المسؤولية الجزائية عن جرائم بطاقات الدفع في القانون العراقي – دراسة مقارنة

Criminal liability for payment card crimes in Iraqi law - a comparative study

م.د. احمد زهير عبد الامير
وزارة التربية – تربية كربلاء
ahmedlsltany777@gmail.com

م.د. علي فلاح حاكم
جامعة كربلاء – كلية التمريض
alifalah19791979@gmail.com

تاريخ استلام البحث: ٢٠٢٥/٩/٨ **تاريخ قبول النشر:** ٢٠٢٥/١١/١٠

الملخص:

يتناول هذا البحث المسؤولية الجزائية عن جرائم بطاقات الدفع الإلكتروني في القانون العراقي باعتبارها من الجرائم الاقتصادية الرقمية المستحدثة التي تتسم بطبيعتها غير المادية، وتطرح تحديات تتعلق بحدود التجريم، والإثبات، وتحديد المسؤولية. وينطلق البحث من تحليل الأركان القانونية لهذه الجرائم، مبيّناً أن الركن المادي يتخذ صوراً تقنية متعددة، أبرزها الاستعمال غير المشروع للبطاقة أو بياناتها، وتزوير المحتوى الرقمي، والاحتيال المعلوماتي الموجّه للأنظمة المصرفية، فضلاً عن الإهمال التقني المؤدي لوقوع الجريمة. كما يبيّن أن الركن المعنوي لم يعد مقصورًا على القصد التقليدي، بل يشمل ما يمكن تسميته بـ"القصد البرمجي" الذي يمتد إلى مرحلة إعداد الوسيلة الإلكترونية لا لحظة تنفيذ الجريمة فحسب، ويبحث البحث كذلك في المسؤولية الجزائية المباشرة لمرتكب الفعل، والمسؤولية غير المباشرة الناشئة عن الإخلال بواجب الإبلاغ أو الرقابة على أنظمة الدفع داخل المؤسسات التجارية والمصرفية، في ضوء النصوص العراقية النافذة، مقارنةً بتشريعات عربية اعتمدت تنظيماً خاصاً لجرائم الدفع الإلكتروني. ويخلص البحث إلى أن الإطار التشريعي العراقي ما يزال يعتمد قواعد عامة لا تستوعب الطبيعة التقنية للجريمة الرقمية، ويقترح سنّ نصوص عقابية مستقلة تتضمن تجريم السلوك الرقمي، والاعتراف بالأدلة الإلكترونية، وتجريم الإهمال التقني والرقابة المؤسسية، ضماناً لحماية الثقة بالنظام المالي والاقتصاد الرقمي في العراق.

الكلمات المفتاحية: جرائم الدفع الإلكتروني، المسؤولية الجزائية، القصد البرمجي، التشريع العراقي، الإهمال التقني.

Abstract:

This research examines criminal liability for electronic payment card crimes under Iraqi law, considering them as emerging digital economic crimes characterized by their intangible nature. These crimes present challenges related to the limits of criminalization, proof, and the determination of liability. The research begins by analyzing the legal elements of these crimes, demonstrating that the material element takes various technical forms, most notably the

unlawful use of the card or its data, falsification of digital content, and cyber fraud targeting banking systems, in addition to technical negligence leading to the commission of the crime. It also shows that the mental element is no longer limited to traditional intent, but includes what can be termed "programmatic intent," which extends to the stage of preparing the electronic means, not just the moment of committing the crime. Furthermore, the research explores the direct criminal liability of the perpetrator and the indirect liability arising from the failure to report or monitor payment systems within commercial and banking institutions, in light of current Iraqi legislation, and in comparison, with Arab legislations that have adopted specific regulations for electronic payment crimes. The research concludes that the Iraqi legislative framework still relies on general rules that fail to encompass the technical nature of cybercrime. It proposes enacting separate penal provisions that criminalize digital conduct, recognize electronic evidence, criminalize technical negligence, and establish institutional oversight to safeguard trust in Iraq's financial system and digital economy.

Keywords: Electronic payment crimes, Criminal liability, Programmatic intent, Iraqi legislation, technical negligence.

المقدمة

اولا: التعريف بموضوع البحث: أدى التحول الرقمي الذي يشهده العراق في السنوات الأخيرة، ولا سيما في قطاع الدفع الإلكتروني، إلى ظهور مرحلة جديدة من المعاملات المالية لم تعد الأموال فيها تُتداول بصورتها المادية التقليدية، بل أصبحت أرقاماً مشفّرة وبيانات مصرفية تُدار عبر الشبكات والأنظمة الآلية. وقد أسهمت بطاقات الدفع الإلكتروني في تسريع النشاط الاقتصادي وتوسيع التعاملات المصرفية، لكنها في الوقت نفسه أوجدت نمطاً خاصاً من الجرائم يقوم على استغلال الوسيط التقني بدل الوسيلة المادية، وهو ما جعل الجريمة المالية تنتقل من نطاق الفعل الملموس إلى الفضاء الإلكتروني غير المرئي.

