*Indian Journal of Fundamental and Applied Life Sciences ISSN: 2231– 6345 (Online)*
*An Open Access, Online International Journal Available at www.cibtech.org/sp.ed/jls/2015/03/jls.htm*
*2015 Vol. 5 (S3), pp. 364-370/Mousavi and Razavifard*
***Research Article***

# CRIMINAL JURISDICTION IN CYBERSPACE OF IRANIAN LAW SYSTEM

**[*]Seyed Nematollah Mousavi[1] and Behzad Razavifard[2]**

*[1]Department of Criminal Law and Criminology, AllamehTabataba'i University, Faculty of Law and Politics (Judge of Tehran Province Justice Administration)*
*[2]Department of Penal Law & Criminology, Allameh Tabataba'i University*
**Author for Correspondence*

## ABSTRACT

Cyberspace and/or virtual space are among concepts that have recently brought about new topics in criminal law. Establishment and innovation of internet and cyberspace were some concepts that created brilliant change in human science and his social behaviors in recent decades. Needless to say that committing a crime was not immune of these kinds of changes. In this situation, discussion and analysis on fighting against different kinds of crimes in this space was of high importance, the most important impact of au courant technology on penal law is bringing about new opportunities of committing crime and finally modern pathways in criminal support, creating criminal liability, etc., for instance, we know that the definition of crime in every society originates from the culture of that society. Crimes against public morals can be a good example in this regard. This issue creates some changes like criminalization and jurisdiction in respect of crimes against public morals. For example in respect of jurisdiction we can say if the local courts be able to consider crimes taking into account actual jurisdiction, they can prosecute ones who violate Iranian society public morals through internet, whether this criminal act is deemed in his/her soil as crime or not, because however, this act created crime effect in Iran. Therefore, it is to be mentioned that making use of internet in committing crime, or on the other hands, committing crime in virtual space can lead to change policies in penal law. There have been raised lots of questions in this regard like this, what is the impact of jurisdiction on cybercrimes? As we are going on, we will consider the concept of cyberspace and jurisdiction categorization and appropriate jurisdiction to fight against cybercrimes.

***Keywords:*** *Cyberspace, Cybercrime, Jurisdiction, Actual Jurisdiction*

## INTRODUCTION

Penalty orientation and criminal fight together with criminal phenomenon require preparing some grounds. Establishment criminal jurisdiction is considered as one of the most important requirements for criminal fighting against criminal phenomena.

With recently new development in technology and computer science and taking into consideration that establishment of cyberspace prepared new conditions and opportunities for crime commitment, fighting against these kinds of crimes is the focus of attention of legislator and policymakers.

In respect of cybercrimes, this is to be mentioned that despite other crime commitment conditions and spaces, cyberspace has no determined and detectable range and scope. For instance, an offender of cybercrimes is easily able to take a seat in his home in one of US states and commit a crime, which is able to have some impacts on Iranian territory. For instance, he can counterfeit the bills of I.R. Iran Central Bank applying computer.

In this case, if the fundamentals for jurisdiction of domestic courts are not according to correct foundation, the Iranian courts will not have the jurisdiction to consider the crime committed by that entity, while its impacts were within the Iranian territory, the material element of the crime had occurred in the American territory.

However, considering this issue requires testing the concept of cyberspace and cybercrime and finally testing the basic fundamentals of applying jurisdiction in the international Penal Law and finally, determination of main fundamentals of applying jurisdiction in respect of cybercrimes.

***Chapter One: Broad Concept of Virtual Space, Computer, Etc.***

Cyberspace and/or virtual space are among the concepts that have recently been focus of attention of lawyers. Considering the concept of this space, whether from criminal or legal viewpoints, is of a brilliant importance. From criminal viewpoint, considering the concept of cyberspace is of high importance, because the above space has prepared a new location or place for crime commitment. Considering the concept of virtual space in civil rights is also of high importance, because it has influenced most arenas of civil rights. In respect of contract rights for instance, it has brought about electronic contracts issues, and for evidence of the civil suit, it has mentioned the possibility of electronic evidence in such claims. We try to consider about new abovementioned concepts in the rest of this paper.

