Dávid Tóth*

Identity crimes on the darknet and the social media

Abstract

Cybercrime is a relatively new phenomenon. There are several ways we can categorize crimes which are committed in the cyberspace. There are some crimes which can exist without the internet, but the cyberspace gives more opportunities for offenders to commit these crimes with more effective methods like child pornography. There are some cybercrimes which cannot exist without the internet (e.g. misuse of cryptocurrencies). In my current research I aim to analyze the misuse of personal information (identity crimes). I try to explore the ways perpetrator commit these crimes and how they use the social media and the darknet as a gateway to obtain and sell personal information. My aim is to give suggestion in the fight against identity fraud.

1. Introduction – generally about cybercrime

As technology advances and Internet-enabled devices become more widespread, new opportunities have emerged for criminals. The result of this that cybercrime became an independent area which is analysed by criminal law sciences. Research on cybercrime seeks to provide up-to-date answers to this area of sui generis.

The concept of cybercrime is not easy to define as it is a controversial concept. In 1991, Martin Wasik published a book titled Crime and the Computer. Back then, even the internet wasn't present in people's lives.[2] According to Walden, cybercrime is a shoulder of computer crime. A computer is needed to connect to cyberspace (the Internet) and commit abuses there. According to Walden, cybercrime is narrower than computer crime.[3] In the opinion of Gillespie it could be questioned whether the differentiation between computer crime and cybercrime continues to be relevant nowadays. We can easily access the internet even on the streets with Wi-Fi hotspots, and mobile technology is rapidly advancing.[4] On the other side we have to mention that the use of smartphones has created also many dangers as well.[5]

David Wall in his book explored why we use this term cybercrime. William Gibson coined and in his book called Neuromancer popularized the term cyberspace which is a virtual environment where networked computer activity takes place. Therefore, cybercrime describes crimes that committed in the cyberspace, and it symbolizes the dangers of the internet.[6]

Several types of cybercrime can be distinguished. Gillespie classifies cybercrime into the following categories:

- crimes against the computers, where the computer is the target of the crime.
- Crimes against property. Here the goal of the criminals is to obtain property (financial or intellectual.
- crimes involving illicit content. In this case the crime is connected to posting, hosting, or accessing of objectionable content.
- crimes against the person. Here technology is used like a weapon against individuals with possible harm to the victim.[7]

Identity theft in this categorization can be classified as a (cyber)crime against property or a crime against the person depending on the exact way and form it is committed. In the case of illegally obtainment of credit card information (credit card fraud) it can be considered as a crime against property. While in another example when the offender aims to destroy the reputation and freedom of the victim with criminal identity theft this can be considered

* Senior Lecturer, University of Pécs, Faculty of Law, Department of Criminology and Penal Execution Law.

[1] „Supported by the ÚNKP-21- 4-II-PTE-962 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund."

[2] Wasik, M. Crime and the Computer. Oxford: Clarendon Press, 1991.

[3] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007.

[4] Alisdair Gillespie, Cybercrime: Key Issues and Debates (London ; New York: Routledge, 2016). 1–3.

[5] Andrea, Kraut, László, Kőhalmi, Dávid, Tóth, Digital dangers of smartphones. Journal of Eastern-European Criminal law 7 : 1 pp. 36-49. , 14 p. (2020).

[6] David S Wall, Cybercrime. (Polity, 2007). 8–10.

[7] Gillespie, Op. cit. 7–8.

as a (cyber)crime against the person. In the following chapter my aim is to discuss what forms of identity theft exist today.

2. The origins and the concept of identity theft

The original form of identity theft was the impersonation of another person with fraudulent intent. An example of a crime can be found in the Bible in the history of Jacob and Esau, where Isaac's firstborn son Esau relinquished his prerogatives for a bowl of lentils in favor of Jacob, but their father was unaware of this. (Genesis 25: 19-34) Later, Jacob went to his already blind father to receive the blessing of the inheritance. He did this in the clothes of Esau and in goatskin so that Isaac would not notice the deception. Among the historical examples we could highlight the case of John Ylmer. Aylmer was practicing medicine in the middle of the 15th century, and in 1449 he escaped to France because he was charged with a murder committed against his wife. Around one year later he went back to England with the Jack Cade pseudonym. He began to organize an army of dissidents against King Henry. He then claimed to be John Mortimer, a relative of Prince Richard of York. Aylmer's army defeated the royal soldiers at Kent. Despite initial success, his army later disintegrated, and Aylmer was killed by Kent Sheriff.[8]

In the modern age, identity theft is an increasing worldwide phenomenon due to the development of information technology. The growth has several reasons. On one hand, more personal information is available on the Internet as people voluntarily share information about themselves on social networks. On the other hand, government, and business agencies store huge amount personal data in large databases. Third, perpetrators constantly attack accessible or hackable sites, cloud services, computers with various techniques (such as hacking, sending viruses) to gain access to this personal information. In addition to cybercrime, we must not forget the physical crimes (theft, fraud), which also increase the scale of this special form of crime.

