




DÁVID TÓTH  
University of Pécs

 <https://orcid.org/0000-0002-2179-7587>

BALÁZS GÁTI  
University of Pécs

 <https://orcid.org/0009-0006-8801-6585>

## The common law approaches to identity theft: Implications for Hungarian law reform

**Abstract:** The incidence of identity theft is escalating, especially in international contexts. Owing to the advancement of information technology, crimes associated with this issue are borderless and can manifest anywhere. The objective of this study is to scrutinize the regulatory frameworks concerning identity theft in foreign jurisdictions. The essay not only considers theoretical aspects but also practical and criminological dimensions of the issue in question. As an outcome of the examination of these regulatory models, it is hoped that proposals *de lege ferenda* (‘regarding future law’) can be articulated for the Hungarian legislature.

The initial segment of the article grapples with defining the phenomenon. There is no universally accepted definition of identity theft. Various terms are employed in foreign literature to describe the very phenomenon, including “identity theft” and “identity fraud.” Subsequent to the conceptual introduction, the study surveys the potential forms of identity theft.

In the subsequent sections of the article, the regulatory models of identity theft in common law jurisdictions are analyzed. The regulatory frameworks of the United States, the United Kingdom, Canada, and Australia are subject to examination.

In the concluding section of the study, recommendations for future legislation (*de lege ferenda*) are proposed.

**Keywords:** identity theft, cybercrime, criminal law, jurisprudence

### 1. Introduction

Identity theft is becoming an increasingly global phenomenon. Due to the advancement of information technology, crimes related to it know

no borders and can occur anywhere. Estimates suggest that victims in Canada and the United Kingdom spend almost 200 hours recovering their financial losses and reputations following identity theft.<sup>1</sup> By examining the regulatory frameworks in force in common law countries and analyzing the key components of the phenomenon and dissecting the most significant elements of identity theft, the study endeavors to articulate *de lege ferenda* proposals for the Hungarian legislation.

## 2. Definition of identity crimes

In the context of identity-related crimes, a variety of terms are commonly used. The term “identity theft” is frequently found in foreign literature, particularly in the United States<sup>2</sup> and Germany (referred to as *Identitätsdiebstahl* in German).<sup>3</sup> In contrast, in the United Kingdom, the preferred term is “identity fraud.” This distinction arises because UK legislation does not explicitly define identity theft within a distinct statutory provision but considers it under the broader category of fraud.<sup>4</sup> While these terms are often used interchangeably, it is important to note that Canadian law makes a clear distinction between the two offenses.

Charles M. Kahn and William Roberds view identity theft as an inherent consequence of the credit and payment system’s structure, highlighting its economic and systemic dimensions. They argue for a balanced approach to reducing surveillance costs and controlling fraud, positioning identity theft as a macroeconomic issue rather than a series of isolated incidents.<sup>5</sup>

Conversely, Katie A. Farina provides a comprehensive outlook on identity theft, emphasizing its execution via the unauthorized access to personal data for various frauds, focusing on the direct impact on victims and the wide range of personal information at risk.<sup>6</sup> While Kahn and Roberds’s perspective is theoretical, examining the broader economic and policy

---

<sup>1</sup> E. Holm: *The darknet: New passageway to identity theft*. “International Journal of Information Security and Cybercrime” 2017, no. 6(1), p. 44.

<sup>2</sup> M. T. Biegelman: *Identity theft handbook: detection, prevention and security*. New Jersey 2009, p. 2.

<sup>3</sup> G. Borges, J. Schwenk, C. Stuckenberg, C. Wegener: *Identitätsdiebstahl und identitätsmissbrauch im Internet. Rechtliche und technische Aspekte*. Heidelberg–Dordrecht–London–New York 2011, p. 9.

<sup>4</sup> A. A. Gillespie: *Cybercrime*. New York 2015, p. 145.

<sup>5</sup> C. M. Kahn, W. Roberds: *Credit and identity theft*. “Journal of Monetary Economics” 2008, no. 55, p. 251.

