International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 13, Issue 12, 2020

# A New Theory of Cybercrime: A Comparative Study between Jordanian and French Law

**Alshible Mohamad[a], Abu Issa Hamza[b],** [a]Associate Professor at Jadara University, Faculty of Law, [b]Assistant Professor at Applied Science University, Email: [a]soramohamad@yahoo.com, [b]hamza_abuissa@msn.com

The theory of an attempt to commit a crime is one of the most important in criminal law. Traditionally, the legislator may adopt into the penal code a specific theory, when punishing the person who attempted to commit a crime. However, this approach may change in the face of cybercrime. This study deals with theories about attempts to commit cybercrime, by explaining provisions and penalties according to their types and conditions. It also compares Jordanian and French legislation, regarding such theories. The study concludes that there is somewhat of a difference between the two approaches. The Jordanian approach needs a comprehensive review, to provide an integrated framework for their legislators' theory of attempt in cybercrime.

**Key words:** *Criminal Law – Cybercrime – Material Element – Attempt Theory – Attempt in Cybercrime*

## Introduction

Talking about attempt theory in cybercrime is inseparable from talking about it in traditional crimes at large. Such crimes have not been there for long, yet they still rotate in the orbit of general rules about criminal law. In relation to the concept for example, the definition of attempt remains the same for kinds of crime; electronic and non-electronic. The attempted crime is one that is 'incomplete' because of the absence of some of its elements, while the presence of all elements renders it a crime that is 'complete'. When the crime is complete the attempt will not be a matter to discuss. The absence of any element will impact the result (Fathallah, 2019, p815), where the perpetrator has already carried out whatever is necessary to achieve this result, but one's action did not lead to the intended result because of reasons outside one's will (Abu Afifah, 2012, p280).

The issue of attempt in cybercrime scope gains importance on several levels. Practically, the crime of attempting cybercrime - as envisaged in this paper - needs more attention in terms of investigation, discovering perpetrators, and the variety of criminal procedures. The process of discovering the complete cyber-crime and arresting the perpetrators is one of the difficult issues in the electronic environment. More exertions and international cooperation are needed. Attempts at cybercrime involve an even more difficult process of justice. The desired outcome of the crime has not be achieved, which makes discovery of the attempt difficult. At the same time, the attempt remains a serious issue because it may be converting into a complete crime. In many cybercrimes, we need a broad confrontation of the behaviour in question; including attempting and reducing the committed crimes, as is the case in the crime of hacking or sexual exploitation of children via the Internet.

Jordanian legislators define attempted crime in their penal code as: 'the commencement committing any obvious action that leads to committing felony or misdemeanour, but the perpetrator could not complete the actions necessary for the execution of that felony or misdemeanour because of reasons outside his will; he will be punished for […] unless the law states otherwise' (Article 68, the Jordanian penal code). Whereas, French legislators define it as 'attempt is if the perpetrator starts committing the complete crime but the effect of it is prevented and its result is not achieved, because of the presence of circumstances outside one's will' (Article 121 – 5 , the French penal code).

The Jordanian Court of Cassation defines the attempt in crime as: 'The conduct through which it is meant to commit a crime, but the intervention of an external factor outside the will of the perpetrator leads to the termination of the criminal act and the disappearance of its effect, and there are two main elements conditional for an attempted crime [substance: that makes the act committed by the perpetrator the first step of directly committing a crime, and the mental element which is the will of committing the crime]' (Jordanian cassation verdict no. 719/97).

The main issue of this research appears thus. It concentrates on Jordanian legislators' attitude toward cybercrime. Whether the source of cybercrime was in the penal code, or cybercrime code or any other codes, differentiates the issues. Crucially, the Jordanian cybercrime code does not mention attempt as a criminalised action. Therefore, the question is whether attempt will be punished regarding the general provisions in the penal code.

## Provisions of Attempt in Cybercrime

### *Imagining Attempted Crimes*

Attempt is related to the commencement of committing the crime (Al Qarani, 2007, p130). Most legislation has not clarified commencement, therefore jurists have greatly emphasised the commencement phase. It delineates what is permissible from what is criminal. Therefore, when the perpetrator starts acting, all the actions necessary to accomplish the crime or give it a start maybe have already been completed, and yet the result may not be achieved, because of externalities (Al Hawawsheh, 2010, p36). Different enactments provide different penalties regarding this phase of the crime.

An attempt may resemble other crimes in some stages. There may be a likeness between an attempt and an impossible crime. An of an impossible crime is when a person pulls the trigger of a gun with the intention to kill, while ignorant of the gun not being loaded, or abandoning a crime. Abandoning a crime is a wilful act decided by the perpetrator, whereas a crime is merely attempted as the result of causes unrelated to the will of the perpetrator.

Attempts to commit crimes in the field of cyberspace raise several issues. The most important is the question of whether an attempt can be imagined. Attempts to commit some non-cybercrimes cannot be visualised in one's mind. They include negative crimes, or when the substantial act is too brief in time, and happens within a moment, or by a simple action like in crimes of contempt of an authority.

