Dirasat: Human and Social Sciences, Volume 53, No. 11, 2026, 14038

Deanship of Scientific Research

The Criminal Confrontation of Attacks on Electronic Financial Wallets and the Role of the Media in Enhancing It under Jordanian Law

Shaima Bani Amer[1*], Abdullah Ehjelah[2], Yusuf Obeidat[3]

[1]Criminal Law, Yarmouk University, Irbid - Jordan.

[2] Public Law Department, Faculty of Law, Yarmouk University, Irbid-Jordan.

[3] Department of Private Law, Faculty of Law, Yarmouk University, Irbid, Jordan

Received: 10/12/2025
Revised: 18/1/2026
Accepted: 19/2/2026
Published online: 18/8/2026

[*] *Corresponding author:*
A.ehjelah@yahoo.com

Citation: Bani Amer, S., Ehjelah, A., & Obeidat, Y. (2026). The Criminal Confrontation of Attacks on Electronic Financial Wallets and the Role of the Media in Enhancing It under Jordanian Law. *Dirasat: Human and Social Sciences*, 53(11), 14038.
https://doi.org/10.35516/Hum.2026.14038

© 2026 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license https://creativecommons.org/licenses/by-nc/4.0/

Abstract

Objectives: The study aims to evaluate the adequacy of traditional and direct penal provisions in protecting electronic financial wallets from potential violations, and to examine the role of Jordanian media in reducing such violations and enhancing legal awareness regarding them.

Method: The study adopted the analytical approach to examine the applicability of traditional and direct penal provisions to offenses affecting electronic financial wallets, in addition to analyzing the preventive role of the media in addressing such violations.

Results: The findings revealed that the direct penal provisions in the Jordanian Cybercrime Law do not cover all forms of offenses against electronic financial wallets. Moreover, the application of traditional penal provisions faces challenges related to insufficient penalties or incomplete applicability to certain incidents. The results also highlighted the role of Jordanian media in raising awareness and contributing to the reduction of such violations.

Conclusion: The study recommended amending both direct and traditional penal provisions to encompass all forms of offenses against electronic financial wallets and to keep pace with legal developments. It also emphasized the importance of strengthening media efforts to enhance public awareness and reduce these criminal violations.

Keywords: Media, Law, Electronic wallet, Violations, Criminal, Acquisition.

المواجهة الجنائية للاعتداءات الو اقعة على المحفظة المالية الإلكترونية ودور الإعلام في تعزيزها في القانون الأردني

شيماء بني عامر[1*]، عبدالله احجيله[2]، يوسف عبيدات[3]

[1] القانون الجنائي،جامعة اليرموك، إربد، الأردن.

[2] قسم القانون العام، كلية القانون، جامعة اليرموك، إربد، الأردن.

[3] قسم القانون الخاص، كلية القانون، جامعة اليرموك، إربد، الأردن.

ملخّص

الأهداف: تهدف الدراسة إلى تقييم كفاية النصوص الجزائية التقليدية والمباشرة في حماية المحفظة المالية الإلكترونية من الاعتداءات المحتملة، مع بيان دور الإعلام الأردني في الحد من هذه الاعتداءات وتعزيز الوعي القانوني بهذه الاعتداءات.

المنهجية: اعتمدت الدراسة المنهج التحليلي لبحث مدى انطباق النصوص الجزائية التقليدية والمباشرة على الاعتداءات التي قد تمس المحفظة المالية الإلكترونية، إلى جانب تحليل دور الإعلام في الوقاية من هذه الاعتداءات.

النتائج: توصل البحث إلى أن النصوص الجزائية المباشرة في قانون الجرائم الإلكترونية الأردني لا تغطي كافة صور الاعتداءات على المحفظة المالية الإلكترونية، كما أن انطباق النصوص التقليدية على هذه الاعتداءات يواجه صعوبات تتعلق بعدم كفاية العقوبة أو عدم الانطباق الكامل لهذه النصوص على الوقائع، إلى جانب دور الإعلام الأردني في التوعية والحد من هذه الاعتداءات.

الخلاصة: اقترحت الدراسة تعديل النصوص الجزائية المباشرة والتقليدية لتشمل كافة الاعتداءات على المحفظة المالية الإلكترونية، مع مواكبة المستجدات القانونية، بالإضافة إلى تكثيف الجهود الإعلامية لزيادة الوعي والحد من هذه الاعتداءات الجرمية.

الكلمات الدالة: الإعلام، القانون، المحفظة الإلكترونية، اعتداءات، جنائية، الحصول.

المقدمة

في ضوء التطورات العلمية والتكنولوجية التي يشهدها العالم، أصبحت التكنولوجيا الحديثة تفرض نفسها على مختلف القطاعات، ومن أبرزها قطاع المعاملات المالية الذي شهد تطورًا متسارعًا، خاصة في مجال الوسائل الإلكترونية المستخدمة فيه، وقد نتج عن هذا التطور ظهور المحفظة المالية الإلكترونية، التي أصبحت إحدى أشهر وسائل الدفع المالي الإلكتروني، لما توفره من سهولة استخدام وانتشار واسع بين مختلف فئات المجتمع.

ونظرًا لأهمية هذه المحافظ، كان من الضروري أن يولي المشرع الأردني اهتمامًا خاصًا بها، لضمان حمايتها وتأمينها قانونيًا من أي اعتداءات قد تطال المحفظة بذاتها أو النقد الإلكتروني المخزن داخلها، وذلك لحفظ حقوق الأفراد المتعاملين بها، ولدعم التطور التكنولوجي والاقتصادي، وتسهيل حياة الأفراد في المجتمع.

ويبرز دور الإعلام كعامل رئيسي في الحد من الجرائم، إذ يسهم في نشر الوعي القانوني والسلوكي بين الأفراد، ويعرفهم بالعقوبات المترتبة على الأفعال الإجرامية، مما يسهم في الوقاية من وقوع الجرائم والاعتداءات على المحفظة الإلكترونية، ومن هنا تصبح الحاجة مُلحة لتعزيز التواصل الفعّال بين وسائل الإعلام، والجهات المختصة، والمجتمع، بما يضمن حماية المجتمع من الآثار السلبية للجرائم المالية الإلكترونية، ويرسخ الأمن والاستقرار، ويبث الطمأنينة في نفوس الأفراد.

إشكالية الدراسة وتساؤلاتها

تتمثل إشكالية هذه الداسة في محاولة الموازنة بين الحماية الجنائية والإعلامية للمحفظة المالية الإلكترونية، من خلال دراسة النصوص الجزائية التقليدية، وبيان مدى استيعابها للاعتداءات التي قد تطال المحفظة أو النقد الإلكتروني المخزن بداخلها، إلى جانب تقييم كفاية النصوص المباشرة في قانون الجرائم الإلكترونية في مواجهة جميع أشكال الاعتداءات على المحفظة المالية الإلكترونية، وبيان الدور البارز لوسائل الإعلام الأردنية في التوعية والحد من هذه الاعتداءات الجرمية.

ويتفرع عن هذه الإشكالية عدد من التساؤلات، وتتمثل فيما يلي:

1. ما المقصود بالمحفظة المالية الإلكترونية؟ وما طبيعتها القانونية؟
2. ما مدى كفاية النصوص الجزائية التقليدية لحماية المحفظة المالية الإلكترونية؟
3. ما مدى مواجهة نصوص قانون الجرائم الإلكترونية للاعتداءات الجرمية على المحفظة المالية الإلكترونية؟
4. كيف يساهم الإعلام في تعزيز المواجهة الجنائية للاعتداءات الواقعة على المحفظة المالية الإلكترونية والحد منها؟

أهمية الدراسة

تكمن أهمية هذه الدراسة في أنها تسلّط الضوء على حماية المحفظة المالية الإلكترونية من منظور مزدوج: الجانب الجزائي، والجانب الإعلامي التوعوي، وتسعى الدراسة كذلك إلى تقييم مدى كفاية النصوص التقليدية والنصوص المباشرة في قانون الجرائم الإلكترونية في مواجهة الاعتداءات على المحفظة، مع إبراز الدور الحيوي لوسائل الإعلام الأردنية في التوعية والحد من الجرائم المالية الإلكترونية، كما تساهم في تقديم توصيات عملية لتعزيز الحماية الجنائية والإعلامية للمحفظة المالية الإلكترونية، بما يدعم الأمن المالي والاستقرار الاجتماعي ويعزز الثقة في الوسائل المالية الحديثة.

منهج الدراسة

تم الاعتماد على المنهج العلمي التحليلي، وهو منهج يقوم على استعراض النصوص الجزائية بهدف فهم بنيتها القانونية واستكشاف مدى انطباقها على الوقائع المستجدة، حيث تم توظيف هذا المنهج لتحليل النصوص الجزائية المتعلقة بالتجريم والجزاء وربطها بالاعتداءات التي قد تطال المحفظة المالية الإلكترونية باعتبارها وسيله دفع إلكترونية مستحدثه، بالإضافة إلى الاعتماد عليه لتحليل الدور الإعلامي في المواجهة والحد من الاعتداءات التي تطال المحفظة المالية الإلكترونية.

خطة الدراسة

تم تقسيم الدراسة إلى ثلاث مطالب رئيسية، تناول المطلب الأول: مفهوما المحفظة المالية الإلكترونية ومحتواها النقدي، وتناول المطلب الثاني: المواجهة الجنائية المباشرة للاعتداءات الواقعة على المحفظة المالية الإلكترونية ودور الإعلام في مواجهتها، وخُصص المطلب الثالث لبيان: مدى انطباق النصوص التقليدية على الاعتداءات الجرميّة الواقعة على المحفظة المالية الإلكترونية.

المطلب الأول

مفهوما المحفظة المالية الإلكترونية ومحتواها النقدي

شهدت الخدمات المالية تحولاً كبيراً بفعل التطور التكنولوجي، فأصبحت المحفظة المالية الإلكترونية من أبرز وسائل الدفع الحديثة نظراً لسهولة استخدامها واتساع انتشارها، ونظراً لأهميتها يُعالج هذا المطلب مفهوم المحفظة الإلكترونية وطبيعتها القانونية ومحتواها النقدي في الفروع الآتية:

الفرع الأول: مفهوم المحفظة المالية الإلكترونية

أولاً: تعريف المحفظة المالية الإلكترونية

تعد المحفظة المالية الإلكترونية من أهم المستحدثات التقنية التي تستخدم في عمليات الدفع الإلكترونية، وعلى الرغم من ذلك لم تحظَ بتنظيم قانوني خاص في المنظومة التشريعية الأردنية، الأمر الذي يجعلها خاضعة لحماية قانونية غير مباشرة تستند إلى مجموعة من النصوص المتفرقة ذات الطابع المالي والجزائي والتنظيمي، هذا بالإضافة إلى الدور الرقابي الفعّال للبنك المركزي الأردني، والذي يشكل إطارًا قانونيًا رقابيًا يهدف إلى ضمان سلامة التعاملات المالية الرقمية، إلا أن هذا التنظيم لا يُعد كافياً لتوفير الحماية اللازمة للمحفظة الإلكترونية، مما يكشف عن وجود فراغ تشريعي يستدعي تدخلًا قانونيًا لحماية هذا النوع من الأموال بموجب نصوص قانونية واضحة ومباشرة.