*Section One: Cyberspace*

We mentioned several definitions for virtual space up to now, some of which limiting the broad concept of virtual space and some developed its scope. By virtue of one of this definitions, cyberspace is said to the electronic information which are transferred via internet. Of course, other definitions tried to describe the differences between cyberspace and virtual issues and net . According to their viewpoint, cyberspace is a series of information saved in a computer and is connected to each other via internet, while net has its own separate definition. Internet is a greatly broad series of computers existing in the computer nets throughout the world which are connected via communication lines and exchange information applying certain protocols. Most of the computers within the internet have stored lots of information and generally, a large amount of information is stored in the internet. The information available in internet is stored through various ways and as a conclusion, it may be presented and transferred via different ways. Among several other ways, webpage is one of the special ways to store and present information. Despite obsolete methods of information storage and presentation in which information is usually stored and transferred in templates of texts, webpage is a graphic page for data storage which works based on hyper media system. Hyper media is actually a good combination of hypertext and multimedia. Electronic evidence in this space means all data stored in cyberspace with any title.

*Section Two: Internet*

A collection of webpages including the homepage and other pages connected to each other, locating in a net, and are owner by a person or organization is called the website. One of the most important features of webpages is that owners of websites are able to link a series of their own credentials, documents and information resources including text, audio, fixed photos, motion pictures (animation), film or a combination of them through webpages and can store and maintain them for personal use or can make them accessible to public or private users. The new concept of World Wide Web or (WWW) is actually the connection of linked pages in different websites of various nets connected to internet all around the world; these kinds of pages include different information databases in nets and different sites throughout the world.

***Chapter Two: Jurisdiction in respect of Cybercrimes***

*Section One: Concept of Jurisdiction*

Trial jurisdiction is among the most important issues mentioned in respect of fighting against cybercrimes. It shall be described that as mentioned previously, some crimes may be committed outside the borders of a country and have some impacts on the public discipline, chastity and morals of that country more than the crimes committed within the territory of that country. On this basis, fighting against cybercrimes necessitates sufficient knowledge and domination over trial jurisdiction and some other issues such as universal jurisdiction and actual jurisdiction. As to the court jurisdiction to consider cybercrimes, this question may be raised if is it possible to acquire jurisdiction for local courts to consider some of the cybercrimes that have a great effect on the public discipline, morals and chastity of Iranian community considering the universal nature of internet. Answering to this question requires a fundamental consideration such as the principle of universal jurisdiction and the principle of actual jurisdiction in relation to Cybercrimes Act. Jurisdiction is the authority assigned to the courts to consider and settle the claims in respect of legal terms. Generally, jurisdiction is the legal authorization of an entity or an official institution to perform some affairs. In Oxford dictionary, jurisdiction is defined as the power

of a court to hear and make decision about a case and/or to issue several judicial orders for that case . Absolute trial jurisdiction of a court means the limitation of a court in respect of a guild, type and rank of that court. In contrast, relative trial jurisdiction means the authorization of a specific court as compared to another specific court, both similar in respect of their type, guild and rank.

*Section Two: Jurisdiction Categorization*

*A) Territorial Jurisdiction*

This maxim is the most important and the most fundamental jurisdiction maxim which has priority upon other maxims, and means that the government whose territory a crime has been committed in, is competent to legally prosecute the committed crime and its perpetrator. Other maxims (including individual competence, countenance competence, and universal competence) are considered somehow complement and somehow exception in respect of this maxim. In article 3 subject to Punishment Act ratified in 2013, this maxim is described as follows: "Iranian penal codes shall be applied in respect of all entities commit crime within the land, sea and air territories of I.R. Iran, unless otherwise stipulated." Territorial jurisdiction cannon be used extensively for the cybercrimes because internet and its application have provided such a huge change and development in international communication and international Penal law that a crime commitment place is easily transferable to the territory of another country or to those regions which are not under the jurisdiction of any government. This form of jurisdiction is approved and accepted by virtue of Para. C, subject to Article 28 of Cybercrimes Act. By virtue of this note, if a crime is committed by any Iranian or non-Iranian entity outside Iranian borders against computer and telecommunications systems, websites used by or under the control of the three forces or leadership institute or official governmental branch office or any institute or institution rendering governmental or public services or against websites with high ranks of Iranian state code, in an extensive level, the legal courts will have required jurisdiction to consider issues. But as previously mentioned, this maxim is not very feasible in respect of cybercrimes.