In general, some attempts to commit cybercrime can be imagined and some cannot. When talking about imagining a criminal attempt, we take some of the following as examples regardless of whether the act is punishable. The penalty in such crimes will be discussed below. Thus, we can imagine attempts in these crimes, as examples.

### *Cybercrime in Jordanian Cyber-Crime Law*

We can search crimes as follows:

1. Unauthorised access crime (Article 3, cybercrime code). When deeply looking into this crime, we can describe the attempt as when the perpetrator has done everything possible to access an information system but one is unable to access it, because of the extreme protective system that prevented one from doing so (Abu Issa, 2019, p42).
2. Data destruction, where an attempted crime can be described such as the perpetrator accomplishing the destruction, but the existence of a recovery system restored the information (Article 4, cybercrime code).

3. Spying on data: Trying to enter a net, system or website with the intention of discovering data not available to the public because it affects public security or the foreign affairs of the kingdom, public safety or the national economy (Article 12, penal code).
4. Child abuse (Article 9, cybercrimes code).

This kind of crime can be imagined as when the perpetrator uses a specific mechanism in a specific way, or prepares, saves, or promotes pornographic activities, to have an effect on children, but futilely; here is an attempted crime.

***Cybercrime outside the Jordanian Cyber-Crime Law***

We can search that crime as follows:

1. Electronic counterfeit (article 260, penal code): this crime can be achieved by using traditional or electronic methods alike, like a scanner and typewriter to alter electronic documents.
2. Electronic terrorism.

Here the perpetrator prepares electronic methods capable of facilitating terror acts, aiding terror organisations, or performing electronic training necessary to commit such crimes.

***Elements of Attempt in Cybercrime***

The Jordanian Court of Cassation clarified that an attempted crime liable to punishment consists of three elements (Jordanian cassation verdict 2/54, 1/1/1954):

***Commencement in Committing Crime***

Most legislation does not define the commencement of the commission of a crime (Al Hawawsheh, 2010, p42), but to define it, two doctrines have emerged (Dalloz, 1970, p362, referred to by Al Hawawsheh, 2010, p43).
**First** is the Substantial Doctrine. It sets the criteria necessary to define the commencement of committing a crime (Ibrahim, 1998, p182 & Salameh, 2001, p392 & Al Alami, 2009, p69 & Aliah, 1998, p235).

**The second** is the Personal Doctrine. It also considered several criteria for defining commencement (Bahnam, 2005, p703).

The Court of Cassation ruled that: ‘as a condition for an action to be an attempt at crime, the perpetrator would have started carrying out an action that obviously leads to committing a

felony or misdemeanour, where he could not accomplish what is necessary for the felony or misdemeanour to take place because of reasons outside his will'. This is complies with Article 68 from the penal code, therefore the mere determination of committing a crime and preparations are not considered an attempt at crime' (Jordanian cassation verdict no. 136/1985).

But the French court of cassation did not consider, as a condition, the commission of any of the substantial elements of the complete crime, and considers this a legal case of its discretion.[1] However, the court of cassation applies diverse phrasings that define the point where a crime is committed:

- Actions directly leading to the commission of a crime;[2]
- Actions of direct and immediate impact in completing the crime;[3]
- Any action that directly leads to committing a crime without the intention to commit the crime;[4] and
- Actions supposed to have a direct and immediate impact in completing the crime after entering the phase of executing the crime.[5] Occasionally the court of cassation avoids using any phrasing where they stress only the attempt. The doctrine of the court of cassation lacks adherence to a specific principle, while they stipulate the existence of a strong and direct tie between the conduct of the perpetrator and the complete crime (substantial element).[6]

Accordingly the rules of attempted crimes and whatever doctrines followed, do not differ in cybercrime from traditional crimes, because these doctrines are not affected by the manner in which the crime is committed; whether electronic or traditional. Consequently, commencement is an element of an attempt at cybercrime.

***The Moral Element***

[1] French court of cassation, Crim. May 1, 1879, S .., 1880.I.233; Jan. 3, 1913, so-called Faubourg Saint Honoré case, D., 1914.I.41, note H. Donnedieu de Vabres; S., 1913.I.281, note J.A. Roux.

[2] 'Acts tending directly to the commission of the offense': French court of cassation, Crim. May 3, 1974, B. no. 157; June 5, 1984, B. no. 212.

[3] 'Acts having the direct and immediate consequence of consuming the offense' French court of cassation, Crim. June 4, 1920, B. no. 257; Nov 3, 1927, S., 1929.I.119.

[4] 'Constitutes a commencement of execution any act which tends directly to the crime when it was done with the intention of committing it'.

[5] 'The acts which must have the direct and immediate consequence of consuming the crime, the latter having entered the period of execution': French court of cassation, Crim. 25 Oct 1962, D. 1963.221, note Bouzat, J.C.P. 1963.II.12985, note Vouin; Dec 29 1970, J.C.P. 1971.II.16770, note Bouzat, R.S.C. 1972.99 obs. legal; June 5, 1984, B. no. 212.

