Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

The Objective Aspect of Online Scam in the Saudi Regulations in Comparison with Egyptian and Kuwaiti Laws

الجانب الموضوعي للاحتيال من خلال المواقع الإلكترونية في النظام السعودي مقارنًا بالقانونين المصري والكويتي

ممدوح بن رشيد بن مشرف العنزي*
قسم القانون، كلية العلوم والدراسات الإنسانية، جامعة شقراء، المملكة العربية السعودية

Mamdouh bin Rasheed bin Moshref Al-Anazi*
Shaqra University, College of Science and Humanities, Department of Law, Shaqra, Kingdom of Saudi Arabia

Received 24 Aprl. 2022; Accepted on 31 May. 2022; Available Online on 20 June. 2022

Abstract

This study deals with the objective aspect of online scam according to Saudi regulations compared to Egyptian and Kuwaiti laws. The study showed that online scam is among financial crimes committed using information systems. The number of online scams has increased as a result of daily use of websites and the widespread use of credit cards in purchases and money transfers.

In the face of the increase in online scams, the Saudi regulator and other Arab legislators realized the seriousness of this offence, and therefore have attached paramount importance to develop appropriate solutions to address this crime through the enactment of laws aimed at combating them.

In conducting the study, the researcher adopted the comparative analytical descriptive approach. The study comprised two chapters. In the first chapter, the researcher elaborated on various topics such as the nature of online scam, relevant legal issues, similarities and differences between online scam and traditional fraud, and types of on-

Keywords: *Security Studies, Financial Fraud, Website, Website Development, Online Scam Methods.*

المستخلص

تناولت هذه الدراسة، الجانب الموضوعي للاحتيال من خلال المواقع الإلكترونية في النظام السعودي مقارناً بالقانونين المصري والكويتي، وبينت أن جريمة الاحتيال من الجرائم التي تمثل اعتداءً على الذمة المالية للشخص من خلال استخدام النظام المعلوماتي، وقد تزايدت بتزايد استخدام الأفراد للمواقع الإلكترونية بشكل يومي وانتشار البطاقات الائتمانية في عمليات الشراء وتحويل الأموال.

وأمام تزايد العمليات الاحتيالية أدرك كل من المنظم السعودي والتشريعات العربية الأخرى خطورة الاحتيال، فكان محل اهتمامها من أجل إيجاد الحلول المناسبة للتصدي لهذه الجريمة من خلال سن قوانين تهدف إلى القضاء على العمليات الاحتيالية، كما اعتمدت الدراسة على المنهج الوصفي التحليلي المقارن، واشتملت على مبحثين، الأول تحدثنا فيه عن ماهية الاحتيال من خلال المواقع الإلكترونية والمشكلات القانونية التي تثيرها الجريمة، وأوجه الشبه والاختلاف بين الاحتيال من خلال المواقع الإلكترونية والاحتيال التقليدي، وكذلك صور الاحتيال من خلال المواقع الإلكترونية، وفي المبحث الثاني تحدثنا

الكلمات المفتاحية: الدراسات الأمنية، الاحتيال المالي، الموقع الإلكتروني، إنشاء موقع، الطرق الاحتيالية.

* Corresponding Author: *Mamdouh bin Rasheed bin Moshref Al-Anazi*
Email: m.alanze@su.edu.sa
doi: 10.26735/WZVV1888

عن أركان جريمة الاحتيال المادي والمعنوي والعقوبة المقررة لها، ومن أهم النتائج التي توصلت إليها الدراسة: تزايد جرائم الاحتيال بشكل يومي بسبب تنوع الطرق الاحتيالية التي يلجأ إليها الجناة وعدم حصرها بطريقة معينة، مستغلين بذلك التطور التقني الحاصل، وصعوبة الوصول إليهم أو اكتشاف أمرهم، إضافة لذلك كثرة المواقع الإلكترونية والإعلانات المضللة من خلالها، وأخيرًا توصي الدراسة بعقد اتفاقيات مشتركة بين التشريعات العربية لمكافحة جرائم الاحتيال والتعاون فيما بينها من ناحية تكثيف الجهود في الوصول إلى الجناة وتسليمهم.

line scam. The second chapter explored the financial and moral elements of online scam and its prescribed penalties. The study yielded numerous findings, the most prominent of which are: online scam is increasing daily due to the diversity of scam methods utilizing current technological development and the difficulty in tracing offenders, in addition to the growing number of websites and misleading advertisements. Lastly, the study recommends concluding joint agreements between Arab legislators to combat online scam and to cooperate in the intensification of efforts to arrest offenders.

1. المقدمة

نتيجةً للتطور التقني الذي يشهده العالم اليوم؛ وما أحدثته الشبكة العالمية «الإنترنت» من ثورة في حياة الملايين من البشر وما صاحبها من انتشار العديد من المواقع الإلكترونية، وما قدمته لهم من تسهيلات من ناحية توفير الوقت والجهد في العديد من المجالات الاقتصادية والتجارية والاجتماعية؛ أصبح باستطاعة الأفراد إجراء تعاملاتهم اليومية من خلال هذه التقنية كالاطلاع على حساباتهم المصرفية أو القيام بإجراء التحويلات المالية أو القيام بعمليات الشراء أو البيع، وبالرغم من المزايا التي تحققت بفضل التقنية الحديثة فإن الاستخدام لها أظهر بعض الجوانب السلبية؛ نتيجة لسوء استغلالها من قبل الجناة على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد، فقد ظهر نوع من الجرائم ترتكب من خلال النظام المعلوماتي، ومنها الاحتيال من خلال المواقع الإلكترونية التي تعتبر ملاذًا آمنًا للجناة لممارسة أفعالهم الاحتيالية دون اكتشافهم، مستغلين النظام المعلوماتي الذي يعتبر الوسيلة المستخدمة لتحقق السلوك الإجرامي، فكثير من تلك المواقع لا تتطلب سوى الدخول المباشر لها أو الاشتراك من خلالها للاستفادة من خدماتها؛ مما يجعل كثيرًا من مستخدمي المواقع عرضةً للاحتيال من قبل الجناة من خلال إنشائهم مواقع وهمية، أو مصطنعة، أصبحت بيئة خصبة لممارسة الجناة لأفعالهم الاحتيالية من خلالها، فلم تعد الجريمة ترتكب بصورتها التقليدية خاصة مع سرعة انتشار وسائل التقنية الحديثة وظهور العديد من المواقع الإلكترونية.

فالاحتيال يقوم بوجه عام على الغش والخداع من أجل الحصول على مال المجني عليه بطريقة غير مشروعة، وتزداد خطورته من خلال استغلال الجناة للتطورات التقنية والعلمية لممارسة أفعالهم الاحتيالية حتى أصبح اليوم يشكل تهديدًا حقيقيًا للأفراد وللتجارة الإلكترونية؛ كما أنه لم يعد مقصورًا على نطاق جغرافي معين؛ إذ أصبح من الجرائم متعدية الحدود، وتعتبر جريمة الاحتيال من أكثر الجرائم خطورة، ولا يكاد يخلو مجتمع منها.

مشكلة الدراسة

تعتبر جريمة الاحتيال من خلال المواقع الإلكترونية من الموضوعات الحديثة التي لها آثار سلبية على المستوى الاقتصادي للمجتمع بشكل عام والفرد بشكل خاص، كما تعتبر من أخطر جرائم الاعتداء على الذمة المالية، ولما لحداثة هذا النوع من الجرائم فقد أدرك كل من المنظم السعودي والتشريعات الأخرى مدى خطورة الاحتيال فكان محل اهتمامهم من أجل إيجاد الحلول المناسبة للتصدي لهذه الجريمة من خلال إصدار القوانين التي تجرمها، ومن ثم تُسلط الدراسة الضوء على النصوص القانونية ومدى كفايتها لمواجهة جريمة الاحتيال عن طريق المواقع الإلكترونية، من خلال الإجابة عن السؤال الرئيس التالي: ما مدى كفاية النصوص القانونية للتشريعات المقارنة لمواجهة جريمة الاحتيال من خلال المواقع الإلكترونية؟ ومن ثم يتفرع عن السؤال الرئيس الأسئلة التالية:

- ما المقصود بالاحتيال عن طريق المواقع الإلكترونية؟
- ما الفرق بين الاحتيال الإلكتروني والاحتيال التقليدي؟
- ما المشكلات القانونية التي تثيرها جريمة الاحتيال من خلال المواقع الإلكترونية؟
- ما صور الاحتيال من خلال المواقع الإلكترونية؟
- ما أركان جريمة الاحتيال عن طريق المواقع الإلكترونية والعقوبة المقررة لها؟

أهداف الدراسة

تهدف الدراسة إلى بيان المقصود بالاحتيال عن طريق المواقع الإلكترونية، والفرق بينه وبين جريمة الاحتيال بصورته التقليدية،

وأيضًا المشكلات القانونية التي تثيرها جريمة الاحتيال، كما تهدف الدراسة إلى بيان صور الاحتيال من خلال المواقع الإلكترونية، وركني الجريمة المادي والمعنوي والعقوبة المقررة لها.

