

Cyberdeviance and the Role of Data Privacy Officer's Sustainable Structures in its Prevention

Silva Ibrahimimi

*Albanian University, Faculty of Social Sciences, Tirana
Department of Psychology and Research Center*

Eglantina Dervishi

*University of Tirana, Faculty of Social Sciences
Department of Psychology and Pedagogy*

Ervin Ibrahimimi

Security Council, Italy

Received 8 July 2018 ▪ Revised 30 November 2018 ▪ Accepted 10 December 2018

Abstract

Prevention is undoubtedly one of the core items of today's health and social care. Mass media, technology and the information technology system are of the most influential tools in the cognitive and psychological development of a person's social life. The objective of the present article is to explore some of the basic aspects of the relationship between cyber deviant behaviors and the role of order security and cyber security structures such as the Data Privacy Officers (DPO) that exist in the cyber-digitalization preventing process. This article intersects the core aspects of deviant cyber subculture and the role of DPO officers in the screening and prevention of criminal extreme acts. The implementation of misguided protection strategies and consumer safety from hazardous navigation and risky online behaviors directly affects the growth of passive and active criminality, qualitative changes of attitudes and behaviors by pointing more towards antisocial personalities and rising risks for a broader national and regional security.

Keywords: cyber deviant behavior, digitalization technology, DPO, national security, prevention.

1. Introduction

Technical and technology developments have made human life changing a lot over the last decades. Within the development and refinement of technology in general and the informative one in particular, remains the *cyberspace* as an important part. The Internet can have a powerful impact on the development of value systems and shaping behavior.

The extraordinary increase in the use of computer technology and information, ICT, has brought a very wide range of exploration opportunities and vulnerability to exposure risk in the juvenile populations. Given its global and easy access character through connected devices, the internet has undoubtedly changed the socio-evolutionary form of the mankind. ICT influences on fluid and crystallized intelligence are two important arguments in support of this premise.

On the hand, the alienization of technology has also provided new crime opportunities that can use the same advantages offered by these technologies to meet their own objectives. The growing number of Internet users offers society the perspective to accelerate communications in everyday life and for the purpose of fostering relationships, reducing transactions and spending, doing business, increasing access to information, and creating a *global identity*.

On one hand, with the development of new opportunities for economic and social growth, the distribution of technology has changed the current picture of the concept of crime and introduced new challenges to the community, for micro and macro policy-makers as well as law enforcement officers. The cyberspace is constantly a major source of various illegal activities that include not only the emerging new types of crime, such as *hacking* or tracking through encryption or spyware programs, but also poses a specific concern in the increasement of the right for the protection of personal data and on the broader national security.

On the other hand, aggressive cyberdeviance has also led to an increased influx of traditional crime migration such as malicious exposure, trafficking, pornography and juvenile abuse, fraud, theft, etc. From the way we build an investigation profile, information sources, designs, stages and the need for and assistance that gives a profile, we can construct data on the psychological profile of the author and the target group as well as with the stimulating behavior and psychological state of an individual in committing a criminal act (Agastra et al., 2017).

Undoubtedly, the fight against cybercrime requires strengthening, either at the legal, but also at the criminal and procedural level, the instruments that allow the investigation and prosecution of persons who abuse with ICT for committing criminal acts. The present global dimension of cybercrime and the transboundary nature of information networks through ICT also bring the need for harmonization of legislative approaches and coordinated actions in the prevention and investigation of cybercrime at national, regional and interregional levels (Gercke, 2006-2009).

Although ICT networks are largely privately owned, the comprehensive cybercrime approach also includes the development of tools for effective cooperation with the industrial informatic sectors that promote the implementation of co-regulatory and self-regulatory methods.

Every actor in this multilateral environment interested in combating and preventing crime in the cyberspace faces a wide range of challenges that may be related to general problems of the global nature of cybernetics or the unique character associated with the change of nature of the tasks, responsibilities and functions of the parties used to act either in the real world or in the cyberspace. Police as a responsible and regulatory entity for maintaining and protecting public order, detecting, monitoring and preventing crime is one of the protagonists in this scene facing a wide range of challenges (Walt, 2007) regarding the migration of traditional crime to the ICT environment and the emergence of new forms of criminal activity with a focus on the juvenile group (Quille, 2009; Kozlovski, 2005; Wall, 2007).

