Eavesdropping in the Iranian Criminal Justice System

Mansour Rahmdel[1,*]

[1]Faculty of Law, Tehran Azad University, Central Branch, Tehran. Iran

*Correspondence: [1]Faculty of Law, Tehran Azad University, Central Branch, Flat 502, Number 13, 17 west, Nord Sarraf ha, Saadat Abad, Tehran. Iran. E-mail: m_rahmdel@yahoo.com

Received: May 11, 2018 Accepted: June 6, 2018 Online Published: July 25, 2018

doi:10.5430/sass.v5n2p60 URL: https://doi.org/10.5430/sass.v5n2p60

Abstract

That the individual shall have full protection in person is a principle as old as the human beings life, but it has been found necessary from time to time to define anew the exact nature and extent of such protection. As civilization advanced, an individual's feelings and intellect, as well as his physical being, came within the scope of the legal "right to be let alone."

Iranian Constitution has guaranteed individual's rights and freedom and has explicitly referred to forbiddance of eavesdropping and interception of conversations in its article 25. Article 582 of Penal Code ratified in 1996 has criminalized eavesdropping by the governmental officials. Article 104 of Criminal Procedure Code, which was abolished in 2014, referred to eavesdropping under the judge's order. Article 150 of new criminal procedure code ratified in 2014, and came into force in October 2014, has provided adequate safeguards to protect the individual's rights.

Keywords: eavesdropping, Constitution, Iran, criminal justice

1. Introduction

Privacy as a general concept and privacy of conversations as one of its ingredients has been considered and acknowledged by international and regional conventions, like international covenant on civil and political rights, global declaration of human rights, European convention of human rights and Islamic convention of human rights. "An urgent problem of our time is the harmonization of man's mastery over nature with freedom and human dignity" (Donnelly, 1963, p. 667) and "Permitting the police and other public authorities to conduct electronic eavesdropping and wiretapping operations in people's homes for the purpose of effective criminal prosecution is always a highly controversial issue within liberal democracies that respect the rule of law and individual privacy." (Nohlen, 2005, p. 680)

"It is regarded one of the fundamental human rights and is protected by Constitution" (Qazi Sha riat Panahi, 2012, p. 146) and because of importance of these fundamental rights, "one of the most important functions of the Constitution is restriction of the government to protect them." (Motameni Tabatabaei, 2011, p. 209) On the other hand, "considering developed technical and electronic instruments, the governments can so easily invade the right to privacy, including telephone conversations." (Hashemi, 2011, p. 332) These devices enable law enforcement officials and private citizens to monitor and record private conversations. Therefore, usually in criminal procedure codes, some guarantees are being provided to protect the privacy and "considering the importance of privacy of conversations, Iranian criminal procedure code has essentially prohibited eavesdropping." (Kooshki, 2007, p. 140)

Putting aside the necessity of protection of privacy of conversations, there is no doubt that eavesdropping is used as a method of detection of crimes and identifying the suspected people.

In every case which is posed at the prosecution office, we cannot expect that there should always be some witnesses which, are attending at the prosecution office or court and testify or the accused confesses or there are some other evidences which prove the case. In some cases, the only way to get and gather information and evidence is eavesdropping. Naturally, the accused manage to flee and go out of the reach of the judiciary system. Suppose that there are some information about the suspect and the nature of the crime is so, that is usually committed

clandestinely or the crime has been committed, but the offender manages to flee or conceal the evidences or other related things. What should the police or the judge do? Can they stop the prosecution?

The answer is clear. They cannot stop it. The reason is very simple. If they stop the prosecution in such cases, there will not be any hope to detect some crimes, or identify the offenders. The problem is that, on the one hand, stopping the prosecution deteriorates the order and safety of the society and on the other hand, resorting to any way or any instrument to detect the crimes or identifying the suspects or acquiring the information or evidences may invade the individual's rights. So, there should be a balance between them.