<sup>6</sup> K. A. Farina: entry *Cyber crime: Identity theft*. In: *International Encyclopedia of the Social & Behavioral Sciences*. Eds. Neil J. Smelser, Paul B. Baltes, 2015, pp. 633.

implications, Farina’s approach focuses more on practical, individual solutions. Similarly, the Canadian legal scholars Philippa Lawson and John Lawford define identity theft as illegally obtaining and using (of) another person’s personal information with fraudulent intent. The primary goal of the perpetrators is financial gain. Personal data can be obtained in several ways, for example, by:

- stealing wallets, laptops, bank cards, hard disk drives;
- “hacking” into computer storage devices over the internet, or
- fraudulently posing as an internet service provider, apparently for market research purposes.<sup>7</sup>

Biegelman frames identity theft as stealing an individual’s good name and reputation for financial gain, emphasizing the impact on victims’ public standing.<sup>8</sup> In contrast, authors of a German book delineate identity theft as the unlawful acquisition of personal identity, clarifying that theft of individual data items does not constitute identity theft. Instead, it becomes identity theft only when a comprehensive set of data sufficient for personal identification is acquired.<sup>9</sup> They clearly distinguish between identity theft and identity misuse, the latter referring to the fraudulent use of personal data, highlighting the nuanced differences in the conceptualization of identity-related crimes.<sup>10</sup>

Similar to foreign terminologies, several technical terms have appeared in Hungary as well. In a joint study by Dániel Eszteri and István Zsolt Máté, the term identity theft is used in connection with crimes committed in the virtual reality simulator software *Second Life*.<sup>11</sup> Balázs Hámori also uses this technical term, and at the center of his definition is the illegal acquisition of personal data: “The illegal appropriation of a person’s data (name, year of birth, address, credit card ID, social security number, and other personal data) with the intention of using them in various transactions for financial gain, from car rental to obtaining a bank loan.”<sup>12</sup>

Contrary to the above, Zsolt Haig uses the term personality theft, citing a book by Winn Schwartz,<sup>13</sup> and classifies personality theft under infor-

<sup>7</sup> P. Lawson, J. Lawford: *Identity theft: the need for better consumer protection*. Public Interest Advocacy Centre Ottawa, Ontario. 2003, pp. 3–19.

<sup>8</sup> M. T. Biegelman: *Identity theft handbook ...*, p. 2.

<sup>9</sup> G. Borges, J. Schwenk, C. Stuckenberg, C. Wegener: *Identitätsdiebstahl und Identitätsmissbrauch im Internet...*, p. 11.

<sup>10</sup> C. Busch: *Biometrie und Identitätsdiebstahl*. “Datenschutz und Datensicherheit – DuD” 2009, no. 5, pp. 317–317.

<sup>11</sup> D. Eszteri, I. Z. Máté: *Identitáslopás a virtuális világban*. “Belügyi Szemle” 2017, no. 3, pp. 79–107.

<sup>12</sup> B. Hámori: *Bizalom, jóhírnév és identitás az elektronikus piacokon*. “Közgazdasági Szemle” 2004, no. 9, pp. 832–848.

<sup>13</sup> W. Schwartz: *Information warfare*. Kindle e-book edition. New York 2010, p. 163.

mation warfare, specifically personal information warfare. In the event of the commission of the crime, their victims may suffer material and moral/emotional damage.<sup>14</sup> Kinga Sorbán is another scholar who uses the term identity theft.<sup>15</sup> According to her, there are two stages to this form of crime. In the first phase, the perpetrator steals the victim's personal data (e.g., social security number). The second phase involves the misuse of the said data. She points out that the Hungarian Criminal Code lacks a distinct provision for this issue, but believes it unnecessary because behaviors pertaining to it can be integrated into existing legal provisions.<sup>16</sup>

### 3. Types of identity theft

Various typologies of identity theft are recognized, but due to the brevity of this study, a comprehensive presentation of each is not possible. According to one typology, we can distinguish among financial, medical, criminal, synthetic, and child identity theft.<sup>17</sup>

For instance, in Hungarian jurisprudence, a case of forgery of public documents may be considered as an instance of criminal identity theft. As per the 2/2004 Criminal Unification Decision, if a defendant, during the course of criminal proceedings initiated against them, assumes the identity of another existing individual, leading to the inclusion of the corresponding data in the public document prepared by the investigating authorities, they may be deemed to have committed the dual crimes of false accusation and “intellectual” forgery of public documents.

Misuses related to personally identifiable information not only have the potential to cause financial harm but can also infringe upon human dignity and indirectly harm one's health.<sup>18</sup>

---

<sup>14</sup> Z. Haig: *Az információs hadviselés kialakulása, katonai értelmezése*. “Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata” 2011, nos. 1–2, pp. 12–28.

<sup>15</sup> K. Sorbán: *Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói*. “Themis” 2015, no. 1, pp. 343–375.

