Asian Social Science; Vol. 11, No. 22; 2015
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Cyberspace Identity Theft: Some Legal Issues under the Iranian Law

Anita Abdul Rahim[1], Nazura Abdul Manap[1], Ramalinggam Rajamanickam[1] & Hossein Taji[1]

[1] Faculty of Law, The National University of Malaysia (UKM), Bangi, Selangor, Malaysia

Correspondence: Hossein Taji, Faculty of Law, The National University of Malaysia (UKM), 43600 Bangi, Selangor, Malaysia. Tel: 60-17-271-3980. E-mail: h.taji359@gmail.com

Received: March 12, 2015 Accepted: July 13, 2015 Online Published: August 26, 2015

doi:10.5539/ass.v11n22p228 URL: http://dx.doi.org/10.5539/ass.v11n22p228

Abstract

The advent of the Internet has introduced many new forms of crimes. It has also transformed old forms of crimes, which are now being committed in new ways. In effect, cyberspace not only offers new and highly sophisticated opportunities for criminal misconduct, but also creates the potential to commit traditional crimes in a modern way. It has opened the door to criminal behavior in ways that would never have been possible in the past. The identity thief uses information relating to the identity of another person's such as name, address, telephone number, mother's maiden name, social security number, social insurance number, health card number, bank account information, driver's license number and date of birth. It is stealing someone's identity information to commit theft, fraud or other crimes. This paper aims to identify the legal issues on the cyberspace theft of identity in Iran, and to identify and analyze the laws relating to theft in Iran.

Keyword: theft, identity theft, cyberspace, Iran

1. Introduction

Theft is one of the oldest crimes against properties. It has been problematic in almost all societies, and has had severe punishments. Currently, being various and extensive, it is divided into different types, each has its specific punishment, such as simple theft, theft with harassment and threat, burglary, bank and exchange robbery, and shoplifting. The most important one is intervention in stolen property.

The crime of computer theft can be conceived in different forms, such as hardware robbery, information data robbery, and software robbery. It is doubted that these forms of crimes can be applied to the crime of classic theft. For instance, in the crime of classic theft, the subject of crime is a physical and tangible object, while computer data's are not tangible; furthermore, in information and data robbery, the information would be copied, and would still remain with their owner. The more precise evaluation of the subject requires studying the regular theft, and analyzing different forms of this crime.

2. Meaning of Cyberspace Identity Theft

Cyberspace identity theft occurs when someone else uses personal identifying information without knowledge or permission to obtain credit cards, obtain loans and mortgages, get a job, and commit other types of criminal acts, in someone's name, leaving someone's responsible for the consequences. The identity thief uses key pieces of someone's information such as Social Security and driver's license numbers to obtain credit, merchandise, and services in someone's name (Marjie, 2007, p. 119).

Cyberspace identity theft is somewhat different from cyberspace identity fraud. However, the term is often used interchangeably. Cyberspace identity fraud is the result of cyberspace identity theft. Someone can steal or appropriate someone's identifying information without actually committing cyberspace identity fraud (Marjie, 2007, p. 125). Cyberspace identity theft involves acquiring key pieces of someone's identifying information in order to impersonate them and commit various crimes in that person's name (Marjie, 2007, p. 123). Besides basic information like name, address and telephone number, identity thieves look for social insurance numbers, driver's license numbers, credit card and/or bank account numbers, as well as bank cards, telephone calling cards, birth certificates or passports. This information enables the identity thief to commit numerous forms of theft: to go on spending sprees under the victim's name, to take over the victim's financial accounts, open new accounts, divert the victim's financial mail to the thief's address, apply for loans, credit cards, social benefits, rent apartments, establish services with utility companies, and more. (Biegelman, 2009).

3. Definitions and Scope of Theft under Iranian Law

In Islamic Penal Code of Iran, Article 197, the theft is defined as "stealing the property of other ones in secret". In this definition, some points should be mentioned.

The essential element of theft in Iranian law is 'stealing'. This description distinguishes it from other crimes against properties, such as fraud, and malversation. In fraud, the offender seized the property using fraudulent means, in malversation the offender loses or wastes the property, which is given to him to be refunded or used for a certain purpose. Stealing has a fraudulent state in itself; it is different from seizing property of others. Stealing would be applied just too movable properties.