There is no uniformly accepted definition of identity theft in the literature. In the foreign literature, several names are used for the same phenomenon. On one hand, it is commonly referred to as identity theft (or in German: identitätsdiebstahl), which is more prevalent in the United States[9] and Germany.[10] On the other hand, in the United Kingdom[11] this form of crime is being apostrophized as identity fraud.

According to Charles M. Kahn and William Roberds, in the case of identity theft offender fraudulently uses another person's personal information.[12] Katie A. Farina›s also emphasizes fraudulent element when she refers to the Identity Task Force definition: "the misuse of another individual's personal information to commit fraud"[13] According to Biegelman, who wrote a handbook on the subject, gives a simple definition: „identity theft is the stealing of your good name and reputation for financial gain."[14]

Erin Suzanne Davis[15] has a more specific and concrete definition. According to her opinion identity theft occurs when criminals use personal or financial information about the person to obtain to create a fake identity for themselves in order to obtain money from either the victim or from an institution.

Several technical terms have appeared in the Hungarian legal literature as well. In a joint study by Dániel Eszteri and István Zsolt Máté, the term identity theft is used in connection with the conducts committed in software called *"Second Life", which* simulates virtual reality.[16] Hámori also uses this term, and his definition focuses on the unlawful acquisition of personal data.[17]

In contrast to the above, Zsolt Haig uses the personality theft terminology. Referring to Scwhartau's book[18] , he classifies personality theft in the category of information warfare. If the crime is committed, their victim may suffer damage to their material and human dignity.[19]

Kinga Sorbán uses the term identity theft.[20] According to her, this form of crime has two moments. In the first phase, the offender steals the vic-

[8] Sandra K. Hoffman and Tracy G. McGinley, Identity Theft: A Reference Handbook (Santa Barbara, CA: ABC-CLIO, 2010), 5–7.

[9] Biegelman, M T.. Identity theft handbook: Detection, prevention, and security: John Wiley & Sons, 2009. 2.

[10] Borges, G, J Schwenk, C F. Stuckenberg and C Wegener. Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte: Springer-Verlag, 2011. 9.

[11] https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft (retrieved August 18, 2019).

[12] Kahn, C M. and W Roberds. „Credit and identity theft." Journal of Monetary Economics Vol. 55 (2008): 251–264.

[13] Katie A Farina, "Cyber Crime: Identity Theft," International Encyclopedia of the Social & Behavioral Sciences., 2015, pp. 633–637, 633.

[14] Biegelman, M T.. Identity theft handbook: Detection, prevention, and security: John Wiley & Sons, 2009. 2.

[15] Erin Suzanne Davis, „A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet," Washington University Journal of Law & Policy 12, no. 1 (2003): 201–228.

[16] See further in: Dániel Eszteri and Máté István Zsolt, "Identity Theft in the Virtual World," Belügyi Szemle, no. 3 (2017): pp. 79–107.

[17] Balázs Hámori, "Bizalom, Jóhírnév És Identitás Az Elektronikus Piacokon," Közgazdasági Szemle, no. 9 (2004): pp. 832–848, 840.

[18] Schwartau, W. Information warfare: Chaos on the electronic superhighway (pp. 3-13). New York: Thunder's Mouth Press, 1994.

[19] Zsolt Haig, "Az Információs Hadviselés Kialakulása, Katonai Értelmezése.," Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata., no. 1-2 (2011): pp. 12–28, 14.

[20] Kinga Sorbán, "Az Informatikai Bűncselekmények Elleni Fellépés Nemzetközi Dimenzió," Themis, no. 1 (2015): pp. 343–375.

tim's personal information (e.g., the Social Security Number). The second phase is about the misuse of data. She points out that the Hungarian Criminal Code does not contain any special statutory provisions, and in her opinion this is not necessary, because the related behaviors establish existing crimes.[21]

In my view, all the technical terms are correct and cannot be ranked among them.

There is also an example of a legal definition in the United States. Section 1028 of Chapter 47 of the 18th title of the U.S. Code states that

"Whoever...

