IDENTITY THEFT AND THE FINNISH CRIMINAL CODE

Juhani Korja

Ph.D. researcher, University of Lapland, Faculty of Law
P.O. Box 122, Rovaniemi, FI
juhani.korja@ulapland.fi

Keywords: ***Identity theft, Identity, Finnish Criminal Code***

Abstract: *Identity theft is not a new phenomenon. But the threat has become more pervasive in the digital age. Also the new online elements have given criminals more sophisticated means to commit identity theft. Identity theft occurs when someone unlawfully obtains another's personal information and uses it to commit theft or fraud. «Identity theft» and «identity fraud» are terms used to refer to all types of crime in which someone unlawfully obtains and uses another person's personal data in a way that involves fraud or deception, typically for economic gain. In Finland, identity theft has been a crime in its own right since 4 September 2015, when the new amendments to the Finnish Criminal Code to that end came into force.*

1. Introduction

Identity theft is not a new phenomenon. It has been a problem for decades. But the threat has become more pervasive in the digital age. The new online elements have given criminals more sophisticated means to commit identity theft.[1]

The increase of identity theft is a part of a bigger picture in computer crime. This is mostly due to the technological development and commercial advances experienced during the last decade or so. Because of these developments, we have witnessed a substantive rise in many different forms of fraudulent use of personal, identifying information by thieves who intends to use this information for their own gain.[2]

This paper examines identity theft from the Finnish legal viewpoint. It discusses the concept of identity as well as the different types of identity theft. Lastly, it reviews the penal sanctions for theft in the Finnish Criminal Code.

2. What do we mean by «identity»?

Identity is a construct that forms the foundation for social interaction. Every individual has his or her individual and unique identity, comprising, among other elements, mental images, attitudes and emotions.[3] Erik Allardt has described a person's identity in the following terms: People's identity is built primarily on their affinity with certain individuals or groups: people need communities and groups, which define with whom

[1] Federal Bureau of Investigations, Identity theft. Available at: https://www.fbi.gov/about-us/investigate/cyber/identity_theft (accessed on 26 January 2016)

[2] Taylor – Caeti – Loper – Fritsch – Liederbach, Digital Crime and Digital Terrorism, p. 108–109. Available at: http://faculty.uml.edu/jbyrne/44.203/digital%20crime.pdf (accessed on 26 January 2016)

[3] One acknowledged point of departure in the theory of identity is that the core of a person's identity is the conception that he or she occupies a particular role. *Stets*, Justice, Emotion, and Identity Theory, p. 105.

they belong.[4]

Lawrence Lessig, for his part, provides the following description: «By ‹identity› I mean something more than just who you are. I mean all the facts about you that are true as well. Your identity, in this sense, includes your name, your sex, where you live, your driver's license number, your social security number, your purchases on Amazon.com, whether you're a lawyer and so on.»[5]

In the modern world, a person's identity is significant not only for him- or herself but for society at large. Using identities, it is possible to distinguish individuals from one another, that is, to identify them. Yet this is only one dimension of a person's identity, the legal or administrative dimension.

Defining «identity» can be considered quite challenging, as the concept is constantly evolving.[6] The digital identity[7] is a good example of how the concept of identity has broadened in the Digital Age. The digitalization of society has resulted in individuals» characteristics and personal data being digitalized as well. This development in turn has highlighted the importance of an identity in digital form in what is a society that relies on networks. Alongside their traditional, physical identity, individuals have acquired an identity in the digital world.

The digital identity falls among the phenomena in the Network Society which law has yet to respond to in any profound way. There are no simple legislative solutions for addressing the associated issues, and any attempts at such solutions must accommodate a wide range of interests. This state of affairs can be considered problematic given that the digital identity is becoming a necessity in the Network Society, where electronic government is dependent on network communications.

In legal perspective, identity is a complex phenomenon indeed. The concept of the human being is easily ignored if identity is approached as a technical consideration and when one reflects on questions such as when a person is, or should be, reliably identifiable and what data are necessary in particular situations. A person's legal identity is one of the key reflections of our concept of the human being. And that concept is fundamentally linked with our notion of identity.[8]

3. What do we mean by «identity theft»?

There is no precise definition of identity theft. The term refers to a broad group of criminal acts whose common element is the unlawful collection of identity-related data and the use of these data either for criminal gain or in another manner that causes detriment to the legitimate data subject. Chapter 38, section 9 a of the Finnish Criminal Code defines identity theft as occurring where, to deceive a third party, a person unlawfully uses another person's personal data, identifying data or other comparable data making it possible to identify the latter uniquely and thereby causes the data subject economic loss or more than insignificant detriment. In addition to personal data proper, identifying data include a variety of codes which identify the holder of the codes or verify the right of the holder to access particular information or a particular service. Examples are the numbers of various cards, access codes for accounts and services and biometric identifiers.