The subject of crime should be 'property'. Therefore, those things, which are not property according to law and custom, and are not ownable, could not be subject of theft. Here it is disputable that whether the 'property', which is subject of theft, should be tangible or not.

The subject of theft should belong to 'other ones'. This means that it should not belong to the thief, but the owner.

The property must be taken out of the custody of another person in a secret manner. This condition is not a general condition in every case of theft. For example, if someone armed attacks another person and steal a property, it would be considered as theft, but since it is not in secret, it will not qualify as theft according to the definition under Article 197 of the Islamic Penal Code (Sadeghi, 1980, p. 283).

An examination of cyberspace identity theft clearly shows that this crime has common features with traditional theft. The common feature, which can be found at first glance, is the definition. There is no problem of defining cyberspace identity theft as 'stealing the properties of others'. The committed theft is considered as real, and without this premise, that is, being in public, it would be virtual. The element of 'stealing' is a common feature. Another common feature is being done in secret, since the nature of virtual space is such that it cannot be observed like the physical environment the stolen property being owned by another person is another element that is common to both forms of theft.

The difference between cyberspace identity theft and classical theft is in the quality of description, and as a result, in the reflection of its legal element. It means that, despite the common aspects of their definitions, these two crimes have some differences. When the data are acquired through theft of the tangible data carriers such as paper lists, tapes, and diskettes, applying the normal penal law would not face any problem in the different legal systems. But given the ability of data processing systems to fast-copy information, many classical thefts are substituted by copying information from information devices (Abadi, 2008, p. 101). Hence, the question arises as to whether classical law could be applied to acquiring intangible information.

The difference between these two types of theft, cyberspace theft and traditional theft is the dispute over the stealing element. It should be reiterated that stealing applies to movable properties. Thus, applying this concept to the theft of information is questionable. In effect, the question is whether computer programs and information can be considered as movable properties.

We may consider some computer programs, which can be cut or copied as movable properties, and apply the relevant rules to them, and consider other programs which are designed in such a way that they cannot be moved, and would be lost just by disturbing the computer hardware, as immovable properties and apply the relevant law to them.

When the relevant hardware is robbed, there would be no problem. But if the data were displayed in virtual space and copying them were unauthorised for users, but someone, nevertheless, copies them without any permission, can he be considered a thief? Moreover, when permission is denied, but the user is able to copy the materials in an unauthorised way, if we assume that other conditions are present, is the haven considered as broken, and can the punishment prescribed for theft be applied to the user?

Such problems and questions are basically raised since the commission of classical theft is based on the principle that the stolen property is evicted from the possession of the victim, whereas in information theft, the property would still remain in the possession of the victim, with the thief having only an image or copy of the property. Not only laying hand on the property of another person is controversial, but also evicting the information from the possession of the owner is questionable too.

About the non-survival of the stolen property with the victim in the case of classical theft, but in cyberspace identity theft, this is not necessarily. If someone steals the personal information of others, considering current advances in computer technologies, there are programs that can enable the recovery of the deleted information.

Therefore, if the victim is able to recover the deleted information by means of a recovery program, can we still say that stealing, and, hence, theft has been committed?

In response to that question, it can be said that since the information is taken by the thief with the intent of theft, and he has attained his goal, that is, the result of his behaviour has been achieved, theft would be consummated. The advances in technology cannot justify the act of the thief, and prevent his penal liability. This is like the situation in classical theft in which after stealing, the stolen money is returned to the victim by any means, such as the arrest of the thief, or the return of the property by the thief. It is obvious that in such a case, that act cannot change the nature of the theft, although in the latter, it can reduce the punishment of the thief. Also, it should be considered that the lost information is not always recoverable, and might be completely removed, or it could be a type of information that can no longer be effective after being stolen.

In respect of the controversial issue of considering computer data as property, data message may include financial rights, or represent some rights, but cannot be considered as property. (Article 2 Electronic Commerce Act 2004) Data are a symbol of reality, information, or concept, which is created, sent, received, stored, or processed through electronic and photonic devices or modern information technologies.