وعليه لم يضع المشرّع الأردني تعريفاً صريحاً للمحفظة الإلكترونية، وذلك على الرغم من أهمية تحديد مفهومها بشكل دقيق، الأمر الذي جعل تحديد مفهومها من اختصاص الفقه، ومع ذلك ورد تعريف لها في الإجراءات الصادرة عن البنك المركزي الأردني، مع تحفظنا، بأنه لا يتمتع بصفة قانونية تخوله وضع تعريفات قانونية، ولعل سبب ذلك هو القصور التشريعي في تعريف المحفظة المالية الإلكترونية، واستناداً إلى صلاحياته في الإشراف على أنظمة الدفع وفق المادة(3/هـ) من نظام الدفع والتحويل الإلكتروني للأموال رقم(111) لسنة2017 والتي جاء فيها: "هـ.للبنك المركزي اعتماد أي من أنظمة الدفع الإلكترونية المستخدمة عالمياً وفقاً للشروط والمتطلبات التي يحددها البنك المركزي لهذه الغاية...".

لذلك عرّف البنك المركزي الأردني على موقعه الإلكتروني الرسمي المحفظة الإلكترونية بأنها:"حساب مالي إلكتروني يستخدم عبر تطبيق على الهاتف النقال لتحويل الأموال واستلامها ودفع الفواتير والادخار والتسوق الإلكتروني وغيرها من الاستخدامات المالية. رقم المحفظة هو رقم الهاتف النقال الذي يتم فتح المحفظة عليه"، وعرفها أيضاً بأنها:" حساب يتم الوصول إليه باستخدام تطبيق الهاتف النقال ويخزن به النقد بشكل إلكتروني".

كما وعرّف مركز الاشتمال المالي في الأردن على موقعه الرسمي المحفظة الإلكترونية بأنها:"حساب مالي إلكتروني يستخدم عبر تطبيق على الموبايل بالقيام بالمعاملات المالية الإلكترونية، مثل عمليات الدفع والتحويل"، حيث يعد هذا المركز وحدة أنشأها البنك المركزي الأردني، مستنداً في ذلك إلى صلاحيته في تنظيم النظام المالي والإشراف عليه بموجب قانون البنك المركزي رقم(23) لسنة1971 وتعديلاته تحديداً نص المادة(4) منه، حيث يعنى هذا المركز بقيادة وتنفيذ الإستراتيجية الوطنية للشمول المالي، وتهدف إلى تمكين الأفراد من استخدام الخدمات المالية الرسمية، ودعم الابتكار المالي الرقمي مثل المحفظة الإلكترونية والأنظمة الحديثة.

وعُرّفت المحفظة الإلكترونية في الفقه بأنها: " نظام مبني على أساس رقمي للقيام بالتبادلات والمعاملات التجارية الرقمية، وباستخدامها يمكن بسهولة القيام بعمليات الشراء من خلال الحواسيب أو الهواتف الذكية أو أجهزة التابلت، وبشكلٍ عام يتم ربط حسابات الأفراد في البنوك مع محفظتهم الرقمية، والتي يتم فيها توثيق وحماية أموال المستهلك ومعاملاته التجارية من شراء وتبادل".(يسعد،ودان،وآخرون،2021).

وعُرّفت أيضاً بأنها:"بطاقة إلكترونية تستخدم في تنفيذ المعاملات المالية عبر الانترنت من خلال الحاسوب أو الهاتف الذكي وتؤدي وظيفتها على نحو مماثل لبطاقات الائتمان أو بطاقة الخصم المباشر على أن يتم ربطها عادة بحساب مصرفي لإتمام عمليات الدفع".(FOUAD، ERAKAT، 2021).

ثانياً: التصنيف القانوني للمحفظة المالية الإلكترونية

أوضحنا فيما سبق أن المشرع الأردني لم يتطرق إلى تعريف المحفظة المالية الإلكترونية، الأمر الذي يعني أن الطبيعة القانونية لها لم يتم توضيحها بشكلٍ قانوني معتمد من قبل المشرع، وباعتماد تعريف البنك المركزي الأردني للمحفظة الإلكترونية سالف الذكر يمكن الاستناد إليه للوقوف على الوصف القانوني لها، حيث جاء في التعميم الصادر عن البنك المركزي الأردني إلى شركات الدفع والتحويل الإلكتروني للأموال رقم (5156/4/26) ما يلي:"حرصاً من البنك المركزي الأردني على الحفاظ على كفاءة وفعالية خدمة الدفع بالهاتف النقال، وتحديداً حسابات النقود الإلكترونية المرتبطة بأداة دفع مدفوعة مسبقاً، المحفظة الإلكترونية التي يتم توفيرها من قبلكم للعملاء...".

وبالرجوع إلى المادة(2) من تعليمات متطلبات تقديم خدمات إصدار النقود الإلكترونية وإداراتها التي عرفت حساب النقود الإلكترونية بأنه:"حساب إلكتروني يتم إنشاؤه من قبل مصدر النقود الإلكترونية للعميل، محمل بالنقود الإلكترونية وترتبط به أداة الدفع المدفوعة مسبقاً"، كما وعرّفت المادة ذاتها أداة الدفع المدفوعة مسبقاً بأنها: "أداة الدفع التي يصدرها البنك أو مصدر النقود الإلكترونية لعميلة، محملة بالنقود الإلكترونية".

كما وجاء في التقرير السنوي لأنظمة المدفوعات لعام 2018 الصادر عن البنك المركزي ما يلي:" تمثل المحفظة الإلكترونية حسابات دفع إلكترونية تقدمها مؤسسات مالية لعملائها من خلال تطبيقات إلكترونية قائمة على أجهزة الهواتف النقالة أو أجهزة الكمبيوتر تمكن أصحابها من تنفيذ عمليات

الدفع والتحويل الإلكتروني للأموال بالإضافة إلى عمليات التغذية والسحب النقدي، وتعد المحفظة الإلكترونية إحدى أدوات الدفع المدفوعة مسبقاً والتي تتطلب تخزين القيم النقدية مسبقاً عليها النقود الإلكترونية".

وفي السياق ذاته، جاء في قرار محكمة صلح جزاء اربد رقم(2022/5344): (...وعليه وحيث إن بطاقات الدفع الإلكتروني تصدر بموجب قانون خاص وأنظمة أدوات الدفع تشمل العديد من الأشكال، البطاقات،المحفظة الإلكترونية،الساعة، الاسوارة أو غيرها.....). وعليه وعلى اعتبار أن المحفظة الإلكترونية تُعد وسيلة دفع معتمدة من البنك المركزي الأردني، فهي بذلك أداة مالية منظمة قانوناً تخضع لرقابة وإشراف البنك المركزي الأردني، وذلك بغية الحفاظ على أموال المستخدمين لها وعلى سلامة عمليات الدفع، وذلك استناداً لنص المادة(4) من نظام الدفع والتحويل الإلكتروني للأموال والتي تنص على أنه:" تعتبر من أدوات الدفع أي وسيلة إلكترونية معتمدة من البنك المركزي تمكّن حاملها من إجراء عمليات الدفع أو التحويل الإلكتروني للأموال...".(بوشلوخ، كريو،2023).

الفرع الثاني: مفهوم النقد الإلكتروني

أولاً: تعريف النقد الإلكتروني

تُعدّ النقود الإلكترونية ظاهرة قانونية مستحدثة تمتاز بطبيعتها الخاصة(Aljazi,2024)، إذ تمثل المقابل الرقمي للنقود التقليدية وتعد من أهم ثمار التطور في وسائل التبادل الإلكتروني السريع، وقد أصبحت وسيلة فعّالة لإتمام مختلف المعاملات المالية عبر شبكة الإنترنت، نظراً لما توفره من سهولة وسرعة وأمان في الاستخدام.

من خلال الرجوع إلى المادة(2) من نظام الدفع والتحويل الإلكتروني للأموال نجد أنها عرّفت النقود الإلكترونية على أنها:"قيم نقدية مخزنة بالوسائل الإلكترونية تلزم مصدرها مقابل استلام قيمتها نقدا"، وتم تعريف النقود الإلكترونية في الفقه بأنها:"قيمة نقدية مدفوعة مسبقاً مخزنة على إحدى الوسيلتين الإلكترونيتين البطاقة البلاستيكية(البطاقة الذكية) ومحفظة النقود الافتراضية وتواجه قبولاً عاماً من مستخدميها غير من أصدرها لتسوية المعاملات المالية والتجارية دون ما حاجة إلى وجود حساب مصرفي عند إجراء التعامل ويلتزم المصدر برد قيمتها الحقيقية عند الطلب".(غنام،2007،إسماعيل،2009).

وبالتالي يُعدّ النقد الإلكتروني شكلاً حديثاً من المال(شريف،2020)، يقوم على وجود قيمة نقدية مخزنة في بيئة رقمية، تُعبّر عن مقابل مالي حقيقي يماثل النقود التقليدية في جوهرها، وتكمن خصوصيته في طبيعته الإلكترونية التي لا تنفي عنه صفة المال، ما دام يمثل قيمة مالية معترفاً بها وقابلة للتداول ضمن إطار قانوني منظم.(بلولة،2024).

ثانياً: العلاقة بين المحفظة الإلكترونية ومحتواها النقدي

ترتبط المحفظة والنقد الإلكتروني بعلاقة تكامل، فالمحفظة هي وعاء لتخزين وتحريك النقود الإلكترونية، ولا تُعد نقوداً بحد ذاتها، إذ تُودع النقود التقليدية لدى الجهات المرخصة فَتُحوَّل إلى نقود إلكترونية تُخزن في المحفظة، يمكن من خلالها التداول والعمل بالمحفظة الإلكترونية، كالدفع والتحويلات وغيرها من العمليات التي تتم بواسطة المحفظة الإلكترونية (أمين،2018)، وذلك بالاستناد للمادة(4/19) من نظام الدفع والتحويل الإلكتروني للأموال الأردني.

وتُعد أدوات الدفع بما فيها المحفظة الإلكترونية وسائل لا تملك قيمة مادية مستقلة، بل تستمد قيمتها من الرصيد النقدي المخزن فيها، فهي ليست نقود إلكترونية بالمعنى القانوني المتعارف عليه، ولا حتى عملة افتراضية، وتعتمد أيضاً على الامتيازات التي تمنحها الجهة المصرح لها بإصدارها سواء كان بنكاً أو غير ذلك أو ارتبطت بحساب بنكي أو دون ذلك ، فألاهم هنا أن تكون جهة الإصدار ضامنة لوسيلة الدفع.(شطا،2022).

كما ويتبيّن من أحكام الفقرة(8/أ) من قانون الجرائم الإلكترونية الأردني رقم(17) لسنة 2023 أن المحفظة الإلكترونية تُعد وعاءً تقنياً قائماً على الشبكة المعلوماتية، فالنص يُجرّم الحصول على بيانات وسائل الدفع الإلكتروني أو برامج وأوامر تشغيلها أو أنظمتها التقنية(8/أ/1و8/أ/2و8/أ/3)، بما يدل على أن الحماية متجهة إلى الوعاء التقني ذاته، لا إلى الأموال المرتبطة به، وبذلك تعتبر المحفظة الإلكترونية وعاءً أو كياناً إلكترونياً مستقلاً بذاته، له حمايةً جنائية مستقلة، بصرف النظر عن محتواه المالي.(الشبول،العدوان،2023).

في حين تنصرف الحماية في الفقرتين(8/ب) و(8/ج) إلى المال والقيمة الاقتصادية التي يمكن الحصول عليها باستخدام بيانات الدفع الإلكتروني، فالمادة(8/ب) تُجرّم استخدام البيانات بقصد الحصول على أموال الغير ولو في حالة الشروع، بينما تُعالج المادة(8/ج) حالة الاستيلاء الفعلي على المال عند استخدام تلك البيانات بصورة غير مشروعة، ويُستفاد من ذلك أن موضوع الحماية في هاتين الفقرتين هو الرصيد المالي، وليس الوعاء الإلكتروني الذي يحتوي هذا الرصيد.

