Collaborative Discussion 1 – Summary Post – Michael Geiger

By examining cyberbullying and its international trends, it was possible to establish that the opportunities offered by the Internet open up new ways and forms of criminal offenses. A relocation of existing criminal offenses into cyberspace can therefore be observed, which have different characteristics and dynamics in comparison to analogous criminal offenses.

These trends are being noticed by states and the first countermeasures such as disclosure of identity in social networks are being laid down by law (GovHK, 2022). An international network of state law enforcement apparatuses can also be observed on the Internet, which is evident from the agreements on standards, laws, but also cooperation for supranational law enforcement (European Union Agency for Cybersecurity, N.D.)

However, it must be noted that these collaborations and de-anonymization measures also come with challenges and potential dangers. The respective state capacities for criminal prosecution are different, so that supranational prosecution of a criminal offense is given less priority by some nations and is therefore not prosecuted. National legal bases also pose obstacles to international cooperation in criminal prosecution (Holt et al., 2022).

In addition, the dangers of de-anonymization must be taken into account. Users' private information can be stolen, distributed and used for criminal activities. But freedom of speech in countries can also be negatively affected by these measures, since the information collected in relation to the identity of the user can be used to politically discredit the person or even to prosecute them under pretext.

Due to the legal measures and international dynamics in response to the possibility of criminal offenses in cyberspace, it can be stated that Grabosky's (2001) thesis "Virtual Criminality: Old Wine in New Bottles?" does not do justice to the complexity of the topic of the legal situation on the Internet becomes. The possibilities for crimes and their execution are so different from those in the analogue world that new legal bases have to be created and national sovereignty in relation to criminal prosecution is not sufficient to guarantee the security of citizens in an international context.

References:

European Union Agency for Cybersecurity (N.D.) NIS Directive. Available from: https://www.enisa.europa.eu/topics/nis-directive [Accessed 30 August 2022].

GovHK (2022) Real-name registration for SIM cards to commence on March 1. Press Releases. Available from:

https://www.info.gov.hk/gia/general/202202/07/P2022020700230.htm [Accessed 30 August 2022].

Grabosky, P.N. (2001) Virtual Criminality: Old Wine in New Bottles. Social & Legal Studies. 10(2): 243-249. Available from: https://heinonline-org.uniessexlib.idm.oclc.org/HOL/Page?public=false&handle=hein.journals/solestu10 &id=239&collection=journals [Accessed 30 August 2022].

Holt, T., Bossler, A. & Seigfried-Spellar, K. (2022) Cybercrime and Digital Forensics. Routledge, New York.