However, from candidate's viewpoint, property is what it has already been defined to be, and data have content, which can be an agreement, a contract, an acceptance, writing or signs and passwords representing the identity of a person or thing. Consequently, it should be noted that if these data are encrypted, and stealing is done by taking their image, so that the data were unknown to the robber, and the original owner of the data suffers from no material, as well as mental loss, and the robber gains no benefit, the consummation of theft is disputable.

In the Computer Crime Act 2009 of Iran, the legislator is required to predict the appropriate punishments for cyberspace identity theft. The text of Article 12 provides that:

"Whoever steal data belonging to others in an unauthorised way, if the exact data were in the hands of their owners, would be condemned to fine in cash from one million to twenty million Rials, and otherwise, would be condemned to imprisonment from 91 days to one year, or fine in cash from five million to twenty million Rials, or both of them".

In general, if the offender does not steal the data directly, but does that through computer viruses, worms and so on, the act of stealing would be attributed to him, and he would be considered as the steward, and as the mental perpetrator of the crime. But if the data and programs were stolen by a person, and placed in the email of someone else, and the latter used those data and information, even if intentionally, he would not be regarded as a thief, and the actual thief would be condemned to the punishments mentioned in Article 12 of the Law on Computer Crimes Act 2009 (Alipor, 2010, p. 255).

Also, if a person accesses the computer of someone else, or the Internet in order to steal some information, but cannot consummate the theft for any reason, that act would not be considered as computer theft, although it might be considered to be an attempted theft, or some other form of crime. Here, one might wonder that, given the lack of appropriate law, what would be the punishment for an attempted cyberspace theft.

There is no consensus among academics and judges on the above issue. But most believe that an attempt to commit a crime is only punishable when mentioned in the law (Rohani, 2008, p. 22). Therefore, given the lack of any law in this regard, an attempt to commit a computer theft would not be punishable. Some academics have suggested that the nature of attempted theft is the same in both classical theft and cyberspace theft. And since the Islamic Penal Code 1970 is a more universal law than the Computer Crimes Act 2009, Article 41 of the Islamic Penal Code should be adopted as far as this issue in concerned.

4. Cyberspace Identity Theft in Iran

Cyberspace identity theft is receiving new attention in Iran. Until 2009, there was no law for computer crimes in general and cyberspace identity theft in particular, the law only provide for classical types of theft. Iranian legislators have adopted new regulations in relation to computer and Internet to provide security in the virtual world. The Islamic Penal Code of Iran has been amended to include offences in relation to cybercrimes and has been enforced on 29 June 2009 by the approval of the parliament. This law comprises of five parts and fifty five sections with two types of punishments, i.e. imprisonment or fine or both. (Manap & Taji, 2012, pp. 404-408)

The Offence on cyberspace theft is discussed in the fourth chapter of Computer Crime Act 2009. The text of Article 12 provides that:

"Whoever steal data belonging to others in an unauthorised way, if the exact data were in the hands of their owners, would be condemned to fine in cash from one million to twenty million Rials, and otherwise, would be

condemned to imprisonment from 91 days to one year, or fine in cash from five million to twenty million Rials, or both of them".

The new computer crime legislation has come into existence to cover those types of crimes, which were not supported by the previous law (Manap & Taji, 2012, pp. 404-408). The Iranian Computer Crime Act 2009 has adopted most of its content from the Budapest Convention.