*B) Universal Jurisdiction*

Application of jurisdiction of criminal courts on different cases may be performed based on different maxims per case. One of the most important principles that can be highly applicable in respect of cybercrimes which may create an appropriate basic for exercising jurisdiction by the courts is the principle of universal jurisdiction. It shall be described that in the international criminal law, some crimes may be committed that are not subject to any of the territorial, personal and actual jurisdictions, on the other hand, negligence of international community to crime issue and negligence of it is an unjustifiable issue . The principle of universal jurisdiction indicates the common ground of international community in declaring disgust on the actions occur throughout the world and hurt the feelings of mankind disregard of nationality of criminal and victim and location of crime commitment. That is why these actions have found a universal description and are called as International Crimes . The term "Universal Jurisdiction" was emerged firstly by Cowles in 1945. Based on comprehensive considerations he done of the performance of governments in relation to bandits, concluded that each government enjoys the jurisdiction to punish severe crimes regardless of the victim nationality. According to him, since war crimes including but not limited to robbery and piracy should be considered as the crimes against conscience of civilized world and whole nations, the interests of all governments necessitates to punish those who have committed such crimes. Several fundamentals have been offered for the principle of universal jurisdiction including the necessity to avoid release of criminals from punishment, preservation of public discipline of the country where the criminal is ceased and public international discipline. The maxim of universal jurisdiction is defined as legal principles in classic viewpoint. On the other hand, domestic criminal courts and governments are not so much interested in exercising this principle in their reviews and qualifications. The reason that the governments do not welcome prosecution and trial of the convicts of the crimes subject to this principle can be summarized in political motivations because as the result of exercising this principle, governments are accused of interference in the affairs of other countries and this will affect the diplomatic and economic affairs between them. Especially when the prosecuting government has no interest in prosecution of perpetrators of such crimes, it is less motivated for

prosecution of such crimes. As to the cybercrimes considering the international nature of internet, this question may be raised if exercising jurisdiction over these crimes can be justified by considering the principle of universal jurisdiction. Recently, in the symposium of overseas challenges of cybercrimes , the scope of computer crimes and cybercrimes and the possibility of exercising universal jurisdiction over these crimes have been mentioned a lot . However, it should be acknowledged that the maxim of universal jurisdiction can be analyzed as an appropriate substitute in respect of internet crimes for applying territorial jurisdiction and other maxims of applying jurisdiction.

*C) Principle of Individual Jurisdiction*

Some may mention that applying individual jurisdiction means applying jurisdiction based on the nationality of criminal may be a substitute for the maxim of territorial jurisdiction. The principle of individual jurisdiction which may also be called "Principle of Jurisdiction Based on the Nationality of the Criminal" is deemed as one of the most important principles for determination of jurisdiction. As it is obvious from its name, this maxim is applied to the nationality of person committed a crime. As by international penal law, the principle of individual jurisdiction includes development of rules and judicial jurisdiction of a country for its citizens. Mancini, the Italian jurist was one of the supporters of applying the principle of individual jurisdiction. He believed that what connects the people together is actually their nationality. People of a nation are inter-linked to each other instinctively due to historical backgrounds and traditional, moral and civilization factors. In the same way, the existence of a unique law for all the nations is another factor to connect them wholly together. This law preserves the interests of persons and always is adjacent to people similar to a shadow locally or overseas. Therefore, violating these rules even overseas, will not release an individual from the domination of domestic law. As according to the author's idea, the individual jurisdiction shall not be deemed as a correct substitute in respect of applying court jurisdiction on cybercrimes. Because as we mentioned earlier, the public moral is wholly dependent on the culture of one society. So, the citizens of a society may perform an act which may violate the morals of Iranian society, and the local courts are not authorized to prosecute or punish the criminal in this case.

*D) Actual Jurisdiction*

Among other maxims which create an appropriate fundamental in the way of fighting against cybercrimes, is the maxim of actual jurisdiction. In the respect it shall be described that the countries always think of developing their locational territory of criminal law outside their sovereignty territory in some exceptional ways and it means that in case of committing crime outside the sovereignty territory, they think of their rules and courts to be competent in jurisdiction of such crimes. One of these items is when the abroad committed crime actually endangers their fundamental resources and vital ones. The jurisdiction established in these conditions is called the actual jurisdiction. A review of the history of criminal law indicates that the principle of territorial jurisdiction has always been the most fundamental principle in the international penal law, a principle that in turn encompasses the three sovereign effects, namely legislation jurisdiction (the right of legislation and laws approval), judicial jurisdiction (the right to interpretation and application of laws) and executive jurisdiction (the right to execute rules and court orders). At the same time, unique features of territorial jurisdiction did not disarm the governments against crimes that occurred outside their territory and threatened their security. On the contrary, history of criminal law indicates that all countries always express reaction against the crimes threatened their essential interests and vital ones, though those crimes are committed outside their sovereignty territory even those committed by the foreigners. Actually, commitment of crime in such cases has several negative effects for the country. As interpreted by some of the professors, the penal reaction adopted by the affected country in such cases is called a legal defense and the damaged government cannot assign the defense to other governments. In this regard, Garo, one of the French jurists has an interesting interpretation, as says: "Actually, government is the victim of those crimes and may prosecute the criminal. No matter whether the crimes are committed overseas. It is on the basis of such thoughts that the maxim of actual jurisdiction is developed to reinforce these fundamental interests. The maxim of actual jurisdiction means the development of legislation and judicial jurisdiction of a country against the crimes that occur outside of the sovereignty territory of that country and damage its essential interests. In this