4 Allardt Ihminen ja moraali hyvinvointivaltiossa, in Juhlajulkaisu Paavo Kastari 1907, 13/11, 1977 (1978), p. 24. See also Cast, Identities and Behavior, p. 43. On identity as a social role, see also Stone, G.P., Appearance and the Self, in A.M. Rose (ed.), Human behavior and social processes. pp. 86–118.

5 Lessig, Code and Other Laws of Cyberspace (1999), pp. 30–31.

6 Nabeth, Identity of Identity, p. 24. See also Hall, Identiteetti, p. 246.

7 A person's digital identity is composed of information recorded in registers and his or her electronic trail. Heinonen, Digitaalinen minä, p. 13 and p. 253.

8 Saarenpää, Tietoturva ja tietosuoja, identiteetin näkökulma, p. 52.

Yet, the term «identity theft» is misleading, as it rarely involves the victim being deprived of the use of his or her identity. Rather, the identity – or, more properly, data pertaining to it – is used by a third party without the victim's knowledge. It would be more accurate to speak of offences relating to another person's identity or «identity offences». Such terms would be sufficiently broad in scope to cover all types of criminal acts relating to identity, such as identity thefts and (unauthorized) use of another's identity.[9] Nevertheless, «identity theft» is used so extensively that it can be considered an established term despite its shortcomings.[10]

Two elements can be distinguished in identity theft. The first is that it involves the unauthorized acquisition and use of identifying information relating to another person's identity or of other identifying information uniquely associated with that person. The second is that the identity-related data in the offender's possession or known to him or her is misused. This may occur in a traditional, manual fashion or electronically. For example, an offender might use the victim's identification card or other identification document without his or her consent and fill out forms for ordering goods or services. In another scenario, misuse of the personal data can occur electronically by using various services and taking on obligations. Identity-related data can also be stolen to be sold to other parties for criminal purposes.[11]

Based on the means by which they are committed, identity thefts can be divided into traditional identity thefts, which take place in the physical world, and those that occur on information networks.[12] Traditional identity thefts are most often cases of what is known as personality theft, in which the offence targets a particular individual and the data collected are personal data. An example is the theft of a wallet and acquisition of information by that means. Then again, the data might end up in the hands of the misuser in an entirely lawful manner, for example from pieces of discarded mail.

In the case of identity theft on information networks, the victim's identity may comprise not only personal data but also any identifying information whatsoever that is used to distinguish entities from one another, to prove that the holder of the information is the person who he or she claims to be, or to show that the holder of the information has a right to access particular information or a particular service.[13] In identity thefts occurring on information networks, identity-related information is sought and obtained from networks.

In terms of the purposes for which they are committed, identity thefts may be divided into three categories: economic or other gains, criminal detriment and other identity thefts.[14] These categories will be elaborated in the following chapters.

3.1. Economic or other gain

In today's Network Society, information has great monetary value and personal data are gathered and sold professionally between companies. Increasingly, the aim of identity thefts is also economic or other benefit. The purpose is to obtain any identity-related information possible on the victim that can be easily resold or

9 This has been stated in the report issued by the EU's Justice and Home Affairs Council in December 2010 and in Handbook on Identity Related Crime published by the UN. Internationally the most common terms referring to identity theft include «identity theft» and «identity fraud». They are particularly common in the United States and Great Britain. To be sure other expressions can be found as well. See Gercke, Legal Approaches to Criminalize Identity Theft, s. 25.

10 The lack of a uniform definition can be seen as one factor impeding efforts to combat identity theft internationally. OECD, Online Identity Theft, p. 9.

11 Kangasniemi, Identiteettivarkaudet – haasteita rikostutkinnalle ja –oikeudelle, paljon vaivaa ja harmia uhrille, p. 218–219. See also Gercke, Legal Approaches to Criminalize Identity Theft, pp. 19–20.

12 Sisäasiainministeriö [Finnish Ministry of the Interior], Henkilöllisyyden luomista koskevan hankkeen loppuraportti, p. 53. See also OECD, Online Identity Theft.