[6] French court of cassation, Crim. June 14, 1977, B. no. 215, R.S.C., 1979.539, obs. J. Larguier; Jan 4, 1978, B. no. 5; May 5, 1997, B. no. 167; 25 Oct 1995, Dt Pen. 1995.63; January 10, 1996, Dt Pen. 1996.97, R.S.C. 1996.846, obs. Bouloc.

A lack in a crime that converts it to a merely attempted crime does not include the moral element. It should only include the substantial element, whether complete or incomplete, whereas the result is not achieved. Consequently, the moral element remains in the attempted crime, and the wisdom behind criminalising attempted crimes lies in the criminal intent of the perpetrator when this intent is close – to a certain degree or wholly – to criminal conduct, even though the desired result is not achieved (Abdulmonim, 2000, p588 – 590). Thus, an attempted crime will not exist according to the legal framework, unless the will of the perpetrator achieves a felony or a misdemeanour; this must be present in the complete crime (Al Shinnawi, 1976, p300-301). For example, if the intention is to enter a military site for spying then this intention is present in a complete crime, and in the intention of an attempted from the beginning, because an attempted crime and its moral element precedes the complete crime (Fathallah, 2019, p819).

The researcher sees that attributing a moral element to an attempted crime assumes that the will of the perpetrator was directed to commit a complete crime, while it is impossible to imagine that the same will was directed to commit only the attempt, as if there was no intent to achieve a complete crime. Even if we imagine this to be the case, the will involved in an attempted crime will not achieve a result for the perpetrator, and he will not be questioned about it (Aliah, 1998, p255).

The Jordanian code of penalties does not stipulate the existence of a moral element in an attempted crime, where it is assumed that the perpetrator commences a criminal act with the intention of achieving a felony or a misdemeanour. The Jordanian Court of Cassation implemented this in much of its rulings. In one ruling it stated: ‘the mere action of lifting the edge of the quilt off the victim with the intention of sexual action does not constitute a complete intention of rape, i.e. the intention is incomplete’ (Jordanian cassation verdict no. 14/72).

When the moral element is present in the perpetrator’s actions, there will be no difference between a direct or probable intention, (such intention is based on expecting the result, and accepting the risk of not achieving it – Article 64 Penal Code, Jordan). Therefore the intention that implies probability is enough to create an attempted crime.

According to the relation between time and the intention of committing a crime, it is essential that intention is concurrent with committing the crime. That is so, because if the intention evolved after the crime, it will not be of concern, and we will not be standing at an attempted crime, where there is no consideration for an intention that succeeds an attempted crime; consideration is only for an intention concurrent with the crime (Al Shinnawi, 1976, p311).

***Non-Achievement of Result Due to Causes outside Perpetrator's Will***

It means that the result is not achieved for reasons outside the will of the perpetrator, i.e. involuntary reasons. This is what distinguishes an attempted crime from a complete crime. This conforms to the logic of the legal frame of the attempted crime. Therefore, an attempted crime differs from a complete crime by its result, whereas in the absence of the relationship the perpetrator will not be accused of an attempted or complete crime. Consequently he will be held liable to an attempted crime when the result is not achieved because of reasons outside his will. Alternately, not achieving the result due to a reason related to the perpetrator means abandoning committing the crime voluntarily, therefore it is not an attempted crime (Al Hawawsheh, 2010, p71).

The researcher sees that (not achieving the result because of reasons outside the will of the perpetrator) is the most significant justification when criminalising the attempted crime. Here the perpetrator is willing to accomplish his criminal act. He does not abandon willingly. Therefore, the punishment will be because of the danger related to the crime. However, the punishment is mostly lighter than the punishment for a complete crime, notwithstanding that in specific situations the punishment is the same for an attempted crime and a complete crime.

***Punishment of Attempt Committing Crimes***

It is a necessity of justice that the legislator sets a punishment for attempted crimes because of the danger exhibited by the perpetrator(Al Hawawsheh, 2010, p71). This danger impacts society, though less than a complete crime would. The other danger is due to reasons not related to the perpetrator. Therefore, it can only be said that danger lies in one's actions, or as a result of the action itself, or as a result related to one in person or related to one's will. Therefore danger comes out from two reasons that should be taken into consideration by the legislator: The actions of the perpetrator, and one's criminal intention (Husni, 1989, p386).

The Jordanian legislator in this way recognises the importance of criminal intention, and criminalises it where questioning perpetrators about their intentions, not about the reason that compelled them to commit the crimes. The Jordanian legislator adopts the theory of attempted crime in general, and it is enough that the perpetrator committed apparent actions that lead to a felony or misdemeanour, even though these actions do not lead to a crime at the time these actions are committed.