2. The role of Data Protector Officer and law enforcement structure in screening and preventing cybercrime

Existing approaches to combating crime in the real world are often not functional in cyberspace or may not be applicable in cases of ICT misuse for criminal purposes. It is therefore important to propose and develop a comprehensive approach to a hierarchy micro and macro-structural to address the various aspects of cybercrime along the unique challenges that seem new to law enforcement and investigative entities.

On a big issue of relevance, the Data Protection Officer structures in the European Union are principally governed by the EU Data Protection Directive 95/46/EC2 (the Data

Protection Directive), which regulates the collection and processing of personal data across all sectors of the economy. The Data Protection Directive has been implemented in all 28 EU Member States through national and an International data protection laws. The reform of EU data protection laws has been the subject of intense discussion in the European Commission's publication in January 2012 of its proposal for an EU Data Protection Regulation, which would replace the Data Protection Directive and introduce new data protection obligations for data users and new rights for individuals, especially in the security and defence of the cybercrime populations. The European Commission proposal was adopted in May 2016 as the EU's General Data Protection Regulation (the Regulation) which entered into force in all Member States from the 25th of May 2018. Personal sensitive data relate to a data subject's race or ethnicity, political life, trade union membership, religious or other similar beliefs, health or sex life that can be processed in specific defined circumstances. For a more secure and safe cyberspace, the EU Electronic Communications proposed a Directive 2002/58/EC (the ePrivacy Directive) for the electronic use and misuse of Data. This ePrivacy Directive imposed requirements on providers of electronic communication services to provide an appropriate security measures and to notify certain security breaches in relation to personal data. The ePrivacy Directive was also amended in 2009 to require that website operators obtain the informed consent of users through website 'cookies' or similar technologies used for storing information. In 10 January 2017, the European Commission issued another draft of the proposed Regulation on Privacy and Electronic Communications to replace the existing ePrivacy Directive, which was formally patterned in 28 May 2018.

More effort from the police structures is needed when we refer to the rights of e-users and juveniles using a safe and protected cyberspace.

Authors have proposed some approaches should be taken into account in the development of strategies to combat crime in the virtual world (Bamberger & Mulligan, 2011):

- **The quantity and number of users.** The proliferation of internet usage in people's daily lives and as a way of doing business is dramatically increasing in the number of users in recent years. So in 2005 the number of internet users in the developing countries for the first time exceeded the number of users of the industrialized countries (Special Immigration and Development Report, Information Society, 2005).

In our country, the data show that in 2016-2017 out of 175 cybercrime cases 143 have the involvement of injured persons or 81.7% of cases, from which 51% are female. 11.8% of cases belong to the 14-18 years old or adolescence (Agastra et al., 2017)

In the global perspective, cybercrime is a form of crime that affects both sexes at the same time, but the long-term exposure of developing ages has already changed the focus of this target group. The increase in the number of users regarding the globalization of the communication network is a new challenge for the police and the cyberspace protection structures for at least two reasons: First, one of the weaknesses that poses an opportunity for criminals is the lack of understanding of individual online security along with the application of social engineering and privacy techniques (Rash et al., 2009).

Secondly, identity theft, *spam* and *phishing* activities can be performed automatically (Berg, 2007; Ealy, 2003) without investing money and efforts, it is therefore very difficult to automate the investigation process (Gercke, 2009).

- **Availability of means and information.** Internet is designed as an open access network to information and now extreme deviants can access sources of information or tools to commit cybercrime. Availability of software or compute softwares and devices that allow password tracing and theft, automation of cyber

attacks, the possibility of using search engines and robots for illegal purposes (Long, Skoudis & van Eijkelenborg, 2005; Dornfest, Bausch & Calishain, 2006) and guidelines on how to commit offenses have facilitated the development of crime both in the real world and cyberspace.

- **Difficulties in tracking offenders.** The various opportunities to conceal identity in ICT networks and the different means, ways and approaches to access anonymous, surfing, and social networking links really complicate the work of law enforcement agencies to track and monitor the offenders (Lovet, 2009).

Opportunities for the use of proxy servers, anonymizers, unprotected public wireless networks and the use of anonymous communication services have been largely exploited by cybercrime. When criminal activity involves different states, it is very difficult to investigate such acts that include both the international aspect and the hidden identity concern.

- **A lack of control mechanisms.** Since its first discovery, in the 1960s, the Internet was not designed to be vertically led. The horizontal structure and decentralized network model hampers control over online activity and makes it difficult to investigate crimes committed in cyberspace. Co-regulatory and self-regulatory approaches and cooperation with infrastructure operators as well as with internet service distributors are needed when dealing with the problem of ICT misuse (Sofaer & Goodman, 2001).

