# جريمة الاحتيال الإلكتروني في التشريع الجنائي الفلسطيني: دراسة تحليلية

**أ. آلاء أسعد إسماعيل كتوع**

محامية، المحاكم الفلسطينية، فلسطين.

**Mrs. Alaa Asaad Ismail Katoa**

Lawyer, Palestinian Courts, Palestine.

alaa.20161831@gmail.com

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

# The Crime of Electronic Fraud in the Palestinian Criminal Legislation: An Analytical Study


## Abstract

*This study addresses a relatively recent crime, namely electronic fraud, in Palestinian criminal law, employing an analytical method. The main focus of this study was to examine whether the traditional provisions of fraud under the Palestinian Penal Code No. (74) of 1936 & Jordanian Penal Code No. (16) of 1960 and its amendments, applicable in the West Bank, can extend to encompass the emerging crime of electronic fraud, which may be committed using computers, smartphones, and other devices. This study relied on analyzing the penal provisions of the previously mentioned Palestinian labor laws and consulted legal opinions to determine the extent to which these provisions apply to electronic fraud. The study also aimed to shed light on the subject matter of this crime (money) to understand its nature in electronic fraud, in light of the inadequacy of current legislation regarding whether it should be classified as material money or informational money. There are various legal opinions on this matter. The study drew several conclusions, the most prominent of which was that the money involved in cyber fraud is informational money that has value. Additionally, Decree-Law No. (10) of 2018 and its amendments, which is in force in the West Bank and Gaza Strip, criminalized electronic fraud and punished it with a penal provision. It also issued recommendations, the most important of which was: The Palestinian legislative council in the Gaza strip must approve and implement Decree-Law No. (10) of 2018 and its amendments regarding cybercrimes, and make it legally and practically effective, because it addresses issues of electronic fraud.*


***Keywords: World Wide Web, Electronic Money, Electronic Crime, Web Marketing.***

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

# جريمة الاحتيال الإلكتروني في التشريع الجنائي الفلسطيني (دراسة تحليلية)

## الملخص

*تناولت هذه الدراسة موضوعاً يتعلق بجريمة مستحدثة نسبياً، وهي جريمة الاحتيال الإلكتروني في التشريع الجنائي الفلسطيني، حيث استُخدم فيها المنهج التحليلي، لقد كان محور هذه الدراسة الأساس هو البحث فيما إذا كانت النصوص التقليدية لجريمة الاحتيال في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م وكذا قانون العقوبات الأردني رقم (16) لسنة 1960م الساري في الضفة الغربية، يمكن أن تمتد لتشمل في إطارها الجريمة المستحدثة (الاحتيال الإلكتروني) التي قد ترتكب بواسطة الأجهزة المحوسبة والهواتف الذكية النقالة وغيرها، واعتمدت هذه الدراسة على تحليل النصوص الجزائية الواردة في القوانين العقابية الفلسطينية السابق ذكرها والاسترشاد بالآراء الفقهية؛ وذلك لمعرفة مدى انطباقها على جريمة الاحتيال الإلكتروني، كما وعمدت هذه الدراسة إلى تسليط الضوء على محل تلك الجريمة (المال) لمعرفة وفهم ماهية هذا المال وطبيعته في جريمة الاحتيال الإلكتروني، حول مدى تصنيفه مالاً مادياً أم مالاً معلوماتياً، وتعددت الآراء الفقهية بهذا الشأن، وقد توصلت هذه الدراسة إلى جملة من النتائج كانت أبرزها؛ أنَّ المال محل جريمة الاحتيال الإلكتروني هو مال معلوماتي ينطوي على قيمة، هذا بالإضافة إلى أن القرار بقانون رقم (10) لسنة 2018م وتعديلاته الساري في الضفة الغربية وقطاع غزة؛ جرّم الاحتيال الإلكتروني وعاقب عليه بنص جزائي، كما خرجت بتوصيات كانت أهمها: على المجلس التشريعي الفلسطيني في قطاع غزة إقرار وتطبيق القرار بقانون رقم (10) لسنة 2018م وتعديلاته بشأن الجرائم الإلكترونية، وجعله سارياً قانونياً وواقعياً؛ لأنه عالج قضايا الاحتيال الإلكتروني.*

***الكلمات المفتاحية: شبكة الإنترنت، المال المعلوماتي، الجريمة الإلكترونية، التسويق الشبكي.***

## المقدمة

لقد شاع استخدام وسائل تقنية المعلومات وتزايد الاعتماد على نظم المعلومات وشبكات الحاسوب إلى الحد الذي أصبح يشمل جميع مجالات الحياة المعاصرة من تجارة واقتصاد وعلوم وغيرها، وعلى الرغم من إيجابيات هذه التقنية العالية، مثل: إرسال واستقبال البيانات بسهولة، وسهولة التواصل مع الأشخاص، التعلّم عن بُعد، إلا أنه كان لها انعكاس سلبي يتمثل في إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبصورة قد تضر بالمجتمع ككل، وقد أدى هذا التطور الهائل إلى ظهور طائفة جديدة من الجرائم نتيجة هذا الاستخدام كالدخول غير المرخص به إلى أنظمة الحاسوب والشبكات والاستيلاء على المعلومات أو إتلافها عبر تقنيات الفيروسات، واختراق المواقع للتجسس على الآخرين، واختراق المواقع وسرقة محتوى الملفات أو تغيير بياناتها، وسرقة بطاقات الائتمان وغيرها، وظهور طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية (المومني، 2010)، وبشكل خاص بظهور البنوك الإلكترونية والتحويل الإلكتروني للأموال تضاعفت نسب الاحتيال الإلكتروني، إذ يتم استخدام الأنظمة المعلوماتية في المصارف والمؤسسات النقدية لعمليات التحويل بشكل يومي، إلا أن الإجراءات الأمنية التي تحيط بالمعلومات يوجد بها ثغرات كثيرة يتم استغلالها من قبل المخترقين لتحقيق أهدافهم الإجرامية حيث يستعملون عدة وسائل للاحتيال الإلكتروني منها الغش باستخدام بطاقة الائتمان من قبل حاملها أو بواسطة الغير، والاحتيال التجاري الإلكتروني، وأيضاً غسيل الأموال، فمن خلال هذه الدراسة سيتم التركيز على جريمة الاحتيال الإلكتروني بالتحديد في ظل وجود النصوص القانونية بصورتها العادية الواردة في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م السارية في قطاع غزة، وكذا قانون العقوبات الأردني رقم (16) لسنة 1960م المُطبق في الضفة الغربية، بالإضافة إلى القوانين المكملة والخاصة كالقرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته الساري في الضفة الغربية، وقانون الاتصالات السلكية واللاسلكية الفلسطيني رقم (3) لسنة 1996م.

### إشكالية الدراسة

مع زيادة الحاجة لاستخدام الحاسوب الآلي وشبكة الإنترنت زاد عدد مستخدمي هذه الشبكة وتبعاً لذلك ازداد عدد المحتالين مع تعدد دوافعهم وأهدافهم في ارتكاب عمليات الاحتيال، ونجاح هؤلاء في تحقيق مكاسبهم؛ يعود لقلة برامج الحماية وعدم متابعة تطور التقنيات الحديثة للمستخدم في عمليات الحماية. مما أوجب تطوير الأنظمة التشريعية الجنائية الوطنية بتشريعات تحوطية وقائية تماثل الذكاء الإجرامي بحيث تعكس فيه الدقة الواجبة على المستوى القانوني، وسائر جوانب تلك التقنيات وأبعادها الجديدة.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

**والسؤال الرئيس هو:** كيف واجه المشرع الجنائي الفلسطيني جريمة الاحتيال الإلكتروني في ظل التشريعات الجنائية الوطنية؟

**تجيب الدراسة على التساؤلات التالية:**

- ما مفهوم الاحتيال الإلكتروني، وما خصائصه؟
- ما الفروقات بين جريمة الاحتيال العادية وجريمة الاحتيال الإلكترونية؟
- ما هو البنيان القانوني لجريمة الاحتيال الإلكتروني؟
- ما طرق ارتكاب الاحتيال الإلكتروني؟
- ما هو موقف المُشرِّع الفلسطيني من جريمة الاحتيال، وكيف عالجها في إطار تشريعاته؟

## أهمية الدراسة

- تكمن في بيان البنيان القانوني لجريمة الاحتيال الإلكتروني، ومقارنتها بجريمة الاحتيال بصورتها التقليدية.
- التعرف على طرقها للحد من وقوعها، ونشر الوعي بين أفراد المجتمع عن كيفية التعامل مع هذا النوع من الجرائم.
- بيان المرجعية القانونية الفلسطينية لجريمة الاحتيال الإلكتروني فالمُشرع الجنائي الفلسطيني لم يتحوط في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م الساري في قطاع غزة من تلك الجريمة، فهو بحاجة إلى تعديلات تضاف إليه بحيث تُجرَّم فيها الجرائم الالكترونية حديثة النشأة، كجريمة الاحتيال الإلكتروني بالإضافة لقانون العقوبات الأردني رقم (16) لسنة 1960م المُطبق في الضفة الغربية، وكل ما في الأمر أنه تم سن تشريع مُكمّل، كالقرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته الساري قانوناً في الضفة الغربية وقطاع غزة دون التطبيق الفعلي له في قطاع غزة، وكذا تشريع خاص كالقرار بقانون رقم (15) لسنة 2017م، بشأن المعاملات الإلكترونية.
- شُحّ وقلة وجود أحكام قضائية فلسطينية بصدد هذا الموضوع في كل من الضفة الغربية وقطاع غزة سواء؛ ذلك نتيجة لحداثة موضوع الدراسة وتنظيمه في التشريع الفلسطيني.

## أهداف الدراسة

- التعرف على جريمة الاحتيال الإلكتروني والسمات التي تتميّز بها أركانها باعتبارها جريمة مستحدثة نسبياً.
- بيان موقف المشرع الجنائي الفلسطيني بالنسبة لهذه الجريمة العصرية، من خلال ما جاءت به التشريعات الوطنية (الفلسطينية) في مكافحة الجرائم الإلكترونية بوجه عام، ومكافحة جريمة الاحتيال الإلكتروني بوجه خاص.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

## الدراسات السابقة

سنتناول فيما يلي بعض الدراسات السابقة ذات الصلة على النحو التالي:

- **دراسة أبو سيدو (2022). جريمة الاحتيال الإلكتروني في التشريع الفلسطيني،** وقد تناولت الباحثة موضوع جريمة الاحتيال الإلكتروني في التشريع الفلسطيني، ذلك بتعريف جريمة الاحتيال الإلكتروني، وبيان خصائصها، وتمييزها عن جريمة الاحتيال بصورتها التقليدية، والتطرق إلى صورها، كما تناولت الباحثة هذه الجريمة في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م وتعديلاته لسنة 2009م المُطبق في قطاع غزة، وكذا القرار بقانون رقم (10) لسنة 2018م، ومشروع القانون بشأن الجرائم الإلكترونية لسنة 2019م، وبحثت الباحثة في أركان جريمة الاحتيال الإلكتروني، وختمت بالعقوبات المقررة لجريمة الاحتيال الإلكتروني في التشريع الفلسطيني.

على خلاف ذلك دراستنا هذه سوف تتمركز بشكل أساسي حول طبيعة المال محل جريمة الاحتيال الإلكتروني، مع توضيح مفهوم تلك الجريمة، وبيان موقف المشرع الفلسطيني بشأن هذه الجريمة، وبالخصوص ما جاء به المشرع في القرار بقانون رقم (10) لسنة 2018م وتعديلاته لسنة 2020م، ولسنة 2021م، بشأن الجرائم الإلكترونية، المُطبق في الضفة الغربية.

- **دراسة العفيفي (2013). الجرائم الإلكترونية في التشريع الفلسطيني،** حيث قام الباحث بتناول موضوع الجرائم الإلكترونية في التشريع الفلسطيني، وذلك بتعريف الجريمة الإلكترونية، وبيان صورها وطبيعتها، وتطرق الباحث لصورها بشكل عام الواردة في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م مع تعديلاته لسنة 2009م المطبق في قطاع غزة، والجرائم الإلكترونية التي أوردها المشرع الأردني في قانون جرائم أنظمة المعلومات رقم (30) لسنة 2010م، ومن ثم أوضحت هذه الدراسة أركان جريمة الاحتيال الإلكتروني، والجزاء الجنائي المترتب على ارتكابها، وأوضح الباحث النقص الحاصل في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م وتعديلاته لسنة 2009م، وختم الباحث دراسته ببيان القواعد الإجرائية التي تمر بها الدعوى الجزائية في الجرائم الإلكترونية، وخرج بتوصية بأنه لا بُدَّ وأن يتم سن تشريع مستقل يكافح الجرائم الإلكترونية بصورة عامة.

