International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp. 1354-1365

The Guarantee for Criminal Execution of Illegal Obtaining of Cybercrimes Evidence in Iranian Law

[1] Javand Entesarian, *Master of Laws**
[2] Farzad Tanhaee, *PhD student in law, University of Tehran*
j.entesarian@yahoo.com, farzad.tanhaee@ut.ac.ir

Abstract

Collecting reasons for crime assignment or type in fair justice system requires complying with legal rules. This issue is of paramount importance in crimes committed on the ground of or against cyber given the unknown cyber space and the different nature of reasons of message data type and computer systems. To detect the illegal cybercrime, the data or computer system of each individual shall not be inspected and seized in contrary to the fundamental human rights on the pretext of being accused. Therefore, using library research, this applied study was conducted to investigate to which consideration is exposed a reason if it indicates the crime occurrence, but is against the fundamental rights of individuals and acquired rules. Can a punishment be determined based on it or cannot? Basically, considering the fundamental rights of individuals, which requirements should be complied with in cyber reason acquisition? It seems that no absolute response can be provided for continuing validity or continuing invalidity and measures should be taken based on the conditions.

Keywords*: Collecting reasons ,cybercrime ,regulation ,invalidReferences*

1) Introduction

In the criminal law system, the evidence for the detection of committing and assigning the crime should follow the legal standards and criteria. The indices like the presumption of innocence, respect to the privacy of people, the necessity to obtain orders from the judiciary, and preservation of respect to the people's communication control by executors of criminal justice are for the regulation of basis for obtaining the ruling evidence. To investigate the subject of the paper and name it, it has to be stated that the purpose of obtaining the evidence is gathering and obtaining the evidence. The evidence that using it, you can accuse someone and condemn him. Obtaining means the gathering and receiving and the reason is a tool to prove something about the claims. The crime is also a forbidden exception, acting or quitting an act that has punishment and might be committed in cyberspace or against cyber. In choosing the cyber world, this point is evident that the words information technology, internet, and cyberspace exist, but they have not sufficient overlapping and are not comprehensive because information technology includes telecommunication besides the internet. In addition, the internet is not comprehensive and at least does not include the intranet. Cyberspace is against the real space, while sometimes the thing that is shown on the internet is true, therefore, the cyber is the most complete term, because it is assigned to

the complex of a connected computer network including the internet, intranet, local, and global networks[1].

Cyberspace makes sense against reality, while the thing that happens in this context, although is not sensible, usually is true and is not material type. The electronics do not have any differences with other electric and electromagnetic devices and include all the devices that work with electricity. On the other hand, the digital includes only the binary numbers and since the internet expresses the network world and does not include the inter-network and meta-network (local and urban networks) and the computer system means a complex of interrelated hardware, it seems that the comprehensive term for this space is the "cyber". Because according to the pre-mentioned terms, essentially, the cyber means the complex of networks that the people are connected via computers[2]. A complex of related networks are called the "cyber"[3] and its area is larger than the internet and also includes the intranet[4].

Generally, if in the cyber area, evidence that is obtained against the law and has resulted in the detection and assigning of the crime, how we should confront the crime? Can we make verdicts according to the reason that has been obtained illegally and has resulted in the crime proofing? The reactions are different from the validity of the evidence that is obtained illegitimately.

2) The validity of various reasons and the importance of the method to obtain evidence

The evidence is defined as a tool used to prove something in the claims and a more comprehensive definition; it is a clear term that is used in judicial references to detect the truth of the claimed issue.

There should exist a rational relationship between the evidence and the claim. Therefore, if the evidence is especially for the claim, it cannot prove completely the claim. If the evidence is included in the claim and the thing that arises from the evidence is a general term, it cannot prove the special condition of the claim. If the evidence is completely strange to the claim, it does not have the necessary overlap for proving the claim (the thesis for investigating the illegally or juridically impermissibly obtained issue, Mohammad Taghi Mehrizi, Marzieh Ghobadi, Summer 2017, Islamic Azad University, Shahrood branch).