To strike a balance between competing interests, the elements on both sides should be measurable and capable of being weighed in similar terms. But, the problem is that the right to privacy and freedom does not lend itself to accurate measurement. So, if a measure in the long run restricts freedom and privacy, nobody can say whether freedom and privacy has been reduced and if yes, by how much.

Some believe that "it is not the survival of society that is at stake in balancing liberty against law and order, but it is the survival of individual's rights that is at stake in balancing. Crime is bad and dangerous, but it is not the atom bomb. The right of privacy and freedom in a democratic society has to be balanced, not with survival, but against the needs of law enforcement and the effectiveness of eavesdropping and there is no contest between liberty and safety. We have the means of enlarging both. Unless we do, we will lose both, because neither freedom nor security can long endure without the other and nothing can so weaken security as the loss of liberty." (Lapidus, 1974, p. 197) In fact, it seems that, it is not a matter of balance, but it is a matter of devotion of adequate resources to secure the public safety and in the confliction between the rights of individual and the safety of the society, the latter weighs. The reason is that the government runs the society and owns all of the powers and facilities in its possession and may be from government view point the argument is that whatever is needed for the survival of society must outweigh the rights of the individual. Even if we regard it a balance, it should be noticed that the balance between competing values of privacy and law enforcement is constantly shifting. One day the fear of crime is so great, that the public may still be willing to accept eavesdropping or at least is ambivalent about it and the other day it may protest against intrusion of privacy of conversations on the excuse of detecting crime or identifying the offender.

What a person exposes to the public, even in his own home or office, is a subject of Constitution protect and what he seeks to preserve private, even in an area accessible to the public is constitutionally protected. The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated. "One of the manifests of freedom and fundamental rights of people is to have a secure instrument of conversation and free of inquisition" (Madani, 1990, p. 121) unless the law allows its inquisition according to a reasonable cause. The question is that what is reasonable or unreasonable? How can the description meet the particularly requirement? Should the same criteria of reasonableness and particularity be applied to wiretapping as to the ordinary search and seizure of tangible objects?

"Warrantless searches and seizures are *per se* unreasonable unless made pursuant to consent or within certain narrowly drawn exceptions." (Blair & Jernigan, 1980, p. 512) It seems that eavesdropping involves a far more serious intrusion on privacy and requires greater safeguards. Something, which is essentially forbidden according to article 25 of Constitution. "The inspection of letters and the failure to deliver them, the recording and disclosure of telephone conversations, the disclosure of telegraphic and telex communications, censorship, or the willful failure to transmit them, eavesdropping, and all forms of covert investigation are forbidden, except as provided by law", article 582 of Iranian Islamic penal code ratified in 1996 which provides "If any state official and civil servant, in cases other than those permitted by law, opens or seizes or destroys or inspects or records or intercepts letter or telegraph or telephone communications of people, or discloses their contents without their owners' permission, shall be sentenced to one year to three years' imprisonment or a fine of six to eighteen million Rials." article 104 of Iranian criminal procedure code ratified in 1999 which provides "In cases where there is a need to inspect and detect mailing, telecom, audio and visual correspondences related to the accused, in connection with investigation of a crime, the judge will inform the respective officers to seizure [these materials] and send them to him or her. Once they are received, they will be presented to the accused, noted in the minutes, and attached to the file after being signed by the accused. Refusal of the accused to sign will be noted in the minutes and in case the items are not of relative importance, and if the confiscation is not necessary, they will be returned to the owner obtaining an acknowledgment of receipt.