- **The lack of boundaries in the cyberspace and the international aspect of cybercrime.** Penology and criminal investigations are considered a matter of national sovereignty in international law and security, while the protocols applied to the transfer of data on the internet are based on the optimum data transfer, so the data transfer processes pass on more than one country (Putnam & Elliott, 2001; Sofaer & Goodman, 2001; Roth, 2005).

Furthermore, because cyberspace has no boundaries, criminals and victims can be found in different countries or even in different continents, requiring a multitude of co-operation by all countries involved in an international investigation. While the formal requirements for cooperation take up its time, the investigation process can often be faced with obstacles (Gercke, 2006; Sofaer & Goodmann, 2001), data and tracks are very delicate and may disappear shortly after the crime has been committed. States, which have no co-operation framework for cybercrime issues, may become a safe shelter for offenders who want to hinder the investigation process. Moreover, the internet can motivate an individual deviant to be physically present in a state while committing a crime to another state.

The role that police and law enforcement agencies must play in combating cybercrime with a focus on juveniles is endangered by all the above-mentioned issues. Not only cybercrime investigation is complicated, but cybercrime investigation policing may also be hindered. It is very difficult for police agencies to initiate investigations mainly because of the low visibility of this crime and the lack of reporting by the victims (Lovet, 2009). The phenomenon of non-declaration of cybercrime, as well as many other phenomena of the social aspect, may occur for various reasons such as the unwillingness of commercial entities and financial companies to report to the police a certain account or threatening injurious behavior, the negligence of individuals involved in cyberbullying in ignoring these issues, the denial and the unknowledge that cybercrime is true and may have involved the individual and at last the lack of trust in police structures (CSI & FBI, 2004; Wall, 2007). Due to the low level of reporting, the lack of resources and reporting to law enforcement agencies, these structures are not able to investigate and prospect more than a "small" fraction of what is happening in cyberspace (Vogel, 2007).

Since the use of internet and ICT technologies, provide researchers the opportunity to create low-impact income to a specific victim as one of the most significant challenges for the

police is the justification of the violation of public order and the opening of investigation procedures.

Differences in criminal acts and offences, cultural differences for the seriousness of crime, great discrepancy over what should be considered illegal, place police units among those most affected units by these contemporary evolution challenges. Finding a fair balance between investigative power and human rights, the application of preventive measures and the preservation of the nature of open access to the Internet remain a serious problem of the police units in the cyberspace.

The lack of control mechanisms, of the initial development of internet and network architecture require the development of cyberspace policing tools, the mechanisms for monitoring ICT networks, of the prevention and detection of illegal activities on the Internet and the net space. Likewise, the initial idea of the internet as a space for open discussion, exchange and sharing of opinions and viewpoints as well as the free flow of information should not be hindered, so, the challenge is also to maintain the network opening and its developing process along with social developments.

According to the National Central Bureaus of Interpol (NCB) published in April 2016, 83% of international offices had dedicated cybercrime units, but lacked the capacity for conducting a high profile incident (Interpol, 2016).

Thus, another necessary and crucial step is to develop effective mechanisms of human resource use and capacity to strengthen national and international cooperation mechanisms.

To enhance the effectiveness of response against cybercrime with a focus on juveniles, studies of the Senior Intelligence Agencies and Crime Prevention have suggested:

- Creating a Task Force working team within the law enforcement and crime enforcement structures with priority in cyberspace crimes;
- Increasing of training capacities for police officers for the psychopathological social structures of the age of the child, the target group with the highest incidence of cyber victimism;
- Increase access and cooperation approaches of police officers with the community they are responding to, with educational institutions, Internet service centers and private sector operators;
- Developing human resource capacities trained and certified for aspects of database creation, mapping of areas and communities with higher risk and Cyber Laboratory for Priority Care and Examination;
- Strengthen legal, civil and criminal penalty acts for abusers and those identified as having high potential of cyberdeviance;
- Coordination of structures at the local and central level for the prevention of cybercrime with a target of juveniles.

The sharing of responsibility and cooperation between the police, community, state and private service sectors seems to be the most effective way of dealing with cybercrime at local and national levels (European Commission and Parliament, Security Council and Regional Committee, 2007). As revealed in a number of studies and publications, such a cooperation with co-ordination and self-regulation can yield even better results than mere enforcement of criminal law *per se* (Sieber, 2010).

