Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes - Fourth Intersessional Consultation, **Vienna, 06-07 March 2023**

Striving to remain one step ahead: thinking beyond traditional prevention approaches

Panel discussion 3

Technoethics, AI and Criminal Law

Dr. Fotios Spyropoulos

Vice President, Center for the Study of Crime

PostDoc - University of West Attica, Greece

Crime in the digital age

- Given the highly adaptable nature and rapid evolution of crime in the digital age, and cybercrime in particular, it is essential to interpret it and formulate prevention measures and practices at the international level based on continuous cooperation and exchange of knowledge.
- New popular (?) norms are formed, which in a dynamic process can lead to elements that constitute technoethics. To what extent will the emerging technoethics influence criminal law in terms of dealing with the criminal phenomenon in a digital environment and will force States think beyond traditional preventive approaches in the elaboration of the future convention?

Criminality and delinquency online

"Digital Criminality" as besides the internet there are other vulnerable computer systems like the internet.

Criminality wherever it is regulated by the legislator – delinquency in the rest of the cases.

However, "*lacking - or, rather, undergoing – is this unofficial norm resulting from a popular belief that will be the 'litmus stone' to characterize an online behavior as a deviant" (F. Spyropoulos, 2009).*

'digital society'

- recognises such technologies as an **embedded part of the larger social entity** and acknowledges the incorporation of digital technologies, media, and networks in our everyday lives (Lupton 2014), including in crime perpetration, victimisation and justice.

Digital Criminology

- Digital criminology refers to the rapidly developing scientific field that applies criminological, social, cultural theory, the theory of technical systems and the corresponding research methods, in the study of crime, delinquent/deviant behavior and justice in the digital society (Stratton G., Powell A. and Cameron R., 2017).
- Renegotiate criminological theories in search of new scientific ideas that challenge the classical dichotomies - internet vs. physical world, virtual vs. real- both for the prevention and treatment of crimes in the digital environment, on the internet as well as more generally in the context of new technologies, in the context of the development of technoethics.
- The boundaries of modern criminological theory and research are expanded and a broader and ongoing discussion of technology, sociality, crime, deviance and justice is fostered in new conceptual foundations and empirical directions in cyberspace and digital crime mapping.

Understanding cybercrime new perspectives and challenges

Breaking through the online/offline and real/virtual binaries

- Sheila Brown (2006: 227) challenges such computer and cyber criminology to look outside of its conventional disciplinary frameworks ➡ 'towards theories of the technosocial'.
- Analyses of cyber crime are likewise caught up in false distinctions between 'virtual' and 'embodied' crime; seeking to develop and translate 'old' legal and theoretical frameworks to understanding the 'new' crimes in cyberspace.
- '**nowhere is captured the vision of the crucial nature of the world as a human/technical *hybrid*** ...' (Brown 2006: 227), in which all crime occurs in networks, which vary only in degrees of virtuality/embodiment.
- A need for criminologists to understand crime and criminality at the intersections of biology/technology, nature/society, object/agent and artificial/human. Computing and information theories, 'will increasingly infuse both domains of Law and Criminology' (Brown 2006a: 236) as social theory is not in itself sufficient to analyse and understand crime in contemporary societies.

Digital society and criminology

- Baym (2015: 1) notes that the distinguishing features of digital technologies are the manner in which they have transformed how people engage with one another.
- This enmeshment of the digital and social has also been referred to as the digitalisation of society in which 'technology is society, and society cannot be understood or represented without its technological tools' (Castells 1996: 5).

Technoethics

- "Ethics" can be defined as a code or set of principles by which people live. Ethics is about what is considered morally right and what is considered wrong. When people make moral judgements, they express normative statements about what should be done, about moral duties and obligations, rather than descriptive statements about what is done. Technoethics is concerned with the implications of ethics for technology, technological change, technological developments and their applications.
- Basically, the problem is that there is a dilemma of doing the right and ethical thing in technological applications.

General prevention ➡ Law

- Effective prevention requires justice system actors to collaborate with actors in other sectors to address the root causes of disputes and prevent conflict, violence and human rights violations.
- In relation to cybercrime, this means that there is a need to move from punitive measures to evidence-based prevention with evidence/science-based legislation that will shape general prevention.