أهمية الدراسة

تظهر أهمية الدراسة من خلال بيان خطورة جريمة الاحتيال، وما تثيره من صعوبة من حيث الوصول إلى مرتكبها والقانون الواجب التطبيق، وبيان أحدث طرق الاحتيال التي يلجأ إليها الجناة اليوم من خلال إنشاء مواقع إلكترونية وهمية أو مصطنعة أو من خلال اختراق تلك المواقع للاحتيال على أفراد المجتمع، مستغلين مدى اعتمادهم عليها؛ نتيجة لتعاملاتهم اليومية، سواء التجارية أو المالية.

2. الدراسات السابقة

- (عبدالرحمن،2011)، جرائم الاحتيال الإلكتروني، مجلة الفكر الشرطي، المجلد العشرون، العدد 79، بينت الدراسة جرائم الاحتيال المصرفي الإلكتروني من خلال استخدام بطاقات الدفع الإلكتروني، والاحتيال المعلوماتي المرتبط بالقسم المالي والاحتيال على أسواق الأوراق المالية، كما تناولت جرائم الاحتيال بإنشاء المحافظ الوهمية (توظيف الأموال) وبيان أساليب الوقاية والمكافحة من جرائم الاحتيال الإلكتروني، وخلصت إلى جملة من النتائج أهمها: أن جرائم الاحتيال المصرفي من الجرائم المالية المستحدثة، سواء أكان عن طريق استخدام بطاقات الدفع الإلكتروني أو عن طريق شبكات المعلومات والعبث بها.
- (سحلول، 2018)، القواعد الموضوعية لجريمة الاحتيال في النظام السعودي، مجلة الاقتصاد والإدارة، جامعة الملك عبد العزيز، العدد الأول، تناولت الدراسة جريمة الاحتيال التقليدي في المملكة العربية السعودية وما يحكمها من تشريعات مقارنة؛ حيث ركزت على القواعد الموضوعية للجريمة وعقوبتها، كما فرقت بين الاحتيال وغيره من جرائم الأموال، وحكم الاحتيال في الشريعة الإسلامية، وأركان الجريمة والعقوبة المقررة لها، كما توصلت الدراسة إلى عدة نتائج من أهمها، أن اللجوء إلى الطرق الاحتيالية وسيلة من وسائل الاحتيال، كما تعتبر جريمة الاحتيال عمدية تتطلب وجود قصد جنائي لوقوعها.
- (السليطي، 2018)، تجريم الاحتيال الإلكتروني في القانون القطري والمقارن، رسالة ماجستير، جامعة قطر، كلية القانون، وتطرقت الدراسة إلى مفهوم جريمة الاحتيال الإلكتروني في قانون مكافحة الجرائم الإلكترونية القطري، وتحديد المقصود بجريمة الاحتيال والطبيعة القانونية، وبيان أركان الجريمة والعقوبة المقررة لها، والصور المختلفة لجريمة الاحتيال الإلكتروني، ومن أهم النتائج التي توصلت لها الدراسة، أن جريمة الاحتيال تعتبر من الجرائم الواقعة على الأموال التي تمس المجتمع من الناحية الاقتصادية، وأن ظهور أنواع مستحدثة من الجرائم التي تقع على حقوق الغير والمجتمع راجع إلى التطور في النظام المعلوماتي.

وإن كانت هذه الدراسة تتفق مع الدراسات السابقة من حيث بيان المقصود بالاحتيال والمشكلات القانونية التي تثيرها تلك الجريمة، وبيان أركان الجريمة المادي والمعنوي والعقوبة المقررة لها، والطرق الاحتيالية التي يلجأ إليها الجناة، إلا أنها تختلف من حيث التركيز على صور الاحتيال من خلال المواقع الإلكترونية، وأوجه الشبه بينه وبين الاحتيال التقليدي، مبرزين دور كل من المنظم السعودي والقانونين الكويتي والمصري في تجريم الاحتيال.

3. منهج الدراسة

اتبعت الدراسة المنهج الوصفي التحليلي المقارن، من أجل بيان ماهية الاحتيال المالي من خلال المواقع الإلكترونية، وركني الجريمة المادي والمعنوي والعقوبة المقررة لفاعلها، وأنواع الطرق الاحتيالية التي يلجأ إليها الجناة للإيقاع بضحاياهم، ومن ثم نقوم بتحليل النصوص القانونية ومقارنتها لكل من نظام مكافحة الجرائم المعلوماتية السعودي، وقانون مكافحة جرائم تقنية المعلومات الكويتي، وقانون مكافحة الجرائم الإلكترونية القطري، وقانون مكافحة جرائم تقنية المعلومات المصري.

3. 1 خطة الدراسة

تناولت الدراسة الجانب الموضوعي للاحتيال المالي من خلال المواقع الإلكترونية في النظام السعودي مقارنًا ببعض التشريعات العربية، بتقسيمها إلى مبحثين: نتناول من خلال المبحث الأول ماهية الاحتيال المالي من خلال المواقع الإلكترونية، والفرق بينه وبين الاحتيال التقليدي والمشكلات القانونية التي تثيرها جريمة الاحتيال، وصور الاحتيال من خلال المواقع الإلكترونية، وفي المبحث الثاني نتحدث عن أركان جريمة الاحتيال والعقوبة المقررة لها، ثم نختم الدراسة بخاتمه متضمنة لأهم النتائج والتوصيات التي تم التوصل إليها.

4. المبحث الأول: ماهية الاحتيال المالي من خلال المواقع الإلكترونية

تعتبر جرائم الاحتيال من الجرائم الحديثة التي تزايدت في وقتنا

الحالي؛ نتيجة لتزايد استخدام الأفراد للمواقع الإلكترونية، كما أنها تشكل اعتداءً على الذمة المالية للفرد من خلال استخدام النظام المعلوماتي الذي يكون فيها هو الوسيلة المستخدمة لإتمام الفعل الإجرامي (البقمي، 2009، ص. 244).

ولذلك سنتناول من خلال هذا المبحث التعريف بجريمة الاحتيال كمطلب أول، والفرق بينه وبين الاحتيال بصورته التقليدية كمطلب ثانٍ، وأيضًا المشكلات القانونية التي تثيرها جرائم الاحتيال، وفي المطلب الأخير نتناول صور الاحتيال من خلال المواقع الإلكترونية.

4. 1 المطلب الأول: التعريف بالاحتيال من خلال المواقع الإلكترونية

نتناول قبل الحديث عن التعريف بالاحتيال من خلال المواقع الإلكترونية، التعريف بالموقع الإلكتروني.

التعريف بالموقع الإلكتروني

يرجع اعتماد الأفراد على المواقع الإلكترونية لإنجاز معاملاتهم اليومية، إلى التطور الذي يشهده العالم اليوم في الشبكة العالمية «الإنترنت»، وبالرغم من الخدمات التي تقدمها تلك المواقع، ظهر على الجانب الآخر احتراف الجناة في ارتكاب جرائم مستحدثة ترتبط بالتقنية الحديثة، ومنها الاحتيال المالي من خلال المواقع الإلكترونية (الخن، 2011، ص11، الملا، 2021، ص. 25).

وقد عرفت المادة (الأولى/9) من نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي (رقم م/17 بتاريخ 1428/3/8هـ)، والمادة (1) من قانون مكافحة جرائم تقنية المعلومات الكويتي (رقم 63 لسنة 2015)، الموقع الإلكتروني بأنه «مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد».

كما عرفته المادة (1) من قانون مكافحة جرائم تقنية المعلومات المصري (رقم 175 لسنة 2018م) بأنه «مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة».

ومن خلال ما سبق فالموقع الإلكتروني يشتمل على العديد من البيانات والمعلومات وفقًا لعنوان محدد، ويرتبط ظهوره بظهور الإنترنت، كما يرتبط بصاحب الموقع؛ مما يجعل له أهمية في مختلف التعاملات التجارية والمالية (كامل، 2016، ص. 59).

التعريف بالاحتيال المالي

تعتبر جريمة الاحتيال من الجرائم الواقعة على الأموال، ومن صورها الاحتيال من خلال المواقع الإلكترونية؛ ولذلك تعددت تعريفات الفقه لهذه الجريمة؛ فمنهم من يعرفها بأنها «الاستيلاء على مال الغير بالخداع عبر تقنية الإنترنت» (الخن، 2011، ص39). وفي تعريف آخر بأنها «كل فعل أو سلوك غير مشروع تستخدم معه شبكة المعلومات الدولية من أجل الاستيلاء على أموال الغير باستخدام الحاسب الآلي أو إحدى وسائل تقنية المعلومات بوصفها أداة إيجابية في هذا الاستيلاء» (السويليمن، 2009، ص. 30).

كما عرف الاحتيال بعض الفقهاء بأنه «كل سلوك احتيالي أو خداع يرتبط بعملية التحسيب الإلكتروني، يهدف إلى كسب فائدة أو مصلحة مادية» (الشوابكة، 2007، ص. 178).