13 Sisäasiainministeriö [Finnish Ministry of the Interior], Henkilöllisyyden luomista koskevan hankkeen loppuraportti, pp. 47–48.

14 Sisäasiainministeriö [Finnish Ministry of the Interior], Henkilöllisyyden luomista koskevan hankkeen loppuraportti, pp. 53–58 and Gercke, Legal Approaches to Criminalize Identity Theft, p. 20.

that can be to commit economic offences, such as fraud, using the stolen identity. Identities can also be stolen to mask the offender's own identity, for example, to deceive public authorities.[15]

3.2. Criminal detriment

In the Information Society, identity theft is one of the new ways to harass others. Thefts are committed to cause economic loss, injury or damage to the victims. One form of identity theft is bullying at school or in the workplace, which does not result in economic loss and is not motivated by economic gain. The motive in such situations is harassment. It is similar to traditional identity offences in the physical world in that it is typically confined to single cases.

3.3. Other identity thefts

This category comprises a very large group of different types of identity theft. Their aim is not economic gain or causing detriment to the object of the theft. For example, a false profile of a public figure can be created in social media without any intention to cause that person harm.

4. Identity theft in the Finnish Criminal Code

Prior to the amendment to the Finnish Criminal Code that came into force on 4 September 2015, the Code had no express penal provision on identity theft. Notwithstanding, an individual's identity already enjoyed a measure of protection, as the Code contains a number of provisions that provide such protection directly or indirectly. For example, Chapter 16 of the Code comprehensively criminalizes impersonating another person to a public authority: such offences may involve giving false identification information or making a false statement to the authority. In addition, the act may fulfil the elements of, among other offences, fraud, counterfeiting, a data protection and registration offence, defamation, or the dissemination of information violating personal privacy.

The use of another person's identity was criminalized extensively even before the amendment. However, impersonating another to a private person was not as such criminalized previously. Presenting an accurate but stolen document to a private service provider did not previously carry a criminal penalty. Problems also arose because in practice cases occurred in which the elements of a more serious offence were not fulfilled but the person misusing the information could have been convicted of identity theft had the new provision been in force. In this light, one can consider that there was a need to fill this gap. The new provision on identity theft clarifies and improves the status of the victim whose personal data has been misused.[16]

The need to criminalize identity theft in Finland was obvious. The older legislation did not provide extensive enough protection of an individual's right to an identity and to security in its use. Government has an obligation to create a foundation that allow individuals to fully and safely make use of their identity.[17] In essence, the question is how effectively a person's identity is acknowledged and its use safeguarded in society, a society where the information that forms the basis for identification is taking on greater significance also in the practical realization of the rights of the individual.

[15] For example, in the United States the Federal Bureau of Investigation has pointed out that identity thefts are generally committed to mask the identity of criminals and terrorists. For more detail, see: http://www.fbi.gov/about-us/investigate/cyber/identity_theft (accessed on 26 January 2016)

[16] Report of the Legal Affairs Committee 29/2014, pp. 3–4

[17] Pöysti, Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta, p. 104.

International legislation on cybercrime has undergone rather intensive development. The central international instrument is the Council of Europe's Convention on Cybercrime, which served as the model for the EU Cybercrime Directive.[18] Owing to cyber-attacks on information networks, the increase in identity offences and the requirements of the Cybercrime Directive, a new penal sanction on identity theft was added to the Finnish Criminal Code. The provision (Chapter 30, section 9 a) came into force on 4 September 2015.[19] According to the provision, a person is to be sentenced for identity theft where, to deceive a third party, he or she unlawfully uses another person's personal data, identifying data or other comparable data making it possible to identify the latter uniquely and thereby causes the data subject economic loss or more than insignificant detriment. Identity theft is punishable by a fine.

Identity theft is an offence that is prosecuted at the request of the injured party; that is, the prosecutor has the right to bring charges only where the victim insists that this be done. The prosecutor may bring charges for identity theft only if the victim makes a notification to that effect. The principal object of protection in the provision on identity theft is the inviolability of the personality of the person whose personal data have been misused. If the victim does not consider that his or her personality has been violated or for some other reason does not want the case brought before a court and charges brought, there is no justification for proceeding against the victim's wishes.[20]

A number of conditions have to be met before a penalty is imposed for identity theft. First, the suspect's intent in using the identifying information must have been to deceive a third party. This party may be an information system created or maintained by people. As regards the deception, it is essential that the third party has been misled expressly with regard to the victim's identity.[21] A second requirement for imposing a penalty is that the person perpetrating the deception has acted unlawfully. A person is not deemed to have acted unlawfully if, for example, he or she has the right to use the IP address in question or has used a name which is the same as his or her own.