ورغم خطورة هذه الجرائم واتساع آثارها على الثقة العامة في النظام المصرفي، ما يزال التشريع الجزائي العراقي يعتمد نصوصاً عامة وضعت لمعالجة جرائم الاحتيال والتزوير التقليدية، دون أن يتبنى تنظيماً خاصاً يحدد الطبيعة القانونية لبطاقة الدفع، أو يعرّف صور السلوك الإجرامي القائم على الاختراق والاستعمال غير المشروع والتلاعب بالبيانات، أو يضع إطاراً حاسماً لمسائل القصد الجرمي الرقمي والإثبات الإلكتروني والمسؤولية المؤسسية. وهو ما يثير فراغاً تشريعياً وقضائياً يتعاظم مع تزايد الاعتماد على وسائل الدفع غير النقدي داخل العراق.

وفي هذا السياق، يتناول هذا البحث بالدراسة والتحليل الأركان القانونية لجرائم بطاقات الدفع، مبرزاً خصوصية الركن المادي في البيئة الرقمية، وما يرتبط به من صور الاستعمال غير المشروع

والتزوير والاحتيال والإهمال التقني، ثم ينتقل إلى تحليل الركن المعنوي بوصفه إرادة تقنية تتجاوز القصد التقليدي إلى ما يمكن وصفه بالقصد البرمجي. كما يدرس البحث المسؤولية الجزائية في هذين الاتجاهين: مسؤولية مباشرة عن الفعل الإجرامي، ومسؤولية غير مباشرة ناشئة عن الإخلال بواجب الإبلاغ أو الرقابة أو حماية الأنظمة. ويُقارن ذلك بالمواقف التشريعية العربية التي جرّمت هذه الأفعال بنصوص خاصة، وصولًا إلى صياغة مقترح تشريعي ينسجم مع الواقع القانوني العراقي ومتطلبات حماية الاقتصاد الرقمي. إن هذا البحث لا ينطلق من أهمية أكاديمية فحسب، بل من حاجة تشريعية عملية، ذلك أن استمرار الاعتماد على النصوص التقليدية يضع القضاء أمام فراغ تفسيري، ويتيح مساحات غير محمية قانونًا في مجال المعاملات الإلكترونية، الأمر الذي يجعل تطوير التجريم في جرائم بطاقات الدفع ضرورة لا ترفًا تشريعيًا.

ثانيا: اهمية البحث: تنبع أهمية هذا البحث من كونه يتناول فراغًا تشريعيًا وجنائيًا قائمًا في القانون العراقي، يتعلق بغياب تنظيم جزائي خاص لجرائم بطاقات الدفع الإلكتروني، على الرغم من دخول هذه الوسائل في صلب التعامل المالي والمصرفي، وتحولها إلى أداة رئيسية في حركة النقد الوطني. وتمثل هذه الجرائم أخطر تحدٍ يواجه السياسة الجنائية المعاصرة، لأنها لا تقوم على السلوك المادي التقليدي، بل على أفعال رقمية محضة كالدخول غير المشروع، واختراق الأنظمة الإلكترونية، وتزوير البيانات المصرفية، والاحتيال القائم على الأوامر البرمجية. ومن ثم فإن هذا البحث يسعى إلى بناء الأساس العلمي والجزائي الذي يُمكّن التشريع العراقي من الانتقال من مرحلة الاستعارة التفسيرية للنصوص التقليدية إلى مرحلة التجريم الرقمي الصريح، حمايةً للثقة العامة، والأمن الاقتصادي، والنظام المالي للدولة.

ثالثا: إشكالية البحث: تتجسد الإشكالية الرئيسة فيما يلي:

هل تكفي النصوص العقابية العامة الواردة في قانون العقوبات العراقي لسنة ١٩٦٩ وقانون التجارة وتعليمات البنك المركزي، لمواجهة جرائم بطاقات الدفع الإلكتروني من حيث تجريم السلوك الرقمي وإثباته وتحديد المسؤولية عنه؟ أم أن خصوصية هذه الجرائم الرقمية تفرض وضع منظومة تشريعية جزائية خاصة بها؟

رابعًا: نطاق البحث: يتحدد نطاق هذا البحث بثلاثة أبعاد رئيسة:

١. **النطاق القانوني:** دراسة موقف القانون العراقي من جرائم الدفع الإلكتروني، مع مقارنة نقدية بالتشريعات المصرية والإماراتية والأردنية والمغربية لبيان مدى كفاية الحماية الجزائية.

٢. **النطاق الموضوعي:** تحليل الأركان القانونية لجريمة الدفع الإلكتروني، من حيث الركن المادي والمعنوي والعلاقة السببية الرقمية، وتحديد حدود المسؤولية المباشرة وغير المباشرة للمساهمين في الجريمة.

٣. **النطاق الفني (الجنائي):** بحث خصوصية الإثبات الرقمي وسلسلة الدليل الإلكتروني وأثرها في تكوين القناعة القضائية، بما ينسجم مع مبدأ الشرعية الجنائية وضمانات العدالة.

خامساً: منهجية البحث: اعتمد البحث منهجين متكاملين:

المنهج التحليلي القانوني: لتحليل النصوص العراقية وتكييفها على السلوك الرقمي، وبيان أوجه القصور التشريعي.