وفي تعريف آخر بأنه «عبارة عن فعل أو سلوك يلجأ إليه الجاني بهدف الاستيلاء على مال المجني عليه نتيجة للغلط الذي وقع فيه؛ مما يترتب عليه تسليم ماله للجاني» (عتيق، 2000، ص. 67).

وفي الأخير نستطيع القول بأن جريمة الاحتيال المالي من خلال المواقع الإلكترونية، هي «كل فعل غير مشروع يرتكبه الجاني عن طريق النظام المعلوماتي من خلال إنشاء مواقع إلكترونية وهمية أو مصطنعة أو عن طريق اختراقها بهدف الاستيلاء على مال الغير دون وجه حق».

4. 2 المطلب الثاني: أوجه الشبه والاختلاف بين جريمة الاحتيال المالي والاحتيال التقليدي

تتفق جريمة الاحتيال من خلال المواقع الإلكترونية والاحتيال بصورته التقليدية من عدة وجوه ويختلفان من وجوه أخرى:

فمن ناحية الاتفاق: تعتبر كلتا الجريمتين من جرائم الاعتداء على الأموال، يحصل الجاني من خلالهما على مال منقول مملوك للغير برضاه عن طريق الغش أو الخداع (حجازي، 2007، ص. 160)، كما أن وسائل الاحتيال لا تنحصر في نطاق معين، فكل ما من شأنه أن يؤدي إلى خداع المجني عليه يدخل ضمن تلك الوسائل، كما يشترطان توافر الركن المادي بعناصره الثلاث الفعل والنتيجة الإجرامية وعلاقة السببية، والركن المعنوي الذي يشترط توافر القصد الجنائي العام بعنصريه العلم والإرادة، إضافة إلى القصد الخاص.

أما الاختلاف فيبرز من حيث إن الاحتيال التقليدي يرتكبه الجاني بعيدًا عن النظام المعلوماتي، وهذا خلاف الاحتيال من خلال الموقع الإلكتروني الذي لا يمكن أن يقع إلا عن طريق استخدام النظام المعلوماتي، وليس على النظام ذاته، أو برامجه الملحقة به، وإنما الجاني يستخدم النظام كوسيلة لتنفيذ جريمته؛ ولذلك يرى أحد الفقهاء أن أموال الغير هي التي يجب أن تكون محلًا للحماية الجنائية

من خلال تجنب مخاطر النظام المعلوماتي وملحقاته وليس النظام المعلوماتي ذاته (الملط، 2005، ص. 216)، كما أن المال المنقول يعتبر محل جريمة الاحتيال التقليدي، بينما يتسع في جريمة الاحتيال من خلال الموقع الإلكتروني ليشمل التلاعب في بيانات الموقع وما يقدمه من خدمات للأفراد (عبد الرزاق، 2021، ص. 432).

كما يبرز الاختلاف أيضًا من حيث إن الاحتيال التقليدي لا يثير مكان وقوعه أي مشكلة، فمن السهل تحديد مكان وقوع الجريمة والمجرم والقانون واجب التطبيق، بينما يصعب ذلك بالنسبة للاحتيال المالي من خلال الموقع الإلكتروني بسبب تنفيذ الجاني جريمته من خلال الشبكة العنكبوتية على وجه السرعة وسهولة التلاعب بالدليل المادي لها، أيضًا لا تتطلب جهدًا من الجاني ولا تترك أثرًا ماديًا ملموسًا يمكن من خلاله متابعته من قبل الجهات المختصة (المناعسة وآخرون، 2001، ص107؛ العمايرة، 2012، ص. 52).

4. 3 المطلب الثالث: المشكلات التي تثيرها جريمة الاحتيال من خلال المواقع الإلكترونية

تثير جريمة الاحتيال المالي العديد من المشكلات القانونية، منها:

القانون الواجب التطبيق

جريمة الاحتيال المالي عن طريق المواقع الإلكترونية من الجرائم التي لا تتقيد بحدود جغرافية معينة، بل تعتبر من الجرائم المتجاوزة لتلك الحدود، وهذا ما سهل على الجناة ارتكابها، نظرًا لصعوبة تحديد مكان ارتكاب الواقعة ومعرفة الجناة (المناعسة وآخرون، 2001، ص. 102؛ العمايرة، 2012، ص. 51)، فهنا تثار مشكلة تحديد القانون واجب التطبيق والقضاء المختص، ولا يمكن التغلب على هذه المشكلة إلا بتضافر الجهود الدولية من خلال عقد الاتفاقيات والمعاهدات في هذا الشأن، وهذا خلاف الاحتيال التقليدي الذي غالبًا ما يسهل تحديد مكان وقوعه ومعرفة الجاني، ومن ثم لا يثير الاحتيال بتلك الصورة أي مشكلة من ناحية القانون الواجب التطبيق، فما يطبق هو قانون الدولة التي وقعت على إقليمها الجريمة، وقضائها هو المختص بنظر الدعوى.

وما يؤكد ذلك المادة (15) من نظام الجرائم المعلوماتية السعودي التي بينت أن النيابة العامة هي من تتولى التحقيق والادعاء العام في جرائم الاحتيال أمام المحكمة المختصة.

وخلافًا لما سبق عالج القانون المصري مسألة تطبيق القانون من حيث المكان من خلال المادة (3) من قانون مكافحة جرائم تقنية المعلومات عندما نصت على سريان القانون المشار إليه على كل من يرتكب جريمة خارج جمهورية مصر العربية من غير المصريين، كما أشارت المادة (4) من ذات القانون إلى مبدأ التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات، من خلال تبادل المعلومات من أجل تفادي ارتكاب جرائم تقنية المعلومات والمساعدة على التحقيق فيها وتتبع مرتكبيها.

لا تتطلب جهدًا بدنيًا لارتكابها

لا تتطلب جريمة الاحتيال من خلال المواقع الإلكترونية جهدًا بدنيًا من الجاني لتنفيذها، فهو يستخدم ذكاءه للإيقاع بضحاياه باحترافية كبيرة من خلال قدراته على التعامل مع شبكة الإنترنت التي لا تترك في الغالب أثرًا ماديًا محسوسًا، كما لا يمكن مشاهدة الجاني أو رؤيته، بسبب أنها ترتكب في بيئة افتراضية غير مادية، فكل ما يحتاج إليه هو الحصول على بيانات العملاء من حسابات وأرقام بطاقاتهم الائتمانية من خلال تعاملهم مع الموقع، ومن ثم يستخدم الطرق الاحتيالية بذكاء من أجل الإيقاع بهم وحملهم على تسليم مالهم (المناعسة وآخرون، 2001، ص. 108)، فالأداة المستخدمة في ارتكاب الجريمة هي الحاسب الآلي، حينما يقوم الجاني بعمل بعض التعديلات على المواقع الإلكترونية أو إنشاء مواقع وهمية يمارس من خلالها أفعاله الاحتيالية (حجازي، 2007، ص. 162).

صعوبة الحصول على أثر مادي لها

من الصعوبات التي يمكن أن تشكل عائقًا أمام جهات الاختصاص، إثبات جريمة الاحتيال من خلال المواقع الإلكترونية ومحاولة الوصول إلى دليل مادي ملموس؛ لأن التعامل مع الموقع الإلكتروني لا يحتاج إلى وثائق أو مستندات مكتوبة، وهذا ما سهل على الجناة إخفاء الأدلة أو محو معالمها خلال وقت وجيز قد لا يستغرق بضع دقائق (حبيباتني، 2018، ص. 88)، فالمجرم يملك الذكاء والمعرفة بالتقنية، وهذا يساعده على عدم ترك أي أثر مادي ملموس أو محسوس يكشف هويته، بل يسعى دائمًا إلى تجنب ذلك؛ مما يثير صعوبة الوصول إلى مرتكبها، أو معرفته، لعدم وجوده في مكان الجريمة (المناعسة وآخرون، 2001، ص52).

4. 4 المطلب الرابع: صور الاحتيال من خلال المواقع الإلكترونية

إنشاء موقع إلكتروني وهمي

تعتبر تلك الطريقة من أكثر أنواع الاحتيال شيوعًا في العالم الافتراضي، فمن خلالها يقوم الجناة بتصميم مواقع على صفحات الويب تبدو وكأنها مواقع صحيحة، خاصة بعمليات البيع أو الشراء

أو تحويل الأموال؛ حيث يقوم الضحايا بإدخال معلوماتهم الشخصية كالاسم وأرقام الحسابات البنكية وأرقام البطاقات الائتمانية وكلمة المرور (Dzomira, 2014, p. 18) (Šepec, 2012, p. 987). كما تتطلب بعض المواقع دفع رسوم اشتراك لإتمام عملية التسجيل، ثم يتفاجأ المشترك بعدها بإغلاق الموقع، وأنه وقع ضحية للاحتيال (الخن، 2011، ص. 50؛ عبد الرزاق، 2021، ص. 437؛ الكعبي، 2009، ص. 231).