وبالاستناد إلى النص السابق يتضح أن الأساس القانوني في التمييز بين الاعتداء على الوعاء الإلكتروني للمحفظة الإلكترونية والاعتداء على المال ذاته يقوم على أساس طبيعة محل الجريمة، فالوعاء الإلكتروني يتمثل في النظام المعلوماتي أو التطبيق الإلكتروني الذي يحتوي بيانات المحفظة ذاتها، ويُمكّن من إدارتها، بينما يتمثل المال الإلكتروني في الرصيد أو القيمة المالية المخزنة داخل النظام المعلوماتي.

وتظهر أهمية هذا التمييز عمليًا في الحالات التي يقتصر فيها فعل الجاني على اختراق النظام أو تعطيله دون الاستيلاء على الرصيد، حيث يُعد الاعتداء منصبًا على النظام المعلوماتي فقط، وفي حال ترتب على هذا الاختراق تحويل الأموال أو الاستيلاء عليها، فإن الجريمة تمتد لتشمل النقد الإلكتروني ذاته، ويجدر بالذكر هنا إن المادة (8 بفقراتها،أ،ب،ج) من قانون الجرائم الإلكترونية الأردني تصدت للحماية الجنائية للمحفظة الإلكترونية ومحتوياتها على نحو سنفصله فيما بعد.

والخلاصة هنا، لتطبيق القانون بشكلٍ دقيق، ينبغي التمييز فيما إذا كانت الجريمة هنا تمس النقد الإلكتروني بذاته أم تمس المحفظة الإلكترونية بذاتها أم تمس كلاهما.

المطلب الثاني

المواجهة الجنائية المباشرة للاعتداءات الو اقعة على المحفظة المالية الإلكترونية ودورالإعلام في مواجهتها

لما كانت الاعتداءات الواقعة على المحفظة المالية الإلكترونية تمسّ نقداً إلكترونياً ذو طبيعة خاصة، فإن مفهوم جريمة السرقة بصورتها التقليدية، وفق المواد(399 وما بعدها) من قانون العقوبات الأردني رقم(16) لسنة1960 لا تنطبق عند الاعتداء على المحفظة المالية الإلكترونية، لذلك فإن النص الواجب التطبيق هو نص المادة(8) من قانون الجرائم الإلكترونية، الأمر الذي لا يدع مجالاً للقول بوجود تنازع ظاهري بين النصين، لأن جريمة السرقة التقليدية تقوم على الاستيلاء المادي على مال منقول مملوك للغير، إلا أن التطور التقني غيّر من طبيعة الاعتداء على الأموال، فانتقل السلوك الإجرامي إلى بيئة إلكترونية أصبح المال فيها نقداً إلكترونياً مخزّناً في وسائط رقمية، وقد خلا قانون الجرائم الإلكترونية من نص واضح ومباشر يجرّم سرقة المال الإلكترونية بوسيلة إلكترونية، فهو اكتفى بالإحالة إلى نصوص السرقة التقليدية بموجب المادة(26) منه، وهذا بتقديرنا لا يواكب طبيعة الاعتداء الإلكتروني على المحافظ الإلكترونية.

وبالنظر إلى أركان جريمة السرقة التقليدية كما جاءت في قرار محكمة التمييز الأردنية بصفتها الجزائية رقم (2023/2095) هي: "...كما واستقر الفقه والقضاء على أن جريمة السرقة تتألف من الأركان التالية-:الركن المادي:1- ويتمثل بأخذ مال الغير المنقول.2- انعدام الرضا لدى صاحب المال. محل السرقة: بأن يكون مالاً منقولاً مملوكاً لغير السارق.القصد الجرمي: ويتمثل باتجاه إرادة الشخص الذي ارتكب فعل الأخذ لانتزاع المال ورفعه من مكانه ونقله وعلم الجاني، بأن المال الذي قام بأخذه مملوكاً للغير مع علمه بانعدام رضا الغير، وأن تتجه إرادته إلى إزالة تصرف المالك فيه بنية تملكه.. .."، ويؤكد هذا المفهوم ما ورد في المادة (399) من قانون العقوبات، إلا أنّ الانتقال إلى السرقة الإلكترونية يثير مسألتين جوهريتين هما:

- **أولاً:** يتحول فعل الأخذ من سلوك مادي قائم على السيطرة الفعلية إلى سلوك تقني يتم دون أي تفاعل مادي، فمفهوم فعل الأخذ التقليدي يقوم على إزالة يد المالك عن المال المنقول ونقله إلى حيازة الجاني، أما فعل الأخذ التقني يقوم على تحويل الأرصدة من مكان لأخر دون أي تفاعل مباشر، مما يجعله خارج نطاق مفهوم الأخذ التقليدي. (المناعسة،2025).
- **ثانياً:** يتحول محل السرقة من مال مادي محسوس إلى نقد إلكتروني ذو طبيعة رقمية غير ملموسة، فهو مال معنوي لا يقبل النقل المادي، وبالتالي يخرج من نطاق الحماية الجزائية للأموال في حالات السرقة التقليدية.

وعليه فالدخول غير المشروع إلى المحفظة الإلكترونية، والعبث بمحتواها وتحويل رصيدها من حساب المالك إلى حساب آخر، لا يعد أخذاً بالمعنى الذي قصده المشرع في جريمة السرقة، لذلك فإن الركن المادي للسرقة التقليدية لا يتحقق في الاعتداء على المحفظة الإلكترونية، لأن النقد الإلكتروني ليس مالاً مادياً يقبل الحيازة التقليدية، مما يجعل نصوص السرقة غير قابلة للتطبيق على هذا النمط من الجرائم.(عمور،2019)

ويعزز هذا الفهم ما ورد في قرار محكمة صلح جزاء عين الباشا(2020/2285) والذي جاء فيه:"...تتلخص وقائع الشكوى وكما جاءت في الملف التحقيقي بأنه وبتاريخ...قام المشتكي...بالذهاب إلى معرض أمنية الكائن في منطقة البقعة وذلك من أجل استلام المبالغ الواردة إلى محفظته والبالغة(475) دينار لدعم الخبز والدعم التكميلي حيث ورد إلى محفظة المشتكية مبلغ136 دينار بتاريخ...ومبلغ(341) دينار بتاريخ...وثم اخبروه بأنه تم صرف المبالغ المالية عن طريق تحويلها للرقم...وتوجه المشتكي إلى مركز أمن عين الباشا وتقدم بالشكوى، وتبين أن المشتكى عليهم قاموا بتهكير محفظة المشتكي...(أمنية) والمسجلة على هاتفه رقم ...حيث قاموا بسحب مبلغ(475) دينار من محفظة المشتكي..."، وقد أيدت محكمة بداية السلط بصفتها الاستئنافيةهذا الاتجاه بقرارها رقم(2023/1668).

وبناءً على هذه الوقائع أدانت المحكمة المشتكى عليه بجرم السرقة خلافاً للمادة(1/407) وذلك لسحب المال من نقاط الصرف فهو الذي شكّل جرم السرقة لتعلقه بمال مادي محسوس، وجرم الحصول قصداً ودون تصريح على بيانات مالية خلافاً للمادة(6) من قانون الجرائم الإلكترونية الملغي، والتي تقابلها المادة(8) من القانون الجديد، وبتطبيق حكم المادة(72) من قانون العقوبات، قضت المحكمة بالعقوبة الأشد، على اعتبار أن الأفعال المرتكبة كوّنت جريمتين مستقلتين لا جريمة واحدة ذات وصفيْن؛ وهو ما يشكل حالة التعدد المادي للجرائم(نمور،2025)، ويؤكد ذلك أن النقد الإلكتروني المخزن في المحفظة الإلكترونية لا يدخل في نطاق جريمة السرقة التقليدية، إلا إذا تمت ترجمة هذا الرصيد إلى مال مادي ملموس، وبذلك يتضح أن نصوص جريمة السرقة التقليدية غير كافية لمواجهة كافة الاعتداءات على المحفظة الإلكترونية، وأن التطور التقني يستلزم نصاً خاصاً يجرّم سرقة

النقد الإلكتروني بشكلٍ واضحٍ وصريح.(المناعسة،2025).

الفرع الأول: مدى انطباق نص جريمة الحصول بدون تصريح على بيانات أنظمة الدفع على المحفظة الإلكترونية

توسّع المشرّع الأردني ليشمل حماية عامة وشاملة لأنظمة الدفع الإلكتروني، وذلك بموجب نص المادة(8) من قانون الجرائم الإلكترونية، ويُعد هذا التوسّع انعكاسًا لاتجاه تشريعي واضح يرمي إلى ملائمة النصوص القانونية مع التطور التقني المتسارع، وتدارك القصور الذي قد يعتري النصوص التقليدية عند تطبيقها على الوسائل الإلكترونية الحديثة.

وفيما يتعلق بالأركان القانونية اللازمة لقيام الجريمة فقد بين قرار محكمة صلح جزاء اربد (2023/12823)هذه الأركان فنص على ما يلي:"...أولاً: الركن القانوني ويتمثل بوجود نص في القانون يُجّرِم الفعل ونص يعاقب عليه، وهو نص *المادة(8) من قانون الجرائم الإلكترونية* ...ثانياً :الركن المادي،في هذه الجريمة، وباعتبارها من الجرائم الشكلية، ومن جرائم الخطر، فيتحقق ركنها المادي، ويكتمل شكلها القانوني، بتمام السلوك الإجرامي فيها، والمتمثل بفعل الحصول بدون تصريح على البيانات أو المعلومات التي تتعلق ببطاقات الائتمان أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية .وطالما أن المشرع لم يشترط تحقيق نتيجة ما فلا يشترط قيام الفاعل باستخدام البيانات أو المعلومات، في هذه الحالة، لتحقيق أية نتيجة، لكي تطبق العقوبة بحقه، ويجب أن يكون فعل الحصول على تلك البيانات أو المعلومات قد تم بدون تصريح .وكما يُشترط أن يتم فعل الحصول على تلك البيانات أو المعلومات عن طريق النظام المعلوماتي للحاسب الآلي أو الشبكة المعلوماتية، ويشمل ذلك المواقع الإلكترونية.ثالثاً: الركن المعنوي، ويتمثل في هذه الجريمة بالقصد الجرمي العام بعنصريه العلم والإرادة، باعتبارها جريمة قصدية...".

وعليه تُظهر المادة(8) من قانون الجرائم الإلكترونية أن المشرّع قرر حماية شاملة للمحفظة المالية الإلكترونية وللنقد الإلكتروني المخزّن فيها، بحيث لم تُحصر الحماية بالرصيد المالي، وقد خُصِّصت الفقرة (8/أ/1) لحماية المعلومات والبيانات المرتبطة بالمحفظة الإلكترونية، إذ يُعدّ مجرد الحصول قصداً ودون تصريح على أي من هذه البيانات عبر الشبكة المعلوماتية جريمة قائمة بذاتها ومعاقب عليها بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات، وبغرامة تتراوح بين(2500و10,000) دينار.

كما جرّم المشرّع اصطناع أو إنشاء أو تصميم أو وضع أي وسيلة تقنية معلومات يقصد منها تمكين الوصول إلى تلك البيانات، وجعلها خاضعة للعقوبة ذاتها وذلك في المادة(8/أ/2) من ذات القانون، الأمر الذي يؤكد توجه المشرّع نحو تجريم السلوكيات التحضيرية التي تمثّل خطورة على المنظومة المالية الإلكترونية، دون انتظار تحقق النتيجة الإجرامية.

