Principles of Digital Forensics and Cyber Law

Expert Report:

Cyber identity theft in Germany

Michael Geiger

Table of Contents

Introduction

The rapid growth of the Internet has created a multitude of possible uses. Online transactions enable quick and easy financial exchange, e-commerce offers convenient advertising, trading of goods and services and messenger services as well as social media platforms offer users a space to communicate almost instantaneously, to exchange opinions publicly, to present themselves, finding like-minded interest groups and striving for self-realization. The rapid increase in Internet users in Germany from 2% in 1995 to 90% in 2020 shows the great importance that these opportunities offer to people and the interest in using them (The World Bank, N.D.).

Associated with all these actions in cyberspace is the injection of personal data into the Internet (Priem et al., 2011). Users pass on personal information such as names, dates of birth, residential addresses, credit card information, ID card numbers and other information to service providers such as online banks, e-commerce companies or other companies, send them to other private users or even share them with the public. In doing so, the principle “Whatever gets on the Internet, stays on the Internet” must be considered. This flood of personal information is used by cyber criminals for their own benefit. Online identity theft allows criminals to use personal information to commit tortuous acts, to generate financial gain through commercial fraud, to disguise one's identity, or to discredit an individual (Saunders & Zucker, 1999).

In order to counteract and prevent these criminal acts in cyberspace, competent investigative authorities as well as appropriate legal framework conditions are necessary in order to be able to protect private users and companies effectively. In the following, the manifestation of cyber identity theft in Germany will be examined, the perception of this crime by perpetrators, victims and society will be analysed and

ethical and legal consequences will be discussed. Finally, the effectiveness of the existing legal basis and the available investigative tools are evaluated.

Manifestation of cyber identity theft in Germany

Identity theft itself is a crime that predated the era and potential for acquiring and misusing identities of the internet (Hille et al., 2015). However, the attack surface for identity theft and possible financial gains for criminals from cyber identity theft have increased significantly due to the increasing networking of the Internet and its use (Meindl, 2012). Cyber identity theft is a serious and growing threat to user and business security in a connected society. The German Federal Criminal Police Office (BKA) has recorded a steadily growing number of cyber identity thefts since 2007, with only a decrease in 2018, followed by a massive increase from 2020 with a recent increase of more than 12% to 146,363 offenses in 2021 (BKA, 2011; BKA, 2018 BKA, 2021). The US Federal Bureau of Investigation (2021) also notes a similar trend of identity theft in the USA, so that it can be classified as international.

According to studies by the Federal Office for Information Security (BSI, 2021) in Germany, cyber identity theft is increasingly being carried out professionally as part of organized cybercrime. The dominant motivation of offenders is financial. The stolen personal data is offered for sale in forums and marketplaces on the deep web, but also via the instant messaging service Telegram, which are later used for criminal acts (BKA, 2021). Such personal data records represent an elementary part of the Cybercrime-as-a-Service offer (CaaS). The central source of personal data records are data leaks, which, according to the Hasso Plattner Institute (N.D.), amount to 184.65 million compromised user accounts in 2021 in Germany. The data is used by

the acquirers for further phishing campaigns, for online goods and services fraud or credit card fraud. Another criminal act using the stolen personal data is the creation of a fake shop in the name of the victim (Verbraucherzentrale Niedersachsen, 2018).

Not only can this damage the victim's reputation, the victim can also face legal consequences if they are unable to prove that they are not responsible for the fake shop and that they themselves have become a victim of the crime. In addition to the financial damage that victims of identity theft face, the damage to their reputation is another consequence that should be given increasing attention in the context of recent abuse. In June 2022, an interview took place between the Mayor of Berlin, Franziska Giffey, and the Mayor of Kiev, Wladimir Klitschko. After the interview, it turned out that the interviewee, Wladimir Klitschko, was not the real person (Laufer, 2022). Old video files were used to make false statements on his behalf. This incident brings into focus the threat of identity theft through deep fakes and other image and sound files and goes hand in hand with the threat of politically motivated crimes and a new means of warfare (Boháček & Farid, 2022).

Perceptions of identity theft from the perspective of perpetrators, victims and the society

As previously mentioned, the predominant motive for identity theft perpetrators is online fraud for financial gain. Taking into account the General Theory of Crime, when making a decision to commit a crime, criminals weigh the benefits of the crime against the potential consequences of their actions (Gottfredson & Hirschi, 2022). These decisions are subject to the socio-economic, social and cultural context of the perpetrators and their perception of the crime (Holt et al., 2022). In a Germany-wide

study, the auditing company PWC found that the realization of a crime in the context of identity theft results in financial damage of 1,366 Euros on average (PWC, 2016). The relatively high profit for the perpetrators is therefore an incentive to commit the crime, while scruples are reduced due to the lack of face-to-face interaction with the victim.