أما في إطار دراستنا هذه فستخص جريمة الاحتيال الإلكتروني في التشريع الجنائي الفلسطيني، وبيان مفهومها وصورها وتميزها عن جريمة الاحتيال الإلكتروني، بداية بقانون العقوبات الفلسطيني رقم (74) لسنة 1936م وتعديلاته لسنة 2009م، المطبق في قطاع غزة، وقانون العقوبات الأردني (16) لسنة 1960م المطبق في الضفة الغربية، والقرار بقانون رقم (10) لسنة 2018م وتعديلاته لسنة 2020م، ولسنة 2021م، بشأن الجرائم الإلكترونية المطبق في الضفة الغربية، الذي تناول غالبية الجرائم الإلكترونية وتقرير العقوبات على ارتكابها، ومن ضمنها جريمة الاحتيال الإلكتروني.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

### منهجية الدراسة

قامت الباحثة باتباع المنهج التحليلي في مفردات هذه الدراسة، وذلك باستقراء وتحليل النصوص القانونية في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م المطبق في قطاع غزة، بالإضافة لقانون العقوبات الأردني رقم (16) لسنة 1960م المُطبق في الضفة الغربية، وكذا النصوص الجزائية المكملة ذات الشأن بموضوع الدراسة السارية في الضفة الغربية وقطاع غزة، كالقرار بقانون رقم (10) لسنة 2018م وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

## المبحث الأول

### ماهية جريمة الاحتيال الإلكتروني

إن الثورة التكنولوجية وما نجم عنها من ظهور البنوك الإلكترونية والتحويل الإلكتروني للأموال ضاعفت من إمكانية ارتكاب الجرائم الإلكترونية وبصفة خاصة الاحتيال الإلكتروني، فالمصارف والمؤسسات المالية في الوقت الراهن يرتكز عملها بشكل أساس على استخدام الأنظمة الإلكترونية لإجراء التحويلات المالية التي تتم بطرق إلكترونية ومبالغ طائلة.

### المطلب الأول: مفهوم جريمة الاحتيال الإلكتروني

يُعدّ الاحتيال الإلكتروني صورة من صور الاحتيال بوجه عام، إلا أنه يمتاز بطبيعة خاصة لارتباطه الوثيق بالحاسبات الآلية وتكنولوجيا المعلومات، وتحاول الباحثة في هذا المطلب التعرف على هذه الجريمة وذلك في فرعين، نبين في الفرع الأول: تعريف شبكة الإنترنت والجريمة الالكترونية، ونوضح في الفرع الثاني: تعريف الاحتيال الالكتروني.

#### الفرع الأول: تعريف شبكة الإنترنت والجريمة الإلكترونية

تُعرّف شبكة الإنترنت بأنها: «عدد الوحدات المرابطة فيما بينها من خلال وسائل الاتصال المختلفة، تقوم بتبادل المعلومات فيما بينها والاشتراك بالمصادر عبر شبكة الإنترنت» (نصيرات، 2018).

وهناك من وصفها بأنها أداة للربط والاتصال بين مختلف شعوب العالم، تشكّل أداة لارتكاب الجريمة، أو محلاً لها، وذلك بإساءة استخدامها واستغلالها على نحو غير مشروع، مما أدى إلى ظهور طائفة جديدة من الجرائم، عُرِفت بالجريمة المعلوماتية (الشوابكة، 2006).

بدايةً لا بد من الإشارة إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها: فهناك من يطلق عليها ظاهرة «الغش المعلوماتي»، وبعض آخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها «بالجريمة المعلوماتية» (الشوا، 1994).

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

عرَّف الخبير الأمريكي «باركر» الجريمة المعلوماتية من وجهة نظره «كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل» (الشوا، 1994).

كما عرفت بأنها «مجموعة العناصر المتداخلة المؤثرة في طبيعة الأفعال الإجرامية المرتكبة والمتصلة اتصالاً وثيقاً بالحاسب الآلي والمعلوماتية» (سكيكر، 2010).

وهناك من عرفها بأنها «الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني» (أبو حجاج، 2010).

وهناك من يرى بأن الجريمة الإلكترونية: «هي نشاط غير مشروع، يتخذ نظم المعلومات ووسائل الاتصال الحديث أداة له، يصدر عن إرادة آثمة، ويقرر له القانون عقوبة أو تدبير احترازي» (القحطاني، 2016).

وفي حدود ما اطلعت عليه الباحثة ترى أن المشرع الفلسطيني لم يتضمن تعريفاً صريحاً للجريمة الإلكترونية في تشريعاته الفلسطينية.

**الفرع الثاني: تعريف الاحتيال الإلكتروني**

يأتي الاحتيال في اللغة بمعنى طلب الحيلة، ويقصد به اصطلاحاً بوجه عام الغش والخداع الذي يعمد إليه شخص للحصول من الغير، بدون حق على فائدة أو ميزة (عبابسة، 2016).

وعرف البعض الاحتيال الإلكتروني بأنه: «كافة وسائل الاحتيال عن طريق الإنترنت بهدف الاستيلاء على المعلومات وأموال المجني عليه بطريقة غير شرعية» (سيار، 2019).

كما عرف الاحتيال الإلكتروني: «فعل غير مشروع ينتهج منهج الحوسبة للحصول على ربح مادي غير مشروع وإلحاق الضرر بالغير» (أبو سيدو، 2022).

يُفهم من التعريفات السابقة، بأن الاحتيال الإلكتروني عبارة عن انتهاج مسلك غير مشروع بواسطة استخدام الجهاز الإلكتروني بغية الاستيلاء على أموال ذات قيمة مادية من الغير بطريق الاحتيال، من أجل تملكها.

والاحتيال لا يقع على الشخص الطبيعي فقط، بل أنه من المسلم به صلاحية الشخص المعنوي لاعتباره مجنياً عليه، فالشركات والمؤسسات العامة أو الخاصة هي من الأشخاص المعنوية في نظر القانون، وحيث الحاسوب والشبكات الداخلية تُعدّ للمنشأة من فروع الشركة أو المؤسسة، فإنها تكون صالحة لوقوع فعل الخداع أو التحايل عليها (الشوابكة، 2006).

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

## المطلب الثاني: خصائص جريمة الاحتيال الإلكتروني وأساليب تنفيذها

نظراً للبيئة الخاصة التي تتصف بها جريمة الاحتيال الإلكتروني، من استخدام وسائل تقنية إلكترونية حديثة ومتطورة عند ارتكابها، مما جعلها تتميز بالعديد من السمات والخصائص عن نظيرتها جريمة الاحتيال العادية. وعلى ذلك سيتم تناول هذا المطلب في فرعين، الفرع الأول: خصائص جريمة الاحتيال الإلكتروني، والفرع الثاني: أساليب تنفيذ جرائم الاحتيال الإلكتروني.

### الفرع الأول: خصائص جريمة الاحتيال الإلكتروني

تتميز جريمة الاحتيال الإلكتروني بمجموعة من الخصائص، تتمثل فيما يلي (الجبوري،2014):

- جريمة الاحتيال هي جريمة التعدي على الملكية، وعلى المال، بخلاف جرائم القتل فالفاعل يخدع المجني عليه لحمله على تسليم مال أو ما في حكمه، ويكون المحرك الرئيس لأنشطة احتيال الجهاز الإلكتروني، هو تحقيق الكسب المالي.
- إن جريمة الاحتيال الإلكتروني ترتكب عبر شبكة الإنترنت وعبر الوسائل الإلكترونية الحديثة، أي أنها ترتكب في بيئة إلكترونية بحتة، وتتطور أساليب ارتكابها بتطور تلك الوسائل وبحداثتها (شريف، 2019).
- تعتبر من الجرائم الهادئة فلا تتطلب القوة أو العنف أو السلاح (بوشعرة وموساوي، 2018).
- جريمة الاحتيال من جرائم السلوك متعدد الحدث، وذلك كون الفاعل يستخدم سلوكاً مادياً ذا مضمون نفسي يتمثل في أساليب الاحتيال التي يلجأ إليها للتأثير على إرادة الشخص المخاطب بهذه الأساليب.
- إخفاء الجريمة إذ يصعب كشفها وإثباتها بسبب غياب الدليل المادي وسهولة طمس ومحو الدليل، كما أنه يصعب الاحتفاظ الفني بآثارها إن وجدت، وتحتاج لخبرة فنية سيما يتعذر على المحقق التقليدي التعامل معها ووصولها، وضعف ثقافته اتجاه تلك الجريمة؛ لأنها تعتمد غالباً على قمة الذكاء المصحوب بالخديعة والتضليل بدس روابط وهمية أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل (طالة، وسلام، 2020).
- غالباً ما يكون مرتكبها واعياً وذكياً ومتعلماً وخبيراً بالأجهزة المحوسبة.
- التنفيذ عن بُعد حيث لا يتطلب من الفاعل التواجد في مسرح الجريمة.
- إنها من الجرائم الواقعة على حرية الإرادة، أي تصيب إرادة المجني عليه بعيب الرضا؛ لأنه بدلاً من أن يتصرف المجني عليه بإرادته الحرة، ويكون على بينة من أمره، ووعي بتصرفاته يضلله المحتال ويغرر به.
- الاحتيال جريمة لا تتطلب الاتصال المادي بين المجرم والضحية، ويظهر ذلك من خلال رسائل البريد الإلكتروني، كأن يتم إرسال رسائل تحيل وتغرير عبر الاستفادة من القدرة على إخفاء الهوية (شريف، 2019).
- عابرة للحدود حيث لا وطن لها فقد ترتكب خارج إقليم الدولة وبوسائل تقنية حديثة، ومتطورة.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

- تتميز هذه الجريمة بسهولة ارتكابها فهي لا تتطلب أي مجهود بدني يذكر لربما تتطلب الضغط على مفتاح معين في الجهاز لتنفيذها، بخلاف الجريمة التقليدية التي تتطلب مجهود بدني، مثل: القتل، والاغتصاب، فالجرائم الإلكترونية بصورة عامة لا تتطلب سوى علم كافي بالجوانب الفنية والتقنية للأجهزة المحوسبة.

**الفرع الثاني: أساليب تنفيذ جرائم الاحتيال الإلكتروني**

تتطور أساليب الاحتيال الإلكتروني؛ نظراً لسرعة التطور الذي شهدته تكنولوجيا المعلومات، فكلما زادت التقنية والحداثة تطورت وسائل الاحتيال وأساليبه، وعليه يستخدم مجرمو الإنترنت مجموعة متنوعة من أساليب الهجوم والاستراتيجيات لارتكاب جرائم الاحتيال الإلكتروني.