2/1) The indicative and declarative evidence

The evidence is classified into two indicative and declarative evidence. The declarative evidence is the external and objective issues that by them we can comprehend the crime committed and assigning to the accused person and are the objectives. They are like the time and place of the victim burial that are external and objective issues that according to them, we can identify the murderer. But the indicative evidence is informing the people named as confession, testimony, and swearing and are not external or tangible issues. Therefore, according to the indicative issues, the properties, conditions, and external moods cannot be considered as valid or invalid terms. However, the judiciary information can be considered as valid or invalid from these properties (illegal obtaining the evidence –

[1] Aalipour, Hasan, Information technology criminal law, Khorsandi publications, 3rd Ed.
[2] Retrieved from the www.criminology.unimelb.edu.v, accessed at 3/11/2017.
[3] Retrieved from the www.sos.state.co.us, accessed at 3/11/2017.
[4] The encyclopedia of Microsoft computer, the staff of authors and reviewers of Microsoft publications, the center for translational science publishing, Farhad GhanbarZaadeh, 1st Ed., 2002.

Abolfazl Heshmati – inquiries in jurisprudence and law – Year one – Number 2 – Fall 2014).

2/2) The system of freedom of reason and the legal evidence system

Presenting the reasons for a criminal hearing can be presented by two different systems. These two systems are the system of freedom of reason and the legal evidence system. In the system of freedom of reasons the search for the reason can be performed by any means, the reasons do not have hierarchy and the judge is not dependent on the presented reasons. But, in the legal evidence system, the parties of the dispute are only allowed to present the evidence that is specified by law. In addition, the evidence has a hierarchy in such a way that some of the evidence have supremacy and validity over the other and the judge is dependent to the contents of the evidence and cannot ignore them (Akhoundi – Mahmoud - Code of Criminal Procedure – 2009 – Publication and press organization – Vol. 5 – P. 29). The thing that the legislator in Iran has followed which of the systems should be investigated. In the Islamic penal code approved in 2013, in articles number 161 and 162, it has been stated that (in the cases that the criminal case is proved by religious evidence like confession and testimony that matters, the judge votes based on them unless he knows it), it seems that the subject law will follow the legal evidence system in some crimes like the punishment and retribution and in other crimes to follow the system of freedom of reason. In the crimes with the punishment penalty, the proof evidence matter and in the exchange of meeting the stipulated evidence the crime would be proved and in other crimes, the evidence have principles and each reason can be one of the ways of this knowledge for the judge (the ruling principles on the determination of reasons in criminal issues in legislative changes route – Kiomarth Kalatari – Ebrahim Rahnama Zadeh). Therefore, according to the opposite concept to the above article (the principle of obtaining the freedom of reason) exist in other criminal disputes of the related subject laws and the crimes that the evidence is dominant, this principle governs.

The principle of free evaluation of the reason is separable with the abovementioned principle. According to this principle, the magistrate can freely evaluate the value of the instrumental evidence and is free in its rejection or acceptance. Therefore, each reason that is presented, the judge should check its validity and should deal with them according to it (the knowledge of the judge). Therefore, if there are tens of reasons and statistics against the verdict of the judge, the judge can still behave according to his knowledge. In this regard, the article number 212 of Islamic Penal Code approved in 2013 states that (if the knowledge of the judge has a conflict with other legal evidence, if the knowledge remains enlighted, that evidence is not acceptable for the judge and the judge can present the verdict by stating his knowledge reasons and for rejecting the other evidence). Of course, the knowledge of the judge is not unknown, but it is a conventional and normal knowledge that its definition in the article number 211 has stated that (the knowledge of the judge is the certainty obtained from the evident documentation in an issue that is discussed in front of him. In the cases that the evidence for the verdict is the knowledge of the judge, he is obligated to mention explicitly his evidence and documentaries of his knowledge. The items like an expert opinion, examination of the place, local researchers, remarks of the informed, the reports of the executive officer, and other evidence that are typically scientific can be considered as the documents of the judge knowledge. Anyway, the solitary of the inferential

science that typically does not result in the certainty of the judge cannot be the criterion for the verdict).