Note – Monitoring telephone calls are prohibited, unless it is deemed appropriate by the judge because the case is related to the country's security or obtaining a right of a person." "In crimes against security of the country, it is not the security officers, but he is the judge who should order of interception." (Madani, 1999, p. 335) As, "the

Constitution has forbidden the eavesdropping, unless the law provides, so allowing the interception of telephones of the people, whether they are accused of a crime or not, is questionable." (Ashouri, 2009, p. 170) So, some believe that "although in Iranian law, essentially interception is forbidden unless the law provides otherwise, and eavesdropping is a crime, but as its sphere has not been determined in the law, it could be misused so easily" (Tadayyon, 2009, p. 153) Criminal procedure code 1999 has been abolished by criminal procedure code 2014, which will come into force October 2014. Article 150 of the new code has provided very hard conditions for monitoring telephone and other communicative instruments. According to it "monitoring communicative communications is forbidden, otherwise it relates to the internal and external security of the country or is necessary to detect the crimes mentioned in items a, b, c and d of article 302.(Note 1) In order to monitoring, the head of the judiciary of the province should agree with it and the time period and numbers of monitoring should be determined. Monitoring of the authorities and persons mentioned in article 307(Note 2) requires the agreement of the head of the justice and he cannot differ making of decision to others.

Note 1: the conditions and qualities of monitoring will be provided by High counsel of national security.

Note 2: monitoring of communicative communications of the convicts is possible only on the discretionary of the primary court which under its control the writ is performed or the special judge for performing of the writ."

Considering the above mentioned discussions, the current paper discusses eavesdropping in Iran in two sections. Section one refers to the crimes in which eavesdropping is allowed and time period for eavesdropping. Section two pays attention to eavesdropping by consent and from innocent people and incriminating out of eavesdropping.

2. Crimes, Reasonable Cause and Time Period of Eavesdropping

2.1 Crimes in Which Eavesdropping is Allowed

Article 104 of criminal procedure code has not determined exactly in which crimes the judge can give an order of eavesdropping and only refers to ambiguous phrases of security of the country or protection of the rights of the people. So, in practice:

1- Offenses for which an order may be obtained are practically unlimited, and are not restricted to those characteristic of organized crime or serious offenses.

2- It is thought that government eavesdropping is an indispensable tool in fighting some crimes. In fact the law permits eavesdropping in investigation of many offenses that are not and will not be associated with organized crime. For example:

A: Offenses relating to espionage, sabotage, treason, riots and offenses relating to atom energy.

B: Bribery of public officials and embezzlement, kidnapping and assault, Terrorism, murder.

C: Manufacture, importation, exportation, receiving, carrying, concealment, buying, selling, or dealing in narcotic drugs and psychotropic substances.

D: conspiracy to commit any offenses relating to security of the country and government.

These offenses were enumerated above, because of their seriousness or because they were characteristic of the security of the country or rights of the people.

But, in new code the legislator has adopted another policy:

1- it has explicitly enumerated the crimes. Crimes against the security of the country have been listed in Islamic Penal Code 1996 (articles 498-512) and Islamic Penal code 2014 (articles 286-288) and crimes listed in article 302 which were mentioned earlier.

2- Eavesdropping requires the agreement of the head of the judiciary in each province. So, the judge cannot independently decide to give an order of eavesdropping. According to new code eavesdropping needs issuance of an order by the judge and agreement of the head of the judiciary of the province with it.

3- with regard to high rank authorities mentioned in article 307, it needs issuance of an order by the judge and agreement of the head of the justice.

Of course, the agreement in two latter cases is only required for giving an order of interception and discontinuance of interception does not require their agreement.

An application for a judge order must show that a particular offense has been, is being or is about to be committed. In some cases prior to application of law enforcement officers may the judge himself issue a warrant of eavesdropping. It seems that two types of judge orders are available:

1- Prosecutorial, to get evidence with respect to a specific offense by the person surveilled.

2- Investigative, to link a subordinate suspected of crime with his unknown superiors and to ascertain their identity and activities.

An order may be issued only upon a showing that normal investigative procedures are inadequate. Different types of surveillance may be needed in different types of cases. For example, in domestic security investigations as distinguished from ordinary crime, the gathering of intelligence is long-range, the exact targets may be hard to identify, and the emphasis may be on prevention of unlawful activity or enhancing preparedness for some future emergency.