يتم تنفيذ هذه الجرائم من خلال عدة أساليب أهمها (حنين، 2020):

- التلاعب حال إعداد وتطوير البرامج ويتم من خلال إجراء عدد من التعديلات القانونية أثناء تنفيذها لتصحيح أخطاء لم يتم من قبل اكتشافها أو إذا ما اقتضى الأمر تطوير تلك البرامج ففي هاتين المرحلتين يمكن لمرتكبي الجريمة إدخال بعض التعديلات غير المرخص بها؛ وذلك لتحقيق ما يصبون إليه من أهداف غير مشروعة (أهمها الحصول على الربح المادي بطريق الاستيلاء والتحايل).
- الاحتيال في العمل، ويتم عندما تقوم إحدى المؤسسات بعدم الالتزام بتقديم الحقائق أو إخفاء أمر من أجل الحصول على ميزة أو تحقيق مكسب (شريف، 2019).
- التصيد الإلكتروني، فهو تكتيك خبيث ينشئ فيه مجرمو الإنترنت رسائل بريد إلكتروني أو رسائل نصية أو مواقع ويب خادعة تُقلّد جهات موثوقة لاستخلاص معلومات حساسة، كدفعهم إلى مشاركة البيانات الشخصية وبيانات اعتماد تسجيل والتفاصيل المالية. غالباً ما تستغل هذه الهجمات نقاط ضعف بشرية، معتمدة على نقر الأفراد على روابط خبيثة أو تقديمهم تفاصيل سرية، ظانين أنهم يتفاعلون مع مصدر موثوق.
- عمليات الاحتيال في التسوق عبر الإنترنت، وتستغل بإنشاء متاجر إلكترونية احتيالية أو التلاعب بالمنصات القائمة. وذلك بخداع المحتالون المستهلكين لشراء منتجات وهمية أو مقلدة، كبيع سلع فاخرة مقلدة أو بيع تذاكر مزيفة؛ مما يؤدي إلى خسائر مادية وخيبة أمل للمشترين غير المنتبهين (حجاج، 2022). وهذه الحالة (الأسواق الإلكترونية) من أكثر الوسائل الشائعة لعمليات الاحتيال.
- الاحتيال بالاستخدام غير المشروع لبطاقات (الائتمان) الدفع الإلكتروني، كأن يقوم الجاني المحتال بتقديم أوراق أو مستندات منسوبة إلى الغير مع البطاقة المزورة؛ وذلك لإيهام التاجر بأنه الحامل الشرعي لها، وبذلك يحصل الجاني المُحتال على ما يريد من سلع وخدمات (أبو سيدو، 2022). وتُمكّن تقنيات مثل أجهزة التجسس في الصراف الآلي أو نقاط البيع مجرمي الإنترنت من الحصول على معلومات البطاقات.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

- الاحتيال على المواقع الإلكتروني، ويقع الاحتيال فيها بالدخول غير المصرح به من قبل الغير والمساس بالسرية التي فيها، ومنها موقع باي بال (PAY PAL) وهو موقع عالمي وأكثر شهرة، فهو يشمل أكثر من خدمة إلكترونية، وحيث يستخدم كوسيلة للدفع، ووسيلة إيداع لاستقبال الأموال. وتم الاعتماد على استخدامها بشكل كبير في قطاع غزة بالأوقات الراهنة في ظل استمرار حرب الإبادة الجماعية التي يواجهها شعب غزة من قبل العدوان الإسرائيلي على قطاع غزة؛ مما سهلت من عملية تداول الأموال فيما بين الأشخاص داخل القطاع وخارجه، وساعدت في عملية الشراء (التسوق الإلكتروني عبر الإنترنت) والدفع الإلكتروني؛ ذلك لعدم توافر السيولة من الأموال في هذا البلد المُحاصر. فهذا من واقع حالنا في قطاع غزة المكلوم.
- الاحتيال على الحوالات المصرفية، ونظام الحوالات المصرفية الإلكترونية يتميز بسهولة نقله وتحويله للمبالغ المالية من حساب بنكي إلى حساب بنكي آخر وتتم عملية التحويل إلكترونياً، عبر أجهزة التقنية الحديثة. غالباً ما تقع عملية الاحتيال على الحوالات المصرفية من خلال اختراق الحواسيب الشخصية للعملاء، المتعاملين مع البنوك، ومن ثم الوصول إلى البيانات المصرفية، وأكواد الحوالات المصرفية وأسرارها، لغاية استخدامها في الوصول إلى الحوالة والاستيلاء عليها (أبو سيدو، 2022). ويُعدّ من أكثر صور الاحتيال الإلكتروني إضراراً وأخطرها على الأنشطة الاقتصادية والاقتصاد ككل، يتمثل في أنظمة التحويل الإلكتروني للأموال والودائع المصرفية، أو ما يقع على الأموال الإلكترونية أو الإفتراضية؛ وذلك نظراً لضخامة حجم ما يتم تداوله عبر هذه الأنظمة من الأموال، واختزالها للزمن اللازم لإتمام التعاملات والتحويلات المالية، وكذلك الزمن اللازم لسلب المال بالاحتيال في ثوان، مما ينجم عن عمليات الاحتيال خسائر فادحة (شريف، 2019).
- عمليات الاحتيال الودية، وهي عملية يظهر فيها المحتال وكأنه الضحية وليس الجاني، حيث يقوم بشراء بعض المنتجات إلكترونياً، وبمجردِ أن يتم خصم المبلغ من رصيده البنكي، يقوم بالاتصال اعتراضاً على عملية الخصم، مدعياً بتعرض حسابه للسرقة، وغالباً ما ينجح المحتال بإقناع البنك بتعرض حسابه للسرقة؛ ويتمكن من استرداد المال المدفوع بجانب احتفاظه بالبضائع (حجاج، 2022).
- هناك ما يسمى بالتسويق الشبكي وهو نوع من تسويق المنتجات أو الخدمات مبني على التسويق التواصلي حيث يقوم المستهلك بدعوة مستهلكين آخرين لشراء المنتج (سلعة) في مقابل عمولة، ويحصل أيضاً المستهلك الأول على نسبة من العمولة في حالة قيام العملاء ببيع المنتج لآخرين بحيث يصبح المستهلك على قمة هرم ويصبح لديهِ شبكة من الزبائن المشتركين بأسفله، أو عدد من العملاء قام بالشراء عن طريقهم، فالمنتج الذي تسوقهُ هذهِ الشركات مجرد ستار وذريعة للحصول على العمولات والأرباح. هذه الطريقة في الآونة الاخيرة تحولت إلى طريقة لتحقيق الأرباح فقط ولم تعد مجرد وسيلة من وسائل التسويق، مما جعلها محط انتقاد الكثيرين نظراً لإضافة منتجات وسلع لا قيمة لها أو زائدة عن قيمتها

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الأصلية، ويلجأ المستخدم لشرائها ليس بهدف الاستفادة منها بل من أجل السعي وراء الربح، مما يجعل المستخدمون على قمة الهرم يحققون أرباح خيالية بينما القاعدة الأكبر من العملاء في هذه الطريقة قد لا يحرزوا أي مكسب في النهاية (ويكيبيديا، 2025)، وهذا النظام يعتمد بالأساس على أن لكل شخص في الشركة ليستطيع تحقيق أرباح بإحضار عدد من 2 أشخاص لدخول الشركة ودفع رأس مال متفاوت من 10000 دولار إلى 30000 دولار ويشترط فيها الربح. وتعتبر شركة كيونت qnet»» من الشركات التي تتبع هذا النظام (التنظيم الهرمي) ودرج في قطاع غزة على تسميته بنظام الشجرة. بحيث الربح الأكبر يكون لأصحاب الشركة والآخرين ربحهم والعائد لهم بسيط جداً، وكلما زاد عدد الأشخاص واستقطابهم بعضهم لبعض في الشركة كلما زاد وارتفعت نسبة أرباح أصحاب الشركة (من قاموا بإنشاء الشركة). وهي مُجرّمة في دول العالم وتعتبر احتيال.

لقد أشار موقع اليوم السابع الإلكتروني، إلى أن هناك 6 أكاذيب تستخدمها حالياً شركات التسويق الشبكي لاصطياد ضحاياها تتمثل في: «كذبة الربح السريع، وتحقيق الحرية المالية، واستغلال الظروف الصعبة للناس والشباب، وشماعة المنتج، ومصداقية وسمعة الشركة، وأخيراً الادعاء بأن المال من هذا العمل قانوني وحلال شرعاً» (اليوم السابع، 2020).

**المطلب الثالث: تمييز جريمة الاحتيال الإلكتروني عن الاحتيال في صورته العادية**

توجد الكثير من القواسم المشتركة بين جريمة الاحتيال الإلكتروني وبين جريمة الاحتيال التقليدية، فكلاهما يعتمد على وسائل الغش والخداع، والجريمتان من الجرائم الواقعة على الأموال، وغاية الجاني تتمثل في الاستيلاء على مال الغير بنية تملكه وحرمان صاحبه منه.

ولهذا فالكثير من الدول لم تشرع نصوصاً قانونية تجرم وتعاقب مرتكبي جريمة الاحتيال الإلكتروني؛ لأن القضاء الجنائي في هذه الدول وسَّع من تفسيره للنصوص القانونية الخاصة بجريمة الاحتيال العادية وجعلها تمتد لتشمل هذه الجريمة، وهذا ما أخذت به كافة الدول الانجلوسكسونية كبريطانيا وأستراليا وكندا، كما ظهرت اتفاقيات على المستوى الإقليمي لمواجهة جرائم الإنترنت مثل الاتفاقية الأوروبية حول الجريمة الافتراضية، والقانون العربي الاسترشادي لجرائم المعلومات على المستوى العربي (نصيرات، 2018).

جريمة الاحتيال بصورتها التقليدية: «هو الحصول على مال منقول مملوك للغير إما باستعمال طرق احتيالية مدعمة بمظاهر خارجية من شأنها خداع المجني عليه في واقعة تنتمي إلى الماضي أو الحاضر، وإما باتخاذ اسم كاذب أو صفة غير صحيحة بما يحمله على الاعتقاد بصدق ما يدعيه الجاني وتسليم المال نتيجة لذلك» (الكرد، 2008).

وتتميز جريمة الاحتيال الإلكتروني بأنها ترتكب باستخدام الحاسب الآلي والشبكات المعلوماتية الدولية والهواتف الذكية النقالة وما شابه ذلك، والجاني (مرتكبها) يكون على دراية وخبرة بتلك

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الاستخدامات، وكأن الحاسب الآلي هنا يشكّل أداة لارتكاب تلك الجريمة أو وسيلة لارتكابها، يمكن لأي شخص الولوج إليها وتنفيذ جريمته. وتعتبر جريمة الاحتيال الإلكتروني من أكثر الجرائم تطوراً حيث إن البعض من هؤلاء المجرمين يعمل بذكاء حاد، ويسعى في خلق حيل وطرق تتناسب مع التطورات والاحتياطات المبذولة حتى ظهرت طرق متعددة ومتنوعة للاحتيال الإلكتروني؛ لأجل تمرير أعمالهم الإجرامية تحت غطاء يوهمون به الآخرين بأن أعمالهم مشروعة.

لا تقف جريمة الاحتيال التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية المستحدثة عند الطبيعة الخاصة بالأفعال التي تتحقق بها هذه الجريمة، وإنما تمتد هذه الطبيعة لتشمل أيضاً البعد العالمي لهذا النوع من الجرائم، فإذا كانت شبكة الاتصالات من بعد ذات نطاق عالمي لا يتقيد بحدود دولة معينة فإنه يتصور تبعاً لذلك أن تتميز الجرائم التي تقع عليها، أو تقع بسببها بالطبيعة العالمية، فيستطيع أي شخص في دولة معينة الدخول إلى شبكة المعلومات الدولية، ويمكنه ارتكاب نشاطه الإجرامي في دولة أخرى أو مجموعة من الدول الأخرى (نصيرات، 2018).

تعتبر طبيعة المال في جريمة الاحتيال المادية أو المعنوية سواء، وتقع على العقارات بصورة غير مباشرة (مستندات) كما تقع على المنقولات، أما بالنسبة لطبيعة المال في جريمة الاحتيال الإلكتروني فالأمر مختلف، إذ طبيعة المال اختلفت فيه الآراء الفقهية وسيتم الحديث بشأنها في عنصر المحل للركن المادي لجريمة الاحتيال الإلكتروني في المطلب الأول من المبحث الثاني في هذه الدراسة.

ترى الباحثة أن الفارق الجوهري بين جريمة الاحتيال التقليدية وجريمة الاحتيال الإلكترونية؛ ينحصر في الأسلوب الإجرامي فقط، بحيث بعد أن كانت الجريمة تتم بطريقة تقليدية؛ أصبحت تقترف في ظل التطور التكنولوجي السريع بأسلوب آخر حديث.