In addition to the financial damage, victims of identity theft can also experience emotional and psychological damage. The study by Li et al. (2019) shows that identity theft victims suffer from the crime. Insecurity, self-blame, and a feeling of powerlessness can result from identity theft, prompting those affected to pursue coping strategies. Denial of what has been experienced or turning away from the use of online offers are possible consequences of the criminal offence. As a result, online companies can also be indirectly affected by the crime. By harming victims, general trust in e-commerce can be undermined, negatively affecting the entire industry and its revenues (Smith & Lias, 2005).

These events also have an impact on general social perception. Under the concept of consumers' fear of online identity theft (FOIT), the negative effect of society's perception of dangers on the Internet in the context of online commerce is considered (Walsh et al., 2019). Hille et al. (2015) found in their study on FOIT in Germany that 88% of respondents are afraid that their personal data could be used for online purchases and 95% are afraid of reputational damage. The fear of identity theft is therefore widespread in society, so that from a legal point of view measures must be taken to ensure the security of the population.

Ethical and legal consequences

As a consequence of the serious and direct threats of identity theft, companies that process and use personal data of users are subject to ethical as well as legal responsibilities. The data leaks listed by the Hasso Plattner Institute (N.D.) show that in the event of a data breach, millions of personal information could be affected by identity theft. Smaller companies in particular face the threat that user data can be stolen, as they have less capital and knowledge to prevent data theft (Bose & Leung, 2013). It follows that companies have an ethical responsibility to handle and store their users' information responsibly, discreetly and securely.

The General Data Protection Regulation (GDPR) provides the legal basis for data protection and handling in Europe. According to Article 5 of the GDPR, personal data from companies must be limited to what is necessary for the purposes of processing on the one hand and on the other hand the security of the processing and storage of this data must be ensured (EUROPEAN UNION, 2016). Furthermore, Article 33 of the GDPR stipulates that in the event of a personal data breach, this breach must be reported within 72 hours to the supervisory authority responsible under Article 55, which in the case of Germany is the respective state data protection authority of the federal state concerned (BfDI, N.D.a). However, it can be observed that companies sometimes do not meet their ethical and legal responsibilities and have an interest in not reporting data leaks and wanting to keep them secret in order to prevent a loss of trust. A controversial example is the American transport company Uber, which in 2016 hid for months that hackers had stolen data from 50 million passengers and 7 million drivers (Symanovich, 2021).

The ethical responsibility of companies contrasts with the ethics of criminal investigation and digital forensic practices on the part of the authorities. For this

purpose, the BSI (2020) has established ethical principles that must be taken into account in digital forensics, which concern integrity and trustworthiness, professional competence, objectivity and diligence, factual presentation, evidence and traceability, and independence and neutrality and must be observed.

Effectiveness of the legal bases

Contrary to the obvious assumption that identity theft is a crime of theft according to § 242 of the German Criminal Code (StGB), the law cannot be applied in cyberspace. Since according to the definition, theft is about someone else's movable property and thus a real physical existing object (Mitsch, 2015). In addition, there is no separate chapter in the German Criminal Code that explicitly refers to cybercrime or identity theft. This is due to the fact that German legislation is fundamentally formulated in a technology-neutral manner and therefore existing laws or standardized criminal offenses are applied to new facts by subsumption (Berwanger, N.D.).

Therefore, in the case of online identity theft, depending on the execution, various criminal offenses are committed under the Criminal Code. The unlawful collection and handling of personal data is anchored in § 202a-d StGB in the context of the violation of the secrecy of letters and refers to the spying and interception of data. The preparation of the spying and interception of data, as well as data theft, whereby the inviolability of the secrecy of correspondence is laid down in Article 10 of the Basic Law (GG) and is therefore a fundamental right of citizens in Germany (Bundesamt für Justiz, N.D.a; Dejure, N.D.). Any unlawful handling of third-party data is therefore prohibited and can be punished with imprisonment of up to one year or a fine. However, a distinction must be made when realizing data theft. While § 202

StGB refers to identity theft through phishing, pharming or spoofing, in the event of exploitation of a data leak, the violation of postal and telecommunications secrecy under § 206 StGB applies and can result in a prison sentence of up to five years (Bundesamt für Justiz, N.D.b). In the context of financial crimes, such as e-commerce fraud, § 263a StGB applies and in the case of extortion § 253 StGB, both of which carry penalties of up to five years imprisonment (Bundesamt für Justiz, N.Dc; Bundesamt für Justiz, N.D.d).