وإلى جانب ذلك اعتبرت المادة(8/أ/3) قبول التعامل بأي وسيلة من وسائل الدفع الإلكترونية المقلدة ومن ضمنها المحفظة الإلكترونية فعلاً مجرّماً معاقباً عليه بالعقوبة ذاتها بشرط علم المتعامل بعدم مشروعية الحصول عليها؛ وبذلك تكون الفقرة (أ) قد أحاطت بالحماية القانونية الكاملة لكل ما يتصل بالمحفظة المالية الإلكترونية من بيانات ووسائل وصول واستخدام غير مشروع. كما وأولت الفقرتان(ب،ج) من المادة(8) حماية خاصة للنقد الإلكتروني المخزّن داخل المحفظة المالية الإلكترونية، فبدأ المشرّع بتجريم الشروع وفق الفقرة(ب)، وذلك عندما يقوم الجاني بالحصول غير المشروع عبر الشبكة المعلوماتية أو الوسائل التقنية على البيانات أو المعلومات المتعلقة بالمحفظة ويستخدمها في محاولة الاستيلاء على أموال الغير دون تحقق النتيجة، وقد أقر المشرّع لهذا السلوك (الذي يُعد بأصله شروعاً) عقوبة الحبس من سنتين إلى ثلاث سنوات وبالغرامة من(5000إلى15,000).

ثم جاءت الفقرة(ج) لتضع الإطار العقابي للجريمة التامة، وذلك عند قيام الجاني باستخدام البيانات أو المعلومات الإلكترونية، التي حصل عليها بصورة غير مشروعة، في الاستيلاء فعلياً على الأموال المخزنة داخل المحفظة الإلكترونية، وهنا يكتمل الركن المادي بنتيجته والركن المعنوي المكونان للجريمة ذات النتيجة، وتُفرض عقوبة أشد وهي الحبس مدة ثلاث سنوات وبغرامة تتراوح ما بين (10,000و20,000) دينار، لكون الجاني تجاوز مجرد محاولة الاستيلاء إلى تحقيق نتيجة الاستيلاء الفعلي على الأموال المخزنة داخل المحفظة الإلكترونية.

ومن خلال تحليل النص السابق، يتضح أن المشرّع الأردني قد تبنى حماية جنائية متدرجة لوسائل الدفع الإلكتروني عمومًا والمحفظة المالية الإلكترونية خصوصًا، ويمكن إجمال مراحلها على النحو الآتي:

1. تجريم الحصول غير المشروع على البيانات أو المعلومات المالية الإلكترونية باعتباره فعلًا مستقلًا.
2. تجريم سلوك محاولة استخدام البيانات للاستفادة من أموال الغير، دون تحقق النتيجة، (هذا السلوك يُعد بأصله شروعاً).
3. تجريم الاستخدام الكامل الذي يفضي إلى الاستيلاء الفعلي على أموال الغير بوصفه الفعل الأشد.

ويُستنتج من ذلك أن المشرّع الأردني وسّع نطاق الحماية بحيث أصبحت البيانات والمعلومات المرتبطة بالمحفظة المالية الإلكترونية محمية بذاتها، دون حاجة إلى تحقق اعتداء مباشر على المال الإلكتروني، بل إن مجرد الدخول أو الحصول على المعلومات ينهض كجريمة قائمة بذاتها، تتدرج خطورتها تبعًا للمرحلة التي يصل إليها الجاني، من مجرد الحصول، إلى محاولة الاستفادة، وصولًا إلى الاستيلاء الفعلي على المال.

ويعكس تشديد العقوبة الوارد في المادة (8) سالفة الذكر توجهًا واضحًا للسياسة الجنائية نحو توفير حماية مشددة للأنظمة المعلوماتية التي تتضمن بيانات ذات قيمة مالية، ومن ضمنها المحفظة الإلكترونية، ويستند هذا التشديد إلى خطورة الأفعال التي لا تقتصر آثارها على ضرر فردي

فحسب، بل تمتد إلى زعزعة الثقة بالمعاملات الرقمية والنظام المالي الإلكتروني ككل، كما ويرتبط هذا الاتجاه بمبدأي الردع العام والخاص؛ فالردع العام يتحقق من خلال بث الخشية في نفوس الأفراد من مغبة المساس بالأنظمة الرقمية، بينما يهدف الردع الخاص إلى منع الجاني من العودة إلى ارتكاب ذات الأفعال عبر فرض عقوبات صارمة تتناسب مع طبيعة الجريمة الرقمية وخطورتها المتزايدة.

وفي التطبيق القضائي(Obeidat & Khasawneh & Al Otoum,2023) على ما سبق فقد جاء في قرار محكمة صلح جزاء جنوب عمان(2023/12082) ما يلي:"...وطلب ذلك الشخص من المشتكي تزويده برقم محفظته من أجل تحويل مبلغ مالي له كمساعدة مالية وقام المشتكي بتزويده برقم محفظته على زين كاش وأخبره أنه يجب أن تكون محفظته فعالة وبها على الأقل مبلغ 110 دنانير وقام المشتكي بإيداع مبلغ 110 دنانير على محفظته وطلب منه رقم OTB وقام المشتكي بتزويده بالرقم وتفاجئ المشتكي بدخول ذلك الشخص إلى محفظته وتحويل مبلغ 110 دنانير من محفظة المشتكي إلى محفظة مرتبطة برقم اورنج وهو...إدانة المشتكى عليه بجرم الاستيلاء على مال مملوك للغير عن طريق بيانات ومعلومات تتعلق بوسائل الدفع الإلكتروني تم الحصول عليها بطريقة غير مشروعة خلافاً لأحكام المادة8/ج من قانون الجرائم الإلكترونية...".

وبعد بيان نطاق المادة(8) وطبيعة الأحكام التي تقررها، يثور عدة إشكاليات تطبيقية تؤثر في فهم النص وتحدُّ من امتداده في بعض الحالات، الأمر الذي يفرض طرح التساؤلات الآتية:

- **التساؤل الأول: هل يشترط لقيام الجريمة الواردة في المادة(8/أ) أن يتم الحصول على البيانات أو المعلومات بطريقة غير مشروعة؟**

يرى الباحثون من خلال استقراء نص المادة (8/أ) أن المشرع اشترط أن يكون الحصول على البيانات أو المعلومات غير مشروع، حيث قصر المشرّع نطاق التجريم على حالتي: الحصول دون تصريح أو بما يجاوز التصريح، وبالتالي فإن الحصول المشروع - أي وفق تفويض قانوني أو إذن من صاحب البيانات–لا يشكل جريمة ما لم يتجاوزه الفاعل، أمّا إذا حصل الشخص على البيانات من دون أي تصريح، أو تجاوز حدوده، فإن الفعل يعدّ مجرّماً(احجيله ،الشّماسي،2026)- وفق المادة(8/أ) من قانون الجرائم الإلكترونية، متى تم ذلك عبر الشبكة المعلوماتية أو تقنيات المعلومات، وبناءً على ذلك فإن الحصول على البيانات والمعلومات المتعلقة بأنظمة الدفع الإلكتروني بطريقة قانونية مشروعة فإن ذلك يخرجها من نطاق التجريم الوارد في المادة(8/أ) من قانون الجرائم الإلكترونية.

- **التساؤل الثاني: هل يشترط لقيام الجرائم الواردة في المادة(8) أن يتم الحصول على البيانات إلكترونياً؟ وماذا لو تم الحصول عليها بطريقة تقليدية؟.**

يرى الباحثون أن المشرع يشترط لقيام الجريمة وفقاً لنص المادة(8) من قانون الجرائم الإلكترونية أن يتم الحصول على البيانات بوسيلة إلكترونية، لأن النص اشترط صراحة أن يكون الحصول عليها قد تم عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات (احجيله،الشّماسي،2026)، وما يؤكد ذلك ما جاء في قرار محكمة صلح جزاء اربد رقم(2023/12823):"... وكما يشترط أن يتم فعل الحصول على تلك البيانات أو المعلومات عن طريق النظام المعلوماتي للحاسب الآلي أو الشبكة المعلوماتية، ويشمل ذلك المواقع الإلكترونية..."، وبالتالي فإن أي حصول يتم بوسائل تقليدية لا ينطبق عليه حكم المادة(8)، ويُعامل وفق النصوص التقليدية في قانون العقوبات وبحسب صورة الفعل، كأن يتم سرقة مستند ورقي يحتوي بيانات المحفظة الإلكترونية، وبالتالي فهنا تنطبق نصوص جريمة السرقة التقليدية، وأيضاً في حال إفشاء الموظف المختص للبيانات الورقية دون استخدام وسيلة تقنية فهنا تنطبق نصوص جريمة إفشاء الأسرار الوظيفية في المادة(355) من قانون العقوبات.

- **التساؤل الثالث: ماذا لو تم الحصول على بيانات المحفظة بطريقة تقليدية(غير إلكترونية)، ولكن تم استخدام هذه البيانات لاحقاً للاستيلاء على النقد الإلكتروني داخل المحفظة؟ ما هو النص الواجب التطبيق؟**

في الإجابة على هذا التساؤل نرى عدم انطباق نص المادة(8) من قانون الجرائم الإلكترونية في هذه الحالة، وذلك على اعتبار أن الحصول على البيانات–وهو الركن الأول للجريمة– لم يقع بوسيلة إلكترونية، والذي يعد ركناً جوهرياً في النص الخاص، وذلك أيضاً وفقاً لقرار محكمة صلح جزاء اربد رقم(2023/12823) سالف الذكر، وعلى الرغم من أن الاستيلاء على النقد الإلكتروني بحد ذاته يُعدّ فعلاً مجرماً، إلا أن استخدم الجاني لبيانات حصل عليها بوسيلة تقليدية لإتمام عملية الاستيلاء على النقد الإلكتروني يخرج فعله من نطاق التجريم وفقاً لنص المادة (8) من قانون الجرائم الإلكترونية لانهدام الركن المادي فيها، وهذا لا يعني خروج هذا الفعل من نطاق التجريم والحماية القانونية، مما يدفعنا إلى الرجوع إلى القواعد التقليدية لحماية المحفظة الإلكترونية والنقد الإلكتروني المخزن بها، ونبحث في مدى انطباق أركانها على أي منها، وهذا ما سيتم بيانه في المطلب الثالث من هذا البحث.

الفرع الثاني: المواجهة الإعلامية للاعتداءات الواقعة على المحفظة المالية الإلكترونية

أصبح الإعلام مع تطور الحياة الاقتصادية والمالية والتقنية، أداة رئيسية في حماية الأمن المجتمعي(الزبيدي،2020) ، ولا سيما في مواجهة الجرائم الإلكترونية التي تستهدف المحفظة الإلكترونية، فالإعلام يمتلك القدرة على التأثير وتشكيل الوعي العام، مما يجعله وسيلة فعّالة لنشر الثقافة الأمنية وتعزيز إدراك الأفراد لمخاطر الجرائم التي تمس أدواتهم المالية الرقمية.(بالعربي،وآخرون،2022).

وتأتي أهمية هذا الدور الإعلامي من أن الجرائم الواقعة على المحفظة الإلكترونية لا تمس الأفراد فحسب، بل تؤثر على المجتمع بأكمله من خلال زعزعة الثقة بالأنظمة المالية الرقمية، وهو ما يستدعي توجيه الخطاب الإعلامي نحو ترسيخ مبادئ احترام القانون، والقيم السلوكية والدينية الداعية للفضيلة، وتحفيز الأفراد على التعاون مع السلطات والإبلاغ عن الأنشطة المشبوهة.(Francisco،2023).

وفي المقابل يقع على عاتق وسائل الإعلام نظراً لقوة تأثيرها واجب الامتناع عن نشر تفاصيل تقنية قد يستغلها الجناة أو تغري ضعاف النفوس بتقليدها، خصوصاً في ظل التطور المتسارع للأدوات الرقمية، فالإعلام مسؤول عن ضبط محتواه بحيث يخدم الأمن المجتمعي ويمنع انتشار أساليب الجريمة (صدارته،مالكي،2020)، وذلك في سبيل منع قيام المسؤولية الجزائية بحق وسائل الإعلام.(بن عيسى،عودي،2023).(المحمدي،2023).