principle, the only criterion and basis for establishment of jurisdiction is the nature and severity of the committed crime which is deemed to have been committed against the essential interests of the country applying jurisdiction. In other words, countries have forcibly and naturally agreed to such jurisdiction considering the threats they feel as the result of commitment of such crimes. The idea of support and protection of public interests has caused the aforesaid principle to be called as the Principle of Support Jurisdiction. Article 5 of the Islamic Punishment Act ratified in 2011 stipulates in this regard that, "Iranian penal codes shall be applied in respect of all entities commit crime within the land, sea and air territories of I.R. Iran, unless otherwise stipulated." Article 4: "In case a crime is committed within the sovereign territory of Iran, wholly or in part, it shall be deemed as a crime committed within the territory of I.R. Iran". Article 5: "Any Iranian or non-Iranian individual who commits outside the territory of Iran one of the following crimes or the crimes stipulated within the scope of specific laws, shall be tried and punished according to the rules of the I.R. Iran. In case considering such crimes outside Iran is concluded in ordering a written judgment and its execution, Iranian court considers the rank of executed conviction in determining discretionary punishments." In the above article, the instances of exercise actual jurisdiction by the Iranian courts are counted as follows; however, they do not include commitment of wrong internet actions in cyberspace. By virtue of the context of article 5, categorization of exercising actual jurisdiction of Iranian courts is as herein described.

A. Action(s) against the system, local or overseas security, territorial entirety or independence of I.R. Iran;
B. Forging or abuse of the seal, signature, fiat, order or handwriting of the Supreme Leader;
C. Forging of abuse of the seal, signature, fiat, order or official handwriting of the president, chairman of the judiciary, head and/or representatives of the Islamic Consultative Assembly, head of the experts assembly, head of the state supreme court, attorney general, members of the guarding council, president and members of the expediency council, ministers or deputy ministers;
D. Forging or abuse the votes released by judicial authorities or writ of executions issued by those authorities or other legal authorities;
E. Forging or abuse of common money papers, binding and banking notes and credentials of Iran, documents of treasury and drafts released or underwrote by the government, prepare or promote forged coins instead of current common Iranian ones.

As mentioned on author's viewpoint, applying jurisdiction on computer crimes shall be done based on the maxim of actual jurisdiction. In other words, considering the effect of the crimes committed abroad on the culture and moral security of the Islamic society of Iran, the most appropriate basis to fight the crimes against public chastity and morality is to develop and apply actual jurisdiction for the Iranian courts in respect of these crimes.

In this case, some of crimes may be committed aboard while having some influences within Iran, for instance, it may be resulted in violation of public chastity, the Iranian courts will be able to exercise jurisdiction and to prosecute the criminals of those crimes because their actions have endangered public chastity and morality of Iranian society. Similarly, in the event that behavior of an Iranian citizen violates pubic chastity of another country, in case applying the maxim of actual jurisdiction over cybercrimes against public chastity is predicted in the law of that country, the criminal can be prosecuted by the court of that country.

*Section Three: Position of Iranian Legislator in respect of Jurisdiction in Cybercrimes*

As according to Article 28 of Cybercrimes Law, the Iranian legislator has mentioned the categorization of applying jurisdiction of Iranian courts in respect of cybercrimes as follow:

*1) Territorial Jurisdiction*

It shall be described that as subject to Para. 1 of Article 28, it is stipulated that if the criminal data or the data used for committing crime, are anyway stored in computer systems or telecommunications carriers existing in land, sea, and air territories of I.R. Iran, the Iranian courts are competent for jurisdiction on such case based on Article 28 of the Law.

*2) Actual Jurisdiction*

Actual jurisdiction of the Iranian courts was fulfilled according to Notes B. & C., subject to Article 28, where the legislator determines further to items provided in other rules, Iranian courts have also jurisdiction in considering below items:

B) The crimes committed via websites with high range having high Iranian state code.