<sup>16</sup> *Ibidem*.

<sup>17</sup> N. A. Manap, A. A. Rahim, H. Taji: *Cyberspace identity theft: The conceptual framework*. “Mediterranean Journal of Social Sciences” 2015, no. 4, pp. 595–605.

<sup>18</sup> D. Tóth: *Személyiséglopás az interneten*. “Büntetőjogi Szemle” 2020, no. 1, pp. 113–119.

#### 4. The crime of identity theft in the United States

Identity theft is one of the most prevalent forms of crime in the United States. It is therefore not surprising that the U.S. was the first country in the world to codify the concept of identity theft in a specific provision.<sup>19</sup> In 1998, an amendment (Identity Theft and Assumption Deterrence Act) introduced this offense into the United States Code. Prior to the amendment, creating a false document with stolen data was considered as forgery, but misuse of personally identifiable information did not constitute a crime in itself. The purpose of the amendment was to subject abuses related to identity to federal criminal threats, which provided law enforcement agencies with broader investigative tools. The aim was also to not only penalize material damage but also other personality rights violations related to identity theft. In addition, the law prescribed a higher penalty than the previous diverse fact situations, which could increase the success of prosecution and the number of plea bargains, which – due to confessions – speeds up the criminal proceedings.<sup>20</sup>

Currently, Chapter 18, Section 1028, Subsection (7) of the United States Code's Government Code states that anyone who

- intentionally and unlawfully
  - transfers, possesses, or uses identification devices
  - of another person,
  - with the aim of – as perpetrator, accomplice, or instigator – carrying out unlawful activities,
- is punishable under member state or federal law.

An identification device, according to the law, is any name or identification number that verifies the identity of a specific individual. This particularly includes the individual's:

- name, social security number, date of birth, state-issued driving license, or vehicle registration number, foreign registration number, passport number, employee or tax identification number;
- unique biometric data, such as fingerprints, voice print, retina or iris image, or other unique physical distinguishing feature;
- unique electronic identification number, address, or routing number; or
- telecommunications identification information or identification device.

The law only contains an illustrative listing of the behaviors.

<sup>19</sup> J. Samaha: *Criminal law*. Wadsworth 2008, p. 393.

<sup>20</sup> G. Borges, J. Schwenk, C. Stuckenberg, C. Wegener: *Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte...*, pp. 338–339.

The U.S. Code<sup>21</sup> protects not only traditional physical documents but also electronic data storage devices containing personal identities. Despite the fact that Title 18 Section 1028 of the U.S. Code is focused on identity theft, unlawful acquisition of identity-related data is not punishable, only the subsequent behaviors involving the data, such as possession, transfer, or use thereof. Section 1028 also protects freely available data, regardless of whether the identity-related information is available online or, for example, may (have been) retrieved from a physical garbage container. Offenders most frequently attempt to obtain bank card numbers, credit card numbers, PIN codes used for ATMs, or social security numbers.<sup>22</sup>

The collection of identity-related data could be considered computer fraud according to Section 1030 of the code. The paragraph states that illegal access to protected data, or password and bank card number acquisition through spyware, for instance, are punishable. The regulation complies with the Council of Europe Convention on Cybercrime, adopted in Budapest on November 23, 2001, which the United States signed in 2001, ratified in 2006, and it came into effect on January 1, 2007.

Section 1030, in its current form, finds its origins in the Comprehensive Crime Control Act of 1984, Title 18, Fraud and related activity in connection with computers and was expanded further by the Computer Fraud and Abuse Act of 1986. Subsequent legal developments culminated in the Identity Theft Enforcement and Restitution Act of September 2008, the introduction of which was aimed at clarifying and broadening of the jurisdiction of law enforcement agencies in relation to identity theft. This law clarified and expanded the jurisdictional authority of law enforcement agencies. Essentially, it facilitated the process for investigative bodies to proceed against identity thieves who commit their crimes via computer. In addition, it defines the victim of cybercrime and mandates compensation for them.<sup>23</sup>

The legal consequence of identity theft can be, for its convicted perpetrator, as severe as thirty years of imprisonment, especially when a crime is related to terrorism. In fact, identity theft is heavily penalized

---

<sup>21</sup> 18 U.S.C. Section 1028, "Fraud and related activity in connection with identification documents, authentication features, and information," <https://uscode.house.gov/view.xhtml?req=identity+theft&f=treesort&fq=true&num=30&hl=true&edition=prelim&granuleId=USC-prelim-title18-section1028> (accessed: 15.05.2023).