5. Legal Analysis in Respect of Cyberspace Identity Theft

5.1 Appropriation

In Article 197 of the Islamic Penal Code of Iran, theft is defined as the "stealing of the property of another person in secret". In this definition, the essential element of traditional theft in Iranian law is 'stealing'. This description distinguishes theft from other crimes against properties, such as fraud. In fraud, the offender seizes the property by using fraudulent means. Stealing inheres a fraudulent element, but it is different from the seizing of property belonging to another person. Stealing applies only to movable properties. Without Stealing, the *actus reus* of the crime of theft would not be present (Sadeghi, 1980, p. 282). Stealing is a fraudulent act without the consent of the owner of the property. Its prerequisite is moving the property from one place to another, and its result is removing the property from the owner's proprietary realm (Sadeghi, 1980, p. 283). Therefore, from the perspective of Iranian law, the crime of theft is only applied to movable properties, properties, which can be moved, and as a result, robbed (Goldoziyan, 2007, p. 99). The prerequisite of stealing is that the thief seizes the property of another person in a secret way, or apparently by surprising the owner, and against his consent. It seems that in Iranian law, the apparent consent of the owner in giving up the property to another person would mean that no stealing is committed. In this sense, whoever takes the property of another person, and flees by threatening the owner, or takes the property from a shopkeeper in order to view it, but then flees with it, is considered to commit the act of stealing, and as a result, theft (Sadeghi, 1980, p. 283). However, the absence of this element (stealing) would prevent the crime of theft from being consummated. Therefore, if someone gives something to another person, and that person takes the thing with the intent to seize it, the act of stealing would not be realized (Zade, 2008).

According to the Article 12 of the Computer Crimes Act of Iran 2009, (Article 740 of the Islamic Penal Code), "whoever steals data belonging to another person in an unauthorised manner, if the exact data were in the hands of their owner, would be condemned to a fine in cash from one million to twenty million Rials, and otherwise would be condemned to imprisonment from 91 days to one year, or fine in cash from five million to twenty million Rials, or both of them".

Theft or stealing data is the required act, and it is carried out in the following two ways: copying data, or cutting it. Therefore, stealing under Article 12 of the Computer Crimes Act 2009 refers to two types of behaviour. One is copying - a state in which the data owner still owns the same data. The act of copying has to be performed in cyberspace. That is to say, the thief copies the data into data storage devices (or compact discs), without taking or destroying them. He may also transfer the data to his mailbox, or those of others, by sending an email. Alternatively, he may copy data through viruses, Trojans, and other such means (Sadeghi, 2011). If someone breaks into another person's computer system, which is protected by security measures, or gains access to the data or information in that system, and then writes the information on a paper, or reads it, or even captures the screen, he can be charged with unauthorised access. The reason is that looking at another person's computer system, and remembering the information stored in it, or writing it on a paper, is a physical act carried out outside of cyberspace. Hence, it is not considered a crime, unless the act leads to criminal consequences such as the violation of copyright.

Secondly, data is said to be cut when they are removed from their storage, and transferred to another place (whether a computer, email, or software). There is no evident distinction between cutting and deleting data. However, since in deletion, the perpetrator of the act deletes the data in order to eliminate them without benefiting from the act, such an act is considered to be data destruction (data sabotage) (Abadi, 2008). But, in the cutting of data, the perpetrator only aims to displace the data. With regard to copying, it can be said that the difference between copying and cutting, is that, in the case of cutting, the data are displaced, and the original data are, therefore, no longer owned by the owner.

Although theft is perpetrated in two ways, copying and cutting, these types of behaviour are forms of cyberspace intrusion that help the perpetrator to benefit from other data or own them. It is not necessary for the perpetrator to have knowledge of the information or data copied, or cut, or to even use them. It is the same as the case when someone steals the car of another person; it does not matter whether the thief knows about the contents of the car, rides it, or benefits from it.

It should be noted that since under the Computer Crimes Act 2009, theft focuses on two forms of behaviour in cyberspace, copying and cutting, it means that it does not address real world acts of theft. Hence, if someone steals the car of another person, for example, but finds a laptop or compact disc containing information in it, or if someone steals the laptop of a person in order to rob his information in the street, in the workplace or at home, or if someone steals CDs and owns them, those acts are not considered to be cyberspace theft, even though their subject is data. Such acts of stealing are prosecuted based on traditional criminal codes (Shirzad, 2012).