The new criminal provision also requires the use of another person's personal data, identification information or other, comparable information making it possible to identify the person uniquely. The purpose here has been to cover all information which could lead a third party to mistakenly think that the person misusing the information is the true data subject.[22] Crucial here is that the information must be associated with or linked to identification, and must make possible the identification of the person and thus the mistaken belief by the third party. Even though the information used in the offence is personal data, this is of no significance in the situation envisaged here unless the data are used in a context where identification becomes possible or in conjunction with such other information making identification possible.[23]

One interesting point in the criminalization of identity theft is that the offence can involve the unlawful use of information that makes it possible to uniquely identify a juridical person. The «another person» referred to in the provision may be a juridical person. Although personal data refer to the personal data of a natural person that are identifiable, the phrase in the provision referring to other information permitting unique identification is intended to cover such information pertaining to a juridical person, for example.

18 Hallituksen esitys [HE]232/2014, pp. 3–4 [Government bill]
19 Hallituksen esitys [HE]232/2014, p. 1 [Government bill]
20 Hallituksen esitys [HE]232/2014, p. 38 [Government bill]
21 Hallituksen esitys [HE]232/2014, p. 36 [Government bill]
22 Hallituksen esitys [HE]232/2014, p. 36 [Government bill]
23 Hallituksen esitys [HE]232/2014, p. 36 [Government bill]

Misuse of personal data will not necessarily fulfil the essential elements of the statutory definition in all situations, however. The use of another person's personal data may, for example, be so minimal, apply to a detail marginal in broader perspective, or otherwise be such that there is no real risk of a third party being misled. This occurs, for example, where the activity in question is clearly recognizable as satire.[24]

Where the elements of the offence are concerned, it is also an essential consideration that the offender's intention has been to deceive the third party into thinking that the misuser of the information was a specific person or persons. Also essential where imposition of a penal sanction is concerned is an assessment of whether the situation in questions posed an actual risk of the third party being mistaken.[25]

For an instance of misuse to be punishable it is necessary that it result in economic loss or other more than insignificant detriment. Economic loss may occur in the form of expenses involved in rectifying the situation. The specifying of «not insignificant» detriment applies to situations other than those causing economic loss, that is, those causing some other form of harm.

In practice, detriment occurs in part as a consequence of the circumstances leading to economic loss. However, detriment also covers situations in which no direct economic loss has occurred. Examples would include situations in which clearing up and rectifying the matter causes the victim a great deal of inconvenience or proves unsuccessful. This might be the case where fraud has been perpetrated using another person's personal data and sorting out the situation and erroneous bills causes the victim considerable inconvenience.

The notion of detriment is also closely linked to protection of the victim's right to free speech. A person is entitled to exercise this right under his or her own name. Detriment may arise where a false profile has been created in social media using another person's details.[26] Removing such a profile might prove difficult. In addition, the victim might have to contact numerous people who thought they were in communication with him or her. By contrast, having to send a single email message to point out the misuse does not generally constitute more than insignificant detriment.

If the deceptive acts form a consistent temporal or substantive whole in which the same person's details have been misused, they are considered only a single instance of identity theft even where a number of third parties have been misled.[27]

5. Conclusions

Identity theft is not a new phenomenon. However, information networks have changed how identity-related information is misused and the opportunities for doing so.[28] Characteristic of the misuse of personal data on information networks is the considerable benefit relative to the cost of carrying out the act and to the risk of being caught. As identity theft on a network can be committed automatically, an offender has an easy opportunity to use a large quantity of unlawfully obtained information at very little expense. The risk of being caught when committing offences on networks is far smaller than in the physical world. The Internet is also a truly global environment, a fact which complicates efforts to solve cases of identity theft.[29]

[24] Hallituksen esitys [HE]232/2014, p. 37 [Government bill]
[25] Hallituksen esitys [HE]232/2014, p. 37 [Government bill]
[26] Hallituksen esitys [HE]232/2014, p. 37 [Government bill]
[27] Hallituksen esitys [HE]232/2014, p. 37 [Government bill]
[28] Back in 1998 the OECD drew attention to the importance of secure online connections, including the implications for identity theft. For more details, see OECD, A Borderless World: Realising the Potential of Global Electronic Commerce.
[29] Sisäasiainministeriö [Finnish Ministry of the Interior], Henkilöllisyyden luomista koskevan hankkeen loppuraportti, p. 53.