المنهج المقارن: لرصد الفارق بين العراق والدول التي نظمت جرائم بطاقات الدفع بنصوص مستقلة، بهدف استنباط نموذج تشريعي قابل للتطبيق محليًا. كما اعتمد البحث منهجًا نقديًا إصلاحيًا يستهدف الانتقال من التشخيص إلى اقتراح بديل تشريعي واضح.

سادساً: أهداف البحث: يسعى البحث إلى تحقيق ما يلي:

١. تحديد الطبيعة القانونية الدقيقة لجرائم بطاقات الدفع الإلكتروني.

٢. تحليل الأركان القانونية للجريمة الرقمية في ضوء الخصوصية التقنية.

٣. التمييز بين القصد التقليدي والقصد البرمجي في الجرائم المستحدثة.

٤. إبراز مسؤولية الفاعل الأصلي والمسؤولية غير المباشرة القائمة على الإهمال أو ضعف الرقابة المؤسسية.

٥. تقديم مقترح تشريعي خاص بجرائم بطاقات الدفع يلائم الواقع القانوني العراقي.

سابعاً: خطة البحث: جاء هذا البحث في مبحثين رئيسيين يتناول كل منهما جانباً جوهرياً من موضوع المسؤولية الجزائية عن جرائم بطاقات الدفع الإلكتروني. تناول المبحث الأول الأركان القانونية لهذه الجرائم، إذ خُصِّص المطلب الأول لبحث الركن المادي، من خلال بيان عناصره المتمثلة بالسلوك الإجرامي والنتيجة الجرمية والعلاقة السببية، مع توضيح الخصوصية التقنية التي تميّز هذا الركن في البيئة الرقمية، ولا سيما من حيث طبيعة السلوك الإلكتروني وصعوبة الإثبات وتحديد مكان وقوع الجريمة. كما تطرق هذا المطلب إلى صور السلوك المادي المتمثلة في الاستعمال غير المشروع للبطاقة أو بياناتها، وتزوير المحتوى الرقمي، والاحتيال الإلكتروني، فضلاً عن الإهمال المؤدي إلى ارتكاب الجريمة. أما المطلب الثاني فقد تناول الركن المعنوي في جرائم بطاقات الدفع الإلكتروني، موضحاً تطور القصد الجنائي من النية التقليدية إلى ما يُعرف بالقصد البرمجي، وهو الإرادة التقنية الممتدة إلى مرحلة إعداد الوسيلة أو النظام الإلكتروني قبل التنفيذ، مع بيان أثر الخطأ غير العمدي والإهمال التقني في قيام المسؤولية، وذلك في ضوء المقارنة بين التشريع العراقي وبعض التشريعات العربية كالسعودي والتونسي.

أما المبحث الثاني فقد خُصِّص لبحث المسؤولية الجزائية عن جرائم بطاقات الدفع الإلكتروني، حيث تناول المطلب الأول المسؤولية الجزائية المباشرة التي تقع على الفاعل الأصلي سواء كان فرداً أو تاجراً أو موظفاً في مؤسسة مالية، عندما يرتكب أفعالاً عمدية كالاستخدام غير المشروع، أو التزوير، أو الاحتيال باستعمال أنظمة الدفع الإلكتروني. كما تناول هذا المطلب صور المسؤولية غير المباشرة التي تنشأ عن إخلال التاجر أو المؤسسة المصرفية بواجب الرقابة التقنية أو التنظيمية، أو عن السماح للعاملين أو الشركاء بارتكاب أفعال غير مشروعة نتيجة ضعف الإشراف أو انعدام المتابعة. أما المطلب الثاني فقد تناول حالات قيام المسؤولية الجنائية، سواء الناشئة عن الأفعال العمدية كالاستخدام غير

المشروع والتزوير والاحتيال المصرفي، أو الناتجة عن الإهمال والتقصير في الإبلاغ أو الرقابة التقنية، لما في ذلك من مساهمة غير مباشرة في وقوع الجريمة.

وتُختتم الخطة بخاتمة تتضمن أهم النتائج التي خلص إليها البحث من أن النصوص الجزائية العراقية التقليدية قاصرة عن استيعاب السلوك الرقمي المستحدث، وأن الركنين المادي والمعنوي للجريمة في مجال الدفع الإلكتروني يتطلبان معالجة تشريعية خاصة تراعي الطبيعة التقنية للفعل الإجرامي. كما تضم التوصيات الداعية إلى استحداث نصوص جزائية خاصة بجرائم بطاقات الدفع الإلكتروني، وتجريم الإهمال التقني، والاعتراف بالقصد البرمجي، وتطوير قواعد الإثبات الرقمي لضمان الحماية القانونية والمعاملات المالية الإلكترونية في العراق.

المبحث الأول: الأركان القانونية لجرائم بطاقات الدفع الإلكتروني.