5.2 Property

With regard to Iranian Law as Article 197 of Islamic Penal Code provides: "stealing the property of other ones in secret". The subject of theft should be property. Therefore, those things, which do not qualify as property according to custom and law, and are not ownable, could not be the subject of theft (Langeroudi, 2007). Here, as has been seen, it remains disputable whether property that is the subject of theft should be tangible, or not. A property is something that has economic value and rational interest. The subject of the crime of theft is property, which can be robbed (Langeroudi, 2007). Therefore, the Internet immovable properties cannot be stolen. But what is recognized as immovable properties in civil law (incidental immovable properties) can be stolen. It should also be noted that the property, which is the subject of theft is the property in itself, not the rights and interests in it (Hojati, 2012). For example, plagiarism is not included in the crime of theft, and is considered as an independent category (Sadeghi, 1980, p. 289). Similarly, the right to seek imprisonment, or interest, or credit cannot be stolen. Also, alcoholic drinks are not considered property according to Islamic law, and, therefore, stealing them is not considered to be theft (Sadeghi, 1980, p. 289). The minority of experts, believed that: 'since the legislator considers the stealing of property as a crime, and property is applied to objects, which are capable of being traded, and such property might be movable (such as money in cash, documents, papers) or immovable, and considering the articles of Islamic Penal Code, the act of stealing computer data is considered as a crime' (Goldoziyan, 2007, p. 122).

The Commission of Judiciary tends to take the position. It states that: data and programs, which are saved in the computer memory or diskette, or are bought, or produced for some costs, would be considered as movable property, and to have the ability to be traded, and seized, and would be bought and sold in free market. Therefore, the theft of data, if the data are possessed by others, falls within the definition of theft in Article 197 of the Islamic Penal Code, and is punishable (Goldoziyan, 2007, p. 105).

Our discussion has so far demonstrated that the theft of credit, and, therefore, personal rights, is a recognised principle in Iranian law. Since credit represents some form of incorporeal property, Iranian courts have basically recognized the theft of incorporeal items. Although the courts have not clearly stated this fact, with time and further development, it will become a reality.

The theft of data, information, or protected ideas should be recognized in Iranian law, similar to the theft of credit, or money. However, the protection should be limited to certain types of information. The category of things capable of being stolen should be extended to include both personal rights, and immaterial property rights (Goldoziyan, 2007, p. 105).

5.3 Property Belonging to Another

With regard to the Iranian Law as Article 197 of Islamic Penal Code provides: "stealing the property of other ones in secret". Another point that is worth stressing is that "other ones", the subject of theft should belong to someone else. This means that in order for the crime of theft to be consummated, the stolen property should belong to another person. It should not belong to the thief, but the true owner. Therefore, the stealing of property, which does not belong to anyone, is also not considered as theft. But this does not mean that in order for there to be theft, the owner of the stolen property must necessarily be known. It is only necessary to show that the stolen property belongs to another person (whether natural or legal) (Zade, 2008).

In the English law, "property" is defined as any right, or interest, which is related to ownership, while in Iranian law, theft laws are applied only to the property. Therefore, in the Iranian law, unlike the English law, by "belonging to others'', the legislator means that the relevant property belongs to others (whether natural or legal persons). It means that if the property belongs to the offender, theft would not be consummated. Thus, stealing a mortgage by a mortgager is not considered as theft. On rent, if the future interest of the rented property has still not accrued, it cannot be stolen (Zade, 2008). Also, if a buyer deprives the seller of his right in the purchased goods before paying the price, his action cannot be regarded as theft, because as soon as the sale contract is concluded, the ownership of the purchased goods is transferred to the buyer.

But according to the English law, the property belongs to the person who enjoys possession related rights and

interests in it. Therefore, copyright, or credit, or the right of a seller in a property he has just sold, or interests in the property, and so on, can be stolen. Also, if the owner of the self of the property deprives another person of his legitimate rights and interests in the property, the crime of theft is committed. For example, a car owner who carried his car out of a garage with the aid of a spare key, without paying his bill was condemned as a thief by the English courts for depriving the repairer of his wage. It is not conceivable in Iranian law to consider such a case as theft.

Stealing a joint property is not considered to be theft, as well. In this respect, two conflicting theories have been adopted. Some believe that because each component of a joint property is owned by all the partners, it cannot be called the property of others vis-à-vis any of the partners. Therefore, a crime against a joint property by one of the partners is not conceivable.

According to the opposing theory, however, someone will be innocent of committing a crime against a property only if he is the owner of that property. In the present case, since all the partners have shares in all components of the joint property, it does not belong to any of them. It is concluded, therefore, that the criminal behavior of any of the partners toward the joint property will be considered to be a crime. From a purely legal perspective, the first theory should be preferred. This is because when two arguments, which are equal in terms of their strengths, are in contention, the argument whose result is favorable to the offender should be adopted; in this case, it is the first theory (Zade, 2008).