وفي تقرير صادر عن البنك المركزي السعودي لشهر إبريل لعام 2022م، ظهر من خلاله أن من أساليب الاحتيال المتبعة التي رصدت مؤخرًا، إنشاء صفحة إلكترونية وهمية يقوم من خلالها الضحية بالدخول عليها، ومن ثم اتباع التعليمات من خلال آلية إضافة وتفعيل المستفيد وتحويل مبلغ الرسوم، وبعدها يتم توجيهه على صفحة لإدخال البيانات البنكية بغرض التوثيق، ثم بإدخال اسم البنك واسم المستخدم وكلمة المرور الخاصة بالدخول على الخدمات البنكية، ثم يحصل المحتال على بيانات الدخول البنكية من الضحية وتنفيذ العمليات المالية (تقرير البنك المركزي السعودي، 2022).

- الاحتيال من خلال الدعاية المضللة

يلجأ الجناة إلى ممارسة الاحتيال من خلال الدعاية المضللة عن طريق المواقع الوهمية، من خلال عرض بضائع أو خدمات وهمية بهدف الإيقاع بضحاياهم، كما يلجؤون أيضًا إلى الأساليب الدعائية لمواقعهم من خلال الشبكة الدولية، أو من خلال إرسال رسائل إلى البريد الإلكتروني توهم أصحابها أنهم قد حصلوا على جوائز مالية، أو أن هناك مشاريع تهدف إلى إحداث أمل أو وعد بتحقيق ربح يعود على المجني عليه (جاد، 2005، ص. 343)، ومن ثم يتطلب منهم الضغط على الرابط المرسل الذي من خلاله يتم نقلهم إلى الرابط الوهمي للموقع.

ويذهب رأي فقهي إلى أن الإعلان عن طريق الإنترنت أصبح محل شك كبير لدى الشخص العادي، وأنه يجب على الأفراد أخذ حذرهم عند اطلاعهم على مثل تلك الإعلانات وعدم الثقة بها، إذا لم يكن هناك تعامل مسبق مع الجهات المعلنة، فإذا سلموا أموالهم دون التأكد من مصداقية الإعلان فإنهم يعتبرون مفرطين في حق أنفسهم، ولا يحميهم القانون بوصفهم مجنيًا عليهم في جريمة الاحتيال (غنام، 2017، ص. 255).

وبالرغم من وجاهة هذا الرأي فإننا نرى أنه مع التطور التقني اليوم ابتدع المحتالون الكثير من الوسائل الاحتيالية التي يلجؤون إليها مستغلين اعتماد الأفراد على المواقع الإلكترونية، فقد تعرض المواقع الوهمية سلعًا من خلال الإعلان عنها من حيث السعر أو جودة المنتج، فحينما يختار الضحية السلعة يقوم بإرسال بياناته المتضمنة أرقام حساباته البنكية أو أرقام بطاقته الائتمانية لإتمام العملية الشرائية، يتم خصم المبلغ، ثم يتفاجأ فيما بعد بأن الموقع مغلق أو لا وجود له (السويلمين، 2009، ص. 90).

وفي تقرير صادر عن البنك المركزي السعودي لشهر إبريل لعام 2022م متضمن بيان أبرز إحصاءات وأساليب عمليات الاحتيال المالي لعام 2021م، منها استخدام مواقع وإعلانات إلكترونية للاستثمار الوهمي مستغلة أسماء أو جهات حكومية أو مشاهير لإيهام الضحايا بالاستثمار والربح السريع، ومن ثم الحصول على مبالغ مالية، وأيضًا من أساليب الاحتيال الإعلان عن عمل أو توظيف وهمي من خلال شبكات التوظيف واستخدام حساباتهم البنكية لتجميع الأموال الناتجة عن عمليات الاحتيال وتحويلها لخارج المملكة العربية السعودية (تقرير البنك المركزي السعودي، 2022).

وفي دراسة حديثة قامت بها جامعة نايف العربية بالتعاون مع منظمة الشرطة الجنائية الدولية (الإنتربول) في يناير 2022م، حملت عنوان (دور المؤسسات المالية في الحد من الجرائم المعلوماتية) حيث بينت تلك الدراسة من خلال تحليل (503) إعلانات احتيالية أن الزيارات لتلك المواقع الاحتيالية تزيد على (137) ألف زيارة في اليوم، وأن الطرق الاحتيالية المتبعة تصدرها الاستثمار، والبريد الإلكتروني للأعمال، والاحتيال الرومانسي عبر الرسائل النصية، وأسلوب الابتزاز الجنسي.

كما كشفت الدراسة عن أسلوب مركب صمم لاستهداف الضحية مرتين وبطريقتين مختلفتين تتطلب في المرة الأولى وقوع الضحية عن طريق الإعلانات الاحتيالية الاستثمارية؛ تمهيدًا للإيقاع به في الطريقة الإجرامية الثانية عبر إعلانات شركات لتقديم الاستشارات القانونية وتدعي استرداد الأموال.

وأكدت نتائج تحليل الإعلانات الاحتيالية أن المحتالين ينشرون إعلاناتهم في المواقع المشهورة والموثوقة عبر وكلاء الإعلانات، وكذلك استغلالهم لنماذج الإعلانات الإلكترونية لوكلاء الإعلانات عبر الإنترنت مستفيدين من تقنيات الذكاء الاصطناعي في شركات الإعلانات للوصول إلى الضحايا المحتملين.

وأخيرًا هناك عدة طرق تهدف إلى التقليل من عمليات الاحتيال، منها وجود مؤسسات مالية تعتبر كوسيط بين العميل والموقع؛ حيث يقوم العميل بإرسال المبلغ المالي لتلك المؤسسة قبل استلام السلعة المشتراة من الموقع التجاري، ولا يتم تحويل المبلغ إلى الجهة صاحبة الموقع إلا بعد التأكد من استلام العميل لسلعته، وفي حال عدم التزام الموقع بما تم الاتفاق عليه مع العميل يتم إعادة المبلغ عن طريق المؤسسة المالية (الصغير، 2003، ص. 39؛ العمايرة، 2012، ص. 149).

- الاحتيال على موقع إلكتروني حقيقي

يلجأ الجناة إلى الاحتيال على المواقع الإلكترونية الحقيقية من خلال قيامهم بشراء بعض السلع من المواقع المخصصة للبيع أو الشراء، ثم يقومون بتسديد قيمتها بواسطة بطاقة ائتمانية مزورة أو مسروقة (القاضي، 2020، ص. 163؛ الملط، 2005، ص. 232)، حيث تتيح هذه البطاقة للعميل الحق في الحصول على السلع والخدمات عبر المواقع المخصصة للبيع أو الشراء بعد خصم المبلغ من الرصيد المتاح للبطاقة (السويلمين، 2009، ص. 69).

وقد يمتد الأمر إلى عرض السلعة المشتراة بالبطاقة المزورة أو المسروقة عن طريق المواقع المخصصة للمزاد المعلن، فحينما يقوم المشتري بحجز السلعة وتسديد قيمتها يتم إرسالها له، وعندما يكتشف أمر البطاقة يخرج الجاني من عملية الاحتيال التي قام بها، بعد أن وقع المشتري وصاحب الموقع ضحية للاحتيال (عبد الرزاق،2021، ص. 433)، حيث يمثل الاحتيال في المزاد عبر الإنترنت مشكلة يتكبد الضحايا بسببها خسائر لأموالهم، وأيضًا ما تعانيه مواقع المزادات من خسارة في سمعتها عند استخدام الجناة طرقهم الاحتيالية (Conradt, 2012, p. 913).

كما قد يحصل الاحتيال من خلال توجيه المجني عليهم من خلال المواقع الحقيقية إلى مواقع احتيالية تبدو متطابقة معها؛ حيث تتطلب تلك المواقع تعبئة البيانات الشخصية كالاسم ورقم الحساب ورقم البطاقة الائتمانية لمستخدميها قبل الدخول لها (Dzomira, 2014, p. 18).

وقد يحصل الاحتيال أيضًا من خلال دخول الجاني بطريقة مشروعة لموقع إلكتروني ممن يسمح له النظام بالدخول للموقع بهدف الاستيلاء على الأموال أو السندات وتوقيعها مستغلًا بذلك النظام المعلوماتي (البقمي، 2009، ص. 252).

ولكن ما مدى وقوع الاحتيال على النظام المعلوماتي للبنك أو أجهزة الدفع الإلكتروني في حال حصل شخص على بطاقة ائتمانية مسروقة ونفذ من خلالها عمليات سحب مبالغ مالية من حساب صاحبها دون وجه حق، فهل يعد ما قام به الشخص من قبيل الوسائل الاحتيالية؟

فإنه وفقًا للسؤال السابق يعتبر ما قام به الجاني احتيالًا على النظام المعلوماتي للبنك، وإن ما قام به يدخل ضمن انتحال صفة غير صحيحة (غنام،2017، ص. 257)، والأمر لا يختلف لو قام بتمريرها على أجهزة الدفع الإلكتروني (Dzomira, 2014, p. 17).