ولتعزيز هذا الدور يقتضي الأمر إنشاء قنوات إعلامية رسمية ومتخصصة يقودها ذوو خبرة في الأمن السيبراني، تبث رسائل توعوية وتحذيرية مستمرة حول أمن المحفظة الإلكترونية، وتوضح للأفراد مخاطر الجرائم وعقوباتها، ويشمل ذلك برامج توعية متخصصة تهدف لبناء ثقافة رقمية راسخة للحد من التحديات التقنية التي تهدد المعاملات المالية الرقمية.(القحطاني،وآخرون،2024) وفي هذا السياق، اضطلعت وسائل الإعلام الأردنية بدور بارز في التوعية من الاعتداءات على المحفظة الإلكترونية، حيث نشرت صحف ومواقع محلية عديدة تحذيرات رسمية صادرة عن الجهات المختصة، فقد قامت مواقع جراسا نيوز والسوسنة بنقل تحذيرات البنك المركزي الأردني بشأن مخاطر مشاركة بيانات المحفظة الإلكترونية وكود التحقق، فيما نشرت مواقع جفرا نيوز وسرايا نيوز بيانات وحدة الجرائم الإلكترونية التي حذّرت من الروابط المشبوهة، والتطبيقات الوهمية، وصفحات التداول المزيفة التي تستهدف مستخدمي المحافظ الإلكترونية، كما نشرت مواقع مثل نبأ الأردن ووطنا نيوز تقارير موسّعة حول ضبط خلايا قامت بالاحتيال على محافظ مالية لمواطنين، الأمر الذي عزّز وعي الجمهور بواقعية هذه الجرائم وخطورتها.

وفي إطار حماية مستخدمي المحفظة الإلكترونية من الجرائم الإلكترونية(Al hilat، 2025)، يعمل البنك المركزي بتنسيق مباشر مع وحدة الجرائم الإلكترونية في مديرية الأمن العام، وذلك من خلال تبادل المعلومات حول أساليب الاحتيال المستجدة، وتزويد الوحدة بالبلاغات الواردة من مقدمي خدمة الدفع، وطلب اتخاذ الإجراءات القانونية بحق من يثبت تورّطه في الاختراق أو الاحتيال أو انتحال صفة الشركات المالية، والتي تقوم بدورها بنشرها على الموقع الرسمي لمديرية الأمن العام، كما يصدر البنك المركزي تعميمات وتحذيرات دورية بالتعاون مع الوحدة لتوعية الجمهور بعدم مشاركة بيانات المحفظة أو رموز التفعيل، والإبلاغ عن أي نشاط مشبوه فوراً.

وعليه فإن الإعلام الرقمي يلعب دورًا وقائيًا بارزًا في الحد من الاعتداءات الواقعة على المحافظ المالية الإلكترونية، حيث أصبح يشكل أداة فاعلة في نشر الوعي المجتمعي حول المخاطر الإلكترونية المرتبطة بوسائل الدفع الحديثة، فمع انتشار الجرائم التي تستهدف المحفظة الإلكترونية عبر الروابط الوهمية أو انتحال الصفات أو رسائل التصيد الإلكتروني، باتت المنصات الرقمية ومواقع التواصل الاجتماعي وسيلة رئيسية لتحذير المستخدمين من الأساليب الاحتيالية المستحدثة. وكما يساهم الإعلام الرقمي في تعزيز الثقافة الأمنية لدى الأفراد من خلال نشر الإرشادات المتعلقة بحماية البيانات الشخصية ومعلومات الدخول إلى المحفظة الإلكترونية، الأمر الذي ينعكس إيجابًا على تقليل فرص وقوع الجريمة، ويُعد هذا الدور مكملًا للحماية القانونية، إذ يشكل نوعًا من الردع غير المباشر من خلال كشف أنماط الاحتيال وفضح الوسائل الإجرامية المستخدمة في الاستيلاء على الأرصدة الرقمية.

وعليه نأمل أن يُسهم الإعلام التقليدي إلى جانب الرقمي في بناء ثقافة مالية رقمية آمنة، تُساعد على الحد من فُرص وقوع المتعاملين بالمحفظة الإلكترونية ضحايا للهجمات والاعتداءات الإلكترونية، مما يجعل دوره جوهرياً في المنظومة الوقائية لمنع وقوع الجرائم على المحفظة الإلكترونية من خلال التأشير على الثغرات التي يمكن استغلالها من قبل المُعتدين، مع ضرورة التنبيه هنا إلى أن هذا الدور يجب أن يبقى مقيدًا بضوابط قانونية تفرضها اعتبارات العدالة الجنائية وخاصة حماية قرينة البراءة، فالنشر الإعلامي غير المتقيد بالضوابط القانونية من الممكن أن يؤدي إلى التأثير سلباً على سير التحقيقات الجنائية أو توجيه الرأي العام نحو إدانة سابقة لأوانها، وهو ما يتعارض مع المبادئ الدستورية التي تكفل للمتهم حقه في محاكمة عادلة وافتراض البراءة إلى حين صدور حكم قطعي.

المطلب الثالث

مدى انطباق النصوص التقليدية على الاعتداءات الجرميّة الو اقعة على المحفظة المالية الإلكترونية

شهدت المحافظ المالية الإلكترونية انتشاراً واسعاً وأصبحت محلاً لصور متعددة من الاعتداءات الإلكترونية، مما يثير التساؤل حول مدى كفاية النصوص التقليدية في استيعاب هذه الوقائع، إلى جانب الدور المحوري للإعلام في تعزيز الوعي العام ومنع الوقوع ضحية لهذه الجرائم، وسيتم بيان ذلك في الفروع الآتية:

الفرع الأول: مدى انطباق نصوص جريمة الاحتيال على المحفظة الإلكترونية

أفرد المشرّع نصًا خاصًا لجريمة الاحتيال ضمن المادة(10) من قانون الجرائم الإلكترونية الأردني الجديد لسنة2023، وقبل ذلك كانت تخضع لأحكام

قانون العقوبات حصراً بموجب نص الإحالة، وقد جاء النص الجديد ليشمل مختلف صور الاحتيال التي ترتكب باستخدام الوسائل التقنية، على التحويلات المالية الإلكترونية.

وبالنظر إلى أنّ المادة(10) من قانون الجرائم الإلكترونية لم تُفصِّل أركان جريمة الاحتيال الإلكتروني (العايب،عرابة،2021)، بل اكتفت بتجريم فعل الاستيلاء على مال الغير بقصد تحقيق منفعة أو إضرار بالغير باستخدام الوسائل التقنية؛ فإن المرجع الأساس لمعرفة أركان وعناصر جريمة الاحتيال(Ehjelah،2023) - يظل المادة(417) من قانون العقوبات الأردني. وقد أوضحت محكمة التمييز الأردنية بصفتها الجزائية بقرارها رقم(2023/4233) أركان هذه الجريمة بقولها :"...*وأركان جريمة الاحتيال* هي-:أولاً: الركن المادي، وعناصره ثلاثة، وهي:1- السلوك الإجرامي، ويتمثل بنشاط إيجابي يصدر عن الفاعل باستعمال طرق احتيالية من شأنها إيهام المجني عليه بوجود مشروع كاذب أو حادث أو أمر لا حقيقة له أو إحداث الأمل عند المجني عليه بحصول ربح وهمي أو بتسديد المبلغ الذي أخذ بطريق الاحتيال أو بوجود سند دين غير صحيح أو سند مخالصة مزور أو بالتصرف في مال منقول أو غير منقول وهو يعلم أنه ليس له صفة التصرف به أو باتخاذ اسم كاذب أو صفة غير صحيحة.2- النتيجة الجرمية، وهي استيلاء الفاعل على المال...3- العلاقة السببية، وذلك بأن يكون تسليم المال للفاعل من قبل المجني عليه نتيجة لما استعمله الفاعل نحوه من الوسائل الاحتيالية...ثانياً: الركن المعنوي، فجريمة الاحتيال من الجرائم القصدية" - ويتطلب المشرع لقيامها توفر القصد الجرمي بنوعيه العام والخاص.(نمور،2018)

أما فيما يتعلق بالأركان الخاصة لجريمة الاحتيال الإلكتروني كما وردت في قانون الجرائم الإلكترونية، فقد بينها أيضاً قرار محكمة صلح جزاء شمال عمان رقم(2024/1169) والذي جاء فيه :"...أولاً :الركن المادي للجريمة:...وهذا السلوك وفقاً لأحكام المادة(10/أ) من قانون الجرائم الإلكترونية يكون سلوكاً إيجابياً يتمثل في قيام الفاعل بالاستيلاء لنفسه أو لغيره بغير حق على أي مال منقول أو غير منقول أو وثيقة تتضمن تعهداً أو إبراء من خلال الاستعانة بأية طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام المعلومات أو إحدى وسائل تقنية المعلومات.ثانياً: الركن المعنوي للجريمة:...القصد الجرمي العام...أما القصد الجرمي الخاص في مخالفة أحكام(10/أ) من قانون الجرائم الإلكترونية تتمثل بوجود نية تملك المال محل جريمة الاحتيال لدى الفاعل بإزالة تصرف المالك الحقيقي عليه والظهور عليه بمظهر المالك...".

وعليه تُظهر الاعتداءات الواقعة على المحفظة الإلكترونية تطابقًا واضحًا مع الأركان التقليدية لجريمة الاحتيال المنصوص عليها في قانون العقوبات الأردني، إذ يقوم الجاني باستخدام وسائل احتيالية إلكترونية من شأنها إيقاع المجني عليه في الغلط وحمله على تمكينه من الوصول إلى المحفظة أو تحويل الأموال منها، فالعبرة في الاحتيال لا تتعلق بوسيلة التنفيذ وإنما بتحقق عناصر الخداع والاستيلاء على مال الغير دون وجه حق. وبالتالي فإنّ جريمة الاحتيال تقوم كلما تسلّم الجاني مالاً من الغير نتيجة استعماله لأحد الأساليب الاحتيالية المنصوص عليها في المادة(417)، وقد جاء قانون الجرائم الإلكترونية الأردني في المادة(10) ليقرّر أن ارتكاب أفعال الاحتيال باستخدام الوسائل الإلكترونية أو الرقمية يعدّ احتيالاً إلكترونياً بكامل أركانه، وبما يشمل الأفعال التي تتحقق عبر الشبكات والأنظمة الإلكترونية، ومنها المحفظة المالية الإلكترونية.

وبالتالي فإنّ أي فعل احتيالي يُرتكب باستخدام الوسائل الإلكترونية بإحدى الصور المشار إليها في المادة(417) من قانون العقوبات، أو عبر الوسائط الرقمية التي تشمل الهواتف الذكية وتطبيقات الدفع والتحويل، يُعدّ جريمة احتيال إلكتروني تنطبق عليها المادة(10) من قانون الجرائم الإلكترونية، متى وقع هذا الفعل على الأموال المخزّنة في المحفظة المالية الإلكترونية أو على البيانات التي تتيح التحكم بها.(خلفة، بعيرة،2024).

ويبرز في هذا السياق عدد من صور الاحتيال الإلكتروني التي تستهدف المحفظة المالية الإلكترونية، ومن أبرزها:

1. خداع المستخدمين لإفشاء رمز التحقق (OTP) الوارد إلى هواتفهم المحمولة، وذلك عبر انتحال صفة موظف شركة، أو مصرف، أو جهة رسمية، بقصد الاستيلاء على الرصيد المتاح وتحويله دون وجه حق، وبالتالي فالاعتداء هنا يشمل المحفظة الإلكترونية بالاستيلاء على معلوماتها، ومن خلالها يقع الاستيلاء على النقد المخزن داخلها.