In previous pages, it has been stated that in the system of freedom of reason, the search for the reason is possible by any means and the evidence has no hierarchy. But in the article number 213 of Islamic penal code approved in 2013, it has been stated with the name of knowledge of the judge (in the conflict of other reasons with each other, the confession to the religious testimony precedes the oath and swearing. In addition, the religious testimony has precedence over the oath and swearing). The legislator has stated the final approach for ending the dispute and has considered the knowledge of the judge (the certainty obtained from the documents between the rules and requirements), the confession, testimony, and making oaths and swearing as the most valid issues, respectively.

Therefore, the reasons that have no issues in this subject can be investigated using the principle of the reason is not free and the principle of freedom of reason as the (knowledge of the judge) and in case of existence of evident evidence, the verdict can be presented that the reasons are not valid.

Article number 187 of Islamic penal code and article umber 171 Islamic penal code state that: in religious testimony, there should be no awareness on the items of the testimony. Whenever the evidence conflicts with the provision of the religious testimony, the court performs the necessary investigations and if it concludes that the testimony is unreal, the testimony is not valid. If the accused confesses committing the crime, his confession is valid and there is no need for other evidence, unless, with the investigation of the judge, the evidence is contrary to the confession items that in this case, the court will perform the necessary investigations and state the evidence contrary to the confession in the verdict.

Tow principles of free evaluation of the reason and freedom of obtaining the reason are separable from the principle of legitimacy of obtaining based on the principle of legality of the reason that is also based on the respect to the dignity of the human and preservation of the credit and dignity of the judicial party. The detection of the truth needs that on one hand, the valid and legitimate evidence to be identified and presented by the legislator so the parties refuse to present the reasons without judicial value and on the other hand, the correct methods and legitimate ways for obtaining the evidence to be expressed so using illegal and indecent methods to obtain the evidence would be avoided. For this reason, article number 38 of the Iran constitution states that any kind of torture to obtain confession or information is forbidden. Forcing someone to testify, confessor swearing is not allowed and this kind of testify, confessor swearing is not valid. The violator of this article will be punished according to law. Therefore, according to the mentioned article, is the confession is recognized as the evidence that matters if it is obtained by illegal methods like torturing, is not valid and even does not have statistical validity. The legislator has not predicted explicitly the problem of legitimacy of obtaining the evidence in the Islamic penal code approved in 2013. But, the prevention from using any kind of deceit, deception, and illegal actions to obtain the evidence could be inferred from the context of the law that would be investigated (Kalantari, the same).

3) The evidence of cybercrimes and their formats

The data as the stem cell of cyberspace is being processed, stored, and transferred in computer systems. The data is any kind of processable information in the computer system (proceedings of the conference on investigating the legal aspects of information technology,

deputy of justice and judicial development of the judiciary, 2004, p. 167). In cyberspace, the evidence is these data messages that have hidden identities like the DNA and are not tangible, identifiable, or inherent properties. For example, the existing data in the memory card is not visible without using special tools.

The meaning of cybercrimes is the guidance that signifies the commitment of cybercrimes. Now, the stated crime may be committed against computer systems or data like data destruction or the crime might be committed in cyberspace – not against the data – and the cyber bases might be abused to commit the crime like the internet fraud to obtain the property, here the objective is both of them.

The nature of the cybercrimes that is the data in hidden and we have to convert it to comprehensible concepts using special tools. For example, the designed map could be displayed only using Photoshop or AutoCAD software. Therefore, the evidence of cybercrimes that are gathered and presented to the court to prove the commitment and assignment of the crime is the same as this cyberspace in nature and its essence is different from the objective evidence in the outside world and is formed in the data. The data message is formed in various formats as the cybercrimes reasons.

The data can appear in the format of the picture and used as evidence. This picture can be taken using a digital camera from a page or an old paper picture that can be scanned using the scanner device and displayed in digital format. Consequent display of the pictures in the movie format in of this kind. Data comprehension in the format of voice is another expression of the emergence of the data. The text and displaying the data in the format of texts as a continuous type is another common format of displaying the data. In addition, combining the data as a consecutive display of the pictures using the special and natural effects, soundtracks, and the subtitle is the format of combining the data.