- *knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;*
- *knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;*
- *knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;*
- *knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;*
- *knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;*
- *knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;*
- *knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or*
- *knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification... shall be punished..."*

If we analyze the definitions, all of them have common elements. All definitions include:

- the object of offense, which is information related to identity;
- a punishable act that can range from acquisition, to misuse;
- a subjective element that typically contains some form of intent (e.g., fraudulent intent),
- lastly, all authors agree that a crime occurs when the victim has not consented to their personal information being accessed and used.

The Hungarian Penal Code does not penalize identity theft as a separate crime, but the conducts related to it can lead to several criminal offenses (fraud, information system fraud, misuse of personal data, misuse of documents, forgery of public documents, misuse of a cash substitute payment instrument).

3. The social media and identity theft

Social media is growing rapidly in the recent years. Webpages, applications, software, which are used to build connection between the people (creating social network) can be considered as are social media. Social media allows its users to create and or share content with the public or private circles. (like friends). Many types of social media exist like:

- social networks. The primary purpose of social networks is to connect their users with each other and allow them to share their thoughts and content with friends, friends, family, or even the public. The most recognized social networks are Facebook and twitter.
- Media networks. These services as it names suggests focuses on the media element and not on the connection between users. The best example for these types of platforms is YouTube where the media element is the video. Instagram can be also mentioned where the pictures are in the center. Although on Instagram you can have followers and on YouTube you can have subscribers but still the focus is on the media with these networks.
- Discussing networks. Here users can bring up a topic or a question which they can discuss among themselves. These sites are similar to forums although they usually offer more social features for them. A good example for this is Reddit.

[21] Ibidem

As of 2021 October, almost three billion people are active users of the Facebook. Around 2.91 billion monthly active users as of the third quarter of 2021, Facebook is the biggest social network worldwide. In 2012 Facebook was the first social network to surpass the one billion active monthly users. Active users are those who have logged into their social media account during the past 30 days. During the first quarter of 2021, Facebook stated that 3.51 billion people were using at least one of the company's core products (Facebook, WhatsApp, Instagram, or Messenger) each month.[22]

Many of the available information on the internet of people are personal, financial or biographical. Especially personal data became valuable recent years, and this is one of the reasons why the European Union adopted the General Data Protection Regulation (GDPR) (EU) 2016/679, to create protection of these data.

There are many daily cases of identity theft on the social media. For example, a woman was prosecuted in the United States after creating a fake Facebook profile that depicted her ex-boyfriend as a drug addict and a narcotics detective. In this case defamation was a motive for committing identity theft. In another case in California an offender stole his classmate's Facebook password to post sexually explicit material about the victim. The perpetrator was found guilty and was sentenced to a period not to exceed one year in a juvenile detention center.

With the growth of the social media, it is much easier to commit online identity theft, and often it is very hard to detect as well if the victim is not registered in a certain social media platform where they created the fake account of him, he may never know about it. In the US many states are attempting to prevent online impersonation and to propose a federal statute to prevent online impersonation.[23]

4. Ways of commission on of identity theft

Without being exhaustive, I will focus on the most common techniques committed for identity theft. According to Zeno Geradts, phishing is most often done by sending fake emails to different accounts. In these they ask to provide their personal information on behalf of the bank. These are usually easy to filter out because they are often sent from free email addresses (gmail, hotmail).[24]

Phishing emails can include a link that can take the user to a cloned page. They typically copy the pages of banks or online stores where the victim can type in their personal information. This phenomenon is called pharming in jargon.[25]

A similar technique to phishing is smishing.[26] In such attacks, the perpetrator sends a short text message (SMS) containing a link to a fake website where the victim can provide its personal information. Criminals usually send text messages asking for a credit card number, personal information, to solve problems that do not otherwise exist (e.g., avoiding blocking a customer's bank account).

There have also been examples of criminals setting up a wireless network (Wi-Fi) to which, if unsuspecting users connect, they expose their personal information. This so-called Wi-phising.[27]

Vishing is also a similar phenomenon to phishing. In such cases, the perpetrators try to obtain data related to bank accounts through a telephone call with psychological manipulation (so-called social engineering). In this case, it is not the technology, but the credulity, naivety of the people that will be the main weapon of the attacker.[28]

Skimming is another common technique nowadays. The essence of this is that the perpetrators install miniature data recording devices in the opening of ATMs and thus obtain our credit card data.[29]

Raznik highlights two form of identity crime:

- Creating a Fake Social Media Site Profile
- Stealing a password information of the social media account.[30]

The latter can be obtained by a classic technique of identity theft is unauthorized intrusion (hacking). An example of this was the attack on the DSW shoe store network in 2005, which resulted in the theft of 1.4 million card traffic data from 108 stores.[31]

[22] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[23] Maksim Reznik, „Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," Touro Law Review 29, no. 2 (2013): 455–484.

