiary and secondary schools to take care of social changes; 2) the Government of Ghana in conjunction with the security services should develop a national cyber security technology framework that specifies cyber security requirement controls for individual network user; 3) the Ghana Police service should develop and maintain a national culture of security standardize to coordinate cyber security awareness and education programme for all levels of students; 4) it is therefore incumbent on Parliament to enact cyber laws to churn out policies geared at equipping judges and lawyers with the requisite knowledge to understand the intricacies of cybercrime and to facilitate effective prosecution of cybercrime cases in Ghana; 5) a cybercrime court could also be established in Ghana to speed up prosecution of cybercriminals and encourage more judges and lawyers to specialize in cyber law; 6) however, relevant Ghanaian authorities must therefore institute appropriate measures to check the influx of e-waste into Ghana to mitigate the incidence of cybercrime in the country [3].

In our opinion, the state’s legal methods to regulate the question of cybercrimes are very important to be not just determined but also implemented. For this, it is needed to improve not just legislation but informational literacy and informational culture in the state.

Literature

1. Ghana National Cyber Security Policy & Strategy. March 2014. 49 p. URL: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Ghana_Cyber-Security-Policy-Strategy_Final_0.pdf. (date of access: 22.01.2019).

2. Jason Warner. Understanding Cyber-Crime in Ghana: A View from Below. International Journal of Cyber Criminology (IJCC) ISSN: 0974–2891 Jan–July 2011, Vol. 5 (1). P. 736-749. URL: https://www.cybercrimejournal.com/ warner2011ijcc. pdf. (date of access: 22.01.2019).

3. Kwaku Anhwere Barfi Mr., Paul Nyagorme Dr., Nash Yeboah Mr. The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region. Library Philosophy and Practice (e-journal). 2018. URL: http://digitalcommons. unl.edu/cgi/viewcontent.cgi?article =4891& context = libphilprac. (date of access: 22.01.2019).

4. Richard Boateng, Longe Olumide, Robert Stephen Isabalija, Joseph Budu. Sakawa - Cybercrime and Criminality in Ghana. Journal of Information Technology Impact. Vol. 11, No. 2, pp. 85-100, 2011. URL: https://www.researchgate.net/ publication/ 265446452_ Sakawa_-Cybercrime_and_Criminality_in_Ghana. (date of access: 22.01.2019).

УДК 34.01(043.2)

Краснобаева Л.А., к.ю.н., доцент,
Белорусский государственный университет,
г. Минск, Республика Беларусь
Лисовская Т.В., к.и.н.,
Брестский государственный технический университет,
г. Брест, Республика Беларусь

ДИСКУРС-АНАЛИЗ КАК ИНСТРУМЕНТ ПРАВОВОЙ КОММУНИКАЦИИ

Правовую коммуникацию в правовой сфере можно определить как процесс передачи правовой информации, процедуру правового общения, включающую в себя стадии обмена информацией, организации взаимодействия и процесса восприятия, оценки, взаимопонимания. На первое место в исследованиях правовой коммуникации выдвигается дискурс как способ «коммуникативно-социальной деятельности по обмену разного рода информацией. Дискурс-анализ относится к качественным инструментам, позволяющим исследователю выявить скрытый смысл, заложенный в нормативно-правовых актах и его проявление в процессе реализации правовой коммуникации. Модель профессионального правового дискурса разработана на основании теоретической модели дискурса М. Хэллидея, с использованием методологии и методики дискурсного анализа Т.А. ван Дейка [1, с. 41].