## المبحث الثاني

### أركان جريمة الاحتيال الإلكتروني (البنيان القانوني لها)

بدايةً لقد اختلف الفقه الجنائي حول أركان الجريمة المكونة لها بصورة عامة، فبعض الفقه ذهب إلى أن الأركان العامة للجريمة تتمثل في الركن الشرعي ويقصد به توفر نص التجريم الواجب التطبيق على ارتكاب الفعل غير المشروع، الركن المادي ويقصد به المظهر المادي للجريمة، ويتكون من نشاط الفاعل والنتيجة الإجرامية التي يحققها بنشاطه وعلاقة السببية بينهما، والركن المعنوي وهو ذلك الجانب من نشاط الفاعل الذي يكمن في نفسيته (أبو عامر، 1993). ورأي فقهي آخر يرى أن العنصر الشرعي لا يدخل في تكوين الجريمة، والقول بغير ذلك لا يتفق مع المنطق؛ لأن معناه إدخال الكل في الجزء، فالنص يخلق الجريمة، ولا يتصور اعتبار الخالق عنصر فيما

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

يخلق، وهذا ما أخذ به غالبية الفقه الجنائي (أحمد، 2019). وعلى ذلك ستتناول الباحثة أركان جريمة الاحتيال الإلكتروني ضمن ثلاثة مطالب على النحو الآتي: المطلب الأول ويشمل الركن الشرعي، والمطلب الثاني ويشمل الركن المادي، والمطلب الثالث ويشمل الركن المعنوي.

## المطلب الأول: الركن الشرعي

لقد ظهرت الحاجة إلى تجريم الاحتيال الإلكتروني في التزايد المستمر في استعمال أنظمة الحاسوب وما ارتبط بذلك من تزايد في الجريمة الإلكترونية بصفة عامة وفي الاحتيال الإلكتروني بصفة خاصة باعتباره واحداً من أهم صور هذه الجريمة، ومع صعوبة تطبيق النصوص التقليدية؛ كان باتجاه بعض التشريعات إلى إفراد نصوص لتجريم الاحتيال الإلكتروني، سواء أكان التجريم بنص عام، أم كان بتناول بعض صور الاحتيال الإلكتروني دون البعض الآخر (عبابسة، 2016). وعليه سوف يتم تقسيم هذا المطلب إلى فرعين: الفرع الأول، الاحتيال الإلكتروني في التشريع الفلسطيني، والفرع الثاني، الاحتيال الإلكتروني في القضاء الفلسطيني.

### الفرع الأول: الاحتيال الإلكتروني في التشريع الفلسطيني

بالنظر إلى التشريعات الجنائية الفلسطينية ومنها قانون العقوبات الفلسطيني رقم (74) لسنة 1936م المطبق في قطاع غزة، وكذا قانون العقوبات الأردني رقم (16) لسنة 1960م المطبق في الضفة الغربية، كون هذه القوانين تم وضعها قبل ظهور الإنترنت والتكنولوجيا الحديثة؛ فإنه لا توجد في فحواه نصوص جزائية تنظم جريمة الاحتيال الإلكتروني بصورة مفصلة ومواكبة للحداثة والتطور ومانعة للجدال بشأن طبيعة أركانها، إلا أن أصدر المشرّع الفلسطيني قانون الاتصالات السلكية واللاسلكية الفلسطيني رقم (3) لسنة 1996م، الذي جاء من أجل ضبط وتنظيم قطاع الاتصالات في فلسطين، وحيث اشتمل على مواد لا تتحدث بصورة مباشرة عن الاحتيال، أما بالنسبة لقانون رقم (3) لسنة 2009م والمعدل لقانون العقوبات الفلسطيني رقم (74) لسنة 1936م المطبق في قطاع غزة، جاء بتنظيم الجرائم الإلكترونية ومع ذلك لم يشمل جميعها كما هو الحال بالنسبة لجريمة الاحتيال الإلكتروني التي لم ينظمها ذلك القانون، وعليه ترى الباحثة أنَّ المشرع لم يكُنْ موفقاً في تصنيف الجرائم الإلكترونية التي يعاقب عليها؛ وذلك لعدم النص التشريعي على كافة الجرائم الإلكترونية، فالمشرع نص هنا على الجرائم الأكثر وقوعاً، ولم يتطرق إلى باقي الجرائم الإلكترونية، واقتصر الأمر على صدور قرارات بقانون تتعلق بالجرائم الإلكترونية والمعاملات الإلكترونية، ومنها قرار بقانون رقم (15) لسنة 2017م، بشأن المعاملات الإلكترونية والذي بالنظر إليه نجد أنه لا يشتمل على أي نص يتحدث فيه عن الاحتيال الإلكتروني.

بدايةً سنواجه بعض المعوقات في هذا الأمر، فالمبدأ الأساس الذي يحكم القانون الجنائي هو مبدأ شرعية الجرائم والعقوبات، حيث لا جريمة ولا عقوبة إلا بنص صريح (القانون الأساسي الفلسطيني، 2003)، بالإضافة إلى حظر القياس في النصوص التجريمية الموضوعية فهو بمثابة

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

عائق أمام إمكانية إدراج الجرائم الإلكترونية بشكل عام ذات الطبيعة الخاصة ضمن النصوص التقليدية في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م، وكذا نصوص قانون العقوبات الأردني رقم (16) لسنة 1960م.

إلا أن هذا النوع من الجرائم (الاحتيال الإلكتروني) في التشريع الفلسطيني ورد ونظم «تنظيم ناقص» بموجب قرار بقانون رقم (10) لسنة 2018م وتعديلاته، والمتعلق بصورة عامة بشأن الجرائم الإلكترونية، في المادة (14) منه.

بدايةً لقد بيَّن في المادة (1) منه بأن المعلومات الإلكترونية: «كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها».

كما أشار إلى أن الاختراق: «الدخول غير المصرح به أو غير المشروع لنظم المعلومات أو الشبكة الإلكترونية» (المادة (1) من قرار بقانون رقم (10) لسنة 2018).

ولقد بيّن وحدد عقوبات للأفعال المجرمة والمتعلقة بتلك الجرائم الإلكترونية وجعل عقوبة الاحتيال الإلكتروني بالتحديد وذكرها في نص المادة (14) منه، بأن: «كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين» (المادة (14) من قرار بقانون رقم (10) لسنة 2018).

وهنا نلاحظ بأن المشرع الفلسطيني يوفر إطاراً قانونياً لمكافحة الاحتيال الإلكتروني، وتشمل العقوبات التي تهدف إلى ردع المجرمين المحتالين وحماية المجتمع، حيث جعل الحد الأدنى في عقوبة الحبس لمن يرتكب جريمة الاحتيال الإلكتروني سنة أو الغرامة، كما جعل الحد الأقصى بحسب ما جاء به في نص المادة (26) من ذات القانون خمس سنوات حبس ولها عقوبة تكميلية ألا وهي الغرامة. نصت المادة (26) القرار بقانون رقم (10) لسنة 2018م على أن: «كل من حاز بغرض الاستخدام جهازاً أو برنامجاً أو أي بيانات إلكترونية معدة أو كلمة سر أو تراميز دخول أو قدمها أو أنتجها أو وزعها أو استوردها أو صدرها أو روّج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً».

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وأن الأموال التي ذكرها كمحل للجريمة أموال معلوماتية بالمنطق (توقيع إلكتروني، بيانات إنشاء توقيع إلكتروني، منظومة إنشاء توقيع إلكتروني) وإن لم يتوسع المشرع هنا في طبيعية هذه الأموال بحيث تشمل البيانات المعلوماتية ومستندات إلكترونية وبرامج الحاسب الآلي فهو حصرها بمسائل الدفع الإلكتروني فقط، إلا أن طبيعة هذه الجريمة الخاصة «الاحتيال الإلكتروني»؛ تستدعي بأن تكون محلها أموال معلوماتية مغايرة لطبيعة المال في صورتها التقليدية والعادية. كما ترى الباحثة بأنه كان على المشرع تشديد العقوبات في حالة تلاعب الجاني بمبالغ مالية ضخمة؛ لتحقيق أكبر قدر من الردع للمجرمين.

كما نصت المادة (21) من القرار بقانون رقم (38) لسنة 2021م، المُعدل للقرار بقانون رقم (10) لسنة 2018م وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وجرائم المعلومات، بأنه: «كل من رخص له قام بغش أو خداع أو تضليل المشترك بأي طريقة كانت، أو الإثراء على حسابه دون مسوغ قانوني، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنتين، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً».

وفي قطاع غزة هذه التشريعات السابق ذكرها؛ غير مُطبقة وسارية المفعول واقعياً، إلا أنه في المقابل هي مطبقة في الشق الآخر من الوطن (الضفة الغربية). بناءً على ما سبق ولأن الأمر مقصور على شق دون الشق الآخر من الوطن؛ فإنه في قطاع غزة يُعالج هذا النوع من الجرائم استناداً لنص المادة (301) المُتحدث عن جريمة الاحتيال التقليدية من قانون العقوبات الفلسطيني رقم (74) لسنة 1936م، والذي وضعت قواعده ابتداءً لحماية الأموال ذات الطبيعة المادية الملموسة في الفضاء الخارجي الذي يتعذر معه حماية القيم غير المادية المتولدة عن المعلوماتية مما يستوجب بالضرورة صدور تشريع خاص في قطاع غزة يجرّم الجرائم الإلكترونية بصورة عامة ومنها الاحتيال الإلكتروني بحيث يتناسب وطبيعتها الخاصة؛ لمكافحة هذه الجرائم الحديثة ومنعاً من مخالفة مبدأين جوهرين في التشريع الجزائي وهما مبدأ لا جريمة ولا عقوبة إلا بنص (القانون الأساسي الفلسطيني، 2003)، ومبدأ عدم جواز القياس في النصوص التجريمية.

**الفرع الثاني: الاحتيال الإلكتروني في القضاء الفلسطيني**

لقد شاع في الآونة الأخيرة إرسال روابط إلكترونية من شركات وهمية للمجني عليهم حتَّى يوضع المال فيها كشركة جونسون فهي شركة وهمية وكذلك شركة instaforex، ومن ضمن الحالات التي مرَّت على نيابة جرائم الأموال عندنا في غزة، ومن خلال الاستجواب تبين حصولهم على مبلغ مليون دولار «الربح السريع» ومن حسابات حقيقية، ولكن لا تعطيهم أرباحهم كلها فقط جزء منها (مقابلة لدى عضو نيابة «وكيل نيابة جرائم الأموال»، 2021). كذلك الأمر حالة أخرى مرّت عليهم بأن امرأة قامت بدفع مبلغ 82 ألف دولار أمريكي تسلمتها الشركة المحتالة على مراحل،

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وتعطيهم أرباح بسيطة على مراحل متباعدة. وبالنسبة لخبرة الجاني، هناك شركات متخصصة تعرض للآخرين العامة دورات معينة فتعرض لهم آلية العمل لكن آلية عملهم غير مجرمة، وفي المقابل تجد دورات يتم تنفيذها على تطبيق zoom تقوم بها شركات وتكون عبارة عن محاضرات لمدة معينة وبالأخير يتضح أنها كلها كاذبة وتسمى (غسيل دماغ).

وتجدر الإشارة إلى ما هو مطبق في قطاع غزة في الحالات السباق ذكرها أعلاه، وما يشابهها من عمليات احتيال إلكتروني، فإنه يتم تطبيق نصوص الاحتيال التقليدية المنصوص عليها في قانون العقوبات الفلسطيني رقم (74) لسنة 1936م في لوائح الاتهام التي ترفعها النيابة للمحكمة المختصة أو المحكمة عند إصدارها للأحكام فالأمر سيان؛ للأسباب التي سبق وأن تم ذكرها. أما بالنسبة لما هو مطبق في الضفة الغربية، فإنه يتم تطبيق قانون الجرائم الإلكترونية رقم (10) لسنة 2018م وتعديلاته، وبالتحديد نص المادة (14) منه التي تتحدث عن الاحتيال الإلكتروني بصورة مباشرة.

في القضاء النظامي الفلسطيني حيث حصلت الباحثة في حدود ما اطلعت عليه على حكم صادر عن محكمة استئناف رام الله في فلسطين يفهم منه من أن هذه الحالات التي تم الحديث عنها، تمر وترفع للقضاء وتنظرها المحكمة المختصة وتطبق عليها نص المادة (14) من قرار بقانون رقم (10) لسنة 2018م، والمواد المرتبطة بالجرائم الإلكترونية.