With respect to cyberspace identity theft, from the foregoing analysis the subject of theft is data owned by another person. Among information, data, hardware, and the system, only data, or information is the subject of identity theft; the system or computer network cannot be stolen. The reason is that the system focuses on the computer functions, and the network is comprised of several interconnected computers. Therefore, in those two cases, stealing can be carried out through unauthorized access to the data or hardware. Stealing hardware and physical items such as monitors, keyboards, or hard disks, is the subject of traditional theft, even if the thief steals them in order to gain access to information.

5.4 Dishonesty

In respect of the *mens rea* of theft in Islamic Penal Code of Iran, firstly, it is necessary for the thief to be aware that the property belongs to another person. Secondly, general intent, that is, the will of the offender to seize the property of another person, as well as specific intent, that is, the will to harm another person, is required: (Abadi, 2008, p. 92).

i) General intent: the crime of theft is an intentional one, so its realization requires a general intent, which is the intent to steal.

ii) Specific intent: this is the intent to take the property, and remove it from the possession of the victim - to seize the property.

iii) Being aware that a property belongs to another person is the common *actus reus* of all crimes against property.

In the English law, the *mens rea* of the crime of theft includes a general intent, which refers to the deliberate taking over of the property, and specific intent, which means to permanently deprive the owner of the property. These are explicitly mentioned in the text of the theft law (Moradi, 2007). There is no explicit text in the Iranian law in respect of this requirement. However, according to Paragraph 14 of Article 198 of the Islamic Penal Code, it seems that if someone takes over the property of another person in order to temporarily use and return it back to the owner after satisfying his own need, it cannot be regarded as theft. If his intent is known, members of the society would also not consider him to be a thief.

In terms of the *mens rea*, the two elements of general and specific intents are common to both types of theft, traditional theft and cyberspace theft. In other words, cyberspace identity theft requires the *mens rea* like classical theft, which includes general and specific intents. As mentioned earlier, general intent is the will of the offender to embark on the act of stealing, knowing that the subject of the stealing is owned by another person, and its stealing is not authorised. And specific intent is the will of the offender to realise the result, which means, taking the stolen item from the possession or exclusive possession of its owner, and into the possession of the offender (Abadi, 2008, p. 92).

6. Conclusion

This article has provided a brief look at the problem of cyberspace identity theft in Iranian Law as “the crime of the new millennium” (Markus & Steven, 2006). Cyberspace identity theft is not an end in itself, but a

fundamental step for the other crimes. It can destroy a person's life, good reputation, the credit agencies' business and a society's security. This paper has examined the cyberspace identity theft in relation to the traditional form of theft. It has also examined the perspectives of Iran on the concept of theft, and how that applies to cyberspace identity theft, together with the associated problems.

A problem that arises is when someone merely copies data. In this instance, the owner has not been deprived of his property since he is still the owner of the original. An act of appropriation has two elements. First, the thief deprives the lawful owner or possessor of his property. Second, the thief himself exercises the rights of an owner with regard to the property concerned. It is possible to argue that the owner has been deprived of his exclusive right to the property. The problem of applying this legislation to cyberspace identity theft offence, however, is that the mere copying of data from a computer system does not fall within the definition of theft since the owner is not getting permanently deprived of his proprietary rights. Jurisprudence has not been developed to that stage, and it is doubtful whether mere copying will constitute an act of stealing. Furthermore, if the information is not stored on some storage device, which is also removed, it will be very difficult to apply the criterion of taking and carrying away. The problem here is whether information might be regarded as property in the law of theft.