Due to the increasing risk of discrediting and spreading misinformation through the false presentation of another personality with the help of image and audio files as well as deep fakes, this fact must also be investigated. Applicable offenses for this would be the criminal offense of slander according to § 186 StGB and the criminal offense of defamation according to § 187 StGB with imprisonment of up to two or five years (Bundesamt für Justiz, N.D.e; Bundesamt für Justiz, N.D.f). However, it must be noted that these laws have at times only been applied in the context of cyberbullying and there is currently no precedent of abusive identity acquisition (Marx, 2016).

Evaluation of the effectiveness of investigative rights, institutions and available investigative tools

Due to the federal structure of the Republic of Germany, the 16 federal states and thus the respective law enforcement authorities of the respective federal state are responsible for the criminal prosecution of cybercrime offenses (Dejure, N.D.b). Only in the case of crimes in the national interest is the higher federal authority BSI responsible for Internet crimes, as well as the Federal Police (BfDI, N.D.b). However,

in the case of cybercrime offenses relating to identity theft, the BSI assumes a coordinating role between the federal authorities.

While these structures can bring advantages in the case of physical crimes, the investigative processes can be hindered in the digital space. A cybercrime crime is not tied to a specific location and can therefore be carried out from anywhere on earth. The speed of investigation can be slowed down due to the bureaucratic framework. In addition, the public broadcaster ZDF found out as part of an investigative research that the competencies and capacities in the prosecution of criminal offenses on the Internet vary depending on the federal state (ZDF MAGAZIN ROYAL, 2022). This is to be viewed critically, particularly in the context of international cooperation to uncover cybercrime, since a competent prosecuting authority of the federal state can be crucial to the success of uncovering the crime.

The same concerns about varying competencies need to be addressed in the context of cybercrime prevention. As with criminal prosecution, the individual federal states are responsible for preventive measures in the event of criminal offenses on the Internet within the framework of averting danger (HJagDG, 2018). The individual federal states are therefore responsible for identifying and counteracting illegal online platforms. It is not just the competences of the investigators that represent limitations, the spatial responsibility of the authority is also limited to the respective federal state. In cross-state cases, cooperation between the authorities is a prerequisite for successful criminal prosecution.

In an international context, the investigative authorities and their powers are limited by EU regulations. The General Data Protection Regulation (GDPR) ensures comprehensive rights for citizens and their personal information in the European Union and thus significantly strengthens the personal rights of the European

population (EUROPEAN UNION, 2016). Due to the obligation for companies based on the GDPR to only store data that is absolutely necessary, important information for the preservation of evidence and detection of the crime may not be available in the event of a crime. In addition, German investigative tools have repeatedly been classified as illegal and thus banned by investigative authorities for criminal prosecution at the European level. This includes the Data Retention Act, which was introduced at European level in 2006 and also implemented in German national law, but was already classified as unconstitutional in 2010 by the Federal Constitutional Court and in 2014 by the European Court of Justice (BfDI, N.D.c). The Data Retention Act obliges telecommunications providers to store personal data and traffic data of their users for at least six months without cause and to make them available to the investigating authorities in the event of suspicion (Roßnagel, 2010). The new edition of the Data Retention Act 2.0 was pushed ahead at national level in 2015, but ultimately failed again in September 2022 due to the decision of the European Court of Justice (Entscheidt, 2022).

Conclusion

It can be summarized that criminal offenses related to identity theft in cyberspace are constantly increasing and pose a serious threat to the population. Crimes in the context of identity theft show different motives for the perpetrators and different consequences for the victims. A dominant motive of a financial nature can be identified. Victims, on the other hand, not only suffer from financial damage, but can also suffer psychological or reputational damage as a result of the crime. Ethical principles for the responsible handling of personal data are therefore necessary, but these are not always observed, so that a legal framework is necessary. In Germany

there are no explicit laws on cyber crimes and identity theft. The existing laws and standardized crimes are applied to the new circumstances by subsumption. The criminal prosecution and investigative possibilities of the authorities are hindered by the federal system in Germany, whereby international rights further restrict the powers of the authorities. Further criminal investigation rights and a restructuring of responsibilities for criminal prosecution on the Internet may therefore be necessary in order to be able to effectively counteract the international threat of identity theft.

References

Berwanger, J. (N.D.) Subsumtion. Available from: https://wirtschaftslexikon.gabler.de/definition/subsumtion-100446 [Accessed 24 October 2022].