يعدّ الركن القانوني في جرائم بطاقات الدفع الإلكتروني المدخل الأساس لفهم الطبيعة الخاصة لهذه الجرائم، لما تنفرد به من سلوكيات رقمية غير ملموسة تختلف عن الجرائم المالية التقليدية في أدوات التنفيذ ووسائل الاعتداء والإثبات. ولأجل ذلك، يتناول هذا المبحث في مطلبه الأول الركن المادي بعناصره الثلاثة: السلوك الإجرامي، النتيجة الجرمية، والعلاقة السببية، مع بيان خصوصيتها التقنية وصورها المتنوعة في البيئة الرقمية. أما المطلب الثاني فيتعلق بالركن المعنوي، محلّلًا القصد الجنائي في الجرائم الرقمية وتحول الإرادة الإجرامية من النية الفردية إلى النية التقنية، إلى جانب إبراز دور الخطأ غير العمدي والإهمال التقني في قيام المسؤولية الجنائية. ومن خلال هذا البناء يتضح الأساس النظري والعملي لمسؤولية الجاني في هذا النوع من الجرائم، بما يمهّد للمعالجة التشريعية المقارنة اللاحقة.

المطلب الأول: الركن المادي في جرائم بطاقات الدفع الإلكتروني

يُعد الركن المادي أساس المسؤولية الجنائية، إذ يُعبّر عن السلوك الخارجي الذي يرتكبه الجاني ويقع به الاعتداء على الحق المحمي قانونًا. وفي جرائم بطاقات الدفع الإلكتروني، تتخذ الأفعال الإجرامية شكلًا تقنيًا معقدًا يختلف عن الجرائم التقليدية من حيث الوسائل وطبيعة السلوك. كما أن هذه الأفعال قد تُرتكب عن بُعد، وفي بيئة افتراضية يصعب فيها تحديد الفاعل أو النتيجة على نحو مباشر. ومن ثم، فإن دراسة الركن المادي في هذا النوع من الجرائم تتطلب بيان عناصره المتمثلة في السلوك الإجرامي، والنتيجة الجرمية، والعلاقة السببية، ثم تحليل خصوصيته في البيئة الرقمية، وأخيرًا بيان صور السلوك الإجرامي في جرائم بطاقات الدفع الإلكتروني وفق المقارنة التشريعية بين العراق وبعض الدول العربية.

الفرع الأول: عناصر الركن المادي

يستند الركن المادي في البناء القانوني للجريمة إلى ثلاثة عناصر رئيسية هي السلوك الإجرامي، والنتيجة الجرمية، والرابطة السببية. ويظهر تميّز هذا الركن في جرائم بطاقات الدفع الإلكتروني من خلال الطابع غير المادي للسلوك، وصعوبة إثبات العلاقة بين الفعل والنتيجة بسبب الطبيعة الرقمية للبيئة التي تُرتكب فيها الجريمة.

أولًا: السلوك الإجرامي: يُعد السلوك الإجرامي العنصر الأبرز في تكوين الجريمة، وهو كل نشاط إرادي يأتيه الفاعل مخالفًا للنص القانوني، سواء أكان إيجابيًا كاستعمال البطاقة دون إذن، أم سلبيًا كالإهمال في الإبلاغ عن فقدانها.

في التشريع العراقي، لم يرد تعريف خاص بالسلوك الإجرامي في الجرائم الإلكترونية، مما يجعل المحاكم تعتمد النصوص العامة في قانون العقوبات رقم (١١١) لسنة ١٩٦٩، ولا سيما المواد (٤٥٥–٤٥٦) الخاصة بالاحتيال والتصرف غير المشروع في المال المنقول [١].

أما المشرّع المصري، فقد نص في المادة (١٣) من قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ على أن "كل من دخل عمدًا إلى موقع أو نظام معلوماتي محظور الدخول إليه يعاقب بالحبس والغرامة، وهو ما يوسع من مفهوم السلوك الإجرامي ليشمل الدخول التقني غير المشروع [٢].وفي الأردن، نصت المادة (٣) من قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ على تجريم "الدخول إلى نظام معلوماتي بأي وسيلة دون تصريح، بينما عرّف القانون الإماراتي رقم (٥) لسنة ٢٠١٢ السلوك الإجرامي بأنه كل استخدام لنظام معلوماتي بقصد ارتكاب جريمة أو تسهيل ارتكابها [٣].

ثانيًا: النتيجة الجرمية: النتيجة هي الأثر الذي يصيب المصلحة المحمية قانونًا جراء السلوك المحظور. وفي جرائم الدفع الإلكتروني، تتمثل النتيجة غالبًا في فقدان الأموال أو إفشاء البيانات أو المساس بالثقة في النظام المالي. ويُلاحظ أن القضاء العراقي تبنى مفهومًا موسعًا للنتيجة، حيث قضت محكمة التمييز الاتحادية في قرارها رقم (٧٤/هيئة جزائية/٢٠٢١) بأن استخدام بطاقة الغير دون إذن يُعد نتيجة جرمية قائمة ولو لم يتحقق الضرر المالي الفعلي، لأن الفعل ذاته يمسّ الثقة العامة في المعاملات الإلكترونية [٤].أما القضاء المصري، فقد أكّد في حكم محكمة القاهرة الاقتصادية رقم (٣٨٤ لسنة ٢٠٢٠) أن النتيجة الجرمية تتحقق بمجرد محاولة سحب الأموال إلكترونيًا دون إذن، حتى وإن لم يتم السحب فعليًا، إذ يكفي تهديد الحق المالي [٥]. وفي الأردن، قضت محكمة صلح جزاء عمان بتاريخ ٢٠١٩/٣/١٢ بأن محاولة استخدام بيانات بطاقة الدفع الخاصة بالغير تمثل جريمة قائمة بذاتها، أما القانون الإماراتي فقد ذهب أبعد من ذلك، حيث نص في المادة (١٠) من قانون الجرائم الإلكترونية على تجريم حتى الشروع في استخدام أدوات الدفع الإلكتروني بطرق غير مشروعة [٦].