In crime detection, the data format is not so important, but the thing that matters is the investigation of the validity, originality, and true assignment. This principle is not deniable that the cyber evidence in the abovementioned format has legal and proof values besides the traditional evidence. Perhaps this evidence can lead us exactly to crime and guilty person detection because they have the recovery and identification capability (the thesis on obtaining and documentation of digital evidence in cyberspace – Ja'far Koosha – Under the advisory of Jalil Maleki – The student: Shahpour Dolat Shahi – Summer 2009 – Islamic Azad University Central Tehran Branch – Law).

4) The legal requirements to obtain the cybercrimes evidence

The necessity to meet the formal substantive regulations in the detection and proving the cybercrimes in one hand, and the ease of committing the crime due to its hidden nature and extension of the cyberspace, on the other hand, respect to the privacy of people and not violating it, preserving the human dignity and not offending the human being due to the cyberspace being free, totally lead us to make special rules in this context. The articles number 664 and 687 of code of criminal procedure approved in 2013 studies this issue and have stated that if there has been no specific ruling predicted about the procedure of computer crimes, it would follow the general rules.

Before the realization of the guarantee for the execution of the requirements for obtaining the evidence of cybercrimes, at first, these requirements should be investigated. In other terms, the methods and ways of legislative obtaining the evidence would be expressed so the opposite concept and the guarantee for its execution would be recognized. According

to article number 36 of the constitution, the verdict for punishment and executing it should only be performed through the competent court and according to the law. The term "according to the law" in the fundamental document of the rights of the nation means the invalidity of any illegal activity from prosecution to execution.

If the preservation of the stored data is necessary for the preliminary investigations and trial, the criminal authority can command to protect it. However, the judicial authority should be informed a maximum of 24 hours after that and act according to his command. It should be noted that data preservation is different from data confiscation and data inquiry.

The legislator has defined the imprisonment and fines as the combination of the substantial and formal discussions of the guarantee for the disclosure of the protected data in stating these items and in case of failure to comply with the command, it has included the guarantee of refusal to execute a judicial order.

Data preservation means the prevention of any kind of changes, destruction, disclosure, and protecting it for exploitation. The validity period for the judicial authority order for protecting the data is about one month and in case of expiry of the deadline, the order would be forcibly destroyed and after that, the guarantee for its execution will not be applied unless extended by the judicial authority.

The inquiry and confiscation of the cyber and telecommunication systems are performed only by the order of the judicial authority and are never performed by the executive officer, contrary to the protection of the data that the executive officer has a temporary qualification.

The conceptual differentiation of the inquiry and confiscation of the cyber and telecommunication systems can be investigated. The executive officers cannot act to protect the data more than 24 hours without taking orders or intractably and without taking orders to act to hold up or inquire about the cyber and telecommunication systems.

Like committing the crime in real-world that each action performed by the executive officer is done with the judicial authority order, the judicial authority should perform the order for confiscation, inquiry, and protection of the data in cyberspace and the executive officers cannot act intractably.

The data inquiry includes access to the software and hardware of the systems and data and a substantial review of it for detecting the crime. The data confiscation means making them inaccessible or sealing them and the systems at the location of their establishment or preservation, so after the confiscation, we could act to the inquiry, review or search among them.

The data and systems confiscation and inquiry are performed with the order of the judicial authority and in the cases that result in the crime detection, accused identification or obtaining the evidence for happening or assignment of the strong suspicion. This suspicion will be obtained with the report of the executor officers, authentic reports or informing the judicial authority. The act to perform the confiscation or the inquiry is performed originally at the presence of a legal entity or the operator of the system unless it is urgent or it is obligated with the discretion of the judicial authority to be performed in the absence of them. The judicial authority should order in written the location of execution, the area of the inquiry and confiscation, the type of the amount of the data and systems, and the time of performing the inquiry and confiscation in the order.