[24] Geradts Zeno, "Identity Theft," in Encyclopedia of Forensic Sciences, ed. Siegel Jay (Amsterdam: Academic Press, 2013), pp. 419–422, 419.

[25] Whitson, J R. and K D. Haggerty. „Identity theft and the care of the virtual self." Economy and Society 37 (2008): 572–594.

[26] Tajpour, A, S Ibrahim and M Zamani. „Identity theft methods and fraud types." IJIPM: International Journal of Information Processing and Management 4 (2013): 51–58.

[27] Ibidem.

[28] Biegelman, M T.. Identity theft handbook: Detection, prevention, and security: John Wiley & Sons, 2009. 37.

[29] See further in: Dávid Tóth, "A Készpénz-Helyettesítő Fizetési Eszközökkel Kapcsolatos Bűncselekmények Büntetőjogi Szabályozása." in Doktori Műhelytanulmányok, ed. Gábor Kecskés (Győr: Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2015), pp. 226-237, 252.

[30] Maksim Reznik, „Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," Touro Law Review 29, no. 2 (2013): 455-484

[31] Chawki, M and M Wahab. „Identity theft in cyberspace: Issues and solutions." Lex Electronica 11 (2006): 14.

5. The darknet and Identity theft

It's true that many personal data can be accessed through the so-called indexed sites just like the social media platforms but more than one billion webpage also exists on the darknet as well. The illegally obtained personal data can be transferred, exchanged, bought, sold, and marketed in the hidden part of the internet which can increase the latency of this crime from. Identity theft can aid in the commission of many more serious crime forms like organized crime and terrorism. Erich Holm gives an example where pseudonym "Charles", the offender collected the names of deceased children from cemeteries, and established illegitimate identities in those names, and the connected crimes occurred over a 9-year period.[32]

There were also many reports in the United States that on darknet sites American children's social security number is used and sold regularly.

Overall the darknet is another place in the cyberspace where identity theft can grow in the future and could be a facilitator for many crimes.

6. Crime prevention suggestions and summary

In my opinion, three actors have a big role to play in crime prevention of identity theft: the state, financial organizations, and individuals.

It is the duty of the state to criminalize the related crimes (even considering a separate statutory provision facts). Law enforcement agencies, however, must enforce the state's criminal power in practice. Finally, there are models abroad for victim support services that deal specifically with victims of identity theft.[33]

Financial organizations have several responsibilities in the context of identity theft, I would highlight the following:

- confidential handling of personal data
- compliance with the law,
- setting up up-to-date security systems against potential attacks.

There are several helpful tips for individuals as well:

- share as little information as possible on social media, and only with friends,
- do not take photographs of personally identifiable documents,
- do not store credit card information online, etc.

If trouble has occurred, it is important for victims to be proactive:

- file a report to the police,
- if credit card details have been stolen, it is advisable to block the card and freeze the account,
- and contact financial institutions and victim support services.

Identity theft is dangerous because there are many ways it can be committed, and it can the catalyst for other crimes like terrorism, terrorism financing[34] fraud, organized crime and terrorism. Identity theft when is committed in the cyberspace has often no borders, so a coordinated inter-state action against offenders is important. This can be particularly effective at the regional level. This requires harmonized legislation and coordinates cooperation between criminal authorities. In this respect, there are positive developments in the European Union. Previously, the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems dealt with this phenomenon only. Another development in this field is the Directive (eu) 2019/713 of 17 April 2019 of the European Parliament and of the Council. This regulation reforms the criminal law regulation of cash substitute payment instruments and deals with the misuse of virtual currencies.

[32] Eric Holm, "The Darknet: A New Passageway to Identity Theft," International Journal of Information Security and Cybercrime 6, no. 1 (June 29, 2017): 41–50, https://doi.org/10.19107/ijisc.2017.01.04.

[33] https://victimsupportservices.org/help-for-victims/crime-types/identity-theft/ (retrieved August 18, 2019).

[34] László István Gál, Some Thoughts About the Fight Against Terrorist Financing in Hungary and in the European Union In: Alan, Brill; Kristina, Misheva; Metodi, Hadji-Janev: Toward Effective Cyber Defense in Accordance with the Rules of Law. Amsterdam: IOS Press, (2020) pp. 71–80.