استئناف حكم صادر عن محكمة بداية رام الله والصادر بتاريخ 18-11-2018م، في القضية رقم 2014/993 والذي جاء فيه «وبالنسبة لمحل المدعي هناك اعتراضات على الحساب حيث كان الاعتراض على أن العمليات مزورة وأن البطاقات التي تم استخدامها على الماكنة هي بطاقات أجنبية وأن قيمة الحركات التي تمت لا تتناسب مع طبيعة تجارة المدعي.. وقد أبلغنا كل من ماستر كارد وفيزا أن هناك عمليات احتيالية تجري على الماكنة وتم وضع التاجر في لائحة العملاء المزورين. وتجد المحكمة أن ما ورد على لسان الشاهد أعلاه قد تأكد من خلال المبرزات س/1 ، وس/2، وس/ 3 والتي هي عبارة عن اعتراضات أصحاب البطاقات الأصلية من خلال البنوك مصدرة تلك البطاقات والكشوفات الصادرة عن ماستر كارد العالمية التي توضح مجموع وقيمة العمليات الاحتيالية وتواريخها والتي تمت من خلال ماكنة الدفع الإلكتروني الموجود لدى المدعي والمبرز س/4 والذي هو عبارة عن مستندات قيد صادرة عن المدعى عليها ثبت من خلالها أن المبالغ التي تم سحبها من حساب المدعي تم تحويلها إلى ماستر كارد...الخ؛ حكمت المحكمة برد الاستئناف موضوعاً وتأييد الحكم المستأنف من حيث النتيجة وتضمين المستأنف الرسوم و...». يُفهم من هذا الحكم السابق تبيانه؛ من أن عملية الاحتيال كانت إلكترونية (جريمة احتيال إلكتروني)، وتمت بواسطة بطاقات دفع إلكتروني حاملها غير شرعي وأصلها أنها منسوبة للغير.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

## المطلب الثاني: الركن المادي

يتمثل الركن المادي في جريمة الاحتيال الإلكتروني في السلوك الإجرامي بوسائل مستحدثة وذكية يلجأ إليها النصاب أو المحتال، وذلك قصد استيلاءه على مال يعود للغير، ومن هنا يتبين لنا أن الركن المادي يتكون من ثلاثة عناصر:

**الفرع الأول: السلوك الإجرامي (فعل الاحتيال)**

يتمثل النشاط الإجرامي في جريمة الاحتيال في فعل الاحتيال أو التدليس الجنائي، ويتم باستعمال طرق احتيالية – اتخاذ اسم كاذب أو صفة غير صحيحة عبر الأجهزة الحاسوبية؛ فينخدع المجني عليه بذلك وإيقاعه في غلط، ودفعه إلى تسليم ماله إلى الجاني المحتال.

وأكدت محكمة النقض الفلسطينية في القضية رقم 2021/53م، الصادر بتاريخ 2021/05/03م؛ «أن جريمة الاحتيال تتطلب بالمقام الأول أن يأتي الجاني فعلاً إيجابياً قوامه استعمال طرق احتيالية من شأنه إيهام المجني عليه بوجود مشروع كاذب أو أمر لا حقيقية له وإيقاعه بالغلط وحمله على تسليم ماله الذي لم يكن يسلمه للجاني لولا هذه الطرق الاحتيالية التي أتاها الجاني بوسائل خارجية دعمتها وألبستها ثوب الصدق» (مقام، 2021).

تجدر الإشارة إلى أن الجرائم الإلكترونية بصورة عامة قد ترتكب من خلال الهواتف الذكية المحمولة، التي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة، والتي من خلالها يتم الاتصال بشبكة الإنترنت، ويسهل تخزين ونقل المعلومات من خلالها، وليس الأمر محصور بالحاسب الآلي كأداة وحيدة في ارتكاب الجريمة الإلكترونية، فإنه تمارس جميع وظائف الحاسب الآلي من خلال الهاتف الذكي، فهو لا يختلف عن الحاسوب سوى في الحجم (العفيفي، 2013). وبالتالي السلوك في الجرائم الإلكترونية يتم عن طريق الوسيلة وهي الجهاز الإلكتروني أياً كان نوعه أو شكله، واتصال بشبكة الإنترنت للجرائم المرتبطة بالإنترنت، وبدون هذه الوسيلة لا يمكن مباشرة السلوك الإجرامي.

**ويثار التساؤل: وهو مدى إمكانية الاحتيال على نظام الحاسب وإيقاعه في غلط؟**

لقد اختلف الفقه بشأن تلك المسألة وسيتم تقسيم هذا الموقف على ثلاث اتجاهات (عفيفي، 2003):

**الاتجاه الأول:**

ويرى عدم إمكانية وقوع فعل الاحتيال على الحاسب الآلي وإيقاعه في غلط وبالتالي لا تتوافر جريمة الاحتيال في حق من ارتكب هذا الفعل، ويبررون لرأيهم هذا بالقول: لكي تتوافر هذه الجريمة يجب أن يكون الجاني والمجني عليه أشخاصاً طبيعيين، وبالتالي فهو متصور إذا تم خداع الشخص المكلف بمراقبة البيانات أو مراجعتها أو فحصها.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

**الاتجاه الثاني:**

ويرى إمكانية وقوع فعل الاحتيال على الحاسب ومن تصور إيقاعه في غلط وهذا الاتجاه يمثله تشريعات الدول الأنجلوسكسونية وبعض التشريعات الصادرة في بعض الولايات الأمريكية وجانب من الفقه الفرنسي.

**الاتجاه الثالث:**

ويمثله الولايات المتحدة، حيث يطبق هناك القوانين الخاصة بالغش في مجال البنوك والبريد والتلغراف والاتفاق الإجرامي لأغراض ارتكاب الغش على حالات النصب المعلوماتي، كما أن بعض الولايات الفيدرالية أصدرت قوانين تضفي مفهوماً واسعاً على المال بحيث يشمل « كل شيء ينطوي على قيمة» ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة (الشوا، 1994). سنوضح هذه المسألة تفصيلاً في عنصر المحل.

ففعل الخداع من المتصور وقوعه على الأنظمة الحاسوبية؛ لأن الحاسوب ليس سوى وسيط يعبر عن إرادة المجني عليه، فهذا الأخير هو من يقوم ببرمجته وفقاً لمتطلباته؛ وبالتالي فخداع الحاسوب هو خداع للمجني عليه، ولا يوجد هناك ما يمنع قانوناً من أن تمارس الوسائل الاحتيالية على الحاسوب (شريف، 2019).

مما سبق ذكره يتبين أن جوهر الاحتيال الإلكتروني هو التلاعب بالبيانات والمعلومات التي يحتوي عليها نظام الحاسب الآلي، ويتسع هذا التلاعب ليشمل إدخال بيانات ومعلومات صحيحة على نحو غير مصرح به، فوسيلة الاحتيال هي التلاعب في صورة إدخال بيانات ومعلومات غير صحيحة إلى الحاسب الآلي، أو تعديل بيانات مخزنة بالفعل (شريف، 2019).

**الفرع الثاني: النتيجة الإجرامية (الاستيلاء على مال يعود للغير)**

من أجل قيام جريمة الاحتيال يجب أن تؤدي وسائل الاحتيال التي نص عليها المشرع إلى إيقاع المجني عليه في غلط يحمله على تسليم ماله إلى الجاني طواعية ويعد هذا التسليم بمثابة النتيجة الإجرامية في جريمة الاحتيال، وبتحققه تصبح الجريمة تامة، فلا يكفي أن يبذل الجاني أحد أساليب الاحتيال بل يجب أن يُسفر هذا الأسلوب عن إيقاع المجني عليه في الغلط، كما يتعين أن يتم تسليم المال إلى الجاني تحت تأثير الغلط الذي وقع فيه. فالتسليم هي النتيجة التي يسعى الجاني إلى تحقيقها من وراء ارتكابه لفعل الاحتيال.

في الواقع يعتبر التسليم هو سلوك صادر عمن خدع بالاحتيال الواقع من الجاني بمقتضاه ينقل إلى الجاني أو إلى غيره المال موضوع الجريمة، وبالنظر إلى بعض الحالات التي تندرج تحت وصف الاحتيال الإلكتروني نجد أن الحاسب الآلي يقوم بفعل التسليم بالمفهوم المادي للكلمة حيث إن التسليم ينطوي على معادلة يدوية كما هو الحال في الاحتيال الذي ينطوي على استعمال غير

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

مشروع لبطاقات الائتمان سواء للوفاء بواسطتها أو لسحب النقود، أمَّا في غير ذلك فإن تسليم المال لا يتم بصورة مادية والتسليم لا يجوز النظر إليه على أنه واقعة مادية تتمثل في مناولة ترد على شيء ينقله المجني عليه من سيطرته إلى حوزة المحتال ولكن يتعين النظر إليه على أنه عمل قانوني عنصره الجوهري إرادة المجني عليه المعنية بالخداع وليست المناولة سوى المظهر المادي لهذا العمل أو هي على الأقل أثره (نصيرات، 2018).

نخلص من ذلك إلى أن الاحتيال الإلكتروني لا يختلف في هذا الشأن عن الاحتيال في صورته التقليدية، فالتسليم لا يعني في كلتا الحالتين المناولة اليدوية فقط بل يتجاوز ذلك على حالات لا تتحقق فيها المناولة، فجوهر التسليم في جريمة الاحتيال هو أن يكون المجني عليه قد اتجهت إرادته إلى وضع الشيء في متناول يد الجاني أو تحت أمره، وكذلك الأمر في الاحتيال الإلكتروني، فالعبرة هنا بوضع المال محل النشاط الإجرامي تحت تصرف الجاني متأثراً بالأساليب الاحتيالية التي مارسها الأخير.

**والتساؤل: ما مدى اعتبار النقود الكتابية أو البنكية من قبيل الأموال المادية التي يرد عليها الاستيلاء، وهل تصلح المعلومات والبيانات لأن تكون محلاً لجريمة الاحتيال؟**

لم يُعرّف قانون العقوبات الفلسطيني رقم (74) سنة 1936م ما المقصود بالمال، لكن القانون المدني نص على أنه: «كل شيء لا يخرج عن التعامل بطبيعته أو بحكم القانون يصح أن يكون محلاً للحقوق المالية، الأشياء التي تخرج عن التعامل بطبيعتها هي التي لا يستطيع أحد أن يستأثر بحيازتها، أما التي تخرج عن التعامل بحكم القانون فهي التي لا يجيز القانون أن تكون محلاً للحقوق المالية» (المادة (64) والمادة (65) من القانون المدني الفلسطيني رقم (4) لسنة 2012م).

لقد اختلف الفقه حول مسألة مدى صلاحية برامج وبيانات الحاسب أن تكون محلاً لجريمة الاحتيال (عفيفي، 2003):

- ذهب الاتجاه الأول إلى القول بعدم صلاحية برامج وبيانات الحاسب لأن تكون محلاً أو موضوعاً لهذه الجريمة، ومبررهم لذلك هو عدم وجود نشاط مادي ملموس يحصل به التسليم والاستيلاء في جريمة الاحتيال.
- ذهب اتجاه ثانٍ من الفقه وهو الراجح بصلاحية برامج وبيانات الحاسب لأن تكون محلاً لجريمة الاحتيال. مع التطورات المذهلة التي حدثت في العقود القليلة الماضية ومازالت مستمرة للآن في مجال تكنولوجيا الأمر الذي جعل الأموال المعنوية تنتشر بصورة كبيرة في مجالات المعاملات المختلفة مما أدى في بعض الأحيان إلى ارتفاع قيمتها عن قيمة الأموال المادية.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

لا يرتب الاستيلاء الناشئ عن الاحتيال على الحاسب الآلي أدنى مشكلة، إذا كان محل الاستيلاء، نقوداً أو أي مال منقول آخر له قيمة مادية، كأن يتم التلاعب في البيانات الداخلة باسمه أو باسم شركائه شيكات أو فواتير مبالغ غير مستحقة يستولى عليها الجاني أو يتقاسمها مع شركائه (الشوا، 1994).

لكن الأمر يثور عندما يكون محل الاستيلاء نقوداً كتابية، كأن يتلاعب شخص في البيانات المختزنة في الحاسب كي يحول بعض أرصدة الغير أو فوائدها إلى حسابه.

رأي فقهي يرى بأن المعيار الأساسي لجريمة الاحتيال الإلكتروني يتمثل في المحاولة التدليسية، وهي عبارة عن أساليب فنية يستخدمها الجاني أثناء تشغيل الجهاز، تتمثل في توافر الخبرة الفنية في خداع النظام المعلوماتي، بالحصول على الهوية واختلاسها وانتحال صفة صاحبها للحلول محله في العمليات الإلكترونية، واستخراج المستندات المعلوماتية ونتائج العمليات الآلية (عبابسة، 2016).