Because the data and systems confiscation and inquiry take the authority from the possessor or the operator, commanding this kind of order should be prevented as possible and the principle is not to confiscate the data. But, with the aim of detecting the crime and the

evidence of the crime, the legislator will permit the data and systems confiscation only if one of the quintet conditions are met and the judicial authority is responsible for reviewing the validity of these items. (In the following conditions the computer or telecommunication systems can be confiscated: if the stored data are not easily accessible or are huge, the inquiry or analysis of the data is not possible without hardware system, the legal possessor of the system is consent, the imaging from the data is technically impossible, and the in-place inquiry of the data will damage them).

The executor officers in reviewing the data should only act in detecting the crime in the limits of the issued order and should not perform the inquiry or confiscate the other data or the systems intractably unless they have ordered. In addition, if they encounter another crime besides the ordered mission while inquiring about the crime, they cannot act intractably to inquire or confiscate that data and can only protect the data for 24 hours.

For example, in order to investigate the crime of threatening to publish private photos, after an inquiry of the system and while confiscating the data for the accused person that denies the existence of the complainant photos in his computer, if the executive officers understand the existence of the data including obscene photos, they cannot inquire them and originally, they should not investigate these data, because the limits of the inquiry are defined and they should not go beyond.

To protect the ownership of the people, keeping the privacy and not disturbing the people affairs the legislator has forbidden completely the data and systems confiscation and inquiry that result in the damage and severe financial damage or disturbance in public services and case of existence of any of the three abovementioned items, the judicial authority should not command for inquiry unless an important issue like the country security has a necessity. It is obvious that the above exceptions are only about the inquiry and do not govern the inquiry.

In case of inquiry of the originality of the data, the beneficiary can have a copy of the data unless the presentation of the data is considered as the provision of the discovery of the truth or damages the research process. The victim including the possessor or someone else can send his objection about data inquiry by the executor officers after 10 days of inquiry to the commander. The rejection of the objection can be objected to higher authorities. However, the legislator has not specified the reference, deadline, and the type of arrangement.

In the data are not in the hands of the accused, but access to it is somehow possible by dispute parties or the third party that would not damage the validity and authenticity of the data, the fixed citation is preserved. For example, if the accused person acts to threaten the complainant in WhatsApp social network, and after threatening deletes the criminal expressions in such a way that it is not visible in the computer system of the accused, but can be observed in the computer system of the complainant in such a way that its validity and authenticity can be confirmed, the citation ability is possible even they are not in the possession of the accused. The reason for that is that its originality can be cited in the cellphone of the complainant and WhatsApp social network. About the cybercrimes, originally, the accused will be condemned in a place that the material element of the crime has happened in that area. However, if the crime scene is not specified, the court can peruse to detect the crime scene (articles number 665 and 310 of the code of criminal procedure). Now, if the committed acts to destroy the data that are uploaded in different areas from his residence and one of these areas arrests him, in this condition, although the degree of the

punishment is the same for all the crimes, the location of the arrestment is not righteous. Because the crime has been committed only in the residential area of the committed and that area is still righteous and in case of detecting it in another place, the file of incompetence will be sent to the righteous court of the residence of the accused person that is the same as the crime scene.

According to the observed items, the necessity for the existence of the judicial order and the limits of the order in issuance and execution to be definite, the existence of special conditions about inquiry and confiscation of the data and systems, the right for objection and taking a copy for the victim and the beneficiary, and the existence of conditions for controlling the transferring or stored communication content is of legal requirements.

5) The guarantee for illegitimate obtaining the evidence for cybercrimes in the constitution and substantive rules

According to the discussions, the substantive rules follow the system of freedom of reason in the crimes except for the crimes like the punishment and retribution that follow the legal evidence system. In this system, the search for a reason is possible by any means and the judge is not dependent on the presented evidence. Besides, besides the system of freedom of reason, the principle of legitimacy of obtaining the reason was introduced that specifies the tools and methods for obtaining the reasons being legitimate and legal and hereby the system of freedom of reason was confined. Therefore, the executor officer cannot resort to any kind of illegal or illegitimate tool with the excuse of detecting the truth and cannot detect the crime, criminal or evidence for committing the crime or assignment of the crime in illegitimate ways. The principle of legitimacy of obtaining the reason dominates the rule of freedom in obtaining the reason and the coded rules cannot be violated in detecting the cybercrimes. In the following, some examples are presented.

