E-Portfolio Activity 2: Computer Forensics – The Investigative Process – Michael Geiger

Walden (2015) argues in the article "Computer forensics and the presentation of evidence in criminal cases" that digital forensics has shifted the political environment, the complex of the compromise compromise has shifted decisively in favour of criminal prosecution. This reduces the defendants' right to privacy and lowers the hurdle to searching the private digital property of those affected. The fitting names of systems and data have been simplified from a legal point of view. However, the counterparty is faced with the time and resource limitations required for the processing and forensic examination of the data. Walden calls for a rethinking of legal and procedural approaches in order to respond appropriately to the complexity of cybercrime, also in an international context.

With his arguments, Walden addresses important points in the context of cybercrime and law enforcement and points out the difficult problem of balancing law enforcement rights and legal processing, in the context of forensics, but also the fundamental rights of private individuals and their right to privacy. The central question of proportionality is therefore taken up, which is of fundamental importance for the balance of the autonomy of individuals and state stability. A predominant shift of rights towards one of the two sides can lead to the destabilization of both parties. If the rights of private individuals are too strong, the legal system cannot act appropriately, resulting in a loss of integrity and trust in the rule of law. On the other hand, too strong rights on the part of the state can lead to democratic systems being undermined, oppositions to legal prosecution and thus the state being destabilized as an organ of the population.

A more in-depth reflection and appropriate adjustments of legal and procedural approaches is therefore generally necessary and appears to be of high priority given

the rapid development in the digital context. The fact that cyber crime can easily transcend national borders of criminal offenses means that analogous legal bases in cyberspace are not sufficient to guarantee the rule of law. I therefore agree with Walden's argument that legal adjustments need to be made and these need to be applied at the international level. However, due to different national perceptions of the value of the right to privacy, there is a risk that rights in countries with large personal rights will be negatively influenced.

Bryant and Bryant (2014) show that shifts in the investigative process have taken place between the law and the police. As an example, honeypots are mentioned, which proactively contribute to criminal prosecution, as this sets a "trap" for potential criminals. While in the classic sense of police investigations these take place after a crime has been committed in order to process them, criminals can be caught committing the alleged crime through honeypots. The question arises to what extent this can be ethically justified, since it can be argued that this provokes the execution of the crime. On the other hand, it can be argued that the offender would have committed the crime regardless of the honeypot, just in a way that would have caused real harm. This reinforces the question of proportionality already raised by Walden.

The ethical question and legal limit to how far the state may use preventive measures to avert danger is narrow. The concept of decoy spy or agent provocateur discusses in particular the problem of criminal liability for those who, for example, act as undercover investigators and incite others to commit a crime precisely in order to arrange for their arrest (Bleckmann, 2021). The state usually uses an agent provocateur on behalf of authorities such as the public prosecutor's office, the police or secret services and ideally aims to commit an unfinished attempted crime with the

possibility of usual preservation of evidence. The aim of such an operation is to lure covert and dangerous crime from impunity. In the cyber context, this can raise some ethical and legal questions, for example how far can security go to find criminals? Can a honeypot be used to identify potential fraudsters or does the honeypot represent such a provocation that it encourages or induces a crime to be committed? How far can a police officer go to find a potential pedophile on the Internet and at what limit does the investigator make himself liable to prosecution? In German law, a distinction is made between criminal prosecution and security. The legal situation for criminal prosecution is provided by the StGB (Criminal Law Book), which is applied at federal level. However, the respective police law of the state (e.g. HSOG, Hessian law on public safety and order) is responsible for averting danger. While criminal prosecution is therefore uniform throughout Germany and is also coordinated at international level with regard to the legal area of the Internet through the Cybercrime Convention, the law is not uniform with regard to averting danger (the Federal Commissioner for Data Protection and Freedom of Information, N.D.). It is therefore evident that the question of the rule of law, the right of individuals to privacy and proportionality are extremely difficult to weigh and unambiguous pleas for a side, that of the police and the possibilities of judicial prosecution of criminals and that of the population and their personal rights fall short in this multidimensional subject area.

References:

Bleckmann, L. (2021) BGH: Neues zur Anstiftung durch den agent provocateur. *Juraexamen*. Available from: https://www.juraexamen.info/bgh-neues-zur-anstiftung-durch-den-agent-provocateur/ [Accessed 23 August 2022].

Bryant, R. & Bryant, S. (2016) Policing digital crime. *Routledge, London*. Available from: https://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=4511974 [Accessed 23 August 2022].

Der Bundesbesbeauftrage für den Datenschutz und die Informationsfreiheit (N.D.) Die Cybercrime-Konvention. Available from: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Polizei-Strafjustiz/Cybercrime.html [Accessed 23 August 2022].

Walden I. (2015) Computer forensics and the presentation of evidence in criminal cases in: Jawkes, Y. and Yar, Y. (eds) Handbook of Internet Crime*. Abingdon, Oxon: Routledge*. Available from: https://www-taylorfrancis-com.uniessexlib.idm.oclc.org/books/edit/10.4324/9781843929338/handbook-internet-crime-yvonne-jewkes-majid-yar [Accessed 23 August 2022].