- اصطناع موقع إلكتروني شبيه بالموقع الصحيح

الاصطناع هو إنشاء موقع إلكتروني غير موجود سلفًا (القاضي، 2020، ص. 168)، ونسبة إنشائه إلى شخص أو جهة لا صلة لها به، بهدف ممارسة الاحتيال من خلاله عن طريق خداع المجني عليهم من أجل الحصول على أموالهم بطريقة غير مشروعة، وتظهر خطورة مثل هذه المواقع من خلال قيام الضحايا بالدخول لها، وإجراء ما يخصهم من عمليات، سواء بالبيع أو الشراء وتسديد قيمتها من خلال البطاقة الائتمانية؛ مما يعني سهولة حصول الجناة على المعلومات الخاصة بتلك البطاقات، كما يتم من خلال هذه المواقع استقبال جميع الرسائل الإلكترونية الخاصة بالموقع الأصلي والاطلاع عليها؛ مما يلحق الضرر بأصحاب المواقع الأصلية، ويُفقد المتعاملين معها الثقة بها (الغافري، 2009، ص. 281؛ الصغير، 2003، ص. 37)، وإحجامهم من خلال التعامل مستقبلًا مع مثل هذه المواقع خوفًا من الوقوع في مصيدة الاحتيال.

وقد نص صراحة على تجريم فعل اصطناع موقع إلكتروني ونسبته زورًا إلى شخص طبيعي أو اعتباري قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م من خلال المادة (24) التي عاقبت كل شخص يقوم باصطناع موقع إلكتروني بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه، ولا تتجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين.

كما عاقبت المادة (3/2) من قانون مكافحة جرائم تقنية المعلومات الكويتي كل شخص زور موقعًا بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى؛ وذلك باستخدام وسيلة من وسائل التقنية بالحبس مدة لا تتجاوز ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار، ولا تتجاوز ثلاثة عشر ألف دينار أو بإحدى هاتين العقوبتين.

وخلافًا لما سبق نلحظ اختلاف المنظم السعودي عن سابقيه من ناحية عدم النص صراحةً على اصطناع موقع إلكتروني إلا أن المادة (3/3) من نظام مكافحة جرائم المعلوماتية عاقبت على فعل الدخول غير المشروع إلى الموقع الإلكتروني أو الدخول لتغيير تصاميمه أو إتلافه أو تعديله أو شغل عنوانه بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال.

فالعلة إذًا من تجريم التشريعات لموضوع الاعتداء على المواقع الإلكترونية تظهر من خلال حمايتها من عمليات الغش والخداع الإلكتروني (القاضي،2021، ص. 1112)، ومما ينبغي إيضاحه أخيرًا أن فعل الجاني هنا لا يقتصر على الاحتيال فقط، بل تتوافر بحقه جريمة التزوير المعلوماتي.

- أسلوب انتحال الشخصية من خلال الموقع المصطنع

يمارس المحتالون احتيالهم من خلال ما يعرف بأسلوب انتحال الشخصية من خلال إرسال روابط وهمية للهواتف النقالة أو لمواقع

التواصل الاجتماعي تهدف إلى خداع المجني عليهم كقيد مخالفة مرورية، أو القيام بالاتصال من أرقام تبدو في ظاهرها صحيحة تطلب منهم تحديث بياناتهم أو معلوماتهم البنكية من خلال الرابط المرسل، وعندما يبادر الضحية بالتجاوب معهم والإفصاح عن الأرقام السرية أو أرقام الحسابات الخاصة به تحصل عملية الاحتيال من خلال نقل الأموال من حساب الضحية إلى حساب المحتال.

وقد أدان القضاء السعودي أحد الجناة بجريمة احتيال بعد اعترافه المدون في محضر الاستجواب بأنه تلقى أموالًا تقدر بحوالي ثلاثمائة ألف ريال قام بسحبها نظير احتياله على أحد الأشخاص بعد أن قام بالاتصال عليه من رقم شخصي يدعي أنه يعمل في أحد البنوك التجارية قسم إدارة العلاقات العامة، وأنه يجب تحديث بياناته ومعلوماته الشخصية، وأنه سيصدر له بطاقة بنكية؛ حيث طلب من المجني عليه القيام بإدخال ما يصله من أرقام عن طريق الهاتف المصرفي لتنشيط حسابه (القضية رقم 35271846، تاريخ 1435هـ، مجموعة الأحكام القضائية لعام 1435هـ، وزارة العدل).

- الاحتيال عن طريق اختراق الموقع الإلكتروني

عرفت المادة الأولى من اللائحة التنفيذية لنظام الاتصالات السعودي الاختراق بأنه «الدخول غير المشروع بأي طريقة، من قبل أي شخص على أي جزء من شبكة اتصالات أو محتوياتها، لأي هدف أو غرض، سواء نتج عن ذلك تخريب أو تعطيل أو لم ينتج عنه شيء»، كما عرفت ذات المادة المخترق بأنه «أي شخص أو مقدم خدمة أو مستخدم قام بعملية اختراق لأي سبب من الأسباب».

ومن ثم فالاختراق يتم بأي طريقة تمكن الجاني من الدخول غير المشروع للموقع الإلكتروني، وغالبًا ما تكون باستخدام برامج متخصصة لاختراق المواقع الإلكترونية (القاضي،2021، ص. 1057) كقيامهم بوضع برامج معينة يتم من خلالها تحويل الشخص أثناء دخوله للموقع الأصلي إلى موقع آخر بديل عنه بعد أن قام الجناة سلفًا باختراق الموقع، من أجل الوصول إلى بيانات العملاء السرية من أرقام بطاقاتهم الائتمانية أو بطاقات الدفع الإلكتروني أو أرقام حساباتهم البنكية، لكي يتم استخدامها بالتحايل على المواقع الإلكترونية على حساب حاملها الأصلي، أو القيام بعمليات التحويل من حساب إلى آخر من أجل الحصول على أموالهم؛ حيث يتعاملون مع الموقع وكأنهم المستخدمون الأصليون له (الصغير، 2003، ص. 38). وقد جرمت فعل الاختراق كل من المادة (3/3) من نظام الجرائم المعلوماتية السعودي، والمادة (18) من قانون مكافحة جرائم تقنية المعلومات المصري، والمادة (3) من قانون مكافحة تقنية المعلومات الكويتي.

ومن أحدث الطرق وأخطرها ما يعرف بالتنصت على البيانات الإلكترونية من خلال قيام الجاني بالاستيلاء على خط الاتصال المؤمن بين أحد العملاء والشركة المعنية، فيقوم بدور الوسيط بينهم دون علمهم لكي تصل إليه كافة المعلومات لاستغلالها فيما بعد كيفما يشاء (الغافري، 2009، ص. 283)، فإذًا الاحتيال بوجه عام يمكن أن يكون مرتكبه من المصرح لهم بالدخول إلى نظام الحاسب الآلي أو استخدامه أو من غير المصرح لهم بذلك (المنشاوي، 2019، ص. 429).

5. المبحث الثاني: أركان جريمة الاحتيال من خلال المواقع الإلكترونية

جريمة الاحتيال من خلال المواقع الإلكترونية من أخطر جرائم الاعتداء على الأموال، وأكثرها انتشارًا في وقتنا الراهن، وينبغي لتحققها توافر ركني الجريمة المادي والمعنوي؛ لذلك سنتناول بشيء من التفصيل هذين الركنين بجانب العقوبة المقررة لها.

5. 1 المطلب الأول: الركن المادي

يتحقق الركن المادي لجريمة الاحتيال من خلال المواقع الإلكترونية بتوافر عناصره الثلاثة، السلوك الإجرامي والنتيجة الإجرامية وعلاقة السببية.

- السلوك الإجرامي

يأتي السلوك الإجرامي في جريمة الاحتيال بعدة معانٍ منها: الاحتيال أو الخداع أو التدليس وإن كانت جميعها تؤدي إلى ذات المعنى، وهي أن السلوك الإجرامي عبارة عن كل فعل يقوم به الجاني، من خلال استيلائه على مال المجني عليه بدون وجه حق، ولا يشترط أن يستولي الجاني لنفسه على مال الغير، فجريمة الاحتيال تقع تامة إذا سهل لغيره فعل الاستيلاء على تلك الأموال من خلال تزويده ببرامج تسهل عمليات الاستيلاء وتمكنه منها بالفعل (السعيد، 2008، ص. 193؛ المنشاوي، 2019، ص. 428).