The judge to whom an application is presented has to determine if all requirements of the law are satisfied. Before signing the order, he must find from the facts set forth in the application that there is reasonable cause for belief that:

1- An individual is committing, has committed, or is about to commit an offense covered by law.

2- Particular communications are to be intercepted through interception.

3- The facilities from which the communications are to be intercepted are being used, or are about to be used, in connection with such offense, or are leased to, listed in the name of, or commonly used by the particular individual.

Any request of eavesdropping by law enforcement officers or issuance of an eavesdropping order by the judge himself requires a justification. The justification is reasonable cause, which indicates that there was no other way to detect the crime or there was very little chance to detect it or identify the suspects without eavesdropping.

2.2 Reasonable Cause

How is a judge to decide if reasonable cause exists? No guidelines are furnished either by Constitution or the criminal procedure code. It could be said that reliance must be placed on the impartial judgment of the law enforcement officer that reasonable cause clearly exists. The trouble is that no one knows what the reasonable cause is and elusive meaning of reasonable cause is hard to pin down. It seems that reasonable cause exists where the facts and circumstances within the affiant's knowledge and of which he has reasonably trustworthy information, are sufficient unto themselves to warrant a man of reasonable caution to believe that an offense has been or is being committed. In addition to findings of reasonable cause, the judge must decide if the facts in the application show that normal investigative procedures have been tried and failed, or reasonably appear to be unlikely or succeed if tried or to be dangerous. But the question is that can a judge ever know whether normal investigative procedures are unlikely to succeed or are too dangerous? He is a judge, not an investigator. So, it is suggested the judgment would involve consideration of all the facts and circumstances and that it has to be tested in a practical and common sense fashion. The question is one of need and what constitutes proof of that need. No one denies that the need for wiretapping is hard to show. Some claim that it is impossible to demonstrate that normal techniques could not produce the same result. An order may require periodic reports to the judge showing what progress has been made and the necessity for continued interception. Progress reports are intended to serve as a check on the continuing need to conduct the surveillance and to prevent abuse. So, at any time the judge is convinced the need is no longer established, he may order the surveillance discontinued. It will serve to insure that extended surveillance is not undertaken lightly and also to insure that it is not unthinkingly or automatically continued without due consideration.

Judges also have responsibility for safeguarding the records. As soon as the time period fixed in the eaves drop order has expired, the recordings must be available to the judge who issued the order and the recordings may not be destroyed except the judgment becomes infinite.

The judge may question the officer with respect to accuracy and sufficiency of the facts, and as to the existence and reliability of his informant. For example, with respect to drug crimes, an officer may say that he has been in the target's apartment, has bought drugs from him freely, and he uses the telephone regularly to make purchases and makes phone calls to his wholesaler to obtain additional narcotics. If normal procedures are adequate the officers shall not ask for a wiretap order. Normal techniques of investigation consist of physical surveillance and use of informants and undercover police officers. But, it should be noted that while the officers are trying other means and holding off on the wire tapping, the evidence may go down the drain and it may be too late, or it may be used less advantageously. In some cases, getting a judge order may make sound foolish. For example, when one is dealing

with bookies, it is obvious that there is no way of getting information about particular betting transactions except through wire tapping. Since the subjects are wary of police interest in their activities, a physical surveillance of the subject would reasonably appear to be unlikely of success. Other investigative techniques are being employed, but they fail to establish affirmatively any links between the perpetrator and other co-conspirators, their source of supply and location of narcotics. So, there are some certain types of crimes where wiretapping might be indispensible and in these cases the judge may himself and without an application from law enforcement officers orders the eavesdropping.