For example, the inquiry and confiscation of computer systems are only in the cases that there is a powerful suspicion on the commitment of the crime. Therefore, the executor officers cannot act on inquiry or confiscation of the data or the systems without the presence of this suspicion or act without the presence of judicial authority order. Because according to the article number 22 of the constitution, the intrusion to the property and privacy of the people is possible only in the legal permissions and doing these acts without obtaining the legal permission from the judicial orders is against the constitution and is not valid.

In another example, as was discussed, the computer systems will be confiscated only by meeting the quintet conditions and if the data inquiry is possible without confiscating them and the data are easily accessible or taking photos are technically possible without confiscation, or the data confiscation results in the injury of severe financial damage or disruption in public services, but the data confiscation has been ordered, according to the article number nine of the constitution, no authority has right to take the legitimate freedoms even in the name of independency or preservation of territorial integrity. Rather act in the name of crime detection. Even in the case of detecting the crime, the obtained reasons are not valid. For example, when the system IP of the criminal can be identified without confiscation of the computer system and by an inquiry from the service provider company, the computer or cellphone of the criminal cannot be confiscated for any reason so the evidence would be detected. In another example, if a person claims that the accused is threatening using the telecommunication system or by sending emails, but he would not present the content data to prove the crime and claims that after sending each content by

the accused, the data are deleted and asks for controlling the computer and telecommunication relation (Email), and after that the command to control the communication is issued and it becomes evident that the accused has acted on threatening, the obtained reasons are not valid. Because according to article number 25 of the constitution, inspection and not delivering the letters, disclosure of the telecommunications, recording the conversations, and eavesdropping is forbidden unless with the rule of law. Therefore, generally, no transferring data content (sending Email) or saved data should not be controlled. The rulings for saved data content mean the control, the transferring data content and these contents will only happen for the crimes included in the authorized items. Because the article number 150 of criminal procedure code states that controlling the telecommunication of people is forbidden unless in cases that are related to the internal or external security of the country or this rule is recognized to be necessary for the crimes in the subject of items (a), (b), (c), and (d) of article number 302. In this case, this would be performed with the agreement of the chief of the justice department of the province and by determining the period and numbers of the controls. Also, the article number 683 has stated that the control of the transferring content of the non-public communications in computer or telecommunication systems is according to the laws related to the telecommunication control established in the code of criminal procedure. The access to the stored non-public communications contents like the Email or SMS is considered as controlling and should meet the related rules.

The non-public communications are the privacy and public inaccessibility to its contents and the evidence that is obtained contrary to the issued permit by the authority is not valid according to article number 22 of the constitution and should only perform in that range.

The inquiry and confiscation should be performed only in the area of crime detection. If the computer system of the accused is inquired and confiscated to investigate the publication and the photos of the complainant and some criminal data in the format of movies or obscene photos, or the text data related to the place of storage of the psychedelic tablets, the executor officers do not have the right to expand the search domain. Because according to the article number eight approved in 2004, the respect to the legitimate freedoms and protecting the civil rights should be performed and intrusion to the documents and objects that are not relevant to the intended crime is forbidden. Therefore, the reason that is obtained in this manner is not valid.

But, what is the guarantee for the execution of failure to comply with legal requirements of detection of the cybercrimes? Does this evidence have no credit at all or are always valid or should be behaved relatively? Generally, in confronting the evidence obtained illegitimately, four different assumptions are discussed:

5/1) Continuous validity: according to this assumption, if there is a reason provided presenting the commitment of the cybercrime because it states the commitment of the cybercrime, it should have continual validity and the method for obtaining the evidence should not be considered. In fact, according to it, considering the principle of crime anomalies and hurting the community body by committing it, the method of crime detection and crime ascertainment is not important and if the reason is provided anyhow, the committed should be punished and even the evidence is obtained illegally it is valid forever.