Punishment for attempted crimes does not include all crimes. Mostly the legislator, under the penal code, distinguishes between crime categories regarding attempted crimes. Therefore, attempted crimes are punishable in general either where there is a special text for each crime,

whereas for misdemeanours there are only punishments when there is a text that incriminates the acts, whereas attempts in minor offences are not punishable.

It is worth noticing that there are non-punishable crimes in the case of attempt, even though they are imaginable and their elements are present. In the domain of electronic misdemeanour such as unauthorised access, deletion and messaging, these can be imagined but the legislator does not penalise them. Some other crimes are not punishable because the presence of the elements cannot be imagined in cybercrime such as insults, or other non-punishable crimes committed by mistake, negligence, or lack of awareness; therefore non-intentional crimes cannot be described as attempted crimes because of the absence of a moral element (Al Hawawsheh, 2010, p88).

Crimes where the result exceeds the intention are not punishable. An example is beating that leads to death, where attempted beating is imaginable but death due to attempted beating is unimaginable. Here the result exceeds the intention; therefore the moral element is absent (Abdul Sattar, 2001, p88).

The Jordanian legislator adopts more than a doctrine in punishing attempted crimes. The general doctrine is as follows. A punishment for attempt is set as less than that for a complete crime, whether a complete or incomplete attempt. The legislator's justification is that the attempt does not achieve what is protected by the law, because it is limited to being a threat, and a threat is of less harm to society than a complete crime. Here the Jordanian legislator sets punishment for two kinds of attempt.

First**:** punishment of incomplete attempt. Article (68) of the penal code refers to an attempt, where the action element of the substantial element is incomplete. The penalty is imprisonment for (7-20 years) if the penalty for this kind of crime is death, five years of the previous sentence if the penalty is life imprisonment, and mitigation of any other timed sentence to one half or two thirds.

Second: punishment of complete attempt. It is an attempt where the action element of the substantial element is complete, but circumstances outside the will of the perpetrator bar the achievement of the expected, criminal, result. A text rules in this kind of matter, under Article (70) of Jordanian penal code, as follows:

1. Life imprisonment or twenty years imprisonment in cases where the crime merits the death penalty. Fifteen years of the same sentence, if the crime merits life imprisonment. Twelve to fifteen years of the same sentence, if the crime merits twenty years imprisonment.

2. Any other penalty will be reduced to one half or two thirds. The special doctrine: Here the legislator rules with a deviation from the general rules. Therefore, he sets a punishment equal to the punishment of a complete crime, as in the case of fraud (article 4/417) which states that "the same penalty applies for attempts in the crimes mentioned in this article".

### *The French Legislator's Approach in Punishing the Attempted Crimes*

According to article 121-42, attempted crimes are punishable in all criminal offences, and attempted misdemeanour is punishable if the legislator explicitly states so. In most cases this ruling is explicit. The main exception is when the incident practically cannot be categorised as an attempt, because categorising depends on the achieved result, and here the result is not achieved according to its definition. There are cases where an attempt is logically impossible, such as manslaughter (because attempt stipulates the presence of the intention) or committing a crime by abstinence. Additionally, a violation cannot be the subject of an attempted crime.

According to article 121-4, the penalty for attempt will be as if the person who attempted has committed a complete crime, and therefore may be subject to the same penalty, while in practice judges exhibit more lenience toward those accused of attempted crimes.

## Punishment of Attempt in Cybercrime

Studying punitive provisions for attempted cybercrimes requires studying cybercrime laws. The presence of a law that addresses cybercrime in Jordan does not mean that all crimes are limited to those listed in this law; there are other laws that imply dealing with cybercrime, or which may be applicable to them. These laws are of two types: Type one: the code of cybercrime. Type two: penal code, publication act, counters prevention act, and a code for protecting the secrets and documents of the state.

### *Punishment of Attempted Cybercrimes that are not Subjected to the Law of Cybercrime*

### *Punishment of Attempted Cybercrime Subject to the Penal Code*

Here we distinguish between two types of crime, the felony and the misdemeanour.

1) Felony: Article 71, the Jordanian penal code. The Jordanian legislator penalises attempt, in all cybercrime, as long as an attempt can be imagined and conditions and elements are present. An example is counterfeiting. Previous laws referred to provisions concerning cybercrime. These provisions made no mention of counterfeit, though counterfeiting can be electronically achieved. This means it was left to the general code of penalties. Therefore, any electronic counterfeit or any other cyber-crime not addressed in the code of cybercrime remains subject to the rules of the penal code.

2) Misdemeanour: Electronic misdemeanour is subject to the penal code where the penalty of non-electronic misdemeanour is applied. Therefore, attempt will not be punishable even though it can be imagined and its conditions are present, unless there is a text that states it is punishable. An electronic fraud is an example of electronic misdemeanour; therefore it will be subject to the penal code because there is no special text related to cybercrime. Consequently it is subject to the rule of article 417 from the penal code, which punish the attempt as the complete crime.