فجاء في قرار محكمة صلح جزاء شمال عمان رقم(2024/1169) ما يلي:"... فعل المشتكى عليه والمتمثل بقيامه باتخاذ صفة كاذبة- موظف لدى شركة أوبر، وبإيهام المشتكين الأول ولغاية الثالث بوجود أمر لا حقيقة له - طلب عبر التطبيق لرجال أعمال أجانب وشخصيات مهمة مقابل مبلغ من المال واستدراجهم لغايات كشف معلوماتهم المالية السرية على محافظهم الإلكترونية ومن ثم إجراء عمليات سحب وتحويل للمبالغ المالية المتوفرة فيها وإدخالها لحسابه الخاص بنية التملك بغير حق...إدانة المشتكى عليه...بجرم الاحتيال الإلكتروني المسند إليه بحدود المادة(10 /أ) من قانون الجرائم الإلكترونية...".

2. انتحال صفة الغير من خلال إنشاء حسابات أو صفحات مزيفة توهم الضحايا بوجود تعامل حقيقي، ثم الحصول منهم على بيانات الدخول أو أرقام الربط الخاصة بالمحفظة.

وفي قرار لمحكمة صلح جزاء الرمثا رقم(3357/ 2022) جاء متضمناً ما يلي:"....قيام المشتكى عليهما وما بذلاه من جهود منظمة من أجل تحقيق غرض معين وهو الاستيلاء على المال، مستعينين ببعضهما البعض واستعمال أساليب احتيالية تمثلت بإنشاء صفحة على موقع التواصل الاجتماعي(الفيس

بوك) باسم البنك المركز الأردني والترويج من خلالها علي قيامهم بتوزيع جوائز نقدية على عملاء البنوك وإيهام المواطنين أن جهات مثل صندوق الائتمان العسكري متعاقدة بصفة رسمية مع البنك المركزي الأردني لإضفاء المصداقية وإيقاعهم في الغلط، مما حمل عدد من الأشخاص إلى إرسال حوالات مالية إلى محافظ إلكترونية قام المشتكى عليه محمد بإنشائها...إدانة المشتكى عليهما بجرم الاحتيال بالاشتراك وفقاً لأحكام المادتين(417 و76) من قانون العقوبات بدلالة المادة 15 من قانون الجرائم الإلكترونية..." ، كما وجاء قرار محكمة بداية الرمثا بصفتها الإستئنافية رقم(2023/920) مؤيداً لقرار المحكمة.

3. الوصلات الاحتيالية التي تُرسل إلى المستخدم على شكل روابط مزيفة تشبه صفحات الدخول الرسمية، ويتم إدخال بيانات المحفظة فيها، لتنتقل مباشرة إلى المحتال الذي يستخدمها لسحب الأرصدة.

4. الاحتيال عبر طلب دفعات مسبقة مقابل خدمات أو سلع وهمية، وتوجيه المستخدم لإتمام الدفع عبر محفظته الإلكترونية، ثم اختفاء الجاني دون تقديم الخدمة أو السلعة. وبذلك جاء في قرار محكمة بداية اربد بصفتها الإستئنافية رقم(2022/5416) ما يلي:"...المشتكية...تملك حساب على موقع الفيس بوك... وفي الشهر العاشر من العام 2022 شاهدت إعلاناً تم نشره داخل السوق الأردني مضمونه أنه يوجد مستثمرين خارج الأردن يريدون تحويل العملات من الدولار إلى الدينار الأردني وأنهم يبحثون عن أناس لشرائها وتواصلت المشتكية مع مستخدمي الأرقام الموجودة على الإعلان عبر تطبيق الواتس أب ...وطُلب منها أن تقوم بتحويل مبلغ (350) دينار أردني في المرة الأولى على المحفظة رقم... ليصبح مجموع المبالغ التي قامت بإرسالها (885) دينار أردني... وعليه فإن ما أقدم عليه المشتكى عليه المستأنف من أفعال إنما تشكل كافة أركان وعناصر جرم الاحتيال خلافاً لأحكام المادة 417 من قانون العقوبات وبدلالة المادة 15 من قانون الجرائم الإلكترونية ، الأمر الذي يستوجب معه إدانته عن هذا الجرم...".

وعليه، فإن هذه الأفعال بمجملها تشكّل صوراً واضحة لجريمة الاحتيال الإلكتروني متى انصبت على المحفظة المالية الإلكترونية وامتدت لتشمل النقد المخزن داخلها، وبالتالي تخضع للحماية والعقوبات التي أقرها قانون الجرائم الإلكترونية.

الفرع الثاني: مدى انطباق نصوص جريمة إساءة الائتمان على المحفظة الإلكترونية

رغم خلو قانون الجرائم الإلكترونية من نص خاص بإساءة الائتمان، إلا أنّ المادة(26) جاءت بإحالة صريحة إلى القوانين التقليدية، وخاصة المادة(422) من قانون العقوبات، التي أوضحت أركان الجريمة وتسمح بتطبيقها على الاعتداءات الواقعة على النقد الإلكتروني بوصفه مالاً منقولاً، وفيما يلي بيان لأركانها:(الشوابكة،2015).

تُجمع جريمة خيانة الأمانة بين عدة أركان أساسية هي: فعل مادي كالاختلاس أو التبديد يحول المال المنقول من حيازة ناقصة إلى كاملة، مع ضرورة أن يكون هذا المال منقولاً وتسلمه الجاني بموجب عقد من عقود الأمانة، ويكتمل الجرم بنية التملك ونكران الائتمان، حيث يُكفي لقيام الضرر مجرد احتماله عند ارتكاب الفعل.(نمور،2018).

وبتطبيق هذه الأركان على البيئة الإلكترونية، يتبين إمكانية قيام جريمة إساءة الائتمان عبر الوسائل الإلكترونية على المحفظة المالية الإلكترونية متى تحققت شروطها القانونية، ولبيان ذلك لابد من البحث في الفرضيات الآتية، ولكن قبل البحث في الفرضيات لابد من التأكيد على أن المحفظة الإلكترونية وسيلة من وسائل الدفع الإلكتروني والتي تُخزن فيها قيم نقدية إلكترونية، وعليه فإن النقد الإلكتروني يُعد مالاً بالمعنى المقصود في المادة(422)من قانون العقوبات، مما يجعل أي اعتداء عليه محلاً صالحاً لقيام جريمة إساءة الائتمان متى توافرت أركانها الأخرى.

- **الفرضية الأولى: وقوع جريمة إساءة الائتمان من قبل مستخدمي مزود الخدمة**

تفترض هذه الحالة قيام أحد موظفي الشركات المرخصة بإدارة المحفظة الإلكترونية بالتصرف غير المشروع في الأموال المخزنة في محافظ العملاء، كتحويلها لحسابه الشخصي أو لحساب وهمي، ومثال ذلك قيام أحد موظفي شركة مرخصة لإدارة المحفظة الإلكترونية- كأن يكون مسؤولاً عن متابعة التحويلات المالية- باستغلال صلاحياته التقنية وتحويل مبالغ من محفظة أحد العملاء إلى محفظة أخرى يملكها باسمه المستعار أو باسم قريب له، دون علم صاحب المحفظة أو إذنه، فإن فعله هذا يُعد تصرفاً غير مشروعاً بالأموال المؤتمن عليها، ويترتب عليه نقل الحيازة من ناقصة إلى كاملة.

وعند تطبيق أركان جريمة إساءة الائتمان على هذه الحالة، نجد أن ركن التسليم على سبيل الأمانة بين العميل والعامل غير متحقق، لأن علاقة العميل القانونية قائمة مع الشركة لا مع الموظف، وبالتالي لا تقوم الجريمة في مواجهة العامل من جانب العميل، وإن بقي للعميل الحق في مطالبة الشركة بحقوقه.

أما بالنسبة لعلاقة العامل بالشركة، فإن عقد العمل بينهما يُعد من عقود الأمانة، ووفقاً للمادة(4/814) من القانون المدني الأردني رقم(43) لسنة1976، والتي نصت على أهم التزامات العامل والمتمثلة في أن يحرص على حفظ الأشياء المسلمة إليه لتأدية عمله بموجب القواعد العامة لعقد العمل(Obeidat,2016) وهذا الالتزام بحد ذاته يعتبر بمثابة عقد أمانة مبرم مع الشركة التي يتبع لها العامل، مما يجعل تصرف العامل في أموال الشركة إخلالاً بعقد العمل، وتقوم في حقه جريمة إساءة الائتمان قبل الشركة، وتطبق عليه أحكام ظرف التشديد المنصوص عليه في المادة(1/423) من قانون العقوبات، مع ملاحقته بناءً على شكوى من الشركة عملاً بالمادة(2/426) منه.

- **الفرضية الثانية: وقوع جريمة إساءة الائتمان من قبل الغير**

يقصد بالغير كل شخص لا تربطه علاقة تعاقدية بالمحفظة الإلكترونية، أي ليس طرفاً في عقد فتح الحساب بين العميل والشركة المرخصة، فإذا سلم صاحب المحفظة محفظته إلى الغير على سبيل الأمانة(وبالتأكيد يكون التسليم هنا حكمياً)، ثم قام الغير بالاستيلاء على محتواها النقدي أو أنكره، فإن فعله يشكل إساءة ائتمان متى توافرت باقي الأركان، وفي هذه الحالة يعاقب الجاني وفقاً لقانون العقوبات، مع تطبيق ظروف التشديد المنصوص عليها في المادة(423)، علماً بأن هذه الجريمة تُلاحق دون الحاجة لتقديم شكوى.

وبشأن جريمة كتم اللقطة(حساسنة،2023) ومدى انطباقها على الاستيلاء على المحفظة الإلكترونية فقد نص عليها قانون العقوبات في المادة(424) منه، وهي جريمة خاصة ملحقة بجريمة إساءة الائتمان، وبموجب نص الإحالة في المادة(26) من قانون الجرائم الإلكترونية تمتد أحكامها إلى الأفعال التي تُرتكب عبر الوسائل الإلكترونية، وتتمثل أركان هذه الجريمة بركن المحل والذي يجب أن يكون مالاً منقولاً مملوكاً للغير وذو طبيعة مادية، والركن المادي الذي يتمثل بقيام الجاني بالتصرف تصرف المالك في مال دخل هفوة في حيازته ثم كتمه أو رفض إعادته إلى صاحبه، وبشأن الركن المعنوي فهي من الجرائم القصدية التي يجتمع فيها القصد العام والخاص،ويتمثل القصد الجرمي فيها بالاستيلاء على مال مملوك للغير، ويمكن إثبات كل هذه الأركان بكافة وسائل الإثبات التقليدية والإلكترونية(Altaani, Ehjelah, Bani Amer, Abu Issa. 2024).

وتتحقق الجريمة في إطار المحفظة الإلكترونية عندما تصل أموال الغير إلى محفظة أحد الأشخاص بطريق الخطأ، كما في حالة التحويل المالي الخاطئ، ثم يمتنع الشخص الذي وصلت الأموال إلى حسابه عن إعادتها، ويظهر بمظهر المالك لها، وفي هذه الحالة، يكون النقد الإلكتروني المخزن في المحفظة هو محل الجريمة، ويقوم فعل الكتمان والقصد الجرمي بنية التملك، مما يستجمع كافة أركان جريمة كتم اللقطة.