لذلك ذهب يوسف خليل العفيفي إلى أن البيانات والمعلومات وبرامج الحاسب الآلي هي مال قابل للنقل والحيازة المشروعة، لها مظهر معنوي يقبل النقل والحيازة، ويكون محلاً للحقوق المالية، وأن القول خلاف ذلك يسبب مشاكل قانونية على الصعيد الجزائي؛ مما يساعد المجرمين الإفلات من العقاب (العفيفي، 2013).

ترى الباحثة طالما توافرت في واقعة الاستيلاء على المعلومات والبيانات أركان جريمة الاحتيال، فإنه بذلك تكون محلاً لجريمة الاحتيال؛ وبالتالي محل الجريمة في الاحتيال الإلكتروني (هو مال معلوماتي)، كما أن المشرع الجنائي الفلسطيني في القرار بقانون رقم (10) لسنة 2018م وتعديلاته بشأن الجرائم الإلكترونية الساري في الضفة الغربية بنص المادة (14) منه: «كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب...» يفهم؛ بأن محل جريمة الاحتيال الإلكتروني والجرائم الإلكترونية التي تحدث عنها بصورة عامة تصلح أن تكون معلومات وبيانات مختزنة في جهاز الحاسب الآلي أو الكمبيوتر.

**الفرع الثالث: العلاقة السببية**

لا يكتمل الركن المادي لجريمة الاحتيال بارتكاب الجاني فعل الاحتيال وحدوث واقعة التسليم، إنما يلزم أن يكون التسليم وقع بطريقة من طرق الاحتيال المستخدمة من الجاني، أي أن علاقة السببية تنص على أن الاحتيال هو السبب الفعلي والدافع على التسليم، وأن يكون التسليم لاحقاً على فعل الاحتيال ونتيجة لانخداع المجني عليه، وأن يكون مبني على الضرر (عبابسة، 2016).

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وعليه قضت محكمة النقض الفلسطينية في القضية رقم 2024/268م، الصادر بتاريخ 2025/01/29م؛ «لما كان الأمر كذلك، ولم يقوم الطاعن في الطعن الأول أو الطاعن في الطعن الثاني بأية أفعال تحمل المشتكي على تسليمه مالاً غير منقول ولم يقوموا بإيهام المجني عليه بوجود مشروع كاذب، ولم يحدثوا الأمل عند المجني عليه بحصول ربح وهمي، وأن الطاعنان لم يتصرفوا في المال غير المنقول تصرف يضر بالمجني عليه، وأن المجني عليه يعلم إبتداءً بهذا الأمر، أي لم تتوافر سوء النية في أفعال المتهمان الطاعنان؛ وحيث أن استخلاص المحكمة مصدرة الحكم المطعون فيه للواقعة التي توصلت إليها كان إستخلاصاً غير سائغاً وغير مقبول ولا يتفق وواقع البينة المقدمة في الدعوى، فإنها بذلك تكون قد طبقت القانون تطبيقاً غير صحيحاً على الواقعة الثابتة، وبالتالي فإن حكمها يكون معتلاً حرياً بالنقض» (مقام، 2025).

في جريمة الاحتيال الإلكتروني تتحقق العلاقة السببية إذا تحققت النتيجة الجرمية المترتبة على ممارسة الجاني للنشاط الإجرامي والمتمثل في التلاعب في البيانات والبرامج وذلك عن طريق الحاسب الآلي بطرق احتيالية تخدع المجني عليه، من أجل الحصول على ربح غير مشروع أو عائد نتيجة ممارسة لهذا النشاط، بحيث يقال بأنه لو لا هذا النشاط أو السلوك لما تحققت هذه النتيجة (نصيرات، 2018).

وتنتفي العلاقة السببية بين الخداع والتسليم، إذا تم التسليم نتيجة لغلط وقع به المجني عليه لا يد للمحتال فيه، كأن يتخذ الشخص على أحد المواقع التجارية اسماً مستعاراً، ويدعي أنه يقوم بتأسيس شركة، ويطلب من المجني عليه مبلغ مالي للمساهمة فيها؛ فيحول له المال عن طريق بطاقة ائتمانية، ثم يتبين بعد ذلك أن الاسم المستعار لم يكن هو الدافع إلى التسليم؛ لأنه لم يكن محل اعتبار في نظر المجني عليه، وإنما ما دفعه إلى ذلك تلك الأقوال الكاذبة المجردة التي أبرزت أهمية الشركة، والتي لا تكفي بذاتها لتكوين فعل الخداع (شريف، 2019).

## المطلب الثاني: الركن المعنوي

يقصد بالركن المعنوي: «علاقة تربط بين ماديات الجريمة وشخصية الجاني، وهذه العلاقة محل لوم للقانون، وتتمثل فيها سيطرة الجاني على الفعل وآثاره» (حسني، 2006).

الاحتيال جريمة عمدية، ويعني هذا أنه يلزم بتوافر عنصرين، العلم والإرادة بخصوص النشاط والنتيجة الجُرمية، وعليه سوف تتناول الباحثة هذه العناصر في فرعين: الفرع الأول، ويشمل العلم، والفرع الثاني، ويشمل الإرادة الجُرمية.

### الفرع الأول: العلم

يُشكّل العلم أحد العنصرين الأساسين في القصد الجنائي لجريمة الاحتيال الإلكتروني، ولا يتحقق هذا القصد إلا إذا ثبت أن الجاني على دراية تامة بأنه يستخدم وسيلة إلكترونية أو تقنية معلوماتية

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

في تنفيذ فعله، كإرسال رسائل احتيالية، إنشاء مواقع أو حسابات وهمية، إدخال بيانات أو معلومات كاذبة أو مُضلّلة، وعلمه بأن سلوكه هذا سيؤدي إلى خداع المجني عليه. فالعلم هنا يتعلّق بأداة الاحتيال ذاتها، وما إذا كان الجاني مدركاً أن هذه الوسائل مُهيأة لخداع المجني عليه، وعلمه بعدم مشروعية نشاطه الاحتيالي ومن شأنه التأثير على إرادة المجني عليه وخداعه.

**الفرع الثاني: الإرادة الجُرمية**

وهو يعني اتجاه إرادة الجاني إلى الولوج والدخول غير المصرح به في جهاز الكمبيوتر أو الحاسب الآلي مُستخدماً وسائل الغش والتحايل؛ بهدف الحصول على قدرٍ عالٍ من الربح غير المشروع بالرغم من علمه بالحظر الوارد على نشاطه. بناءً عليه يقوم الركن المعنوي في جريمة الاحتيال بتوافر القصد العام والقصد الخاص «نية الاستيلاء والتملك». لم يضع المشرع الفلسطيني تعريفاً للقصد الجنائي؛ ترك هذا الأمر للفقه الجنائي، وعرفه الفقه بأنه: «انصراف إرادة الجاني إلى ارتكاب الجريمة مع العلم بأركانها كما يتطلبها القانون» (خوري، 2011/2010م).

الخطأ متصور في بعض الجرائم الإلكترونية، كمن يدخل النظام أو الجهاز الإلكتروني، وهو لا يعلم بأن الدخول في النظام أو البقاء فيه محظور(كأن يكون الجاني من المستخدمين الجدد للحاسب الآلي) (العفيفي، 2013). لكن جريمة الاحتيال الإلكتروني لا يتصور وقوعها بالخطأ، فهي لا تقع إلا عمدية، والقصد الجرمي في جريمة الاحتيال الإلكتروني هو قصد خاص والذي يتمثل في الإستيلاء على الحيازة الكاملة لمال الغير.

وأكدت محكمة النقض الفلسطينية في القضية رقم 2023/311م، الصادر بتاريخ 31/ 2024/01م؛ «أن يأتي الجاني ادعاءاته وأفعاله وهو عالم بأنها كاذبة وأن تنصرف نيته إلى الاستيلاء على مال جزء من ثروة الغير بدون وجه حق هو ما يعبر عنه بالقصد الجنائي الخاص» (مقام، 2024).

لم يتم التطرق للركن المعنوي يشكل مُفصّل؛ لانطباق القواعد العامة للقصد الجنائي في جريمة الاحتيال في المجال التقليدي على نظريتها في المجال الإلكتروني.

## المبحث الثالث

**الآليات لمواجهة جريمة الاحتيال الإلكتروني**

بداية سيتم التطرق لمخاطر تلك الجريمة، ومن ثم التعرف على سبل الوقاية منها قدر الإمكان وملاحقة ما هو مُستجد.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

## المطلب الأول: مخاطر جريمة الاحتيال الإلكتروني

وتتمثل أبرز مخاطرها في الآتي (الجبوري، 2014):

- تشكل جرائم الحاسوب تهديداً مباشراً للحق في المعلومات؛ لأنها تعطل الوصول إلى البيانات، وتعيق تدفقها الطبيعي بين الأفراد والمؤسسات، وقد تؤدي إلى تغييرها أو إتلافها أو سرقتها. وهذا يجعل تداول المعلومات أقل أماناً ويُفقد المجتمع الثقة بالأنظمة الرقمية، مما ينعكس سلباً على الحقوق المرتبطة بالمعرفة والشفافية والخدمات الرقمية كالخدمات المصرفية والتجارة الإلكترونية.
- إن هذه الجرائم تخلف ورائها إلى جانب الضرر الكبير بالشخص المستهدف في الاعتداء من ناحية (ماله)، شعوراً عريضاً لدى الأفراد بمخاطرة التقنية.
- إن جرائم الكمبيوتر والإنترنت بصورة عامة أو بعضها على نحو أدق لا يمس التقنية ذاتها في درجة شيوع الثقة بها سواء الأفراد أو الدولة فحسب بل تهدد مستقبل صناعة التقنية وتطورها وهذا يتحقق في الواقع في ثلاث فئات من جرائم الكمبيوتر والإنترنت، جرائم قرصنة البرمجيات وجرائم التجسس الصناعي وجرائم احتيال الإنترنت المالي.
- جرائم الإنترنت كثيرة ومتنوعة ويصعب اكتشافها وحصرها ومتابعة مرتكبها؛ لأن تلك الجرائم لا تترك أثراً يقود إلى مرتكبها مثل الجرائم التقليدية التي دائماً تترك أثراً يقود إلى مرتكبها. فهذه الخاصية تقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم (آل ثنيان، 2012).
- شبكة الإنترنت قدمت خدمة كبيرة للمحتالين من خلال قدرتهم على سهولة الاتصال بشكل سريع بملايين الضحايا ضعيفة الوعي، وقدرتهم على إخفاء هويتهم؛ ومن ثم صعوبة إمساكهم ومعاقبتهم.

نظراً لحداثة تلك الجريمة فإنه يصعب إثباتها بطرق الإثبات الجنائي التقليدية؛ لذلك بادرت أغلب التشريعات بالنص على بعض الدلائل الإلكترونية لإثبات هذا النوع من الجرائم؛ حتّى لا يفلت المجرم فيها من التجريم والعقاب. كالتفتيش الذي يقع على نظم المكونات المعنوية للحاسبات الآلية (حمودة، 2009).

## المطلب الثاني: مكافحة جريمة الاحتيال الإلكتروني

تشير الإحصائيات التي نشرتها جريدة لوسيل الاقتصادية في مارس/2016 حول خسائر الجرائم أو الاحتيال الإلكتروني عبر العالم إلى أن إجمالي الاحتيال المالي العالمي عبر التكنولوجيا الحديثة التي جعلت من العالم قرية صغيرة والمعنية بشبكة الإنترنت يفوق 312 مليار دولار سنوياً وأن الجرائم الإلكترونية بمختلف أصنافها تكلف العالم أكثر من 400 مليار دولار سنوياً، حتى إن بعض تقديرات خبراء الأمن في المجال الإلكتروني أكدوا أنه كل14 ثانية يتم تسجيل ما يزيد على 400 مليون عملية احتيال مالي (السماك، 2016).

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وتقول الإحصاءات الرسمية في بريطانيا إن 1,9 مليون بلاغ تم تقديمه لحوادث تتعلق بالاحتيال عبر الإنترنت في العام في إنجلترا، ولكن الرقم قد يكون أكبر من ذلك حيث لا يتم الإبلاغ عن كل الحوادث، وتقول إحصاءات أسترالية أن حوالي 10 ملايين دولار أمريكي هي محصلة النصب لهذا العام باسم الحب فقط في أستراليا (موقع فجر، 2020).