ثالثًا: العلاقة السببية: تُعد العلاقة السببية الرابطة التي تربط بين الفعل الإجرامي والنتيجة الجرمية. ويشترط القانون أن تكون النتيجة متولدة مباشرة عن الفعل.

وقد بيّنت محكمة جنايات الكرخ في حكمها رقم (٨٨/ج/٢٠٢٢) أن العلاقة السببية في الجرائم الإلكترونية تُثبت عبر التحليل الفني للأدلة الرقمية مثل سجلات الدخول وأكواد التعامل الإلكتروني، معتبرة أن انقطاع هذه السلسلة يُسقط التلازم السببي [٧].

وفي مصر، أخذت محكمة النقض بمعيار السبب الفعّال في القضايا المتعلقة بالاحتيال الإلكتروني، حيث أكدت أن استخدام البطاقة أو البيانات المزورة الذي يؤدي إلى تحويل مالي مباشر يُعد السبب القانوني للنتيجة [٨].

أما القضاء الأردني، فقد اعتبر في حكم صادر عام ٢٠٢٠ أن إهمال الشركة المزودة لخدمة الدفع الإلكتروني في تأمين نظامها يمثل سببًا قانونيًا مساهمًا في النتيجة الجرمية [٩]وفي الإمارات، قضت محكمة دبي الابتدائية بالقرار رقم (١١٢/ج/٢٠٢٠) بأن العلاقة السببية يمكن إثباتها من خلال تتابع الأفعال الإلكترونية متى أفضت إلى تحويل غير مشروع [١٠].ومما تقدم يتبين إن العناصر الثلاثة للركن المادي في جرائم بطاقات الدفع الإلكتروني تتداخل في الواقع العملي بسبب الطابع التقني للجريمة. ويرى الباحث أن المشرّع العراقي بحاجة إلى تنظيم خاص للركن المادي في الجرائم الإلكترونية يحدد مفهوم السلوك الرقمي والنتيجة الرقمية وآليات إثبات العلاقة السببية بالوسائل التقنية الحديثة، انسجامًا مع الاتجاهات التشريعية المقارنة.

الفرع الثاني: خصوصية الركن المادي في البيئة الرقمية

أحدثت الثورة الرقمية تحولًا جوهريًا في مفاهيم الجريمة والعقاب، إذ لم تعد الأفعال الإجرامية مقصورة على النطاق المادي، بل امتدت إلى الفضاء الإلكتروني حيث تُرتكب أفعال لا يمكن إدراكها بالحواس التقليدية. وفي هذا السياق، اكتسب الركن المادي في الجرائم المعلوماتية، ولا سيما جرائم بطاقات الدفع الإلكتروني، طابعًا خاصًا يتميز بثلاث خصائص رئيسية: الطبيعة التقنية للسلوك الإجرامي، خصوصية الإثبات الرقمي، وتحدي تحديد المكان القانوني للجريمة الإلكترونية.

ويؤكد بعض الفقهاء أن هذا الاتجاه التشريعي يعبّر عن توسّع في مفهوم الركن المادي بما يشمل النية التكنولوجية التي تسبق تنفيذ الجريمة في الفضاء الرقمي [١١].يرى الباحث أن خصوصية السلوك التقني في جرائم الدفع الإلكتروني تستلزم إعادة صياغة النصوص العقابية في القانون العراقي لتشمل الأفعال الإلكترونية الصرفة، بما يحقق مبدأ الشرعية ويمنع تباين الاجتهاد القضائي.

ثانيًا: خصوصية الإثبات في الجرائم الرقمية: يُعدّ الإثبات في البيئة الرقمية من أكثر المسائل تعقيدًا، لأن الفعل لا يُترك أثرًا ماديًا ملموسًا كما في الجرائم العادية. ويعتمد الإثبات هنا على البيانات الإلكترونية والسجلات الرقمية التي يمكن أن تُعدل أو تُمحى بسهولة .ويشير الفقه إلى أن الأدلة الرقمية تتطلب معايير فنية دقيقة تضمن سلامتها ومصداقيتها، أبرزها ما يُعرف بـ سلسلة حفظ الدليل الرقمي، التي تؤكد تتبّع البيانات منذ جمعها وحتى تقديمها للمحكمة [١٢].وفي مصر، اعتمد المشرّع هذا المفهوم ضمنيًا في المادة (٢٧) من قانون مكافحة جرائم تقنية المعلومات، التي أجازت استخدام البيانات الإلكترونية كبينة جنائية متى تم الحصول عليها بطرق مشروعة [١٣].وفي الإمارات، أكدت المادة (٣٥) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ أن الأدلة الرقمية المستخرجة من الأنظمة التقنية تُعتبر أدلة رسمية متى صدرت عن جهة مختصة [١٤]. ويشير الفقه العربي إلى أن القاضي في الجرائم الإلكترونية لا يستطيع تكوين قناعته إلا بمساعدة فنية من خبراء مختصين في تحليل الأنظمة الرقمية، وهو ما يجعل الإثبات عملية جماعية تجمع بين القانون والتقنية [١٥].يرى ضرورة إدراج الأدلة الرقمية في قانون الإثبات