C) The crime committed by every Iranian or non-Iranian abroad against the computer and telecommunication systems and websites under application or under control of three forces, supreme leader organ or official representative of the government, or any other organ or institute rendering public services or against websites with high range having Iranian state code in a wide range.

*3) Passive Individual Jurisdiction*

This is stipulated in Para. D, subject to Article 28 as follows:

D) Cybercrimes is in respect of abuse of people below 18-years old, whether the committed or victim is Iranian or non-Iranian.

Of course currently, the maxim of application of territorial jurisdiction is based on the cybercrimes, it shall be described that as by Article 29 of Cybercrimes Act, it is stipulated that:" if a cybercrime is detected or reported in a place, but its place of commitment is not known, the prosecutor's office of the place of detection is obliged to perform local initial researches in this regard. If the location of commitment is not known, the prosecutor's office shall order judgment after completing researches, and the related court shall accordingly take action to issue written judgment in this regard. So, in respect of cybercrimes, the legislator accepts the maxim of territorial jurisdiction, or on the other hand, the maxim of jurisdiction of commitment location.

***Conclusion***

One of the most important issued may be mentioned in respect of cybercrimes is the issue of jurisdiction to the crimes committed in cyberspace, and the importance of this issue is mostly derived from the specific conditions of cybercrimes, it shall be here described that due to nature of computer crimes (cybercrimes), this kinds of crimes is called borderless crimes, cause the cybercrimes, taking advantage of modern technology, are not dedicated to a limited physical space or specific location. A clear instance in this regard is the transnational range of cybercrimes in the field of viruses which are able to be developed quickly and cause disorder in total international net programs resulting harmful impacts on their function and application.

As a result, taking into consideration the ever-increasing development of cybercrimes, determination of jurisdiction for fighting against the, is of greatly high importance. From among different principles and maxims mentioned in law to determine court jurisdiction, the principles and maxims of territorial jurisdiction, universal and actual ones are accepted in respect of cybercrimes, seemingly, according to the conditions of cybercrimes, one can conclude that the most importance aspect of court jurisdiction in considering the cybercrimes is the principles of actual jurisdiction, and if this principles in based on initial fundamental of considering cybercrimes, if a crime is committed and threat the benefits of a country, only that respecting country is competent to consider that crime, taking not into account the place of crime commitment, and it means that the court of country sustained damage of that crime, and on the other hand the country in which soil the crime can have some effects, is competent for jurisdiction on that crime.

**REFERENCES**

***A) Persian References***

**Diana Holmes (1998).** *An Introduction to Information Technology*, 1st edition, translated by MajidAzarakhsh and Jafar Mehrdad (Samt Pub.) Tehran.

**Hosseini Nejad Hosseingholi (1994).** *Islamic International Criminal Law* (Mizan Pub.).

**Jafari Langroudi Mohammadjafar (2009).** *Terminology of Law* (Ganj-e Danesh Pub.) Tehran, under Jurisdiction term (3258).

**Mehdi Momeni (2009).** *Fundamentals of Iran International Penal Law* (Shahr-e Danesh Pub.) Tehran.

**Menotti Kaminga, translated by Shariat Bagheri Mohammadjavad (2003).** Exercise of Universal jurisdiction in respect of Heavy Crimes against Human Rights, Tehran. *International Legal Journal* (28).
**Pourbaferani Hassan (2011).** *International Criminal Law* (Jangal Pub.) Tehran.
**Pourbaferani Hassan (2012).** Development of Principle of Actual Jurisdiction in the New Islamic Punishment Draft. *Quarterly Journal of Judicial Law Viewpoints*, Tehran, period 17 (58).

***B) English References***

**DaviD'Agostino Greg Wilshusen (2011).** *Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities* (DIANE Publishing).
**Keller Linda (M).** The False Dichotomy of Peace versus Justice and the Internal Criminal Court. *Hague Justice Journal* **3**.
**Macedo Stephen (2006).** *Universal Jurisdiction: National Courts and the Prosecution of Serious Crimes under International Law* (University of Pennsylvania Press).
**Mo'ayyeri A (No Date).** Studies of international law. Available: http://www.shakuri.blogfa.com/post-19.aspx.
*Oxford Dictionary of Law* (Tehran, Mizan Pub.) Jurisdiction.
**Ploug Thomas (2009).** *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction* (Ballerup Denmark, Springer pub).
**UNIS/CP/390 (2000).** Challenge of borderless ceber crime to international efforts to combat transnational organized crime discussed at symposium.
**Willard B Cowles (No Date).** Universal Jurisdiction over War Crimes. *California Law Review* **33**(2) 2-6.