PRINCIPLES of prevention activity

- *Lawfulness* ➡ subject to the observance, enforcement and application of the laws and other delegated legislation and statutory acts by both the institutions and the citizens.
- *Cooperation and partnership*
- *Comprehensiveness and coordination* ➡ the optimal combination of measures conducted in accord by individual state institutions and structures of civil society.
- *Sustainability* ➡ Prevention is a leading and continuing policy of the government and its bodies to ensure public security and safety.
- *Scientific validity, Flexibility, Unavoidability, timeliness and adequacy of punishments etc.*

The Social Science & Cybercrime Prevention

- regard cybercrime as a result of human and societal deviation and dysfunctional behavior, attitude, norms in the process of communication with others through the Internet and cyberspace as a user.
- put more emphasis on the violation and transgression of morals, values, norms and attitudes as primary bases in the promulgation of a law, policy or regulatory to prevent the occurrences of cybercrime.
- interpret and apply cybercrime prevention from the over aching political, legal, social, economic, cultural and moral dimensions (see more Blanco, 2013).
- views technology as irrelevant and inconsequential in the understanding the complexities and intricacies of cybercrime (Soumyo Moitra (2005). David Wall (2007; 2000), Kim –Kwang Choo (2008) and Stewart and Fritsch (2011).

Target…to make cyber crime law more comprehensive and effective

- through the mechanism of an international convention, implemented into national law by the states who are parties to the convention
- through harmonization or approximation of national laws, as the result of conscious decision of the national governments to remove the differences between them
- through what might have been described as accidental or fortuitous convergence, as described above for digital signature laws (Reed, 2011:311).

Technology & Cyber Crime Prevention

- view cyber crime prevention as not a matter of public policy, legislation, policy reforms instead it attempts to posit a remedy through information technology support, virtual communities, computer technology [open source software model, computer networking model and virtual community neighborhood (Benjamin Jones (2007), Samuel Mcquade III (2007) and S. Jaishankar (2011)].
- cyber crime prevention laws and policies would require a solid technological support and dimension to enable cyber crime prevention more effective and efficient in its formulation, legitimization and implementation.
- But technological innovation and creativity alone would also not suffice in breaking down the puzzle of the cyber crime, it would require a strong and robust legislation which would provide a legal and political bases for its actions (Blanco, 2013: 16-17).

Bridging the Social Science and Technology Challenges…

- bridge the common differences between causes and effects, the causes and symptoms of cyber crimes specifically that of the free speech, free expression and free press doctrine and the behavior exhibited that goes along with it with that of the laws and policies which regulates it (Blanco, 2013: 18-20).
- through the empowerment and strengthening the participation of the stakeholders between and among the social science and technological paradigm to further consult, discuss and consolidate their varied interpretations and applications on cyber crime prevention so as to share a common language and vision on how to regulate cyber crime (Blanco, 2013: 18-20).
- by way of discovering and recognizing that symptoms of cyber crimes do exist and reversibly provide a strong linkage with its causes in finding the coherent structures, systems, process and policies which may be promulgated and enforced in solving cyber crime Stephens, 2008: 34).

the preventive role of the Convention

The time of divided perspectives and dichotomies is over; it is now the time to work together. Why dichotomize, when we can harmonize?

- *'digital society'- the embedded nature of technology in our lived experiences of criminality, victimisation and justice; the emergence of new technosocial practices of both crime and justice; and the continued relevance of social, cultural and critical theories of society in understanding and responding to crime in a digital age.*
- *'…the vision of the crucial nature of the world as a human/technical hybrid …' (Brown 2006: 227), in which all crime occurs in networks, which vary only in degrees of virtuality/embodiment.*

Democracy's bet to secure the freedom to use the internet.

Criminological theories and new approaches should be used for this purpose.

Before we get to the final text of the Convention, a relevant criminological study should be carried out on how this text is applied and functions in practice.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes - Fourth Intersessional Consultation, Vienna, 06-07 March 2023

Thank you for your attention!

Dr. Fotios Spyropoulos

Vice President, Center for the Study of Crime

PostDoc - University of West Attica, Greece

e-mail: ***fspyropoulos@gmail.com***