العراقي باعتبارها وسيلة قائمة بذاتها، مع تحديد شروط فنية لجمعها وتحليلها، لأن غياب هذا التنظيم يُضعف القدرة على مكافحة الجريمة الإلكترونية بصورة فعالة.

ثالثًا: تحديد المكان القانوني للجريمة الرقمية: تتميز الجرائم الإلكترونية بأنها لا ترتبط بمكان محدد، إذ يمكن أن يُرتكب الفعل في دولة وتتحقق نتيجته في أخرى، مما يجعل تحديد الاختصاص المكاني مسألة معقدة. وفي العراق، يُعتمد مبدأ مكان تحقق النتيجة وفق المادة (٦) من قانون العقوبات، بحيث تعتبر الجريمة واقعة داخل الإقليم العراقي متى ظهر أثرها فيه [١٦] اما في مصر، نصت المادة (٢٩) من قانون مكافحة جرائم تقنية المعلومات على أن القانون يسري على كل من ارتكب فعلاً داخل الدولة أو خارجها إذا ترتبت عليه نتيجة داخل الإقليم [١٧]وفي الأردن، جاء النص في المادة (٣) من قانون العقوبات مؤكدًا أن القانون يسري على الجرائم التي تقع في المملكة أو التي ينتج عنها أثر فيها [١٨].

ويؤكد الفقه أن هذه الاتجاهات تمثل تحولًا نحو السيادة الإلكترونية، التي تمنح الدول سلطة قانونية على الفضاء الرقمي كلما مسّ مصالحها الحيوية [١٩].يرى الباحث أن اعتماد مبدأ مكان تحقق النتيجة هو الأنسب للبيئة العراقية، شرط أن يُدعم بتشريعات ثانوية تنظّم التعاون التقني مع الدول الأخرى وتحدد ضوابط تبادل المعلومات والأدلة الرقمية.

الفرع الثالث: صور السلوك الإجرامي في جرائم بطاقات الدفع الإلكتروني

تُعد بطاقات الدفع الإلكتروني من الوسائل المالية الحديثة التي سهلت إجراء التعاملات التجارية والمصرفية، لكنها في الوقت نفسه أوجدت أشكالًا جديدة من السلوك الإجرامي تختلف عن الجرائم المالية التقليدية. وتظهر خطورة هذه السلوكيات في كونها تُرتكب بوسائل تقنية يصعب كشفها أو تتبعها، مما يجعل دراسة صور الركن المادي فيها ضرورة علمية وقانونية لتحقيق الحماية الجنائية للنظام المالي. تتعدد صور السلوك المادي في هذه الجرائم بحسب طبيعة الفعل ووسيلته، ويمكن تصنيفها إلى أربع فئات رئيسية: لاستخدام غير المشروع للبطاقة، وتزوير بيانات البطاقة، والاحتيال الإلكتروني، والإهمال المؤدي للجريمة.

أولًا: الاستخدام غير المشروع للبطاقة: يقوم هذا النوع من السلوك الإجرامي على استعمال بطاقة دفع إلكتروني من قبل شخص غير مخول، سواء كانت البطاقة مسروقة أو مفقودة أو تم الحصول عليها بطريقة احتيالية. ويتحقق الركن المادي بمجرد إدخال البيانات الخاصة بالبطاقة في نظام إلكتروني لإجراء عملية مالية دون إذن من مالكها [٢٠].ويُعد هذا الفعل اعتداءً مباشرًا على حق الملكية الرقمية، إذ يُمارس الجاني سلطة فعلية على أداة الدفع بغير حق، مما يُشكل صورة من صور الاستيلاء الإلكتروني المعاقب عليه في التشريعات العربية الحديثة [٢١].

وتشير بعض الدراسات إلى أن هذا السلوك غالبًا ما يكون ناتجًا عن اختراق أنظمة الدفع أو سرقة بيانات المستخدمين عبر البريد الإلكتروني أو المواقع المزيفة [٢٢].يرى الباحث أن الاستخدام غير المشروع للبطاقة يُعد من أخطر صور الجريمة الإلكترونية، لأنه يجمع بين الاحتيال التقني والمس بحقوق الأفراد، ويقترح أن يُفرد له المشرع العراقي نصًا خاصًا يعاقب عليه بعقوبة مشددة تتناسب مع خطورته الاقتصادية والاجتماعية.