It is remarkable that the crime of theft, in its traditional sense, may no longer be suitable in the present world largely driven by technology where all the requirements of that crime may not be present. As we have seen, in most cases, personal information does not fit neatly into the traditional notion of theft. Personal information is not covered by such traditional legislation, and if it is not recognized in law, the accused person cannot be charged with the theft of information because it is not a crime. Given the growing use of Internet, and the resulting crimes, new mechanisms are needed in order to grapple effectively with the theft of information on cyberspace. However, this does not require the adoption of new cyber specific criminal law. Instead, the problem can be addressed by modifying the existing laws, that they can cover the theft of intangible items, such as personal information and data, through copying. Alternatively, the phrase, 'depriving the owner of his property', could be interpreted flexibly as to mean that since copying has devalued the information, it amounts to depriving the owner permanently of it because its value is no longer the same. Of course, this also means that the concept of 'property' should be revised in order accommodate intangible items.

Therefore, it is problematic to fit these cases into the crime of traditional theft. It is a troublesome process, due to the basic differences between these two notions. The elements of crime in the real world are totally different from those of the virtual world. For instance, in the crime of traditional theft, the subject of crime is a physical or tangible object, whereas computer data are not tangible. Furthermore, in information and data robbery, the information would only be copied, and still remain with their owner. These differences make it problematic to apply real world theft laws to cyberspace identity theft. However, the more precise evaluation of the subject requires studying traditional theft, and analyzing the different forms of this crime in their computerized forms.

In the above connection, it is worth reiterating that the theft of credit, and, therefore, personal rights, is a recognized principle under Iranian law. Since credit is incorporeal property, this amounts to apparent judicial endorsement of the fact that incorporeal things can be stolen. Although the Iranian courts are yet to say so explicitly, with time, this principle is likely to become ingrained in Iranian law.

The category of things capable of being stolen should be extended to include both personal rights, and immaterial property rights. In particular, the theft of data, information, or protected ideas, deserves to be recognized in law, in the same way that the theft of credit, or money has been recognized in Iranian law. This should, however, only be extended to a limited class of information.

But if the theft of data, information, or protected ideas is to be recognized in law, then they should be reported, investigated and prosecuted frequently so that they can help in generating the needed jurisprudence. One difficulty, here, however, is that an accused person is likely to challenge being charged with the theft of information on the basis that it is not a crime. Moreover, since the sanctions could be severe, courts may not be willing to expand the scope of the notion of theft. In addition, due process forbids a person from being charged and punished for an act that was not a crime at the time it was committed. The courts may refrain from extending the definition of theft to informal because of this fundamental principle.

Acknowledgments

This article is written as an output for the research of FRGS/1/2014/SSI10/UKM/02/6.

References

Abadi, A. K. (2008). *Computer Crime* (p. 101). PhD thesis, University of Tehran.

Alipor, H. (2010). *Information Technology Law* (p. 255). Khorsandi Publication, Tehran.

Garner, R. (2000). An overview of computer-related crime. *Telemasp Bulletin, 7*(1), 1. Retrieved January 6, 2015, from http://www.lemitonline.org/publications/telemasp/Pdf/volume%207/vol7no1.pdf

Goldoziyan, I. (2007). *Specific Criminal Law* (2nd ed., p. 99). Tehran Publication, Tehran.

Hojati, S. M. (2012). *Islamic Penal Code* (2nd ed., p. 392). Beheyne Publication, Tehran.

Langeroudi, M. J. (2007). *Terminology of Law* (p. 286). Ganj Danesh Publication, Tehran.

Manap, N. A., & Taji, H. (2012). Cybercrimes: Lessons from the legal position of Malaysia and Iran. *IJIEE, 2*(3), 404-408.

Marjie, T B. (2007). C*omputer forensics and cybercrime* (2nd ed., p. 119).

Markus, J., & Steven, M. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (p. 1).

Martin, T. B. (2009). *Identity Theft Handbook* (1st ed., p. 3).

Moradi, J. (2007). Crime in Cyber Space. *Informatics* (p. 9).

Sadeghi, H. M. M. (1980). *Crimes against Properties and Possession* (p. 283). Mizan Publication, Tehran.

Sadeghi, H. M. M. (2011). Viewpoint on Computer Crime. *Andishe* (p. 4). Retrieved February 8, 2015, from http:// www.majlis.ir

Shirzad, K. (2012). *Computer Crimes Viewpoints Iranian Criminal Law and International Law* (p. 120). Beheyne Publication, Tehran.

Zade, M. J. H. (2008). *Theft Crime in Iran* (p. 102). Dadgostar Publication, Tehran.