No single one of the considerations mentioned above can be cited as the reason why identity theft has become more common. The crux of the issue is that identifying information in our society has taken on heightened importance.[30] With people and services operating extensively on networks the need for identification in social participation has radically changed. One could with good reason speak of the instrumentalization of identification, a development in which a person's identity is transformed into measurable information; identification takes place through an instrument.[31] The digital data created in the process can be then used in both the physical and digital environments, making it easier to misuse them.

Finland's enacting of a specific provision on identity theft in its Finnish Criminal Code making such theft a criminal act in its own right can be seen as a reaction to a changed world. With the emergence of the Network Society and development of technology, what used to be no more than a prank has become a punishable offence.

Even though the Finnish Criminal Code had no express provision criminalizing identity theft before the amendment, the Code protected the identity of individuals through a number of other provisions. The provision on identity theft thus can be seen as complementary, for many of the situations that can be viewed as instances of identity theft were already offences. An offender could be sentenced for defamation, dissemination of information violating personal privacy, fraud or providing false personal data.

The new provision is not without its shortcomings, however. It requires that identity theft cause «not insignificant detriment» and this is its most principal weakness. Detriment is construed as the trouble which the victim must go to in order remove a false profile. But when is the threshold for «not insignificant» crossed? We will have to wait for case-law to answer this question – if cases come before the courts. After all, identity theft is only prosecuted if the injured party so requests. The victim can decide whether or not to seek justice through the courts. And at most, a convicted offender need only pay a fine.

The true significance of the amendment to the Criminal Code on identity theft lies in the message it sends to those contemplating such an act: identity theft is a proper criminal offence, one for which the offender might have to answer even if he or she only sought to play a joke on or tease another person.

6. References

Allardt, Erik, Ihminen ja moraali hyvinvointivaltiossa. In: Juhlajulkaisu Paavo Kastari 1907 – 13/11 – 1977. 1978.

Caeton, Daniel, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web. Bulletin of Science, Technology and Society, Vol. 27, no 1. February 2007. pp.11–23.

Gercke, Marco, Legal Approaches to Criminalize Identity Theft. In: Handbook on Identity-Related Crime. United Nations Office on Drugs and Crime. Vienna 2011. pp. 1–54.

Hallituksen esitys [HE]232/2014 (Government Bill) eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

Heinonen, Risto, Digitaalinen minä. Edita. Helsinki 2001.

Kangasniemi, Tea, Identiteettivarkaudet – haasteita rikostutkinnalle ja – oikeudelle, paljon vaivaa ja harmia uhrille. In: Perus- ja ihmisoikeudet rikosprosessissa. Helsingin hovioikeuden julkaisuja. Hakapaino. Helsinki 2012. pp. 217–238.

Lessig, Lawrence, Code and other laws of cyberspace. Basic Books. New York. 1999.

Nabeth, Thierry, Identity of Identity. In: Rannenberg, Kai / Royer, Denis / Deuker, André (Eds.) The Future of Identity in the Information Society, Springer Berlin Heidelberg, 2009. pp. 19–69.

OECD, Online Identity Theft. March 2009.

Pöysti, Tuomas, Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta. In: Oikeus 1/2000, pp. 91–112.

30 OECD, Online Identity Theft, p. 16.

31 Caeton, The Cultural Phenomenon of Identity Theft…, p. 20

Report of the Legal Affairs Committee 29/2014.

Saarenpää, Ahti, Tietoturva ja tietosuoja, identiteetin näkökulma. In: Pohjois-Suomen tuomarikoulu. Julkaisuja 2/2002. Rovaniemi 2002, pp. 33–76.

Sisäasiainministeriö [Finnish Ministry of the Interior], Henkilöllisyyden luomista koskevan hankkeen loppuraportti. Sisäasiainministeriön julkaisuja 32/2010, Helsinki 2011.

Stets, J.E.: Justice, Emotion, and Identity Theory. In: Burke, Peter J. / Owens, Timothy J. / Serpe, Richard / Thoits, Peggy (Eds.). Advances in Identity Theory and Research. Kluwer Academics / Plenum Publicshers. New York 2003. pp. 105–122.

Taylor – Caeti – Loper – Fritsch – Liederbach, Digital Crime and Digital Terrorism, pp. 108–109. Available at: http://faculty.uml.edu/jbyrne/44.203/digital%20crime.pdf .