ويتفق كل من المنظم السعودي والقانون الكويتي من ناحية تحديدهم لصور الاحتيال على سبيل الحصر، فالمادة (4/1) من نظام الجرائم الإلكترونية السعودي، والمادة (3/ 5) من قانون مكافحة جرائم تقنية المعلومات الكويتي حددتا صور الاحتيال بالطرق الاحتيالية، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

- الطرق الاحتيالية

تعرف الطرق الاحتيالية بأنها المظاهر الخارجية التي يلجأ إليها

الجاني لتأييد كذبه بهدف الاستيلاء على مال الغير، وبمعنى آخر هي كل كذب مصحوب بوقائع خارجية أو أفعال مادية تؤدي إلى إيهام المجني عليه بتصديق ما يدعيه الجاني؛ مما يدفعه إلى تسليم ماله بإرادته (القاضي، 2013، ص. 307؛ جاد، 2005، ص. 335؛ السعيد، 2008، ص. 201) فهي إذا عبارة عن أساليب غير مشروعة يلجأ إليها الجاني بهدف الاستيلاء على مال المجني عليه بإرادته عن طريق خداعه، ومن ثم يقع الاحتيال إذا استعان الجاني بأحد المظاهر الخارجية التي تؤيد ما يسعى إليه، وهو عبارة عن كل سلوك كاذب يؤدي إلى خداع المجني عليه، ولا يختلف الأمر إذا كان الكذب كليًا أو جزئيًا، مادام منصبًا على واقعة معينة، فالجاني يستفيد من النظام المعلوماتي من خلال التلاعب فيه لكي يوهم المجني عليه بحقيقة ما يدعيه (الشاذلي، 2020، ص. 608؛ عتيق، 2000، ص. 67؛ السعيد، 2008، ص. 194).

وقد أدانت المحكمة الجزائية في أبها بالرقم 9/2/ض/143/2 في 1428/1/9هـ أحد الجناة لقيامه بالاحتيال على سيدة والاستيلاء على أموالها، وإقناعها بالتقدم لإحدى الشركات المصرفية للاستثمار للاقتراض منها عدد خمس سيارات، بعد إيهام الشركة بأنه خالٌ للسيدة، والمصادقة على المستندات الخاصة، ثم قام ببيع تلك السيارات واستلمت السيدة قيمتها، وتسليمها للجاني نتيجة لاحتياله عليها وإيهامه لها بالزواج منها، وقد حكمت المحكمة عليه بالسجن لمدة سنة وثمانية أشهر (الشبرمي، 2008، ص. 196).

ونظرًا لتطور وسائل التقنية الحديثة واستعانة الجناة بها لتنفيذ جريمتهم، فإنه لا يمكن حصر الطرق الاحتيالية في طريقة معينة أو محددة، فهناك طرق محلها البريد الإلكتروني، أو التوقيع الإلكتروني، أو الحسابات المصرفية، أو الحصول على أرقام بطاقات الائتمان، إلا أن العامل المشترك بين هذه الطرق أنها تؤدي إلى نتيجة واحدة هي خداع المجني عليه من خلال تسليم ماله للجاني (الشاذلي، 2020، ص. 608)، ومن ثم تستوي أي طريقة منها لتحقق جريمة الاحتيال، وما يؤكد ذلك أن المنظم السعودي لم يعرف الطرق الاحتيالية كما لم يحددها، فالمادة (4/1) من نظام الجرائم الإلكترونية السعودي ذكرت عبارة «عن طريق الاحتيال»، وهذا ما يتفق مع المادة (3/5) من قانون مكافحة جرائم تقنية المعلومات الكويتي التي ذكرت عبارة «باستعمال طريقة احتيالية»، وأن القانون الكويتي أكثر وضوحًا من المنظم السعودي عندما ذكر في ذات المادة عبارة «متى كان ذلك من شأنه خداع المجني عليه»؛ مما يعني أنه لا مجال لتحقق جريمة الاحتيال إذا لم ينتج عن الطرق الاحتيالية خداع للمجني عليه، ومن ثم نرى أنه لا خلاف حيال العبارة المذكورة «عن طريق الاحتيال»، فهي تشمل الطرق الاحتيالية بأنواعها.

- اتخاذ اسم كاذب

تعتبر هذه الصورة من صور الاحتيال التي نص عليها صراحةً المنظم السعودي والقانون الكويتي، وتتمثل باتخاذ الجاني اسمًا غير اسمه الحقيقي بهدف خداع المجني عليه من أجل الاستيلاء على ماله دون وجه حق، ولا أهمية إذا كان الاسم المنتحل لشخص حقيقي له وجوده الفعلي أو من وحي الخيال، أيضًا لا أهمية إذا كان الانتحال للاسم كاملًا أو لجزءٍ منه (جاد، 2005، ص. 351)، فجريمة الاحتيال تتحقق بمجرد الاستيلاء على المال المنقول أو السندات أو توقيع هذه السندات، سواء وقع الفعل على حساب مصرفي أو بطاقة ائتمانية أو سند مالي من السندات المثبتة للحقوق أو المنشئة لها (البقمي، 2009، ص. 254).

وقد أدانت المحكمة الجزائية ببريدة بقرارها الشرعي رقم 256/4 في 8/5/1428هـ، أحد الجناة بجريمة النصب والاحتيال بالسجن مدة ثلاثة أشهر وبغرامة مالية قدرها خمسة آلاف ريال بعد قيامه بالإعلان عن حملة باسمه لنقل الحجاج خلال موسم الحج لعام 1427هـ، مع عدم وجود تصريح من الجهات المسؤولة وقيامه بالتزوير والتوقيع على محررات ومستندات لا تخصه (الشبرمي، ص. 196).

ولكن بمجرد اكتشاف المجني عليه خداع الجاني له، وأن ما يدعيه من اسم مخالف للحقيقة، فهنا لا تتحقق جريمة الاحتيال، وإنما تقف عند مرحلة الشروع إذا لم يقم بتسليم ماله للجاني (الشاذلي، 2020، ص. 609؛ عقيدة، 1998، ص. 247). لأن وقوع الاحتيال يقتضي حصول الجاني على مال المجني عليه بطريقة غير مشروعة نتيجة لخداعه واعتقاده بصحة ما يدعيه الجاني (Šepec, 2012, p. 985).

كما قد يقع الاحتيال من خلال حصول الجاني على بطاقة ائتمانية صحيحة صادرة من المؤسسة المصرفية عن طريق تقديم مستندات مزورة منتحلًا بها صفة الغير، أو تقديم بيانات غير صحيحة، بناءً عليها تصدر له المؤسسة البطاقة الائتمانية، ومن ثم يستغلها في عمليات الشراء أو تسديد الخدمات الإلكترونية (حجازي، 2007، ص. 166؛ الملط، 2005، ص. 232).

- انتحال صفة غير صحيحة

نص المنظم السعودي صراحةً على هذه الصورة «انتحال صفة غير صحيحة» من خلال المادة (4/1) من نظام جرائم المعلوماتية، وأيضًا المادة (3/5) من قانون جرائم تقنية المعلومات الكويتي، ومن ثم تتحقق جريمة الاحتيال من خلال هذه الصورة عن طريق ادعاء الجاني كذبًا صفة ليست له أو زالت عنه وأصبح ليس لها وجود؛ مما يجعله محل ثقة لدى المجني عليه (الشاذلي، 2020، ص. 609؛

عقيدة، 1998، ص. 247؛ جاد، 2005، ص. 353)، ومن ثم لا توجد صفة معينة يعتمد عليها الجاني في ممارسة احتياله تجاه المجني عليهم (السعيد، 2008، ص. 223)، فأي صفة غير صحيحة تكفي لتحقق جريمة الاحتيال، فقد يدعي الجاني ملكيته لموقع إلكتروني يختص بتقديم الخدمات للأفراد، أو يختص بالتحليل المالي، أو أنه وكيل عن أحد المواقع العالمية، أو يكون مختصًا بالاستشارات المالية، إلى غير ذلك من الصفات التي تجعله محل ثقة للمجني عليه الذي يقوم بتحويل أمواله إلكترونيًا لتلك المواقع، أو الخصم مباشرة من حسابه الشخصي.

كما يتحقق الاحتيال من خلال هذه الصورة بحصول الجاني على أرقام البطاقات الائتمانية للمجني عليهم من خلال الموقع الإلكتروني، ومن ثم إعطاء أمر إلى البنك مصدر البطاقة بالتحويل من حساب المجني عليه إلى حساب آخر منتحلًا صفة صاحبها، ومن ثم فإن ما يقوم به الجاني يعد من قبيل انتحال صفة كاذبة (المنشاوي، 2019، ص. 429).

وخلافًا لما سبق حددت المادة (23) من قانون مكافحة جرائم تقنية المعلومات المصري صور الاحتيال، وعاقبت عليها من خلال استخدم الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية، كما عاقبت الجاني إذا قصد من استخدامها الحصول على أموال الغير أو توصل إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

- النتيجة الإجرامية

بجانب توافر عنصر السلوك الإجرامي، يشترط لتحقق جريمة الاحتيال أن تتحقق النتيجة الإجرامية المتمثلة في استيلاء الجاني على مال المجني عليه برضاه نتيجة لوقوعه ضحية للاحتيال، ولا يشترط في التسليم أن يتم مباشرة للجاني بنفسه، فقد يسلم إلى شريكه أو إلى أي شخص آخر حسن النية، ولكن يتعين في التسليم أن يكون ناقلًا الحيازة الكاملة للشيء بعنصريها المادي والمعنوي (القاضي، 2013، ص. 321؛ عقيدة، 1998، ص. 248)، كما تتحقق النتيجة الإجرامية من خلال اشتراك المجني عليه في مواقع وهمية أو مضللة أو مصطنعة بهدف الحصول على ما تقدمه من خدمات، ثم يقوم بعدها بتحويل المبالغ المالية لصاحب المواقع الاحتيالية، كما قد يحدث العكس بأن يحتال الجاني على مواقع إلكترونية حقيقية من خلال استخدامه لبطاقة ائتمانية مسروقة أو مزورة.