Of course, reasonable time differs from crime to crime. In some cases, may he determine one week or lesser and in other cases one month or lesser or more. It seems that, if extension of the time period applied for, the judge can do it with an unlimited number of extensions. Undoubtedly, to obtain an extension, new reasonable cause would have to be shown. It means that the judge should not be a rubber-stamping extension application. If he finds the application for extension justified, with respect to the reasonable causes that the officers show, he will extend the time period, otherwise he will reject the application. So, privacy ultimately depends on the judge and competent, alert, and aggressive judges are the key to maintaining the safeguards provided by law. It could be said that judicial control is interposed at various stages of the proceeding in ordering and extension of eavesdropping. So, the judge to whom an application for an order is presented must be satisfied that reasonable cause is shown in the application and that normal investigative procedures would be inadequate; of course neither of these is easy to judge.

So, the question of reasonable cause is very important in the opinion of judge and he should refuse to sign an order or extension of order when he feels that the facts set forth in the application are inadequate. If an extension of an order is requested, the judge must be sure that reasonable cause has not become stale; new reasonable cause must be shown.

2.3 Time Period for Listening

Article 104 does not refer to the time period at all. When the judge does not determine a specified time for interception, authorization to intercept must be executed as soon as practicable and interception must end automatically when the described time of communication has been first obtained, unless the application shows reasonable cause to believe that additional communications of the same type will occur later. It could also be said that, the order must include a statement as to whether or not interception shall terminate automatically when the described conversation has been obtained. But, it seems that recording of one conversation may not furnish adequate evidence for conviction.

Although, the new code requires the judge to determine a time period for eavesdropping, but it has not determined a specified time, like 30 days or 60 days and the judge itself determines such a time. The time length raises policy as well as constitutional issues. Should it be so long? It seems that the duration of surveillance would have to be justified on a case by case basis and what is important is that the facts in the application on a case by case basis justify the period of time of the surveillance. For example in drug trafficking, murder and armed theft and crimes against the security of the country in which identifying the accused or his aiders and abettors or participants takes a long time, but in other crimes may it does not take a long time. As a matter of policy, if an application asks for a period that is longer than necessary, it may indicate a lack of caution and sloppiness in preparing the application. There should be no greater invasion of privacy than is necessary under the circumstances.

The question is that if the law enforcement officers continue listening after they have obtained a recording of conversation as specified in the order, does continuance of surveillance constitute an invasion of privacy that invalidates all the interceptions? It seems that an invasion of privacy by the law enforcement officers constitutes a crime according to article 576 ISLAMIC PENAL CODE 1996, but does not invalidate all the interceptions. The reason is that, the interception has been done legally, but after obtaining the described conversation the officer has abused the order and power. Of course, difficulty of proving such an abuse should not be ignored.

Although, the crimes against security of the country have been listed in ISLAMIC PENAL CODE, but, the phrase of national security is so brief and nebulous that creates greater turmoil. National security is not defined, nor does the law indicate explicitly what offences are characteristic of national security and in addition to listed crimes may the court regard other crimes (for example high jacking) as crimes against security. Moreover, there can be no doubt that there are today in our country organizations which intend to use force and other illegal means to invade the privacy and intercept the electronic devices on the excuse of protection of national security of combating the official corruption especially in respect to judges. Although, according to law, any government officials cannot intercept without a court order and the emergency is not the real reason for eavesdropping first and getting a court order later, even in emergency cases like kidnapping the officials need a court order, but, by no means of least importance will

be the assurance of the public generally that wiretapping and bugging cannot occur without court order. In fact, there is no way for the public to know how much eavesdropping is going on if no court order is obtained. National security is a vague concept and it may be difficult to determine if a threat is foreign or domestic without first tapping or bugging. But, in foreign law, in case of Snowden, the court has held that "the phrase national security and serious crime were sufficiently clear justifications for public authorities rely to on when justifying the grounds for an act of surveillance." (Stratford & Johnston, 2014, p. 134)

