Mid-Module Assignment 2: Blog Post – Principles of Digital Forensics and Cyber Law – Michael Geiger

Identity theft is the unauthorized acquisition of personal data by third parties and the improper use of this data (Gercke, 2007). Criminals are interested in all kinds of personal data with which they can make decisions on the Internet to the detriment of third parties and for their own benefit (BKA, N.D.). The Personal Data can be obtained through phishing, malicious programs such as Trojans or data leaks from databases of service providers (BSI, N.D.). The aim of identity theft can be to gain fraudulent financial gain or to discredit the rightful owner of the identity.

In a Germany-wide study, the auditing company PWC (2016) states that one in three respondents has already been a victim of identity theft. 30% of the victims suffered financial damage as a result, with 27% suffering a loss of more than € 1,000. With an average cybercrime clear-up rate of just 29.3% and an estimated cost of phishing services of $ 100 per month, identity theft appears to be an attractive crime for criminals (BKA, 2021).

While human rights and the General Data Protection Regulation (GDPR) of the European Union are intended to reinforce the rights to privacy of citizens at an international level and contribute to people's security, the effectiveness of the national Law enforcement may be impeded by these laws.

According to the GDPR, people have the right to information about their personal data from companies that, in the event of identity theft, can help to identify the criminal. The right to information according to Article 15 GDPR refers to personal data, which, according to the definition of Article 4 No. 1 GDPR, is all information relating to an identified or identifiable natural person (EUROPEAN UNION, 2016).

This is unproblematic as far as the data of the identity holder is concerned. However, as soon as it concerns the data of the data thief, for example the email- or a delivery address, it could be argued that it concerns the data of a third party and not that of the identity holder. As a result, companies can be reluctant to disclose the data, as they could run the risk of making themselves liable to prosecution by providing unauthorized information. This can hinder the investigation process. According to Article 6 No. 1 of the GDPR, state investigative authorities have the right to get information about data for criminal prosecution, but according to the Code of Criminal Procedure (§§160 ff StPO) there must be an investigation with an investigation number or a "imminent danger" (Dejure, 2022). These legal hurdles can delay an effective criminal investigation, reducing the chance of a successful prosecution.

Furthermore, on 20th September 2022, the European Court of Justice (ECJ) decided that the German law on data retention violates Art. 8 of the European Convention on Human Rights and must therefore be deleted (Stein, 2022). The Data Retention Act obliges telecommunications companies to store the usage information of their customers for six months and to make it available to the investigating authorities in the event of suspicion. While the ECJ's decision strengthens citizens' right of privacy, investigating authorities note that this judgment makes criminal prosecution in cyberspace more difficult (Entscheidt, 2022).

It can therefore be concluded that international law can have a negative impact on investigative processes at the national level.

References:

BKA (2021) Cybercrime – Bundeslagebild 2021. Available from: file:///C:/Users/Fridolin/Downloads/cybercrimeBundeslagebild2021-1.pdf [Accessed 29 September 2022].

BKA (N.D.) Identitätsdiebstahl/Phishing. Available from: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html [Accessed 28 September 2022].

BSI (N.D.) Identitätsdiebstahl durch Datenleaks und Doxing. Available from: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html [Accessed 28 September 2022].

Dejure (2022) Strafprozeßordnung. Available from: https://dejure.org/gesetze/StPO [Accessed 30 September 2022].

Entscheidt, E. (2022) Anlasslose Vorratsdatenspeicherung rechtswidrig. Frankfurter Allgemeine Zeitung. Available from: https://www.faz.net/aktuell/politik/inland/eugh-anlasslose-vorratsdatenspeicherung-rechtswidrig-18329550.html [Accessed 29 September 2022].

EUROPEAN UNION (2016) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. Official Journal of the European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 30 September 2022].

Gercke, M. (2007) Internet related identity theft. *Project on Cybercrime*. Available from: https://www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf [Accessed 28 September 2022].

PWC (2016) Identitätsklau – die Gefahr aus dem Netz. Available from: https://www.pwc.de/de/handel-und-konsumguter/cyber-security-identitaetsdiebstahl-2016.pdf [Accessed 29 September 2022].

Stein, A. (2022) EuGH: Vorratsdatenspeicherung rechtswidrig. ZDF. Available from: https://www.zdf.de/nachrichten/digitales/eugh-vorratsdatenspeicherung-deutschland-100.html [Accessed 29 September 2022].