5/2) Continuous invalidity: according to this assumption, if a reason for the commitment or the assignment of the crime is obtained, the detection method of the cybercrime should be matched with the law. If the evidence obtaining method is legal, that evidence is valid and

the prosecution can be started and the issuing of the punishment verdict can be done according to it. According to this, the reason that does not have the necessary conditions and is not obtained legally has no guarantee to perform the prosecution. For example, if the computer system is confiscated for items other than the specified issues or the transferring non-public communications content is accessed and listened other than the specified items like checking the Emails of the accused person for the crime of threatening, because it is obtained without the permission of law and according to the criminal procedure code approved in 2013 is not valid and is always invalid.

5/3) the validity or invalidity of the reason according to the type of the reason: according to this hypothesis and according to the thing that was discussed about the classification of the evidence to the indicative and declarative, the type of evidence that shows the happening and assignment of the crime, is effective in its validity or invalidity. In other words, if the evidence is obtained illegally and shows the commitment of the crime, it can be valid or invalid dependent on being indicative or declarative. Therefore, depending on that the evidence is obtained by external and objective affairs (declarative), or informs about the happening that this information is in terms of confession, testimony, and swearing, the type of the guarantee would be different.

Therefore, by patterning the conditions of invalid – invalidating of the contract and the conditions of invalid – non-invalidating of the contract, if the reason for illegally obtaining the evidence matters, the provided reason is invalid and the prosecution cannot be started according to it (confession under torture). But if the evidence that is illegally obtained has the doctrine aspect, if it has sufficient validity but does not deny the prosecution start and does not have any effects on the principle of crime happening and the necessity to punish the criminal (the confiscation of the computer system without obtaining the judicial order by the executor officer). Like the conditions of invalid – invalidating of the contract that has no effects on the essence of the contract, it does not have any effects on the essence of punishment. Therefore, the type of evidence should be investigated and if the evidence has the aspect of the method, and is illegally obligated, it should be punished and the prosecution should start. But if the evidence has the subjectivism aspect, the evidence does not have the necessary validity to start the prosecution and issuing the verdict.

5/4) Conditional validity: According to this hypothesis, the evidence that is obtained illegally, is not always valid and is not always invalid and the type of evidence does not affect its validity. But the important thing is that the obtained reason should have general conditions. Therefore, the obtained evidence has the necessary validity to start the prosecution. If any evidence that states the crime commitment has the principal and verdict conditions, then the prosecution can be started and if it does not have the fundamental and general conditions, it is invalid and its validity is only dependent on having the fundamental conditions and for this reason, it is called the conditional validity.

In subjective law, the legislator has stated two reasons as the fundamental conditions of this issue in the article number 36 of the code of criminal procedure. (The report of the executor officers is valid if they are not against the certain conditions of the issue and are regulated according to the legal rules and regulations). The first condition is that the obtained evidence is not against the conditions and the second condition is that it is adjusted according to the legal rules and regulations. The term condition shows simultaneously the mentioned conditions and is considered as the fundamental condition in obtaining the crime evidence and if it does not have these conditions the prosecution could not be started. In the

example, if the executor officer as the keeper and the preserver of the evidence, in a hypothesis that has strong suspicion to the crime committed and can preserve the data for 24 hours in the format of data preservation, he can keep the data for more than 24 hours and can inspect the computer or telecommunication system like the cellphone of the accused without the permission from the judicial authority so by investigating the Instagram page of the accused he could check the assignment of the drug dealing and the ownership of the Instagram page. If the executor officer understands that this crime has been committed, but because he has no permits from the judicial authority because according to article number 36 of the code of criminal procedure approved in 2013, the above report is not provided according to legal criteria, this reason is invalid for condemnation of the accused person. And it should be acted on some other reasons for punishing the criminal in case of committing the crime because this reason does not have the fundamental condition for observing the legal regulations.