Eavesdropping without court order is strongly condemned and is a crime. Invasion privacy by officials without court order and judicial control is more appropriate to totalitarian than a democratic society and a kind of abuse of power. So, the legislator in trying to circumvent, has criminalized it to protect constitutional requirements of freedom of speech and association. So, "giving an order of interception is only in the capacity of judges, which should determine a specified time and numbers of interception." (Haji Zade & Motavalli, 2004, p. 355) and "if we allow the security officers to intercept without a judicial order, it contradicts the human rights criteria" (Akhoondi, 2009, p. 186)

"Information on official eavesdropping is not revealed readily. The surreptitious nature of wiretapping and electronic surveillance makes law enforcement officers wary and secretive. Continued criticism of eavesdropping under law has produced great sensitivity and defensiveness in officials. They must be convinced that objective discussion is possible." (Lapidus, 1974, p. 106)

3. Eavesdropping by Consent and from Innocent People and Incriminate out of Eavesdropping

3.1 Eavesdropping by Consent

Article 582 only refers to the employees of the government, and as some believe, "employees of telecommunications office may more than others commit this crime" (Pad, 2006, p. 243) and it means that if a layman eavesdrop the conversations, there will be no crime. If we can regard the content of conversation as secret, a kind of privacy which none of the parties like others to know about it, man will be much surprised when sees article 669 of ISLAMIC PENAL CODE 1996. According to this article threat to disclosure a secret is a crime, but disclosure of a secret or eavesdropping is not a crime. Regarding article 582, a question which has been left unsettled by the Constitution and statutes is whether consent by one of the parties to a conversation to listening by a third person or to recording the conversation removes it from the prohibition of the laws against unreasonable search and seizure. In other words, suppose that a police officer listens to a conversation by the consent of the other party, and then disclosures it at the court. The question is that, is it a crime? And can the court regard the recorded conversation as an evidence? The point is that the second party was not consent of recording the conversation and disclosure it.

It seems that there will be no unlawful invasion of the office, for the agent was in the office with the owner's consent. The traditional principle on which the validity of consent eavesdropping rests is that a party to a conversation takes his chances that the other participant may increase his present or future audience. But it seems that in a free society people ought not to have to watch their every word so carefully. But the issue of consent eavesdropping now appears to be settled, and it seems that the Constitution is not violated by governmental electronic eaves dropping effected by wiring a police officer for sound, having him talk to the suspect, and then having agents to whom the conversation is transmitted repeat the communications at the suspect's trial. So, it is not unlawful for a law enforcement officer to intercept a wire or oral communication if he is a party to the communication or if one of the parties gave prior consent to the interception. A police agent who conceals his identity may write down his conversations with a defendant and testify concerning them without a warrant. No different result is required if the agent records the conversations with electronic equipment which transmits the conversations to recording equipment located elsewhere or to agents monitoring the transmitting frequency.

Sometimes may law enforcement officers are wiretapping illegally to get leads prior to making an application for a judge order.

3.2 Overhearing Innocent Conversations

Eavesdropping would inevitably result in intercepting innocent conversations and we should try to deal with the problem. Unfortunately, the law does not explicitly refer to the case and it does not require that every order of eavesdropping shall be conducted in such a way as to minimize the interception of innocent conversations. So, the question is that how is it to be kept to a minimum? In fact when the judge orders of tapping a telephone number, the officers not only listening to the specified person, but also they are listening to every individual who may choose to call the tapped telephone. So, it seems that overhearing of innocent conversations and privileged communications is unavoidable and many innocent conversations would be overheard and there is no way to limit the tap to the persons

or conversations in which the law enforcement officers may have a legitimate interest. Such invasions cannot possibly be avoided once the tap is put in the telephone, so the necessary confidentiality of legally privileged conversations is inescapably destroyed, even if unintended.

The other problem is the meaning of a non-criminal conversation and irrelevant conversation or innocent or non-incriminating. Sometimes may some information could be gathered from innocent or irrelevant conversations. For example, they may talk about the people they were out with and where, and about matters that lead to incriminating evidence. Wives talk to one another and sometimes tell where their husbands are going and why. So, it seems that there is no certain way to avoid overhearing of innocent or irrelevant people.