وما يؤكد ذلك ما جاء في قرار محكمة صلح جزاء شمال عمان رقم (2023/7372) والذي جاء به:"...بالتدقيق تجد المحكمة أن وقائع هذه الشكوى التي خلصت إليها المحكمة تتلخص في أنه بتاريخ 5/6/2023 توجه المشتكي إلى شركة...من اجل تحويل مبلغ 300 دينار لشخص يدعى...إلا أنه قام بتحويل المبلغ بطريق الخطأ إلى المشتكى عليه... عبر محفظة زين كاش وقام المشتكي بالاتصال بالمشتكى عليه وطلب منه إعادة المبلغ إلا أن المشتكى عليه كتم المبلغ ولم يقم بإعادته...إدانة المشتكى عليه...عن جنحة التصرف تصرف المالك في المال الذي دخل بحيازته نتيجة هفوة من المالك خلافاً لأحكام المادة 424 من قانون العقوبات...".

ولا تقتصر الحماية القانونية في جريمة كتم اللقطة على مستخدمي المحفظة الإلكترونية فقط، بل تمتد لتشمل الشركات المرخصة المزودة بالخدمة أيضاً، فقد يحدث أن تُودع أموال مملوكة للشركة في حساب أحد العملاء بطريق الخطأ، ويمتنع هذا الأخير عن إعادتها، مما يُشكل جريمة كتم اللقطة متى توافرت أركانها، وتُلاحق هذه الجريمة بناءً على شكوى من الشركة المتضررة، وفقاً للمادة(1/426) من قانون العقوبات الأردني.

وعليه جاء في قرار محكمة صلح غرب عمان رقم(2022/797) ما يلي:"...الشركة المشتكية تعمل في مجال تقديم خدمات الدفع الإلكتروني من خلال محافظ (قدها) وأنه بتاريخ 1/1/2022 تم تحديث النظام في الشركة ونتيجة لحدوث خلل سمح للمشتكى عليهم بسحب مبالغ مالية من خلال تلك المحفظة دون أن يكون لهم رصيد فيها، حيث قدمت الشكوى وجرت الملاحقة... إدانة المشتكى عليهم بجرم كتم اللقائط بالوصف المعدل..."، ويتضح من هذا القرار أن الخلل الحاصل أدى إلى دخول أموال الشركة في حسابات العملاء، والذين قاموا بدورهم في كتمها وسحبها ورفض إعادتها إلى الشركة، مما استجمع كافة أركان جريمة كتم اللقطة.

ونخلص مما سبق أن النصوص التقليدية في قانون العقوبات الأردني ما تزال قادرة على استيعاب بعض حالات الاعتداء على المحفظة الإلكترونية، سواء بصورتها الاحتيالية أو بصورتها القائمة على إساءة الائتمان وكتم اللقطة، وذلك إلى جانب قانون الجرائم الإلكترونية والذي جرّم مختلف الأفعال التي ترتكب عبر الوسائل الإلكترونية، ويمكن إثبات ذلك بكافة وسائل الإثبات الجنائية بما في ذلك الاعتراف المأخوذ قانوناً من الجاني(Ehjelah ,Bani Amer,2023).

الخاتمة

خلص البحث إلى مجموعة من النتائج والتوصيات فيما يلي أبرزها:

أولاً: النتائج

1. أغفل القانون الأردني وضع تعريف قانوني دقيق للمحفظة المالية الإلكترونية، الأمر الذي أوجب الاعتماد على تعريفات البنك المركزي بوصفها إحدى وسائل الدفع المالي المعتمدة لديه، وهو ما خلق غموضًا في تحديد طبيعتها وتصنيفها القانوني.
2. إنّ العلاقة بين المحفظة الإلكترونية والنقد الإلكتروني علاقة تكاملية؛ فالمحفظة لا تملك قيمة ذاتية ولا تُعدّ مالًا بحدّ ذاتها، وإنما تستمد قيمتها من الرصيد المالي المخزّن داخلها، وبناءً عليه فإن الاعتداء قد يردّ على المحفظة باعتبارها وعاءً إلكترونياً، وقد يقع مباشرة على النقد الإلكتروني ذاته.
3. إن النصوص التقليدية لجريمة السرقة لا تستوعب صور الاعتداءات على المحفظة المالية الإلكترونية أو على النقد الإلكتروني المخزّن بداخلها، نظرًا لاختلاف مدلول "الأخذ" واختلاف مدلول "المال" في البيئة الإلكترونية.

4.وفّرت المادة (8) من قانون الجرائم الإلكترونية حماية جنائية مباشرة للمحفظة المالية الإلكترونية وللنقد الإلكتروني المخزّن داخلها، ولكن اشتراط الحصول على البيانات أو المعلومات «بوسائل إلكترونية حصراً» لقيام النماذج الجرمية المنصوص عليها في هذه المادة ضيّق نطاق هذه الحماية.

5.إن المادة (10) من قانون الجرائم الإلكترونية الأردني جرّمت الاحتيال الإلكتروني وفق الصور التقليدية الواردة في المادة (417) من قانون العقوبات، مع تشديد العقوبة عند وقوع الاحتيال بوسائل إلكترونية، لاسيما إذا طال وسائل الدفع الإلكترونية.

6.لم يُنظّم المشرع الأردني أحكام جريمة إساءة الائتمان وجريمة كتم اللقطة ضمن نصوص قانون الجرائم الإلكترونية، وإنما أحالها إلى قانون العقوبات في الحالات التي تُرتكب فيها باستخدام الوسائل الإلكترونية،على الرغم من تصوّر ارتكابها على المحافظ المالية الإلكترونية.

7.تعمل الجهات الإعلامية، بمختلف أشكالها، جنبًا إلى جنب مع البنك المركزي الأردني ووحدة مكافحة الجرائم الإلكترونية في تعزيز الحماية المسبقة للمحفظة المالية الإلكترونية، من خلال نشر التحذيرات والتعليمات المتعلّقة بالمحافظ المشبوهة، والتنبيه إلى الروابط الوهمية وأساليب الاحتيال الإلكتروني، إضافة إلى توعية الجمهور بضرورة عدم مشاركة بيانات المحافظ مع أي جهة.

ثانياً: التوصيات

1.نوصى المشرّع الأردني بوضع تعريف واضح للمحفظة المالية الإلكترونية لضبط طبيعتها وتصنيفها.

2.يُوصى بتدخل المشرّع الأردني لمعالجة ازدواج نطاق الحماية القانونية للمحافظ الإلكترونية، من خلال النص بشكلٍ واضح على حماية المحفظة ذاتها بوصفها وعاءً إلكترونياً، وحماية ما تحتويه من أرصدة مالية إلكترونية.

3.يُوصى بتعديل المادة (8) من قانون الجرائم الإلكترونية الأردني، بما يسمح بامتداد الحماية لتشمل جميع صور الحصول غير المشروع على البيانات، سواء تم ذلك بوسائل إلكترونية أم تقليدية، توحيدًا للحماية ومنعًا للرجوع إلى النصوص التقليدية في قانون العقوبات.

4.يُوصى بقيام المشرع الأردني بتنظيم أحكام جريمة إساءة الائتمان وكتم اللقطة ضمن قانون الجرائم الإلكترونية، مع تشديد العقوبة المنطبقة عليها بما يتوافق مع الجرائم الإلكترونية الأخرى.

5.يُوصى بتكثيف الجهود الإعلامية الموجهة لتعزيز الوعي المجتمعي بمخاطر مشاركة البيانات المالية، وبخطورة الروابط والرسائل الوهمية والإعلانات غير الموثوقة، لترسيخ دور الإعلام كخط دفاع وقائي في حماية المحافظ الإلكترونية.

المصادروالمراجع

إسماعيل، أ. (2009). *أساليب الحماية القانونية لمعاملات التجارة الإلكترونية: دراسة مقارنة*. (ط1). بيروت: منشورات الحلبي الحقوقية. ص330.

أمين، ي. (2018). المسؤولية الجنائية عن الاستعمال غير المشروع لبطاقات الدفع الإلكتروني. *مجلة مصر المعاصرة*، 109 (3)، ص391.

أنوار، ح. (2024). العدالة والإعلام: أي توازن بين قرينة البراءة والحق في المعلومة. *مجلة جامعة العين للأعمال والقانون*، (ع2)، ص17 وما بعدها.

بلعربي، غ. (2022). دور الإعلام في الوقاية من الجريمة". *مجلة التغير الاجتماعي*، 7(1)، ص74–75.

البلولة، ح. (2024). النقود الإلكترونية: صور وإشكال – خصائص ومزايا. *مجلة ابن خلدون للدراسات والأبحاث*، 4(10)، ص424.

بن عيسى، ع. وعودي، م. (2023). *الجرائم الإعلامية*، جامعة عين تموشنت - بلحاج بوشعيب، الجزائر، 54 وما بعدها.

بوشلوخ، ع. (2023). *الجرائم المرتبطة بالوسائل الحديثة للدفع الإلكتروني في التشريع الجزائري*، جامعة محمد البشير الإبراهيمي، الجزائر، 7 وما بعدها.

حساسنة، س. (2023). *جريمة كتم اللقطة في التشريع الفلسطيني*، جامعة القدس، فلسطين، 17 وما بعدها.

خلفة، س. وبعيرة، أ. (2024). الحماية الجزائية لوسائل الدفع الإلكتروني. *مجلة حقوق الإنسان والحريات العامة*، 9(2)، ص249.

الزبيدي، ه. (2020). *القيود القانونية على حرية التعبير في الإعلام*. (ط1). القاهرة: المركز القومي للإصدارات القانونية.ص64.

شبول، ش. والعدوان، م. (2023). الحماية الجنائية لوسائل الدفع الإلكتروني – دراسة مقارنة. *مجلة جرش*، 24(2)، ص63–64.

شريف، ه. (2020). النقود الإلكترونية: ماهيتها وأنواعها. *مجلة الشريعة والقانون*، (ع84)، ص415 وما بعدها.

شطا، م. (2022). العملات الافتراضية المشفرة وأثرها. *مجلة كلية الشريعة والقانون*، 37(1)، ص1796.

شوابكة، ع. (2015). *ضوابط التمييز بين جريمة إساءة الائتمان وجريمة الاختلاس*، جامعة الشرق الأوسط، الأردن، 11 وما بعدها.

العايب، ت. وعرابة، م. (2021). الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني. *مجلة هيرودوت*، 5(3)، ص229 وما بعدها.

عمور، ط. (2019). السرقة الإلكترونية: تكييفها الشرعي وطرق إثباتها. *مجلة الإحياء*، 19(22)، ص407–408.