**الفرع الأول: طرق الوقاية من الاحتيال الإلكتروني**

الوقاية والمكافحة من الاحتيال الإلكتروني تعد من المواضيع الحيوية في ظل تزايد استخدام التكنولوجيا في حياتنا اليومية. فيما يلي بعض الطرق التي يمكن من خلالها الوقاية والتصدي لهذا النوع من الاحتيال:

- أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
- التحقق من المصادر قبل فتح الروابط والنقر عليها ذلك عند تلقي رسائل بريد إلكتروني أو رسائل نصية تحتوي على روابط مشبوهة.
- وضع الرقم السري بشكل مطابقة للمواصفات الجيدة التي تصعّب من عملية القرصنة للوصول إليه من هذه الواصفات (بأن يحتوي على أكثر من ثمانية أحرف، أن يكون متنوع الحروف، والرموز، واللغات) (حنين، 2020). بالإضافة إلى تجنب استخدام نفس كلمة المرور لحسابات متعددة.
- تمكين المُصادقة الثنائية على الحسابات المهمة مثل البريد الإلكتروني، والحسابات المصرفية، ووسائل التواصل الاجتماعي لزيادة الأمان.
- مراقبة الحسابات والمعاملات المالية بانتظام لاكتشاف أي نشاط غير اعتيادي.
- تثقيف أفراد الشركات المصرفية والبنكية حول أساليب الاحتيال وكيفية تجنبها، والاطلاع الدائم بأحدث الأساليب الاحتيالية.
- استخدام وسائل تأمينية إلكترونية متقدمة للتعرف على الهوية مثل التعرف على الوجه أو استخدام البصمة؛ لتحسين عملية التحقق من الهوية.
- اتخاذ تدابير ضرورية من الواجب اتباعها، كتدريب رجال الضبط القضائي وأعضاء التحقيق والقضاة على كيفية كشف هذا النوع من الجرائم وإثباتها.
- التشفير للمعلومات والمقصود هو تغيير مظهرها بحيث يختفي معناها الحقيقي بحيث تكون غير مفهومة لمن يتلصص عليها من مرتكبي الجرائم الإلكترونية.
- استخدام برامج مكافحة الفيروسات والبرامج الضارة بشكل دائم للمساعدة في اكتشاف ومنع الهجمات.
- التحديث المنتظم لبرامج النظام والتطبيقات بما في ذلك برامج الأمان؛ لتأمين الأجهزة من الثغرات التي يمكن استغلالها من قبل المُحتالين.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

فمن خلال اتباع هذه الإجراءات الوقائية والتصدي الفعَّال؛ من الممكن تقليل مخاطر الاحتيال الإلكتروني بشكل كبير.

## الخاتمة

الحمد لله الذي بنعمتهِ تتم الصالحات رب الأولين والآخرين وأحمد الله كثيراً الذي وفقني في إتمام هذه الدراسة البسيطة، وأسأل الله تعالى التوفيق والسداد فيها.

وعليه لقد توصلنا من خلال التحليل القانوني والآراء الفقهية والقضائية في هذه الدراسة إلى مجموعة من النتائج والتوصيات.

## النتائج

- جريمة الاحتيال الإلكتروني من الجرائم المستحدثة وهي جريمة من الجرائم التي يرتكبها الجاني من دون مشقة بمجرد الضغط يدخل إلى شبكة الإنترنت ويبدأ في اصطياد ضحاياه.
- تعتبر جريمة الاحتيال الإلكتروني من الجرائم العمدية قائمة على العلم والإرادة، وتتوافر فيها القصد العام والقصد الخاص.
- ساعدت شبكات الإنترنت العالمية كثيراً من المجرمين على التخفي وراءها لممارسة أفعالهم الجرمية؛ نظراً لكون الأخيرة (جرائم الإنترنت) عابرة للحدود مما يصعب كثيراً اكتشافها وضبطها، كما يصعب ملاحقة ومتابعة مرتكبيها، كما أن الاحتيال لا يقع على الشخص الطبيعي فقط، فقد يقع على الشخص المعنوي كالشركات والمؤسسات؛ بوقوع فعل الخداع على أجهزتها وشبكاتها الداخلية.
- مرتكبي هذه الجريمة غالباً من الأفراد ذو المهارات الفنية والتقنية العالية، فهي جريمة خبراء التقنية الحديثة.
- على الرغم من حملات التوعية المتعلقة بمختلف الوسائل الإعلامية حول الجرائم الإلكترونية بشكل عام والاحتيال الإلكتروني بشكل خاص، إلا أن العديد من الأشخاص مازالوا ضحايا تلك الجرائم؛ طمعاً بالحصول على الأموال والأرباح الوهمية.
- يعتبر محل جريمة الاحتيال الإلكتروني هو مال معلوماتي، وليس مال مادي كما ذكر البعض فهو يشمل كل شيء ينطوي على قيمة، وهذا ما أخذ به المشرّع الجنائي الفلسطيني في قانون الجرائم الإلكترونية رقم (10) لسنة 2018م.
- لا وجود لأي نص قانوني خاص بالاحتيال الإلكتروني مطبق في قطاع غزة بشكل فعلي والأمر محصور في تطبيق النصوص الجزائية لجريمة الاحتيال بصورتها التقليدية؛ وهذا يتعارض مع مبدأ قانوني شرعية الجريمة والعقوبة، ومبدأ عدم جواز القياس على النصوص التجريمية الموضوعية.
- لم يتحوط قانون العقوبات الفلسطيني رقم (74) لسنة 1936م وتعديلاته، وكذا قانون

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

العقوبات الأردني رقم (16) لسنة 1960م الساري في الضفة الغربية، من تلك الجريمة في ظل السرعة المذهلة لتطور التكنولوجيا، وعدم مواكبته ومسايرته لهذا التطور الذي استخدمه الإنسان في أغراض إجرامية، في حين أن القرار بقانون رقم (10) لسنة 2018م وتعديلاته، جرّم الاحتيال الإلكتروني وعاقب عليه بنص جزائي، لكن هذه النصوص من هذا القانون مقصور تطبيقها على الضفة الغربية دون قطاع غزة؛ وهذا الاختلاف في التطبيق يعود إلى الانقسام السياسي والإداري بين الضفة الغربية وقطاع غزة، مما أدى إلى وجود أنظمة قانونية مختلفة في كل منهما، كما أن المجلس التشريعي في قطاع غزة؛ لم يسن تشريعات تواجه هذا النوع من الجرائم باستثناء بعض التعديلات التي أجراها سنة 2009 على بعض مواد قانون العقوبات الفلسطيني المُطبق في قطاع غزة.

- اعتبر المشرع الفلسطيني في القرار بقانون رقم (10) لسنة 2018م، الاحتيال الإلكتروني من جرائم الجنح؛ وبالتالي فالجزاء الجنائي الذي قرره المشرع غير رادع بصورة كافية، ولا يتناسب مع جسامة الخسائر الذي يوقعها هذا النوع من الجرائم الإلكترونية التي من الممكن أن تصل تكلفة الخسائر فيها بالمليارات.

## التوصيات

- ضرورة تفعيل دور الأجهزة الأمنية والقضائية لمواجهة تلك الجريمة، كإعطاء دورات تدريبية متخصصة لمأموري الضبط القضائي ولأعضاء النيابة العامة والقضاة؛ من أجل معرفة الطبيعة الخاصة لتلك الجرائم المرتكبة بواسطة شبكة الإنترنت، ومعرفة التعامل معها والبت فيها.
- إدراك أن جريمة الاحتيال عبر شبكة الإنترنت ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والتعاون الدولي من أجل المكافحة والتصدي لتلك الجريمة.
- ضرورة استحداث نصوص جزائية من قبل المشرع الفلسطيني في قطاع غزة وتطبيقها في القطاع، بحيث تتواءم وصعوبة مخاطر هذه الجريمة في المجتمع ومواجهتها بحيث تكفل الحماية الجزائية فيه، ونوصي المجلس التشريعي الفلسطيني في قطاع غزة بإقرار وتطبيق القرار بقانون رقم (10) لسنة 2018م وتعديلاته بشأن الجرائم الإلكترونية، وجعله سارياً قانونياً وواقعياً؛ لأنه عالج قضايا الاحتيال الإلكتروني.
- على دول العالم تطوير التقنيات التي تسهل من الكشف عن هوية مرتكب جريمة الاحتيال الإلكتروني، والاستدلال عليه بوقت سريع، حيث لابد من تضافر وتعاون الدول فيما بينها على المستوى الإقليمي والدولي، لإيجاد تشريعات قادرة على مواجهة هذا النوع من الجرائم، ومن الضرورة رفع سقف العقوبة المقررة لمرتكب جريمة الاحتيال الإلكتروني لتحقيق أكبر قدر ممكن من الردع.
- استغلال الحكومة الفلسطينية لخبرات المُحتالين التقنية؛ ذلك بإستدراج كل ما هو مستجد منها لديهم، والتصدي لها على الفور ومنع تطورها.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

## قائمة المراجع

### أولاً: المراجع العربية


أبو حجاج، يوسف (2010). أشهر جرائم الكمبيوتر والإنترنت. مكتبة جامعة الأزهر، غزة: دار الكتاب العرب.

أبو سيدو، حسنة محمد مصطفى (2022). الاحتيال الإلكتروني في التشريع الفلسطيني: دراسة تحليلية مقارنة بالفقه الإسلامي، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة.

أبو عامر، محمد ذكي (1993). شرح قانون العقوبات: القسم العام، الإسكندرية: منشأة المعارف.

أحمد، هلالي عبد الله (2019). الوجيز في شرح قانون العقوبات: القسم العام، كلية الحقوق، جامعة الفيوم، مصر.

آل ثنيان، ثنيان ناصر (2012). إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، السعوديه.

بوشعرة، أمينة، وموساوي، سهام (2018). الإطار القانوني للجريمة الإلكترونية: دراسة مقارنة، رسالة ماجستير، جامعة عبد الرحمن ميرة، بجاية، الجزائر.

الجبوري، سامر سلمان عبد (2014). جريمة الاحتيال الإلكتروني: دراسة مقارنة، رسالة ماجستير، جامعة النهرين، العراق.

حجاج، وليد (2022). طرق ووسائل عمليات الاحتيال والنصب الإلكتروني وكيفية تجنبها، استرجعت بتاريخ 2025/07/09م، من موقع الجريدة الإلكتروني: https://ar.m.wikipedia.org/w/index.php?title=%D8%AA%D8%B3%D98%8A%D9%88%D9%8A&wprov=rarw1%83%D9%D8%B4%D8%A8%D9%_2

حسني، محمود نجيب (2006). النظرية العامة للقصد الجنائي» دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، مصر: دار النهضة العربية.

حمودة، علي محمود علي (2009). أدلة الإثبات الجرائم الإلكترونية وتقديرها في إطار نظرية الإثبات الجنائي، مجلة الأمن والقانون، أكاديمية شرطة دبي، 17(1): 1-86

حنين، جورج اسحق (2020). تقرير عن الجرائم المعلوماتية والإلكترونية عبر شبكة الإنترنت وسبل مواجهتها، استرجعت بتاريخ 2024/07/09م، من: https://egyls.com/wp-content/uploads/2020/06/الجرائم-الالكترونية.pdf


https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

خوري، عمر (2011/2010). شرح قانون العقوبات: القسم العام، الجزائر: المكتبة القانونية.

سكيكر، محمد علي (2010). الجريمة المعلوماتية وكيفية التصدي لها، مصر: دار الجمهورية للصحافة.

السماك، زينب شاكر (2016). جرائم الاحتيال الإلكتروني، استرجعت بتاريخ 2025/07/09م، من: https://annabaa.org/arabic/informatics/8390

سيار، ناهد علي (2019) ضحايا الاحتيال الإلكتروني في المجتمع الإماراتي. الشارقة، الإمارات العربية المتحدة: مركز بحوث الشرطة.

شريف، شيلان محمد (2019). الأحكام الموضوعية والإجرائية في جريمة الاحتيال الإلكتروني، أطروحة دكتوراه، كلية القانون، جامعة السليمانية، العراق.