- علاقة السببية

يشترط لتحقق جريمة الاحتيال أن تتوافر علاقة السببية بين طرق الاحتيال التي يلجأ إليها الجاني والنتيجة المترتبة عليه والمتمثلة في حصول الجاني على مال المجني عليه بإرادته نتيجة لخداعه على أن يكون هذا الخداع هو الدافع إلى تسليم ماله، وبالرغم من اشتراط توافر علاقة السببية فإنه ينبغي أن يكون الاحتيال سابقًا على التسليم، وأن يؤدي إلى خداع المجني عليه، وأن يتم التسليم بناء عليه (القاضي، 2013، ص. 322؛ عقيدة، 1998، ص. 251).

ولا تتحقق جريمة الاحتيال إذا لم يترتب على فعل الخداع تسليم المجني عليه ماله للجاني لانتفاء علاقة السببية بين فعل الاحتيال وتسليم المال (السعيد، 2008، ص. 231)، أما إذا كان استيلاء الجاني على مال المجني عليه يرجع إلى الوسيلة الاحتيالية التي ترتبط برابطة السببية بينها وبين فعل الاحتيال، فهنا تتحقق جريمة الاحتيال (الشاذلي، 2020، ص610)، وتؤكد المادة (3/5) من قانون مكافحة جرائم تقنية المعلومات الكويتي بأن جريمة الاحتيال لا تتحقق إلا إذا كانت الوسيلة المستخدمة من شأنها أن تؤدي إلى خداع المجني عليه.

- الركن المعنوي

تعتبر جريمة الاحتيال جريمة عمدية يشترط لتحققها توافر القصد الجنائي لدى الجاني الذي يقوم على عنصرين: هما العلم والإرادة.، فلا يتصور وقوعها بطريق الخطأ (المنشاوي، 2019، ص. 430؛ غنام، 2017، ص. 247).

ومن ثم يشترط لتوافر القصد الجنائي في جريمة الاحتيال أن يعلم الجاني أن ما يقوم به جريمة يعاقب عليها النظام، وأن فعله الذي يقوم به يهدف إلى خداع المجني عليه وإيقاعه في الغلط الذي بناءً عليه يقوم بتسليم ماله إليه، وأن هذا المال تعود ملكيته للغير (عقيدة، 1998، ص. 254) سواء أكان المال مملوكًا للمجني عليه أو مجرد حائز له.

ومما ينبغي إيضاحه أنه لا يشترط لتحقق جريمة الاحتيال وجود سابق معرفة بين الجاني والمجني عليه؛ لأن محل الجريمة هنا المال المملوك للمجني عليه، ولا أهمية إذا كان المال خاصًا به أو كان دينًا للغير بذمة المجني عليه، فالجاني حينما يقوم بإنشاء موقع إلكتروني وهمي أو يصطنعه أو يخترقه إنما يقوم بهذا الفعل من أجل الحصول على مال مملوك للغير.

وبجانب توافر عنصر العلم ينبغي أن تتجه إرادة الجاني مباشرة إلى الفعل الإجرامي المتمثل في الاحتيال، وإلى نتيجة هذا الفعل، وهو حمل المجني عليه على تسليم ماله نتيجة للاحتيال الذي وقع

فيه مع علمه بالتجريم (عقيدة، 1998، ص. 255)، وبجانب توافر القصد الجنائي العام تتطلب جريمة الاحتيال توافر القصد الخاص المتمثل في النية الخاصة التي تتجاوز الاستيلاء على المال، وهي نية تملك المال الذي تعود ملكيته للغير والاستفادة منه، فإذا انتفت النية لدى الجاني فهنا ينتفي القصد الجنائي لديه (البقمي،2009، ص255، ص144؛ الشاذلي، 2020، ص. 611)، وقد أكدت المادة (4/1) من نظام مكافحة جرائم المعلوماتية السعودي ذلك حينما عبرت بقولها «الاستيلاء لنفسه أو لغيره»، وهذا ما يتفق مع المادة (3/5) من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (23) من قانون الجرائم الإلكترونية المصري.

إلا أن بعض الفقهاء يرى أنه لا يشترط توافر القصد الجنائي الخاص لقيام جريمة الاحتيال، فهي تتحقق بمجرد توافر القصد العام (المنشاوي، 2019، ص. 430) وأخيرًا فإنه لا عبرة بالباعث في حال تحقق القصد الجنائي، فالجريمة تقوم ولو كان هدف الجاني مشروعًا.

5. 2 المطلب الثالث: العقوبة

يستحق الجاني بارتكابه فعل الاحتيال العقاب المقرر له، وتجمع التشريعات محل الدراسة على تطبيق عقوبة السجن بحق الجاني أو الغرامة المالية أو الجمع بينها، إلا أن الخلاف موضعه ما بين مدة السجن وقيمة الغرامة المالية.

فالمنظم السعودي يفرق بين عقوبة الاحتيال كجريمة إلكترونية وكجريمة تقليدية، فإذا نظرنا إلى المادة (4/1) من نظام مكافحة الجرائم المعلوماتية نجد أنها عاقبت بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

في حين أن المادة الأولى من نظام الاحتيال وخيانة الأمانة (الصادر بالمرسوم الملكي رقم (م/79) وتاريخ 1442/9/10هـ) عاقبت بالسجن مدة لا تتجاوز سبع سنوات وبغرامة مالية لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين، كل من استولى على مال للغير دون وجه حق بارتكابه فعلًا أو أكثر ينطوي على استخدام أي من طرق الاحتيال بما فيها الكذب أو الخداع أو الإيهام. ومن خلال النصين السابقين يتضح أن المنظم السعودي أراد التفرقة بين الاحتيال بصورته التقليدية والاحتيال كجريمة معلوماتية، لاسيما أنه جاء في عجز المادة (4/1) من نظام الجرائم الإلكترونية ما نصه أنه «يرتكب أيًا من الجرائم المعلوماتية» وذكرت طرق الاحتيال، ولكن ما يتضح من خلال النصين السابقين أن الاحتيال بمجمله هو الاستيلاء على مال الغير مع اختلاف الوسيلة، فهو لا يقع على برامج النظام المعلوماتي أو ملحقاته، ولكن الجاني يستخدم النظام المعلوماتي كوسيلة لتنفيذ جريمته.

ومن خلال ما سبق نجد أنفسنا أمام عقوبتين مختلفتين لذات الفعل مع اختلاف طريقة ارتكابه، فالأولى تختص بالاحتيال كجريمة إلكترونية، والثانية تختص بالاحتيال كجريمة تقليدية، وبالرغم من ذلك فإن المادة التاسعة من نظام الاحتيال المالي وخيانة الأمانة نصت على أنه «إذا شكل أي من الأفعال المشار إليها في المادتين (الأولى) و(الثانية) من هذا النظام جريمة بموجب أنظمة أخرى فتطبق العقوبة الأشد». وهذا يعني أن الجاني إذا ارتكب جريمة الاحتيال كجريمة إلكترونية، فالعقوبة المطبقة بحقه هي ما جاء بنص المادة التاسعة من نظام الاحتيال المالي وخيانة الأمانة، أي أن المادة الأولى من نظام الاحتيال المالي وخيانة الأمانة نسخت العقوبة المقررة بموجب المادة (4/1) من نظام الجرائم الإلكترونية، ومن ثم نرى أنه من الأجدر بالمنظم السعودي تدارك مثل هذا الأمر والمبادرة بتعديل نص المادة (4/1) من نظام الجرائم المعلوماتية، لكي يصبح نصها بعد التعديل كالتالي «مع عدم الإخلال بالعقوبة الواردة في المادة الأولى من نظام الاحتيال المالي وخيانة الأمانة يعاقب كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية.... إلى آخر النص»، وذلك لكي يتسق نص المادة السابعة مع النظامين المشار إليهما.

وأيضًا عاقب القانون الكويتي من خلال المادة (3/5) من قانون مكافحة جرائم تقنية المعلومات الكويتي بالحبس مدة لا تتجاوز ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار، ولا تتجاوز عشرة آلاف دينار أو الجمع بين العقوبتين كل من توصل عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال أو منفعة...

أما بالنسبة للقانون المصري فعاقب بموجب المادة (23) من قانون الجرائم الإلكترونية بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن مئة ألف جنيه، ولا تتجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين كل شخص توصل إلى الاستيلاء لنفسه أو لغيره على مال الغير، وبما أن القانون المصري حدد المدة الأقل لعقوبة الاحتيال بما لا يقل عن سنة دون تحديد حدها الأعلى، فهذا يعني ألا تزيد على ثلاث سنوات وفقًا للمادة (18) من قانون العقوبات.