***Punishment of Attempted Crimes Subject to the Code of Publication***

Punishment is mentioned in the code of publications. Article 42/b states that 'the chamber of publication, exclusive of Amman's instant courts, specialises in the following crimes:

1. Crimes that take place in the Capital, referred to in paragraph (a); and
2. Crimes that concern internal and external security in the penal code, if committed in printed, video or audio media. Regarding attempts to commit crimes, there are two notifications:

a. Crimes related to publication: those committed in print media, or by a licensed video or audio media according to this text. They may constitute a felony or misdemeanour, where some concern state internal and external security matters in the valid penal code; and
b. Crimes committed in print, video or audio media may use electronic means. Therefore the concept is electronic. Consequently attempted crimes related to electronic publication may be punishable as follows:

b.1 felonies: They are punishable if imaginable according to attempt provisions mentioned in the penal code (article 68 & 70); and

b.2 misdemeanour**:** There is no reference regarding them. However, the space is open to the probability of committing a crime punishable if committed in print media or any means known to the Law of Publication. It is worth noticing here that the nature of the attempted crimes may render attempts to perform them unimaginable, being publication crimes where the substantial element may not take time. Thus, we cannot say there is a probability of not achieving the result. Therefore, we revert to the general rules that require two conditions, to be punishable: the attempt must be imaginable and there must be presence of its elements, in addition to the existence of legislative articles for punishment.

***Punishment of Attempt Committing Cybercrime those Subject to Terrorism Prevention Act***

Crimes punishable by article (3/e) of the Terrorism Prevention Act no. 55 for the year 2006 are accomplished by electronic means. Such means are numerous. They include information systems, information nets, any other publication or media means, establishing a website that

eases the carrying out of terrorist acts, supports a group or organisation which carries out terror acts, promotes its ideology, or finances it, and any action that may subject peoples or their properties to the danger of offensive acts or revenge. According to article (7) of the same act, the attempt is punishable with a specific sentence. Such punishment for an attempt will be similar to that of a complete crime as stated (the terrorist act is considered as complete either the actions which constituted it were complete or an attempt). It is noticed in Article (3/e) that the punishment of a cyber-crime mentioned therein is (3-20 years) of imprisonment, while not distinguishing between the sentence for attempted crimes and complete crimes. Therefore, the sentence for attempt is the same for both types of attempt (complete or the incomplete).

Here we find that legislators have a clear attitude toward the attempted crime. It may put us in doubt as to whether they intend to punish the attempt of crimes mentioned in the Cybercrime Act or not, because they did not stipulate specific punishments for attempts in this law, as they did in the Terrorism Prevention Act.

***Punishment of Attempt Committing Cybercrime those Subject to the Act of Protection of State Secrets and Documents***

This enactment incriminates some acts in different texts. Some of it is not applicable to electronic acts, such as article (14) which relates to substantial entry. Article (15) of the same enactment appears without identifying the means of spying; therefore it applies to cybercrime (Husni, 1989, p386). The Article is about the crime of acquiring state secrets. The punishment will be as follows: any person who steals or gets hold of secrets or things, or documents, or information that must stay secret for the sake of the state security, will be punished with imprisonment from (3-10 years). If it was for the benefit of a foreign country the punishment will be life imprisonment, and if it is for the benefit of a country that is a foe, the penalty will be death. Other provisions relate to substantial entry. This does not apply to cybercrime as mentioned in article (16) of the same act which mentions the crime of divulging secrets acquired by the nature of a person's work. Here the means of entry are not defined; therefore the provision applies to electronic means.

In light of this, the punishment for attempting to commit these crimes raises two possibilities: The first is that the attempt will be punished in accordance with the general provisions in the Penal Code (Husni, 1989, p184). The second possibility is that attempt will not be punished, in the absence of stipulation for punishment or for the failure to refer to the general provisions in the Penal Code.

The researcher agrees with the second possibility, especially in light of the absence of an attitude by the Court of Cassation, as there is scarcity of case law related to these articles, except a few precedents. But unfortunately it did not relate to attempt.

***Punishment of Attempt Committing Cybercrime those Subject to Cyber-Crime Act***

By looking at cybercrime act, it appears the Jordanian legislator does not mention attempt at all either, in a special article or implicitly within texts. Therefore a question pops out, does the legislator want to penalise attempts or not?