So, although according to law only the telephone of an accused could be overheard, not innocent or irrelevant or privileged conversations, but the law does not say how overhearing of the latter persons is to be avoided. It could be said that, the law enforcement officers should turn the recording devices off, when a non-criminal conversation is taking place. It is, however, difficult because it is left to law enforcement officers to determine whether it is innocent or a criminal conversation. It is hoped that law enforcement officers are honest, but may be they are corrupted.

3.3 Incrimination out of a Conversation

We have to spell incrimination out of a conversation. Many telephone calls may be made between conspirators. If some of the conspirators do not appear to be incriminating, it does not mean that in fact they were not incriminating. It simply means that it gave us no information. The most important thing in a wiretapping is that it results in getting information or arrest the accused and in fact it is the police officer manning the electronic device decides when to stop listening to the particular conversation. Because, he knows that when he is getting the information that he wants or the judge has ordered and whether he should spend time on it and whether he should try to apprehend the suspect now or delay arrest while he seeks additional evidence. So, the wire tap may terminate before expiration of the period allowed by the order. It seems that although the judge has not explicitly included a statement as to whether or not the interception shall automatically terminate when the communication has been first obtained, but as the order has been issued to get the needy information, it shall automatically terminate when the police officer has got the wanted information. But, if initial conversations do not reveal the crime enterprises, the police officer is not obliged to terminate immediately on hearing one conversation of the type specified in the order and he can continue till the end of determined time period.

One of the most important points of the interception is that in some crimes like drug crimes or organized crimes much of the language is in code and the perpetrators or groups have their own terminology and although the police officers usually know their terminology, but the criminals are very ingenious in developing new language to confound the eavesdropper and to make it difficult for law enforcement officers to use intercepted conversations as proof of crime. Of course, it should be mentioned that the fact that a wiretap order has been obtained and information gathered does not mean that intercepted communications will be used in evidence at the trial even if there is an arrest and indictment.

One of the questions which could be posed here is that, if the judge should listen to the conversation or it suffices to read the report of the law enforcement officers? It seems that basically the judge accepts the reports unless he has doubts about the originality, accuracy and fluency of the report or according to the defenses of the accused thinks that the content of the conversation has been diverted.

Unwarranted intrusions on customers' phone conversations has been criminalized in article 582 of Islamic penal code, ratified in 1996. The idea is that, secrecy of communications is a basic concept in communications business and the public has an inherent right to feel that they can use the telephone with confidence, just as they talk face to face. Any undermining of this confidence would seriously impair the usefulness and value of telephone communications.

Employees of the telephone company are trained and supervised to minimize intrusions, and are subject to discharge for violations of rules of secrecy of communications and records.

4. Conclusion

Eavesdropping as a way of detecting some crimes or offenders is used in all criminal justice systems. In some cases it is nearly impossible to identify the offender or get some information about the crime without overhearing the telephones of the suspect persons. So, it seems that in some cases like organized crimes or crimes against the security of the country resorting to it is unavoidable. Of course, it should be noticed that "Neither structural criteria (eg, the

degree or organization or the internal sanction system etc.) nor material criteria (eg, the kind of offences concerned such as drug trafficking, traffic of arms etc.) seem to suffice to construct a coherent description of the concept of organized crime." (Joubert, 1995, p. 310)

Despite the difficulty involved but, no doubt that in some cases it is in conflict with the rights of innocent persons and examination of the law in operation reveals that overhearing breaches the privacy of a vast number of innocent conversations. So, there should be some mechanisms to reduce these kinds of intrusions. It seems that, invasion of privacy can be minimized only by limiting the duration of orders to a short period, restricting them to serious cases where less intrusive tools of law enforcement are clearly not serviceable. The most careful scrutiny by an impartial judge of applications for orders and continued judicial concern throughout the period of the order are essential if safeguards are to be meaningful and invasion of privacy is to be kept to a minimum.