احجيله،ع. الشّماسي، أ. (2026).الأوصاف القانونية لجريمة الحصول غير المشروع على المعلومات المصرفية والمالية الإلكترونية - دراسة مقارنة بين قوانين

دول مجلس التعاون الخليجي والقانون الأردني، *مجلة الحقوق والعلوم السياسية*، العدد47-1، ص297-298.
غنّام، ش. (2007). *محفظة النقود الإلكترونية – رؤية مستقبلية*. (ط1). القاهرة: دار الجامعة الجديدة. ص12.
قانون البنك المركزي رقم(23) لسنة 1971 وتعديلاته. الجريدة الرسمية: العدد (2301)، بتاريخ1971/5/25.
قانون الجرائم الإلكترونية الأردني رقم(17) لسنة 2023. الجريدة الرسمية: العدد(5874)، بتاريخ2023/8/13.
قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته. الجريدة الرسمية: العدد (1487)، بتاريخ 1960/5/1.
القانون المدني الأردني رقم(43) لسنة 1976.الجريدة الرسمية: العدد (2645)، بتاريخ 1976/8/1.
القحطاني، أ.(2024). دور الإعلام الرقمي السعودي في توعية المواطنين بتقنيات الجرائم الإلكترونية في المملكة العربية السعودية (دراسة ميدانية). *مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع*، (ع 104)، ص283-320.
قرار محكمة التمييز الأردنية بصفتها الجزائية رقم (2023/2095)، بتاريخ 2023/11/21، موقع قرارك.
قرار محكمة التمييز الأردنية بصفتها الجزائية رقم (2023/3448)، بتاريخ 2023/12/18، موقع قرارك.
قرار محكمة التمييز الأردنية بصفتها الجزائية رقم (2023/4233)،بتاريخ 2023/10/17، موقع قرارك.
قرار محكمة بداية إربد بصفتها الإستئنافية رقم (2022/5416)،بتاريخ 2022/11/30، موقع قرارك.
قرار محكمة بداية الرمثا بصفتها الإستئنافية رقم (2023/920)،بتاريخ 2023/12/17، موقع قرارك.
قرار محكمة بداية السلط بصفتها الإستئنافية رقم (2022/1668)،بتاريخ 2022/12/11، موقع قرارك.
قرار محكمة صلح جزاء إربد رقم (2023/12823)،بتاريخ 2023/12/10، موقع قرارك.
قرار محكمة صلح جزاء إربد رقم (2022/5344)،بتاريخ 2024/2/12، موقع قرارك.
قرار محكمة صلح جزاء الرمثا رقم (2022/3357)،بتاريخ 2023/11/12، موقع قرارك.
قرار محكمة صلح جزاء جنوب عمان رقم (2023/12082)،بتاريخ 2024/1/7، موقع قرارك.
قرار محكمة صلح جزاء شمال عمان رقم (2024/1669)،بتاريخ 2024/3/13، موقع قرارك.
قرار محكمة صلح جزاء شمال عمان رقم (2024/1669)،بتاريخ 2024/3/13، موقع قرارك.
قرار محكمة صلح جزاء شمال عمان رقم (2023/7372)،بتاريخ 2023/8/15، موقع قرارك.
قرار محكمة صلح جزاء عمان رقم (2024/19581)،بتاريخ 2024/12/19، موقع قرارك.
قرار محكمة صلح جزاء غرب عمان رقم (2022/797)،بتاريخ 2022/7/21، موقع قرارك.
قرار محكمة صلح عين الباشا رقم (2020/2285)،بتاريخ 2022/10/3، موقع قرارك.
المحمدي، إ. (2025). الجريمة الصحفية والإعلامية وأسباب إباحتها. *مجلة أبحاث الدراسات*، 15(91)، ص4 وما بعدها.
المناعسة، أ. (2025) . *شرح قانون الجرائم الإلكترونية*. (ط1). عمان: دار الثقافة. ص90-96.
نظام الدفع والتحويل الإلكتروني للأموال رقم (111) لسنة 2017. الجريدة الرسمية: العدد (5487)، بتاريخ 2017/11/16.
نمور، م. (2018). *الجرائم الواقعة على الأموال*. (ط6). عمّان: دار الثقافة. ص238–408.
نمور، م. (2025). *شرح قانون العقوبات – القسم الخاص*. (ط9). عمّان: دار الثقافة. ص480 وما بعدها.
يسعد، ع. بو عبد الله، و. وآخرون. (2021). دور المحفظة الإلكترونية في تعزيز الشمول المالي. *مجلة المنتدى للدراسات الاقتصادية*، 5(1)، ص405.

References

Al-Ayyab, T. & Arraba, M. (2021). Penal Protection of the Consumer Against the Crime of Electronic Fraud.. *Herodotus Journal*, 5(3), p. 229 ff.

Al-Baloula, H. (2024). Electronic Money: Forms and Issues – Characteristics and Advantages. *Ibn Khaldun Journal for Studies and Research*, 4(10), p. 424.

Aljazi, J. D., Alzubidi, K. L., & Al-Shibli, F. S. (2024). The role of the Anti-Corruption Commissions in controlling the administrative decisions [Special issue]. *Journal of Governance & Regulation*, 13(1), p 406 ff.

Al hilat, B. aldeen, & Aljazi, J. D. (2025). The Impact of Job Rotation on the Constitutional Rights of Public Employee: A Comparative Study. *An-Najah University Journal for Research - B (Humanities*), 39(2),p 83 ff

Al-Mana'seh, A. (2025). *Explanation of the Cybercrimes Law*. (1st ed.). Amman: Dar Al-Thaqafa. pp. 90–96.

Al-Mohammadi, E. (2025). Journalistic and Media Crime and the Grounds for Its Permissibility. *Journal of Research Studies*, 15(91), p. 4 ff.

Al-Qahtani, A. (2024). The Role of Saudi Digital Media in Raising Citizens' Awareness of Cybercrime Techniques in the

Kingdom of Saudi Arabia (A Field Study). *Journal of Arts Literature and Humanities and Social Sciences*, (Issue 104), pp. 283–320.

Altaani, D., & Ehjelah, A., & Bani Amer, S., & Abu Issa, H. (2024). Virtual Justice: Navigating the Challenges of Remote Testimony at the International Criminal Court. *International Journal of Criminal Justice Science*, 19(2), p.15–26.

Ehjelah, A., & Al-Shamasi, A. (2026). The legal characterizations of the crime of unlawful access to electronic banking and financial information: A comparative study between the laws of the Gulf Cooperation Council states and Jordanian law. *Journal of Law and Political Science*,1- 47, p.297–298.

Al-Zubaidi, H. (2020). *Legal Restrictions on Freedom of Expression in the Media*. (1st ed.). Cairo: National Center for Legal Publications. p. 64.

Amin, Y. (2018). Criminal Liability for the Illegal Use of Electronic Payment Cards. *Misr Al-Mu'asira Journal*, 109(3), p. 391.

Ammour, T. (2019). Electronic Theft: Its Sharia Characterization and Methods of Proof. *Al-Ihyaa Journal*, 19(22), pp. 407–408.

Anwar, H. (2024). Justice and Media: What Balance Between the Presumption of Innocence and the Right to Information. *Al-Ain University Journal of Business and Law*, (Issue 2), p. 17 ff.

Belarabi, G. (2022). The Role of Media in Crime Prevention. *Journal of Social Change*, 7(1), pp. 74–75.

Ben Issa, A. & Oudi, M. (2023). *Media Crimes*. Ain Temouchent University – Belhadj Bouchaib, Algeria, p. 54 ff.

Bouchlouk, A. (2023). *Crimes Related to Modern Electronic Payment Instruments in Algerian Legislation*. Mohamed El-Bachir El-Ibrahimi University, Algeria, p. 7 ff.

Central Bank of Jordan Law No. (23) of 1971 and its amendments, Official Gazette No. (2301), dated 25/5/1971.

Decision of the Ain Al-Basha Magistrate Court No. (2285/2020), dated 3/10/2022, Qararak website.

Decision of the Amman Magistrate Criminal Court No. (19581/2024), dated 19/12/2024, Qararak website.

Decision of the Irbid Court of First Instance, sitting as an Appellate Court, No. (5416/2022), dated 30/11/2022, Qararak website.

Decision of the Irbid Magistrate Criminal Court No. (12823/2023), dated 10/12/2023, Qararak website.

Decision of the Irbid Magistrate Criminal Court No. (5344/2022), dated 12/2/2024, Qararak website.

Decision of the Jordanian Court of Cassation, sitting as a Criminal Court, No. (2095/2023), dated 21/11/2023, Qararak website.

Decision of the Jordanian Court of Cassation, sitting as a Criminal Court, No. (4233/2023), dated 17/10/2023, Qararak website.

Decision of the Jordanian Court of Cassation, sitting as a Criminal Court, No. (3448/2023), dated 18/12/2023, Qararak website.

Decision of the North Amman Magistrate Criminal Court No. (1669/2024), dated 13/3/2024, Qararak website.

Decision of the North Amman Magistrate Criminal Court No. (1669/2024), dated 13/3/2024, Qararak website.

Decision of the North Amman Magistrate Criminal Court No. (7372/2023), dated 15/8/2023, Qararak website.

Decision of the Ramtha Court of First Instance, sitting as an Appellate Court, No. (920/2023), dated 17/12/2023, Qararak website.

Decision of the Ramtha Magistrate Criminal Court No. (3357/2022), dated 12/11/2023, Qararak website.

Decision of the Salt Court of First Instance, sitting as an Appellate Court, No. (1668/2022), dated 11/12/2022, Qararak website.

Decision of the South Amman Magistrate Criminal Court No. (12082/2023), dated 7/1/2024, Qararak website.

Decision of the West Amman Magistrate Criminal Court No. (797/2022), dated 21/7/2022, Qararak website.

Ehjelah, A. (2023). Criminal Modus Operandi in Bahraini Tax Law No. (40) of 2017. *Pakistan Journal of Criminology*, 15(4), p.389–400.

Ehjelah, A., & Bani Amer, S. (2023). Impact of Confessions Taken Remotely Via Modern Technology on the Conscientious Conviction of the Criminal Judge. *Pakistan Journal of Criminology*, 15(3), p.211-223.

Electronic Payment and Funds Transfer Regulation No. (111) of 2017, Official Gazette No. (5487), dated 16/11/2017.

Forum Journal for Economic Studies, 5(1), p. 405.

Fouad, K., & Erakat, A. (2021). Assessing Resistance to Accept Electronic Wallets in Egypt. *Journal of Economic and Legal Studies*, (18)5,P209.

Francisco Falkembach dos Santos, Media Criminology – The role of the media and its influence on contemporary society.

Available at file:///C:/Users/HP/Downloads/sevened2023.006-152.pdf. See also European Anti-Fraud Office, USING MASS MEDIA TO FIGHT ORGANISED CRIME, available at.

Ghannam, S. (2007). *Electronic Money Wallet – A Future Vision*. (1st ed.). Cairo: New University House. p. 12.

Hassasneh, S. (2023). *The Crime of Suppressing Footage in Palestinian Legislation*. Al-Quds University, Palestine, p. 17 ff.

Ismail, A. (2009). *Legal Protection Methods for Electronic Commerce Transactions: A Comparative Study*. (1st ed.). Beirut: Al-Halabi Legal Publications. p. 330.

Jordanian Civil Code No. (43) of 1976, Official Gazette No. (2645), dated 1/8/1976.

Jordanian Cybercrimes Law No. (17) of 2023, Official Gazette No. (5874), dated 13/8/2023.

Jordanian Penal Code No. (16) of 1960 and its amendments, Official Gazette No. (1487), dated 1/5/1960.

Khalfa, S. & Bouaira, A. (2024). Penal Protection of Electronic Payment Instruments. *Journal of Human Rights and Public Freedoms*, 9(2), p. 249.

Namour, M. (2018). *Crimes Against Property*. (6th ed.). Amman: Dar Al-Thaqafa. pp. 238–408.

Namour, M. (2025). *Explanation of the Penal Code – Special Part*. (9th ed.). Amman: Dar Al-Thaqafa. p. 480 ff.

Obeidat, Y. & Khasawneh, M . &. Al Otoum, N .(2023). The Jurisprudence of the Court of Cassation in Jordan: Interpreting Judicial Decisions and Case Law, *Information Sciences Letters*,.12(. 7), p.9 ff.

Obeidat, Y. (2016). The Efficient Breach Theory under Jordanian Civil Law. *Journal Arab Law Quarterly*, 30(4), 336-356.

Shatta, M. (2022). Cryptocurrencies and Their Impact. *Journal of the College of Sharia and Law*, 37(1), p. 1796.

Shawabkeh, A. (2015). *Criteria for Distinguishing Between the Crime of Breach of Trust and the Crime of Embezzlement*. Middle East University, Jordan, p. 11 ff.

Shbool, S. & Al-Adwan, M. (2023). Criminal Protection of Electronic Payment Instruments – A Comparative Study. *Jerash Journal*, 24(2), pp. 63–64.

Yassad, A., Abu Abdullah, W., et al. (2021). The Role of the Electronic Wallet in Enhancing Financial Inclusion.