Going back to the beginning of this study reminds us of the legislator addressing the sentencing of attempted crimes. It depends on the danger involved, whereas danger is not limited to certain crimes, especially given that most legislators penalise attempting committing felonies in general without an explicit text which means that an attempt in any felony constitutes danger. On the other hand, by looking at the provisions of cybercrime in the cybercrime code, legislators inclines to strictness from their point of view, depending on the idea of danger. Therefore, legislators impose the same penalty for all participants. It is deduced that the Cybercrime Act is specific for cybercrimes mentioned in it.[7]

[7] That was corroborated by the interpretation of the Bureau for the interpretation of the laws. The Bureau was asked to interpret articles (42) and (45) of the Press and Publications Law, and Article (11) of the Electronic Crimes Law, regarding publishing on websites and social media sites. Publication includes defamation or vilification, or an insult covered by Articles (42) and (45) of the Press and Publications Law, or by virtue of Article (11) of the Electronic Crime Law. The decision indicated that the Press and Publications Law No. (8) of 1998 in relation to crimes committed through publications and electronic newspapers is considered a general law. In all of these publications, the law stipulated that it be licensed, and the law gave the electronic publication the option to register. As for the electronic crime law, it is a special law in relation to the crimes committed in accordance with the texts developed therein. It is a special law that has reorganised some provisions related to crimes of defamation and slander. Therefore, the law applied in this case will apply Article 57/2 of the Penal Code, which states (If a general description and a special description are applied to the verb, the special description is taken): Resolution No. (8) of the Bureau of Law Interpretation. **This is also corroborated by** the decision of the Amman Court of Appeal regarding the statute of limitations for crimes of defamation and slander that are carried out by electronic means, which considered that crimes of defamation, slander and degrading that are done through electronic means are subject to general rulings in the initiation of the criminal case, as they are, according to the Penal Code, … crimes that require filing a complaint within three months, in accordance with the Code of Criminal Procedure. Therefore, submitting them after three months opens them to the statute of limitations. The decision stated that: "... our court finds that the crimes assigned to the appellant - on the assumption of its evidence - are among the crimes in which the prosecution ceases to file a complaint or claim the personal right, so because the crimes attributed to the appellant occurred on 6/17/ 2016 and 15/6/2016, and the complainant filed her complaint on 3/3/2017 with the Public Prosecutor of Amman, that is, after the passage of the legal period mentioned in Article 2/3 of the Criminal Procedure Law, and it is also one of the crimes that require the submission of a complaint or claim of the personal right. The fact that the right to file a complaint or claim the personal right is forfeited after the lapse of three months, from the date of the victim's knowledge of the crime, and because the complaint was filed after the passage of this period, the court of first instance had to reject the public right claim by reason of the statute limitation that prevented it from being heard (statute of limitations) according to the text of Article 3/2 of the Code of Criminal Procedure. Its decision is incorrect and must be overturned for reasons of appeal against it": Amman Court of Appeal Decision No. 29409/2018, Qastas Publications.

This attitude of not addressing the punishment for an attempted crime in Cybercrime Act puts us in doubt, as to whether the legislator intended to punish attempts through the general rules in the penal code, or to exculpate it. Two possibilities appear:

***Punishment of Attempt***

This will be through the general rules of the Penal Code – unclear until now. Therefore, two judgments are deduced here:

a. There is no penalty for attempting the commission of misdemeanours mentioned in the cybercrime act because no text penalises it.
b. Attempting committing felonies mentioned in the cybercrime code will be punished according to general rules that penalise attempting felonies in articles 68 & 70 of the penal code as follows:

***Felonies Mentioned in the Cybercrime Code***

a. Actions considered as felonies due to strict conditions:
1. Unauthorised access to information systems, information net or electronic site (article 3),
2. Deletion of information in an information system, information net or electronic site (article 4),
3. Intercepting, altering or deleting any material sent through an information net or information systems (article 5)
4. Acquiring data or information related to bank cards without permission.

Originally, these crimes were considered misdemeanours, whereas in compliance with article (7) of the cybercrime code, they will be considered felonies. The penalty will be (3-20 years imprisonment) in strict circumstances that change the criminal description. These circumstances represent crimes befalling information systems or electronic sites, information nets or transfer of funds, payment services, financial clearance or financial settlement or any banking services provided by banks or financial companies (Article 7 cybercrimes code).

Because these actions are taken as felonies, and because the Jordanian legislator does not state special or specific penalties for attempts, if general rules were applied, the penalty would be in accordance with articles 68 & 70 of the penal code.

***Felonies Originally***

1. Sexual abuse of children

Article (9) of the cybercrime code mentions several unlawful acts, where some rise to the level of a felony; paragraph (c): "anyone who intentionally uses an information system or information net with the purpose of abusing whoever is under the age of eighteen years, or a person who is psychologically or mentally disabled, in prostitution or pornography, will be subject to a penalty of (3-20 years) of imprisonment and with a fine (5000 -15000 JD).

2. Electronic spying

Article (12) of cybercrime code, mentions several unlawful acts which are felonies as follows:

Article 12/b mentions the felony of entering an information system or information net by any means, with the intention of looking at data or information not available to the public (it concerns the national security or foreign affairs of the kingdom or the national economy) without permission, or with the intention of deleting, discarding, destroying, modifying, altering, transferring, copying or divulging it. The legislation penalises it with (3-20 years) of imprisonment and a fine (1000 -5000 JD).

Article 21/(c) addresses the felony of intentionally entering an electronic site to look at data or information not available to the public (it concerns the national security of the kingdom, foreign affairs or public safety, or national economy), with the intention of cancelling the data or information, or discarding, destroying, modifying, altering, transferring, copying or divulging, the legislator penalises it with the same punishment as the previous felony.