ثانيًا: تزوير بيانات البطاقة الإلكترونية: تتحقق هذه الصورة عندما يقوم الجاني بتغيير أو تعديل البيانات الرقمية الخاصة بالبطاقة، مثل الرقم السري أو اسم المستخدم أو الرمز المصرفي، باستخدام وسائل تقنية متطورة، بغرض تضليل النظام الإلكتروني أو تمكينه من استعمال البطاقة بصورة غير مشروعة [٢٣],ويرى الفقه أن هذا الفعل يجمع بين ركني التزوير المادي والمعنوي؛ المادي لأنه يتمثل في تغيير البيانات، والمعنوي لأنه يقصد من ورائه خداع النظام المالي لإحداث أثر قانوني معين [٢٤].كما أن التزوير في هذه الحالة لا يقتصر على البطاقات المصرفية، بل يشمل التلاعب بالبطاقات الافتراضية المستخدمة في التجارة الإلكترونية أو المحافظ الرقمية، وهو ما يستلزم توسيع مفهوم المستند الإلكتروني في التشريع الجنائي [٢٥],ويُعد تزوير بيانات البطاقة جريمة مستقلة عن استعمالها، إذ يكفي مجرد إجراء التعديل غير المشروع في البيانات لتوافر الركن المادي للجريمة دون حاجة إلى تحقق أثر مالي فعلي [٢٦], يعتقد الباحث أن المشرع العراقي بحاجة إلى تعديل نصوص التزوير التقليدية بحيث تُدرج التزوير الإلكتروني ضمن أشكال الجريمة المعلوماتية المستقلة، مع تحديد طبيعة البيانات المشمولة بالحماية القانونية، ولا سيما بيانات بطاقات الدفع.

ثالثًا: الاحتيال الإلكتروني: تُعد هذه الصورة الأكثر شيوعًا في جرائم بطاقات الدفع الإلكتروني، وتتحقق عندما يستخدم الجاني وسائل تقنية لتضليل النظام المالي أو المجني عليه بقصد تحقيق مكسب غير مشروع. ويتخذ الاحتيال الإلكتروني عدة أشكال، منها انتحال الهوية المصرفية، أو إنشاء مواقع وهمية (Phishing) لجمع بيانات البطاقات، أو إرسال رسائل مزيفة تطلب تحديث المعلومات البنكية [٢٧].ويؤكد الفقه أن الاحتيال الإلكتروني يختلف عن النصب التقليدي في أن وسائل الخداع فيه تعتمد على التكنولوجيا لا على الاتصال المباشر، مما يجعل إثباته أكثر تعقيدًا من حيث تتبع مصدر الفعل [٢٨].وقد ذهب الاتجاه الحديث في الفقه الجنائي إلى أن الاحتيال الإلكتروني لا يقوم فقط على استخدام الوسيلة التقنية، بل على نية الخداع المسبق التي تميز الجريمة الإلكترونية عن الأخطاء التقنية أو العمليات المصرفية الفاشلة. يرى الباحث أن جوهر الاحتيال الإلكتروني يكمن في استغلال الثقة الرقمية للنظام المالي، وأن تجريمه يجب أن يمتد ليشمل كل محاولة لتهيئة بيئة تقنية مضللة، ولو لم تتحقق النتيجة المادية، تحقيقًا للردع الوقائي.

رابعًا: الإهمال المؤدي إلى الجريمة: قد لا يكون الجاني في بعض الحالات فاعلًا مباشرًا للجريمة، لكنه يُسهم في وقوعها عن طريق الإهمال أو التقصير في حماية بيانات البطاقة أو النظام المالي, ويُعدّ هذا الإهمال صورة من صور السلوك المادي السلبي الذي يُفضي إلى ارتكاب الجريمة من قبل الغير.

وتشمل صور الإهمال ترك البيانات المصرفية مكشوفة، أو إهمال تحديث برامج الحماية، أو تجاهل الإبلاغ عن فقدان البطاقة أو الاشتباه في استخدامها[٢٩].ويذهب بعض الفقهاء إلى أن هذا السلوك يجب أن يُعاقب عليه متى كان الجاني قادرًا على منع النتيجة ولم يفعل، تأسيسًا على مبدأ المسؤولية عن الامتناع في الجرائم ذات الطابع التقني .ويرى آخرون أن المسؤولية عن الإهمال في المجال الرقمي يجب أن

تُقاس بمعيار المستخدم الحذر تقنيًا، لا بمعيار الشخص العادي، لأن التعامل مع أدوات الدفع الإلكتروني يتطلب مستوى من الدراية الفنية والحذر المهني [٣٠].يؤكد الباحث أن الإهمال في حماية بيانات الدفع الإلكتروني يُسهم بصورة غير مباشرة في تسهيل الجريمة، ويقترح أن يُنظم المشرع العراقي نصًا خاصًا يُقرر مسؤولية جزائية لحامل البطاقة أو المؤسسة المصرفية عند ثبوت الإهمال الجسيم في صيانة الأنظمة أو تأمين البيانات.