<sup>22</sup> G. Borges, J. Schwenk, C. Stuckenberg, C. Wegener: *Identitätsdiebstahl und Identitätsmissbrauch...*, pp. 338–339.

<sup>23</sup> *Ibidem*, pp. 339–340.

precisely because in many cases it can be conducive to the financing of terrorism.<sup>24</sup>

American law also penalizes attempted identity theft with an equal severity.

## 5. Regulation in Canada

In Canada, the need for special regulation arose in the 2000s. During this period, a surge in the number of offenses, notably those involving misuse of bank card data, was observed. This tendency was not exclusive to Canada but was observed globally, with countries such as Hungary also experiencing an increase in incidents of credit card fraud.<sup>25</sup> In the year 2006, over 12,000 individuals in Canada fell victim to identity theft, culminating in a loss amounting to 16.2 million dollars.<sup>26</sup>

In March 2009, the House of Commons of Canada passed an amendment, and since then, identity theft has been regulated under a specific statutory provision.

Section 402.1 of the Canadian Criminal Code defines personal identification data, which is considered to be any data, including biological or physiological information, that is generally used independently or in combination with other information to identify individuals. This includes, in particular, fingerprint, voice print, iris image, DNA profile, person's name, date of birth, signature, username, credit card number, debit card number, financial account number, passport number, social security number, health insurance number, etc.

The law differentiates between identity theft and identity fraud. The crime of identity theft is contained in Section 402.2 of the said code. Under the law, a crime is committed by anyone who acquires or possesses another person's identifying information with the intent to use it to commit an indictable offense. Moreover, a crime is committed by anyone who transfers, makes accessible, distributes, sells, offers for sale, or unlawfully possesses another person's identifying information. From the subjective side, the perpetrator's legally evaluated aim is to use these personal identifiers to commit a crime.

---

<sup>24</sup> I. L. Gál: *Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása*. "Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata" 2012, no. 1, pp. 5–15.

<sup>25</sup> L. Kóhalmi: *The Economic and Organized Crime*. In: *Introduction to Criminology*. Ed. E. Váradi. Miskolc 2007, pp. 141–155.

<sup>26</sup> J. Winterdyk, N. Thompson: *Identity theft: Another thing to worry about*. "Law Now" 2008, no. 4, p. 31.

The law lists the following offences:

- forgery of or uttering forged passport,
- fraudulent use of certificate of citizenship,
- personating peace officer,
- perjury,
- theft, forgery, etc., of credit card,
- false pretence or false statement,
- forgery,
- use, trafficking or possession of forged document,
- fraud, and
- identity fraud.

Identity theft is punishable by up to five years in prison. Section 403 of the Canadian Criminal Code contains the offense of identity fraud. According to the factual basis of the offence, a crime is committed by anyone who fraudulently personates another person, regardless of whether the person is alive or dead.

The law also defines the purposes for which the crime can be committed:

- with intent to gain advantage for themselves or another person;
- with intent to obtain any property or an interest in any property;
- with intent to cause disadvantage to the person being personated or another person; or
- with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.

Identity fraud is considered a more serious crime than identity theft, and the penalty is imprisonment for up to ten years.<sup>27</sup>

## 6. Australian legislation

It was the state of South Australia that pioneered legal measures against crimes pertaining to identity. In 2003, amendments were made to the state's Criminal Law Consolidation Act 1935, leading to the establishment of the following offenses:

- false identity (Section 144B),
- misuse of personal identification information (Section 144C).

Subsequent legal evolution brought other Australian state, Queensland, into focus, where the Criminal Code Act 1899 was amended in 2007. As per Section 408D of the said code, a person who obtains or deals

---

<sup>27</sup> Borges G. et al.: *Identity theft and fraud legislation in Canada*. "Canadian Law Journal" 2011, vol. 4, no. 120, pp. 341–343.



with another entity's identification information for the purpose of committing, or facilitating the commission of, an indictable offence commits a misdemeanor is liable to a prison sentence of up to three years. Importantly, Queensland's legislation criminalizes not only the misuse of natural persons' identification data but also that of legal entities. The Australian Federal Parliament amended the Criminal Code Act 1995 in 2008, thus officially recognizing identity theft as a distinct category of crime at the federal level.