The Jordanian legislature does not state a special or specific penalty for attempt in the cybercrime code. However, if general rules were applied, the penalty would be in accordance with articles 68 & 70 of the penal code.

***Non-Punishment of Attempt***

This possibility is considered the original according to the principles of criminal law. Punishment is permissible only in accordance with the principle of legality, which stipulates that “There is no crime and no penalty except that provided for by law”. Therefore, we conclude that it is not possible to punish an attempt at cybercrime in accordance with the cybercrime code, which is devoid of the provision for punishment for attempt, for the following reasons:

1. The non-existence of provisions for attempt punishment in cybercrime code.

2. If Jordanian legislators were heading towards punishment for attempting cybercrime, they would have stipulated it, or stipulated the imposition of this punishment in accordance with the general provisions, as did the French legislator who stipulated the punishment for attempting cybercrime in the same chapter that punished cybercrime in the French Penal Code. Also, most Arab cybercrime laws penalise attempts at cybercrime.
3. Referring to the Arab Convention on Combating Information Technology Crime (cybercrime)[8], we find stipulated in article 19/2 the punishment of attempt. However, in article 19/3 it granted the right for state parties to reserve their right not to apply provisions of article 19/2 which relate to attempt. Consequently, the Jordanian legislator has exempted himself according to this text from punishing attempt, in contrast to what most Arab countries have legislated on.
4. Explanatory document for Cybercrime Law: It is the explanatory note for the Information Systems Crimes Temporary Law No. 30 of 2010, which also considers the Explanatory document for Cybercrime Law No. 27 of 2015[9]. This explanatory document did not indicate the intention of the Jordanian legislator to punish attempts at cybercrime, or if the general provisions of the Penal Code will be applied on the issue of attempt.
5. The Jordanian judiciary, as we have seen previously from court decisions and the Bureau of Laws Interpretation (resolution no.8), considered that cybercrime code as a special code for the crimes mentioned therein. Therefore the general provisions of the Penal Code cannot apply to the crimes mentioned therein.

This attitude of the Jordanian legislator raises several national and international problems. On the national level, there will be controversy and inconsistency in law enforcement. On the other hand, while not resolving the controversy, amending the cybercrime code will lead to decriminalising attempt, and thus impunity for perpetrators of attempted crimes. This contrasts with the legislative policy that tends to tighten punishment for cybercrime, especially with regard to the commencement of felonies because of the grave consequences that appear from attempts at crimes, especially in the case of full attempts because the perpetrator completes all the elements of the material element of the crime. Internationally, non-punishment for the attempt of cybercrime will narrow and hinder the prospects for international cooperation in the field of combatting cybercrime, by hindering the mechanisms for extraditing and exchanging criminals.

### *Punishment of Attempting to Commit Cybercrime according to French Law*

French legislators developed French criminal law, to meet whatever is new in the criminal arena. In 1988 they issued act no (19 – 88), which added cybercrime and its penalties to the penal code. In addition, there was an amendment by act no. 575/2004 date 21/6/2004. The

[8] Jordan signed it in 2010 and ratified it in 2013.
[9] : https://www.slideshare.net/UrdunMubdi3/31-72010-2

French Government also ratified a 2006 European treaty about cybercrime. The law incriminated assaults on electronic means. Therefore, it incriminated all kinds of illegal unauthorised access. Either these actions targeted the electronic device itself or the systems that operate it (article 323/1). The law also incriminated deceptive data entry to default data processors, and deceptive altering of data in the processor (article 323/2). It incriminated acts applying fake or altering general electronic data (article 323/3). Additionally, participation in a group or a conspiracy established with the intention of preparation for a crime mentioned in articles 323-1 to 323-3, which has been verified by means of one substantial procedure or more (article no. 323/4), was incriminated.

The attitude of one who is a French legislator, regarding attempts at these crimes is clear. One does not leave it to the general rules. One takes a different route and imposes independent penalties regarding attempt. Article (323-7) of the French penal code says: "attempted misdemeanours referred to in article 323-1 to 323-3 subject to the same penalty for the complete crime".

**Conclusions**

**First:** Cybercrime is subject to most rules and provisions of traditional crimes. Therefore, the commencement phase in the attempt of cybercrime is subject to the same, traditional rules and provisions, in regard to imagining it or not. In some cybercrime the attempt can be imagined and in others it cannot.

**Second:** The Jordanian legislator (in Penal Code) penalises attempts to committing felonies in general, either with or without an explicit text. However, in misdemeanour cases there must be a text for punishment. Here the punishment estimate will be different from those set for felonies, and the punishment may not differ in the attempted misdemeanour from that of the misdemeanour itself. But that is still not sure to be applied to attempts of committing cybercrime stipulated in the cybercrime code which did not stipulate a punishment for attempt, despite it not referring it to the general principles.