6. الخاتمة

تناولت الدراسة الجانب الموضوعي للاحتيال من خلال المواقع الإلكترونية في النظام السعودي مقارنًا ببعض التشريعات العربية؛ حيث بينت ماهية الاحتيال الذي يقوم على خداع المجني عليه وإيقاعه في الغلط ليقوم بتسليم ماله للجاني، وبالرغم من المزايا التي تؤديها المواقع الإلكترونية للأفراد، كالقيام بعمليات البيع أو الشراء، أو الاطلاع على حساباتهم المصرفية، والقيام بتحويل الأموال، ظهر على الجانب الآخر فئة من الجرائم ترتكب من خلال النظام المعلوماتي، ومنها الاحتيال من خلال المواقع الإلكترونية بسبب التزايد المستمر في استخدامها من قبل الأفراد، كما تتنوع الوسائل والطرق الاحتيالية التي يلجأ إليها الجناة، فقد يكون محلها حسابات مصرفية أو الحصول على أرقام البطاقات الائتمانية للقيام بعمليات السحب والدفع منها، ومن ثم يصعب حصر الطرق الاحتيالية، كما تناولت الدراسة صور الاحتيال من خلال المواقع الإلكترونية، وأركان الجريمة وعقوبتها، ثم ختمنا دراستنا بأهم النتائج والتوصيات.

7. النتائج

توصلت الدراسة إلى مجموعة من النتائج نستطيع إيجازها فيما يلي:

1 - تزايد جرائم الاحتيال بشكل يومي من خلال المواقع الإلكترونية بسبب تنوع الطرق الاحتيالية التي يلجأ إليها الجناة، مستغلين بذلك التطور التقني الحاصل، وصعوبة الوصول إليهم.

2 - كثرة المواقع الإلكترونية الخاصة بالتجارة الإلكترونية والإعلانات المضللة دون فرض رقابة عليها؛ مما يزيد من عمليات الاحتيال.

3 - لم ينص المنظم السعودي صراحةً على تجريم اصطناع موقع إلكتروني أسوة بالقانون المصري والكويتي اللذين نصا صراحةً على تجريم اصطناع أية مواقع إلكترونية ونسبتها زورًا إلى أشخاص طبيعيين أو اعتبارين.

4 - لم يفرق المنظم السعودي بين عقوبة الاحتيال كجريمة إلكترونية، وبين عقوبة الاحتيال كجريمة تقليدية، ويتضح ذلك من خلال المادة التاسعة من نظام الاحتيال المالي وخيانة الأمانة التي نصت على أنه «إذا شكل أي من الأفعال المشار إليها في المادتين (الأولى) و(الثانية) من هذا النظام جريمة بموجب أنظمة أخرى فتطبق العقوبة الأشد». وهذا يعني أن الجاني إذا ارتكب جريمة الاحتيال كجريمة إلكترونية تطبق بحقه العقوبة المشار إليها.

8. التوصيات

توصلت الدراسة إلى مجموعة من التوصيات نستطيع إيجازها فيما يلي:

1 - نظرًا لصعوبة الوصول إلى الفاعل أو تحديد مكان وقوع ارتكاب جريمة الاحتيال باستخدام النظام المعلوماتي، توصي الدراسة التشريعات العربية بعقد اتفاقيات مشتركة لمكافحة جرائم الاحتيال والتعاون فيما بينها من ناحية تكثيف الجهود في الوصول إلى الجناة وتسليمهم.

2 - أن تتضافر جهود مؤسسات الدولة التقنية من خلال العمل على حجب المواقع الوهمية أو المصطنعة أو الإعلانات المضللة من خلال المواقع الإلكترونية، وأيضًا إنشاء منصات إلكترونية تختص بتسجيل جميع المواقع الصحيحة التي من خلالها يستطيع مستخدم الموقع التأكد من صحته، كما ينبغي للمؤسسات المصرفية التنبه إلى العمليات الحسابية التي يقوم بها عملاء البنك من خلال المواقع الإلكترونية، وذلك بتحديد مبلغ يخصم من حساب العميل، أو قيام البنك بتأخير خصم العملية الشرائية إلى حين التأكد من صحتها.

3 - أن يساير المنظم السعودي كلًا من القانون المصري والكويتي بالنص صراحةً على تجريم اصطناع أية مواقع إلكترونية ونسبتها زورًا إلى أشخاص لا علاقة لهم بها، وأيضًا العقاب على انتحال صفة أو شخصية مالك الموقع.

4 - أن يبادر المنظم السعودي بتعديل نص المادة (4/1) من نظام الجرائم المعلوماتية، لكي تصبح بالنص التالي «مع عدم الإخلال بالعقوبة الواردة في المادة الأولى من نظام الاحتيال المالي وخيانة الأمانة يعاقب كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1 - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند؛ وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة.

الإفصاح عن تضارب المصالح

يعلن جميع المؤلفين أنه ليس لديهم أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف (المؤلفون) بأن البحث المنشور لم يتلق منحة مالية من أية جهة تمويل في القطاعات العامة أو التجارية أو المؤسسات غير الربحية.

أولًا: المراجع العربية

البقمي، ناصر (2009م)، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، مكتبة القانون والاقتصاة، الرياض، المملكة العربية السعودية.

حبيباتني، بثينة (2018م)، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة الأخوة، الجزائر، عدد 50 ديسمبر، المجلد أ، ص، ص 97-85.

حجازي، عبد الفتاح (2007م)، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، مصر.

الخن، محمد طارق (2011م)، جريمة الاحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان.

السعيد، كامل (2008م)، شرح قانون العقوبات، الجرائم الواقعة على الأموال، دار الثقافة للنشر والتوزيع، عمان.

السويلمين، إبراهيم (2009م)، جريمة الاحتيال عبر شبكة المعلومات الدولية، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، عمان، الأردن.

الشاذلي، فتوح (2020م)، جرائم التعزير المنظمة في المملكة العربية السعودية، الطبعة الرابعة، مكتبة الرشد، الرياض. المملكة العربية السعودية.

الشبرمي، عبدالعزيز(2008م)، جريمة النصب والاحتيال، مجلة العدل، ع39، ص، ص 200-174.

الشوابكة، محمد أمين (2007م)، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان.

الصغير، جميل (2003م)، الحماية الجنائية والمدنية لبطاقات الائتمان المغنطة، دار النهضة العربية، القاهرة.

عبد الرزاق، رانا (2021م)، تأثير الذكاء الاصطناعي على الجريمة الإلكترونية، مجلة العلوم الإنسانية والإدارية، جامعة الملك فيصل، المجلد22، العدد (1)، ص 430-437.

عتيق، السيد (2000م) جرائم الإنترنت، دار النهضة العربية، القاهرة.

عقيدة، محمد أبو العلا (1998م)، شرح قانون العقوبات، القسم الخاص، جرائم الاعتداء على الأموال، الطبعة الثالثة، دار الفكر العربي للنشر، القاهرة.

الغافري، حسين (2009م)، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة.

غنام، محمد (2017م)، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، الطبعة الأولى.

القاضي، رامي (2020)، شرح قانون مكافحة تقنية المعلومات رقم (175) لسنة 2018 مقارنًا بالتشريعات المقارنة والمواثيق الدولية، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، الجيزة، مصر.

القاضي، رامي (2021م)، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري، العدد، 75 مارس، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، ص 997 - 1353.

القاضي، محمد مصباح (2013)، قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة وجرائم الأموال، منشورات الحلبي الحقوقية، بيروت، لبنان.

كامل، خطاب (2015/2016م)، الحماية الجزائية للتجارة الإلكترونية، رسالة دكتوراه، جامعة جيلالي اليابس، كلية الحقوق والعلوم السياسية، الجزائر.

الكعبي، محمد (2009م)، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة.

الملا، معاذ (2021م)، جرائم تقنية المعلومات وجائحة كورونا بين الواقع والمأمول، مجلة كلية القانون الكويتية العالمية، السنة التاسعة، العدد 2، يونيو، ص 64-17.

الملط، أحمد خليفة (2005م)، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر.

المناعسة، أسامة وآخرون، (2001م)، جرائم الحاسب الآلي والإنترنت، دار وائل للنشر والتوزيع، عمان.

منذر العمايرة، (2012م)، مدى الحماية الجنائية للمعلومات عبر الحاسوب والإنترنت، رسالة دكتوراه، كلية القانون، جامعة عمان العربية، عمان، الأردن.

المنشاوي، محمد (2019م)، النظام الجزائي الخاص، جرائم التعزير المنظمة في المملكة العربية السعودية، دار الكتاب الجامعي، الرياض، المملكة العربية السعودية.

ثانيًا: المراجع الأجنبية

Conradt, C. (2012). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. International Journal of Cyber Criminology, 6(1).923-912

Šepec, M. (2012). Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis. International Journal of Cyber Criminology, 6(2).984 -1000

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Governance and Control: Financial Markets and Institutions, 4(2), 16-26.