The legislator has stated in the article number 67 of the abovementioned law that (the reports and letters that the identity of their reporter or writers is unknown, cannot be considered as the basis for the prosecution, unless if it indicates an important issue that results in the disruption in the public security and order or includes some evidence that suffices for prosecution start). The awareness of the judicial authority from the reports and letters of the evidence for the crime committed should be specified by the identity; in case, that the identity is unknown it cannot be considered as the basis for prosecution started. However, it has two exceptions ad those are when it implies an important issue that results in the disruption in the security or the obtained information from the unknown identity is accompanied by some readings that in these cases the prosecution can start.

Therefore, the subjective law by accepting the fourth hypothesis considers the evidence as valid if the obtained evidence has fundamental conditions of accommodation with the conditions and preparation according to the rulings and otherwise, considers it as invalid and the magistrate of the court can proceed to issue the prosecution according to the articles number 340 and 4 of the code of criminal procedure.

Conclusion

The data appear as the evidence for cybercrimes in the format of the text, photo, voice, film, or the combination of them. Preservation, confiscation, and inquiry of the data to detect cyber crimes have special requirements. The definite principle of the constitution as the most fundamental document of the nation has considered the verdict to the punishment only according to the law. It is obvious that this requirement applies from the start of the prosecution until the end of the implementation of the verdict. If the evidence in cybercrimes is obtained without meeting the requirements stated in the subjective rulings about the validity of the evidence, the legal system will face it with relative attitude depending on the general conditions defined in the rules.

References

1- Tadayyon Abbas 2001, A Comparative Study of the Principle of Legitimacy Education in the Criminal Procedure of Iran and France, the Ph.D. Thesis for Criminal Law and Criminology, Shahid Beheshti University.
2- Ja'fari Abbas 2006, An investigation on the privacy right, Monthly Journal of Law Excellence, Year 1, Number 2.

3- Goldozian, Iraj, Bita. The quality of obtaining the evidence in French criminal law, Hagh Quarterly, issue number five.
4- SadrZaadeh Afshar, Seyyed Mohsen, 1997, The evidence for proving the dispute in Iranian law, Tehran, University publication press.
5- The comparative study of obtaining the reasons by recording the voice and picture, Abbas Tadayyon, 2008, Jurisprudence and law, Year 4, Number 16.
6- Illegal obtaining the evidence – Abolfazl Heshmati – inquiries in jurisprudence and law, 2014, Year one, Number 2.
7- Karimi, Dr. Abbas, The evidence for proving the dispute, 2007, 1st Ed., Tehran, Mizan publications.
8- Jabbari Ghareh Bagh, Saber, the thesis on the effect of obtaining the reasons illegally on the essence of the true reason in the light of Islamic jurisprudence, international documents, and Iranian criminal law, under supervision of Mansour Rahmdel, Islamic Azad University Central Tehran Branch, Spring 2013.
9- Dolatshahi, Shahpour, The thesis on obtaining and documentation of the digital evidence in cyberspace, under supervision of Ja'far Koosha, Islamic Azad University Central Tehran Branch, Summer 2009.
10- Mehrizi, Mohammad Taghi, An investigation on the validity of the illegitimately and illegally obtained evidence in terms of jurisprudence, under supervision of Marzieh Ghobadi, Islamic Azad University, Shahrood branch
11- Kalantari, Kiomarth, Rahnama Zaadeh, Ebrahim, the governing principle for obtaining the evidence in criminal issues in the course of legislative developments, International congress on Iranian law, 2015.
12- Hosseini Nezhad, Hossein-Ali, 1995, The evidence for proving the dispute, Mizan, 1st Ed.
13- An investigation on obtaining the evidence in code of criminal procedure 2013, Yari Hosna, Kazemi Ghobad, National conference of novel projects, Iran and management world, Economy, accounting, and humanities, 2017.
14- Yavari, Asadollah, The right to have the fair trial and new rules of procedure, The Islamic law publications, Year 2, Number 2, 2004.