**Third:** In regard to cybercrime from outside the cybercrime code, we will search whether the legislator stipulated a punishment for it, or whether the general principles in the Penal Code were referred to. Also, we have to investigate whether the judiciary system or law interpretation departments subject it to general principles. The Cybercrime Code is unclear. There are no articles that punish attempt or refer it to the general principles. This is the same situation for courts and law interpretation departments which did not pursue this issue.

**Fourth:** French legislators adopted the theory of attempt, where they penalised attempt in cybercrime regardless of the kind of crime, setting a special text that addressed the

punishment of attempts. The penalty for electronic, attempted crimes is equal to that of a complete crime.

**Fifth:** This controversial attitude adopted by Jordanian legislators, in punishing attempts, has been described in this article as creating conflicts in the application of law to perpetrators of attempted crimes. That is so at both national and international levels, especially within relationships with most Arab countries which punish attempting to commit cybercrime, but also the rest of the world. Cybercrime is considered a cross-boundary crime. It may be committed within the jurisdiction of more than one country. That means we need unified legislation, to combat it. This surely requires punishing attempt in different enactments.

**Recommendations**

**First:** It is recommended that Jordanian legislators amend the Cybercrime Act. They should stipulated definitions of attempt, determine which crimes are attended by punishment for attempt, and to set different penalties for attempts. It is preferable if the legislator follows the same approach of punishing attempt as the traditional penal code.
**Second:** Attempted misdemeanours should not be punishable unless they pose a danger. The penalty should not be equal to that of a complete crime.
**Third:** Jordanian legislators should provide a text in Penal Codes that imply applying general attempt provisions, regarding cybercrime, which are subject to other laws; it remains the original law for incrimination.
**Fourth:** Jordanian and French legislators are asked to consider the different provisions that may affect theories of attempt. For example, they should consider that the harm resulting from an attempt does not rise to that of an achieved result. Therefore the penalty should be less than that of a complete crime.

**REFERENCES**

Abdul S. F. (2001). Interpretation of penal code. Special Department (Cairo: Dar Alnahdah publishers.

Abdulmonim, S. (2000). General theory of penal code (Alexandria: Dar Al jami'ah Al Jadidah publishers.

Abu, A. T. (2012). Interpreting the penal code, the public section, (Amman: Dar A thaqafah publisher, 1st ed.

Abu, I. H. (2019). Information technology crimes, comparative study in Arabic legislations. (Amman: Dar Wail publisher. 2nd ed.

Abu, K. A. (1989). Interpreting general rules of the penal code. (Cairo: Dar Al arabieh publishers.

Al-alami, A. (2009). Interpreting Moroccan penal code, public section (Casablanca: Al najah press.

Al-haniss, A. J. (2010). illegal use of magnetic credit cards in the view of the penal code, magazine of Damascus University of Science of Economy and Law, vol.26, no.1.

Al-Hawawsheh, A. (2010). The impossible crime, comparative study (Amman: Dar A thaqafah publisher.

Al Murri, B. (2019). Interpreted the code of information technology crimes, and the digital degree of power in the verification (Egypt: Alarabieh publishers).

Al-qarani, A. (2007). Interpretation of the Omani penal law, (Cairo: Dar Al nahdah A arabiah.

Al-Said, K. (2011). Interpretation of general rules of penal code (public section) (Amman: Dar Al Thaqafah publishers.

Al-sarour, A. (1983). Al wasit in punishment, the public section, 1996, p303, & Mustaffa, Mahmoud, interpretation of penal code, public section, 10th ed.

Al-shathily, F. and Alqahwaji, A. (1997). General theory of crime (Alexandria: Dar Al Matbouat Aljamieieh publishers.

Aliah, S. (1998). Interpretation of penal code, public section (features, applicability, crime, liability, penalty) (Beirut: Almoassasah Al jamieieh publishers.

Bahnam, R. (2005). General theory of the penal code (Alexandria: Mansha'at Alma'arif publishers.

Fathallah, M. (2019). Interpreting the code of actions against the crimes of information technology in the Egyptian law no 175 / 2018, analytical and comparative study (Alexandria: dar al jamiah publisher

French penal code, (1994). Group of French court of cassation verdicts.

Homid, A. (1990). Detailed interpretation of the penal code (Damascus: Al matba'ah Al jadidah publishers.

Husni, M. (1989). Interpretation of lebanese penal code. public section (Cairo: Dar Al nahdah publisher.

Ibrahim, A. (1998). General rules in comparative penal code. Jordanian cassation verdicts, Jordanian Bar association magazine.

Najim, M. (2000). Penal code, public section, general theory of crimes (Amman: Dar Al Thaqafah publishers,

Rifat, A. (2005). Interpretation of Libyan penal code, public section (Cairo: Dar Alnahdah Al Arabieh publisher, Salameh, Mamoun, interpretation of penal code (Cairo: Dar Al fikr Alarabi.

Shinnawi, S. (1976). Attempted crime, comparative study (Cairo: Dar Al Nahdah.