BfDI (N.D.a) Kontakt zu den Landesbehörden. Available from: https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html;jsessionid=A503DF6C646E24F21E75A6FD87A01436.intranet222 [Accessed 23 October 2022].

BfDI (N.D.b) Bundespolizei. Available from: https://www.bfdi.bund.de/DE/Buerger/Inhalte/Polizei-Strafjustiz/National/Bundespolizei.html [Accessed 26 October 2022].

BfDI (N.D.c) Historie zur Vorratsdatenspeicherung. Available from: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/Historie_zur_Vorratsdatenspeicherung.html [Accessed 23 October 2022].

BKA (2011) *Cybercrime Bundeslagebild 2011*. Available from: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2011.html?nn=28110 [Accessed 19 October 2022].

BKA (2018) *Cybercrime Bundeslagebild 2018*. Available from: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html;jsessionid=F32A63AD26CA00187A4A51F8C6C99544.live612?nn=28110 [Accessed 19 October 2022].

BKA (2021) *Cybercrime Bundeslagebild 2021*. Available from: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110 [Accessed 19 October 2022].

Boháček, M. & Farid, H. (2022) Protecting President Zelenskyy against Deep Fakes. *arXiv preprint arXiv:2206.12043*. Available from: https://arxiv.org/pdf/2206.12043.pdf [Accessed 21 October 2022].

Bose, I. & Leung, A. C. M. (2013) The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems* 55(3): 753-763. Available from: https://www.sciencedirect.com/science/article/pii/S016792361300081X [Accessed 23 October 2022].

BSI (2020) Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-nachweise.pdf?__blob=publicationFile&v=8 [Accessed 24 October 2022].

BSI (2021) *Die Lage der IT-Sicherheit in Deutschland 2021*. Available from: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3 [Accessed 20 October 2022].

Bundesamt für Justiz (N.D.a) Strafgesezbuch (StGB) § 202 Verletzung des Briefgeheimnisses. Available from: https://www.gesetze-im-internet.de/stgb/__202.html [Accessed 25 October 2022].

Bundesamt für Justiz (N.D.b) Strafgesetzbuch (StGB) § 206 Verletzung des Post- oder Fernmeldegeheimnisses. Available from: https://www.gesetze-im-internet.de/stgb/__206.html [Accessed 25 October 2022].

Bundesamt für Justiz (N.D.c) Strafgesetzbuch (StGB) § 263a Computerbetrug. Available from: https://www.gesetze-im-internet.de/stgb/__263a.html [Accessed 25 October 2022].

Bundesamt für Justiz (N.D.d) Strafgesetzbuch (StGB) § 187 Verleumdung. Available from: https://www.gesetze-im-internet.de/stgb/__187.html [Accessed 25 October 2022].

Bundesamt für Justiz (N.D.d) Strafgesetzbuch (StGB) § 253 Erpressung. Available from: https://www.gesetze-im-internet.de/stgb/__253.html [Accessed 25 October 2022].

Bundesamt für Justiz (N.D.e) Strafgesetzbuch (StGB) § 186 Üble Nachrede. Available from: https://www.gesetze-im-internet.de/stgb/__186.html [Accessed 25 October 2022].

Dejure (N.D.a) Grundgesetz: Art. 10. Available from: https://dejure.org/gesetze/GG/10.html [Accessed 25 October 2022].

Dejure (N.D.b) Strafprozeßordnung: § 163 Aufgaben der Polizei im Ermittlungsverfahren. Available from: https://dejure.org/gesetze/StPO/163.html [Accessed 26 October 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 23 October 2022].

EUROPEAN UNION (2016) *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 23 October 2022].

Federal Bureau of Investigation (2021) *2021 Internet Crime Report*. Available from: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [Accessed 19 October 2022].

Gottfredson, M. R. & Hirschi, T. (2022) *A General Theory of Crime.* Stanford University Press. Available from: https://www.degruyter.com/document/doi/10.1515/9781503621794/html?lang=de [Accessed 22 October 2022].

Hasso-Plattner-Institut (N.D.) *Erfasste veröffentlichte Leaks der letzten Monate*. Available from: https://sec.hpi.de/ilc/statistics [Accessed 16 October 2022].

Hille, P., Walsh, G., & Cleveland, M. (2015) Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing* 30: 1-19. Available from: https://www.sciencedirect.com/science/article/pii/S1094996814000498 [Accessed 18 October 2022].