الشوا، محمد سامي (1994). ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة: دار النهضة العربية.

الشوابكة، محمد أمين (2006). جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، عمان: دار الثقافة.

طالة، لامية، وسلام، كهينة (2020). الجريمة الإلكترونية «بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي»، مجلة الرواق للدراسات الاجتماعية والإنسانية، 6(2): 62-91.

عبابسة، إيمان (2016) جريمة النصب المعلوماتي «دراسة تحليلية»، رسالة ماجستير، جامعة العربي بن مهيدي «أم البواقي»، الجزائر.

عبابنة، محمود أحمد (2009). جرائم الحاسوب وأبعادها الدولية، عمان: دار الثقافة للتوزيع والنشر.

عفيفي، عفيفي كامل (2003). جرائم الكمبيوتر ودور الشرطة والقانون: دراسة مقارنة، غزة: مكتبة جامعة الأزهر.

العفيفي، يوسف خليل (2013). الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الإسلامية، غزة.

القحطاني، مداوي سعيد مداوي (2016). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية، الأمانة العامة، قطر.

الكرد، سالم أحمد (2008). الجرائم الماسة بالمصلحة العامة وجرائم الاعتداء على الأموال، (ط4)، غزة: مكتبة جامعة الأزهر.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

موقع اليوم السابع (2020). التسويق الإلكتروني، استرجعت بتاريخ 2025/07/13م، من: https://www.youm7.com/story/2020/3/3/لملايين-الحالمين-بالثراء-السريع6--أكاذيب-تستخدمها-شركات-التسويق-الشبكي/4655163

موقع فجر الإلكتروني (2020). جرائم النصب والاحتيال الإلكتروني، استرجعت بتاريخ 10/20/ 2024م، من: https://www.elfajr.org/

المومني، نهلا عبد القادر (2010). الجرائم المعلوماتية، (ط2)، عمان: دار الثقافة.

نصيرات، وائل محمد (2018). جريمة الاحتيال عبر شبكة المعلومات الدولية: دراسة مقارنة بين النظام السعودي والقانون الأردني، دفاتر السياسة والقانون، (19) جوان.

ويكيبيديا، «الموسوعة الحرة» (2025). التسويق الشبكي، استرجعت بتاريخ 2025/07/13م، من: https://ar.wikipedia.org/wikihttps://ar.wikipedia.org/wiki/%D8%AA%D8%B3%D9%88%D9%8A%D9%82_%D8%A8%D8%A7%D9%84%D8%B4%D8%A8%D9%83 /

- **التشريعات والقوانين والاحكام**

حكم حضوري صادر عن محكمة استئناف رام الله، بتاريخ 04--12 2019م.

حكم محكمة النقض الفلسطينية في القضية رقم 2024/268م، الصادر بتاريخ 2025/01/29م، استرجعت من موقع مقام الإلكتروني «موسوعة القوانين وأحكام المحاكم الفلسطينية»: https:// maqam.najah.edu/judgments/10387/

حكم محكمة النقض الفلسطينية في القضية رقم 2023/311م، الصادر بتاريخ 31/ 2024/01م، استرجعت من موقع مقام الإلكتروني «موسوعة القوانين وأحكام المحاكم الفلسطينية»: https:// maqam.najah.edu/judgments/9355/

حكم محكمة النقض الفلسطينية في القضية رقم 2021/53م، الصادر بتاريخ 2021/05/03م، استرجعت من: موقع مقام الإلكتروني «موسوعة القوانين وأحكام المحاكم الفلسطينية»: https://maqam.najah.edu/judgments/7671/?utm_source=chatgpt.com

قانون الاتصالات السلكية واللاسلكية الفلسطيني رقم (3) لسنة 1996م، مجلة الوقائع الفلسطينية (11)، والمُطبق في الضفة الغربية وقطاع غزة

القانون الأساسي الفلسطيني لسنة 2003م، مجلة الوقائع الفلسطينية، (43). والمُطبق في الضفة الغربية وقطاع غزة

قانون العقوبات الأردني رقم (16) لسنة 1960م وتعديلاته، والمطبق في الضفة الغربية.

قانون العقوبات الفلسطيني رقم (74) لسنة 1936م وتعديلاته، والمُطبق في قطاع غزة.

القانون المدني الفلسطيني رقم (4) لسنة 2012م، مجلة الوقائع الفلسطينية، والمُطبق في قطاع غزة والضفة الغربية.

القانون رقم (3) لسنة 2009م والمعدل لقانون العقوبات الفلسطيني رقم (74) لسنة 1936م المطبق في قطاع غزة.

قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، مجلة الوقائع الفلسطينية، (16).

قرار بقانون رقم (15) لسنة 2017م بشأن المعاملات الإلكترونية، مجلة الوقائع الفلسطينية، (89).

قرار بقانون رقم (38) لسنة 2021م، المُعدل للقرار بقانون رقم (10) لسنة 2018م وتعديلاته بشأن الجرائم الإلكترونية، مجلة الوقائع الفلسطينية، (177).

## ثانياً: المراجع العربية المترجمة

Ababneh, M. A. (2009). Computer Crimes and Their International Dimensions. Amman: Dar Al-Thaqafa for Distribution and Publishing.

Ababsa, I. (2016). Cyber Fraud: An Analytical Study. Master's Thesis, Al-Aarbi Ben Mhidi University, Oum El Bouaghi, Algeria.

Abu Amer, M. Z. (1993). Commentary on the Penal Code: General Part. Alexandria: Manshat Al-Maaref.

Abu Hajjaj, Y. (2010) Prominent Computer and Internet Crimes, Al-Azhar University Library, Gaza: Dar Al-Kitab Al-Arabi.

Abu Sido, H. M. (2022). Electronic Fraud in Palestinian Legislation: An Analytical Study in Light of Islamic Jurisprudence. Master's Thesis, Faculty of Sharia and Law, Islamic University of Gaza, Palestine.

Afifi, A. K. (2003) Computer Crimes and the Role of Law Enforcement and Legal Framework: A Comparative Study. Gaza :Al-Azhar University Library.

Al-Afifi, Y. K. (2013). Electronic Crimes in Palestinian Legislation: An Analytical Comparative Study. Master's Thesis, Faculty of Sharia and Law, Islamic University of Gaza, Palestine.

Ahmed, H. A. (2019). Brief Explanation of the Penal Code: General Part. Faculty of Law, Fayoum University, Egypt.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

Bouchaara, A., & Moussaoui, S. (2018). The Legal Framework of Electronic Crime: A Comparative Study. Master's Thesis, Abdelrahman Mira University, Bejaia, Algeria.

Fajr Electronic Website (2020). Electronic Fraud and Scam Crimes, Retrieved on 20 October 2024 from: https://www.elfajr.org/

Hajjaj, W. (2022). Methods and Means of Electronic Fraud and Scam Schemes and How to Avoid Them. Retrieved on 9 July 2025 from: https://ar.m.wikipedia.org/w/index.php?title=%D8%AA%D8%B3%D988%%D98%A%D982%_%D8%B4%D8%A8%D983%%D98%A&wprov=rarw1

Hammouda, A. M. (2009). Evidence in Electronic Crimes and Its Assessment within the Framework of the Theory of Criminal Evidence. Security and Law Journal, Dubai Police Academy, 17(1): 1-86.

Hanin, G. I (2020). Report on Cyber and Electronic Crimes through the Internet and Methods of Addressing Them. Published June 30, 2020. Retrieved July 9, 2024, from: https://egyls.com/wp-content/upload /

Hosni, M. N. (2006). The General Theory of Mens Rea: A Comparative Foundational Study of the Mental Element in Intentional Crimes. Egypt: Dar Al-Nahda Al-Arabiya.

Al-Jubouri, S. S. (2014). The Crime of Electronic Fraud: A Comparative Study. Master's Thesis, Al-Nahrain University, Iraq.

Khoury, O. (2010/2011). Commentary on the Penal Code: General Part. Algeria: The Legal Library.

Al-Kurd, S. A. (2008). Crimes Affecting Public Interest and Property Offenses, (4th ed.). Gaza: Al-Azhar University Library.

Al-Momani, N. A. (2010). Cybercrime, (2nd ed.). Amman: Dar Al-Thaqafa.

Nusairat, W. M. (2018). Electronic Fraud via the International Information Network: A Comparative Study between the Saudi System and Jordanian Law. Notebooks of Politics and Law, (19).

Al-Qahtani, M. S. (2016). Electronic Crime in Gulf Society and Methods of Addressing It. Gulf Cooperation Council, General Secretariat, Qatar.

Al-Samak, Z. S. (2016). Electronic Fraud Crimes. Retrieved on 9 July 2025 from: https://annabaa.org/arabic/informatics/8390

Shareef, S. M. (2019). Substantive and Procedural Provisions in Electronic Fraud. Doctoral Dissertation, Faculty of Law, University of Sulaimani, Iraq.

Al-Shawa, M. S. (1994). The Information Revolution and Its Reflections on Penal Law.

Cairo : Dar Al-Nahda Al-Arabiya.

Al-Shawabkeh, M. A. (2006). Computer and Internet Crimes (Cybercrime), Amman: Dar Al-Thaqafa.

Siyar, N. A. (2019). Victims of Electronic Fraud in Emirati Society. Sharjah, UAE: Police Research Center.

Skiker, M. A. (2010). Cybercrime and Methods of Countering It. Egypt: Dar Al-Gomhoria Press.

Talla, L., & Salam, K. (2020). Electronic Crime: A New Dimension of Criminality through Social Media Platforms. Al-Riwaq Journal for Social and Human Studies, 6(2): 62-91.

Al-Thunayan, T. N. (2012). Proving Electronic Crime: A Doctrinal and Applied Study. Master's Thesis, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

Wikipedia – The Free Encyclopedia (2025). Network Marketing, Retrieved on 13 July 2025 from: https://ar.wikipedia.org/wikihttps://ar.wikipedia.org/wiki/%D8%AA%D8%B3%D988%D98%A%D982%_%D8%B4%D8%A8%D983%%D98%A /

Youm7 Website (2020). Electronic Marketing. Retrieved on 13 July 2025 from: https://www.youm7.com/story/2020/3/3/لملايين-الحالمين-بالثراء-السريع6--أكاذيب-تستخدمها-شركات-التسويق-الشبكي/4655163

## ● Legislation and regulations

Decree-Law No. (10) of 2018 concerning Cybercrimes, Palestinian Official Gazette (16). Decree-Law No. (15) of 2017 concerning Electronic Transactions, Palestinian Official Gazette. (89).

Decree-Law No. (38) of 2021 amending Decree-Law No. (10) of 2018 and its amendments concerning Cybercrimes, Palestinian Official Gazette, (177).

Jordanian Penal Code No. (16) of 1960 and its amendments, applicable in the West Bank.

Judgment issued in absentia by the Ramallah Court of Appeal, dated December 4, 2019.

Law No. (3) of 2009 amending Palestinian Penal Code No. (74) of 1936, applicable in the Gaza Strip.

Palestinian Civil Law No. (4) of 2012, Palestinian Official Gazette, applicable in the Gaza Strip and the West Bank.

The Palestinian Court of Cassation's ruling in Case No. 268/2024, issued on January 29, 2025, retrieved from the Maqam website, "Encyclopedia of Palestinian Laws and Court Rulings": https://maqam.najah.edu/judgments/10387/

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

The Palestinian Court of Cassation's ruling in Case No. 311/2023, issued on January 31, 2024, retrieved from the Maqam website, "Encyclopedia of Palestinian Laws and Court Rulings": https://maqam.najah.edu/judgments/9355/

The Palestinian Court of Cassation's ruling in Case No. 53/2021, issued on May 3, 2021, retrieved from the Maqam website, "Encyclopedia of Palestinian Laws and Court Rulings": https://maqam.najah.edu/judgments/7671/?utm_source=chatgpt.com

Palestinian Basic Law of 2003, Palestinian Official Gazette (43), applicable in the West Bank and Gaza Strip.

Palestinian Penal Code No. (74) of 1936 and its amendments, applicable in the Gaza Strip.

Telecommunications Law Palestinian Law No. (3) of 1996, Palestinian Official Gazette (11), applicable in the West Bank and Gaza Strip.

https://journal.pass.ps « DOI: 10.36554/1796-011-002-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854