Under Section 372 of the Australian Federal Criminal Code, a compendium of crimes pertaining to identity fraud is defined. These include (the illegal):

- dealing in identification information,
- possession of identification information, and
- possession of equipment used to make identification documentation.

Of these, the gravest is the first crime, carrying a punishment extending to five years of imprisonment. The said code stipulates that data or documents affiliated with a person, whether living or deceased, actual or fictitious, is considered identification information, provided it is used for the purpose of identification. An indispensable requirement is that the data should serve the identification of someone. The law contains a listing akin to the U.S. regulation, delineating what specifically qualifies as such data.<sup>28</sup>

## 7. UK regulation

Contrary to other common law countries, English law does not contain a specific *actus reus* pertaining to identity theft; related behaviors are covered under the Fraud Act of 2006. The following can be considered crimes related to identity theft:

- fraud by false representation,
- fraud by failing to disclose information, and
- abuse of position.

Each of these crimes carries a sentence of up to ten years' imprisonment.

The offence that most closely approximates to identity theft is the one described as fraud by false representation. This is defined in the law as a “dishonest false representation.” Such representation could pertain to either facts or law. There are no restrictions on how the representation is made; it may be expressed in writing or verbally. A typical manifestation

---

<sup>28</sup> Ibidem, pp. 343–347.

in English practice is the act commonly known as phishing. For instance, the offence is perpetrated by an individual who, under the guise of a bank, sends fraudulent emails to unsuspecting victims requesting them to disclose their personal information. The materialization of damage is not a prerequisite; the offence is considered an immaterial crime. The action of the perpetrator must be intentional, and they must realize that their act embodies a falsehood or incorporates deception. The legally evaluated aim of the perpetrator lies in financial gain, or causing financial detriment to others.<sup>29</sup>

## 8. The necessity for specific regulation of identity theft in Hungary

As previously mentioned, the Hungarian Criminal Code does not currently contain a specific statutory provision for identity theft. However, the rates of certain crimes that might fall under the phenomenon of identity theft indicate that there is a need for a new statutory provision. The data presented in this section is sourced from the Bűnügyi Statisztikai Rendszer (Criminal Statistics System), which is the official system used by the Hungarian government to collect, process, and report statistical data on criminal activities in the country. This system includes data on various types of crimes, including their frequency, geographical distribution, and trends over time. The data collected in the Criminal Statistics System is used for official reports, policymaking, and law enforcement purposes. From 2018 to 2022, there were significant increases in several categories of crimes that are related to identity theft<sup>30</sup>:

- Fraud showed a 128% increase from 2018 to 2019.
- The use of forged private documents increased by 59% from 2018 to 2019.
- Counterfeiting of cash-substitute payment instruments saw a dramatic increase of 1408% from 2019 to 2020.
- Cash-substitute payment instrument fraud increased by 167% from 2018 to 2019.
- Forgery of administrative documents increased by 123% from 2018 to 2019 and by 50% from 2019 to 2020.
- Criminal offenses with authentic instruments experienced a 101% increase from 2018 to 2019.

---

<sup>29</sup> A. Savirimuthu, J. Savirimuthu: *Identity theft and the issue of jurisdiction: A comparative analysis*. “European Journal of Law and Technology” 2007, vol. 4(4), pp. 440–442.

<sup>30</sup> Cf. <https://bsr-sp.bm.hu> (accessed: 15.05.2023).

- Misuse of personal data saw a dramatic increase of 686% from 2018 to 2019, a 14% increase from 2020 to 2021, and a 103% increase from 2021 to 2022.

It is important to note that the data for 2023 is not yet complete. However, the significant increases in these categories of crimes over the years indicate that identity theft and related crimes are a growing problem in Hungary. This highlights the necessity of introducing specific regulations for identity theft within the Hungarian Criminal Code by drafting a new statutory provision as a separate provision.

In light of the substantial increases in various categories of crimes related to identity theft, it is clear that the current provisions of the Hungarian Criminal Code are insufficient to address this growing problem. This insufficiency not only hampers the effective prosecution of these crimes but also leaves a legal void that needs to be filled in order to provide comprehensive protection against such offenses.

Therefore, to fortify the legal framework and ensure comprehensive protection against identity theft, we propose the following amendment to the Hungarian Criminal Code:

#### Identity theft

[...]§ (1) Anyone who

- a) unlawfully acquires or possesses another person's identification data for the purpose of using it,
  - b) unlawfully transmits or makes available another person's identification data for the purpose of committing a crime specified in ... §, ... § (...) paragraph ... point or ... §, is guilty of a felony punishable by imprisonment not exceeding three years.
- (2) The penalty shall be imprisonment between one to five years for a felony if the offense is committed in criminal association with accomplices or on a commercial scale.
  - (3) The penalty shall be imprisonment between two to eight years if the offense causes substantial injury to interest.