Although the new criminal procedure code has provided some guarantees to the privacy in comparison to the former one, but as it has not determined a fixed time period and it is the judge who decides to give an order of eavesdropping or to extend it unlimitedly, it seems that the guarantee provided for individual's right in article 9 of the Constitution has not been respected by the statutes. The most important problem is the ease with which it is possible to go to a friendly judge who will sign an order for whatever period a law enforcement officer asks, which leaves the door open to unjustified invasions of privacy. In fact in this situation the court order gives them a piece of paper and they use it to justify listening to everything. Once you give them the tool, you can't stop it. The police with wiretapping equipment listen to everything, if only out of curiosity.

The use of eavesdropping presents a very serious problem and as a society we should not authorize judges to use these techniques except where it is absolutely necessary and a serious danger criminal problem is presented. If we found that the possibility of abuse is higher in certain cases we should exclude them.

References

Akhoondi. M. (2009). *Criminal Procedure*, Volume 4, Majd Publications, Tehran. Iran.

Ashouri. M. (2009). *Criminal Procedure*, Volume 2, Samt Publications, Tehran. Iran.

Blair. A. L., & Jernigan. W. (1980). Criminal Procedure, *Washington and Lee Law Review*, *37*, 510-595.

Donnelly, R. C. (1963). Electronic eavesdropping, *Notre Dame Law Review*, *38*, 667.

Haji Zade, H. R., & Motavalli. Y. (2004). *Criminal Procedure code in the current legal order*. Khatte Sevvom Publications, Tehran. Iran.

Hashemi, M. (2011). *Constitutional law and political structure*. Mizan Publications, Tehran. Iran.

Joubert, C. (1995). National and International aspects of Undercover Policing. *The Police Journal*, *68*, 305-318. https://doi.org/10.1177/0032258X9506800404

Kooshki. G. (2007). Protection of Privacy. *Judiciary law Journal*, *1*(71), 135-150.

Lapidus. E. J. (1974). *Eavesdropping on trial*. Hayden Book Company.

Madani, J. (1999). *Criminal Procedure*. Paydar Publications, Tehran. Iran.

Madani. J. (1990). Constitutional law in the Islamic republic of law, vol. 7. Soroosh Publications, Tehran. Iran.

Motameni Tabatabaei. M. (2011). *Constitutional law*. Mizan Publications, Tehran. Iran.

Nohlen, N. (2005) Germany: The Electronic Eavesdropping Case. *International Journal of Constitutional Law*, *3*(4), 680-685. https://doi.org/10.1093/icon/moi046

Pad, E. (2006). *Private criminal law*. Daneshvar Publications, Tehran. Iran.

Qazi Shariat Panahi. A. (2012). *Precise of Constitutional Law*. Mizan Publications, Tehran. Iran.

Stratford. J. QC., & Johnston. T. (2014). The Snowden Revelations: Is GCHQ Breaking the Law. *European Human Rights Law Review*, *2*, 129-144.

Tadayyon. A. (2009). *Obtaining evidence in criminal procedure*. Mizan Publications, Tehran. Iran.

Notes

Note 1. A: crimes with capital punishment

B: crimes with life imprisonment

C: crimes which require the cutting the member of the body and intentional crimes which require one third of the blood money or more

D: crimes which require more than 5 years imprisonment or 180000000 Rials fine or life expel from governmental jobs

Note 2. Heads of three independent forces, their deputies and counselors, the head and members of the Nation's Exigency Council, members of Gaurdian Counsel, members of the Islamic Consultative Assembly, experts Assembly, Ministers and their deputies, Judges, the head and prosecutor of the national accounting agency, Ambassadors, governors of the provinces, governors of capital cities, public crimes of military and disciplinary officers with a rank of Brigade or higher or second grade Brigades who are commander of major-general groups or commander of independent brigade.