3. Conclusions

The fight against cybercrime needs a comprehensive approach involving the development, application and revision of technical, legal, structural and social measures, with the construction of specified organizational structures to address this global-scale problematic as Central Bureau of Investigation in Cybercrime and Data Protection Privacy, Article 7, 8 and 18 of the Data Protection Directive. Moreover, cybercrime treatment requires effective national and international coordination with regard to cybercrime issues that need to be built on coordination of local and national policies (Report of WGIG, 2005). The approach of many participants, including the community, pre-university and university education institutions, defense and law enforcement agencies, social protection structures, etc., implemented at national level should be coherent with the regional and international developments where the harmonization of tools for treating Cybercrime has shown positive and efficient results. Macro-social efforts to establish policies and legal coercive measures should necessarily be based on respect for the Human Rights and Freedom Declaration (Declaration of Human Principles and Rights, Artc. 11 – 2003) as well as technical and economic expertise, civil society readiness, and ease of interaction with organizations and support structures that develop common application standards. Despite the challenges faced, police and juvenile protection units in the regional states of European Union and especially between Neighborhood countries, as one of the key parties in the cybercrime, can act as a central encouraging model for building links between different actors, developing co-operation and developing national and international approaches to address the problem ICT of misuse and harm.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The authors declare no competing interests.

References

- Agastra, A., Ibrahim, S., & Ibrahim, E. (2017). *Profilet psikologjike, domosdoshmëri për hetimin* [Psychological profiles, necessity for investigation]. Pg. 173.
- Bamberger, K. A., & Mulligan, D. K. (2011). Privacy on the books and on the ground (18 November 2011), *Stanford Law Review*, Volume 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Online: www.ssrn.com/abstract=1568385.
- Berg, T. (2007). The changing face of cybercrime – New Internet threats create challenges to law enforcement. *Michigan Bar Journal* 2007, 18-22.
- CSI and FBI (2004). Computer Crime and Security Survey. San Francisco.
- Gercke, M. (2006). The slow wake of a global approach against cybercrime. *Computer Law Review International*. 140-145.
- Gercke, M. (2009). *Understanding cybercrime: A guide for developing countries*. Geneva: ITU. Online: www.itu.int/ITU-D/cyb/cybersecurity/legislation.htm.
- Ealy, K. (2003). *A new evolution in hack attacks: A general overview of types, methods, tools, and prevention*. <https://cyber-defense.sans.org/resources/papers/gsec/evolution-hack-attacks-general-overview-types-methods-tools-prevention-105082>

- Interpol (2016). Crimes against children. *Factsheet*, pg 11.
- Kozlovski, N. (2005). *A paradigm shift in online policing – Designing accountable policing*. Yale Law School Dissertation.
- Long, J., Skoudis, E., & van Eijkelenborg, A. (2005). *Google hacking for penetration testers*. Syngress.
- Lovet, G. (2009). Fighting cybercrime: Technical, juridical and ethical challenges, *Virus Bulletin Conference*, September 2009.
- Putnam, T. L. & Elliott, D. D. (2001). International responses to cybercrime. In: A. D. Sofaer & S. E. Goodman (Eds.), *Transnational Dimension of Cyber Crime and Terrorism* (pp. 31-67). Hoover Institution Press.
- Quille, M. (2009). *Keynote address. Current threats and future challenges posed by cybercrime*. Octopus Conference, CoE.
- Rash, H. et al. (2009). Crime online. Cybercrime and illegal innovation. NESTA. Research Report. July.
- Roth, B. (2005). *State sovereignty, international legality, and moral disagreement*. Oxford University Press.
- Sieber, U. (2000). Legal Regulation, Law Enforcement and Self-regulation. In: J. Watermann & M. Machill, M. (Eds.), *Protecting Our Children on the Internet*, Gütersloh, Bertelsmann Foundation Publishers.
- Sieber, U. (2010). Internet Crimes – Annex 1 to the Questionnaire for the 18th International Congress of the IACL.
- Sofaer, A. D. & Goodman, S. E. (2001). Cybercrime and security – The transnational dimension. In: A. D. Sofaer & S. E. Goodman (Eds.), *Transnational Dimension of Cyber Crime and Terrorism*. Hoover Institution Press.
- Vogel, J. (2007). Towards a global convention against cybercrime. World Conference on Penal Law, Guadalajara, Mexico.
- Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, 8(2).
- (1995). European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free.