**Note:** In the proposed statutory provision, the sections indicated by “...” would be substituted with the actual crimes from the code listed in the crime rate section.

## 9. Conclusions and suggestions

Predominantly, common law jurisdictions implement distinctive statutory provisions to penalize identity-associated transgressions.

As we navigate the 21st century, the inherent value of personal and identifiable data continues to rise, and the misappropriation of such data can inflict substantial damage on individuals, legal entities, and states alike. It is of utmost importance to extend the shield of criminal law over information closely bound to one's identity. In our perspective, the formulation of specific legal provisions serves as the most efficient mechanism to achieve this aim. Taking into account the existing provisions of Hungarian legislation and inspired by the American and Canadian legislative models, we have drafted a proposal, *de lege ferenda*, for Hungarian legislators to consider. Implementing a specific proposal like this would not only introduce a distinctive statutory provision for the safeguarding of identity data but also represent a crucial step towards bolstering the legal protections against identity theft and related crimes in Hungary.

## Bibliography

- Alisdair A. G.: *Cybercrime*. New York 2015.
- Biegelman M. T.: *Identity theft handbook: Detection, prevention and security*. New Jersey 2009.
- Borges G., Schwenk J., Stuckenberg C., Wegener C.: *Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte*. Heidelberg–Dordrecht–London–New York 2011.
- Borges G. et al.: *Identity theft and fraud legislation in Canada*. “Canadian Law Journal” 2011, vol. 4, no. 120, pp. 341–343
- Busch C.: *Biometrie und Identitätsdiebstahl*. “Datenschutz und Datensicherheit – DuD” 2009, no. 5, pp. 317–317.
- Eszteri D., Máté I. Z.: *Identitáslopás a virtuális világban*. “Belügyi Szemle” 2017, no. 3, pp. 79–107.
- Farina K. A.: entry *Cyber Crime: Identity Theft*. In: *International Encyclopedia of the Social & Behavioral Sciences*. Eds. N. J. Smelser, P. B. Baltes, 2015, pp. 633–637.
- Gál I. L.: *Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása*. “Szakmai Szemle: A katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata” 2012, no. 1, pp. 5–15.
- Haig Z.: *Az információs hadviselés kialakulása, katonai értelmezése*. “Hadtudomány, a Magyar Hadtudományi Társaság Folyóirata” 2011, nos. 1–2, pp. 12–28.
- Hámori B.: *Bizalom, jóhírnév és identitás az elektronikus piacokon*. “Közgazdasági Szemle” 2004, no. 9, pp. 832–848.

- Holm E.: *The darknet: New passageway to identity theft*. “International Journal of Information Security and Cybercrime” 2017, no. 6(1), pp. 41–50
- Kahn C. M., Roberds W.: *Credit and identity theft* “Journal of Monetary Economics” 2008, no. 55, pp. 251–264.
- Kóhalmi L.: *A gazdasági és a szervezett bűnözés*. In: *Bevezetés a bűnügyi tudományokba*. Ed. E. Váradi. Miskolc 2007, pp. 141–155.
- Lawson P., Lawford J.: *Identity theft: The need for better consumer protection*. Public Interest Advocacy Centre 2003.
- Manap N. A., Rahim A. A., Taji H.: *Cyberspace identity theft: The conceptual framework*. “Mediterranean Journal of Social Sciences” 2015, no. 4, pp. 595–605.
- Samaha J.: *Criminal law*. Belmont 2008.
- Savirimuthu A., Savirimuthu J.: *Identity theft and systems theory: The fraud act 2006 in perspective*. “SCRIPTed: Journal of Law, Technology and Society” 2007, no. 4(4), pp. 436–461.
- Schwartau W.: *Information warfare*. Kindle e-book edition. New York 2010.
- Sorbán K.: *Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói* “Themis” 2015, no. 1, pp. 343–375.
- Tóth D.: “Személyiséglopás az interneten.” *Büntetőjogi Szemle* 2020, no. 1, pp. 113–119.
- Winterdyk J., Thompson N.: *Identity theft: Another thing to worry about*. “Law Now” 2008, no. 4, pp. 30–34.