HJagdG (2018) *Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG)*. Available from: https://beck-online.beck.de/Print/CurrentDoc?vpath=bibdata/komm_pdk/pdk-he-d7he_13/ges/hessog/cont/pdk-he-d7he.hessog.htm&printdialogmode=CurrentDoc&hlword= [Accessed 21 October 2022].

Holt, T., Bossler, A. & Seigfried-Spellar, K. (2022) *Cybercrime and Digital Forensics.* Routedge, New York. Available https://essexonline.vitalsource.com/reader/books/9781000553406/epubcfi/6/52[%3Bvnd.vst.idref%3Dchapter16]!/4/2/2/2[chapter16]/6/1:0[%2C16 [Accessed 22 October 2022].

Laufer, D. (2022) Was gegen ein Deepfake spricht. *Tagesschau*. Available from: https://www.tagesschau.de/investigativ/rbb/deep-fake-klitschko-101.html [Accessed 21 October 2022].

Li, Y., Yazdanmehr, A., Wang, J. & Rao, H. R. (2019) Responding to identity theft: A victimization perspective. *Decision Support Systems* 121: 13-24. Available from: https://www.sciencedirect.com/science/article/pii/S0167923619300612 [Accessed 22 October 2022].

Marx, K. (2016) ‚Virtueller Rufmord – Offene Fragen aus linguistischer Perspektive', in: Marx, K. (eds) *Sprache und Kommunikation im technischen Zeitalter*. Berlin: de Gruyter. 237-266. Available from: https://ids-pub.bsz-bw.de/frontdoor/index/index/docId/5560 [Accessed 25 October 2022].

Meindl, F. (2012) *Identitätsdiebstahl und Identitätsmissbrauch im Internet*. Available from: https://www.law.tuwien.ac.at/DA_Meindl.pdf [Accessed 18 October 2022].

Mitsch, W. (2015) ’Diebstahl, §§ 242 ff. StGB‘, in: Mitsch, W. (eds) *Strafrecht, Besonderer Teil 2*. Berlin: Springer 3-149.

Priem, B., Leenes, R., Kosta & E., Kuczerawy, A. (2011) ‘The Identity Landscape‘, in: Camenisch, J., Leenes, R. & Sommer, D. (eds) *Digital Privacy*. Berlin: Springer 33-51. Available from: https://link.springer.com/chapter/10.1007/978-3-642-19050-6_3 [Accessed 15 October 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 22 October 2022].

Roßnagel, A. (2010) Das Bundesverfassungsgericht und die Vorratsdatenspeicherung in europa. *Datenschutz und Datensicherheit-DuD* 34(8): 544-548. Available from: https://link.springer.com/content/pdf/10.1007/s11623-010-0187-z.pdf [Accessed 23 October 2022].

Saunders, K. M. & Zucker, B. (1999) Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology* 13(2): 183-192. Available from: https://www.tandfonline.com/doi/abs/10.1080/13600869955134 [Accessed 16 October 2022].

Smith, A. D. & Lias, A. R. (2005) Identity theft and e-fraud as critical CRM concerns. *International Journal of Enterprise Information Systems* 1(2): 17-36. Available from: https://web.archive.org/web/20190308024559id_/http://pdfs.semanticscholar.org/eb76/a83e9cf0abdd2e51fa837f9fe4c808575346.pdf [Accessed 22 October 2022].

Symanovich, S. (2021) Uber Data Breach Affects 57 Million Rider and Driver Accounts. *Life Lock*. Available from: https://lifelock.norton.com/learn/data-breaches/uber-data-breach-affects-57-million-rider-and-driver-accounts [Accessed 23 October 2022].

The Word Bank (N.D.) Individuals using the Internet (% of population) – Germany. Available from: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=DE&most_recent_year_desc=true [Accessed 15 October 2022].

Verbraucherzentrale Niedersachsen (2018) Fake-Shops nutzen geklaute persönliche Daten. Available from: https://www.verbraucherzentrale-niedersachsen.de/presse/fake-shops-nutzen-geklaute-persoenliche-daten [Accessed 21 October 2022].

Walsh, G., Shiu, E., Hassan, L., Hille, P. & Takahashi, I. (2019) Fear of online consumer identity theft: Cross-country application and short scale development. *Information Systems Frontiers* 21(6): 1251-1264. Available from: https://link.springer.com/article/10.1007/s10796-019-09958-2 [Accessed 23 October 2022].

ZDF MAGAZIN ROYAL (2022) *Wo die deutsche Polizei bei der Verfolgung von Straftaten im Internet versagt |ZDF Magazin Royal*. [online video] Available from: https://www.youtube.com/watch?v=Xdm8SG8_v0I [Accessed 23 October 2022].