المطلب الثاني: الركن المعنوي في جرائم بطاقات الدفع الإلكتروني

يُعد الركن المعنوي حجر الزاوية في المسؤولية الجنائية، لأنه يمثل الإرادة الواعية التي تحرك السلوك المادي للجريمة. غير أن تطور الوسائل التقنية وتحوّل المعاملات المالية نحو البيئة الرقمية قد نقل هذا الركن من إطاره التقليدي القائم على النية الفردية إلى نطاق الإرادة التقنية التفاعلية، أي الإرادة التي تتولد من تفاعل بين الإنسان والآلة في بيئة معلوماتية معقدة. وهذا التحول أحدث انزياحًا في الفقه الجنائي من النية الذاتية إلى القصد البرمجي، أي أن الفاعل لم يعد وحده من يُحدث النتيجة الإجرامية مباشرة، بل النظام الذي صممه أو وجهه.

ويُعالج هذا المطلب بعد توسع مفاهيمي ودليل فقهي وقضائي في فرعين رئيسيين:

الفرع الأول: القصد الجنائي في الجرائم الرقمية (مقارنة بين العراق والسعودية).

الفرع الثاني: الخطأ غير العمدي والإهمال التقني (مقارنة بين العراق وتونس).

الفرع الأول: القصد الجنائي في الجرائم الرقمية – دراسة تحليلية مقارنة بين القانون العراقي والنظام السعودي

أولاً: التحول المفاهيمي من النية الفردية إلى النية التقنية: القصد الجنائي في الجرائم الرقمية لا يمكن النظر إليه كحالة نفسية مجردة من الزمان والمكان، بل كإرادة واعية تتفاعل مع أنظمة معقدة.

فالمجرم التقني لا يُقدم على فعله بدافع لحظي، بل بعد تصميم بنية تقنية تتيح تنفيذ الفعل الإجرامي بصورة متكررة أو مؤجلة.

وقد عبّر الفقيه عبد العزيز عبد الجواد عن هذا المعنى بقوله إن الإرادة الإجرامية في الفضاء السيبراني تتحقق من خلال عمل ذهني مزدوج: الأول إنساني إرادي، والثاني تقني حسابي [٣١].فمن يُنشئ برنامجًا لنسخ بيانات بطاقات الائتمان يعلم مسبقًا أن البرنامج سيُستخدم بصورة تلقائية لاحقًا لتحقيق النتيجة الإجرامية، وهذا العلم يُعدّ نية ممتدة وليست لحظية. وهذا التمييز جوهري في الركن المعنوي للجريمة الرقمية، إذ يتحول القصد إلى وعي مستمر بتبعات الأداة التقنية التي تم إنشاؤها.

ثانيًا: القصد الجنائي في القانون العراقي: في التشريع العراقي، لا توجد نصوص خاصة تعالج القصد في الجرائم التقنية، لذلك يُطبَّق المبدأ العام في المادة (٣٣) من قانون العقوبات رقم (١١١) لسنة ١٩٦٩، الذي يعتبر الجريمة عمدية إذا ارتكب الجاني الفعل بإرادته وكان عالمًا بأنه مخالف للقانون. غير أن التطبيق القضائي لهذا النص في المجال المعلوماتي لا يزال محدودًا. ففي قرار لمحكمة جنايات الرصافة رقم (٢١٧/ج/٢٠٢٠)، أُدين موظف مصرفي بتسريب بيانات حسابات إلكترونية، واعتبرت

المحكمة أن النية تتوافر متى ثبت أن الفاعل كان على علم بطبيعة المعلومات التي سلّمها[٣٢].ورغم أهمية هذا القرار، إلا أنه لا يميز بين النية التقنية (العلم بآلية النظام) والنية المادية (العلم بالنتيجة)، وهو تمييز ضروري في ضوء التطور الرقمي. ويشير فاضل الشاوي إلى أن الفاعل في الجريمة المعلوماتية يمارس سيطرة رقمية على النظام وليس مادية عليه، وهو ما يجعل نية السيطرة التقنية جوهر الركن المعنوي[٣٣]. وهكذا يمكن القول إن الإرادة في البيئة الرقمية تتخذ شكلاً مركّبًا: إرادة إنشائية (في مرحلة إعداد الوسيلة) وإرادة تنفيذية (في لحظة استعمالها).

ثالثًا: القصد الجنائي في النظام السعودي: أما النظام السعودي فقد اتخذ موقفًا أكثر وضوحًا، إذ نص نظام مكافحة الجرائم المعلوماتية لعام ٢٠٠٧ في المادة (٣) على معاقبة كل من ارتكب عمدًا دخولًا غير مشروع إلى موقع إلكتروني أو نظام معلوماتي. ويتضح من لفظ عمدًا أن المشرّع السعودي اشترط نية واعية ومحددة. لكن ما يميز التطبيق السعودي هو اعتبار تصميم البرنامج أو إعداد النظام دليلاً على القصد ، كما قضت المحكمة الجزائية بالرياض في حكمها رقم (٣٤٢/ق/٢٠٢١)، حيث رأت أن تكرار البرمجة وتهيئة النظام بما يؤدي إلى نقل الأموال آليًا يُعدّ عملاً عمديًا متكامل الأركان [٣٤].ويُعد هذا الحكم شاهدًا على تبني القضاء السعودي لمفهوم القصد البرمجي، أي النية التي تتحقق عند إعداد الأداة التقنية وليس فقط عند تشغيلها .ويرى عبد الله الأنصاري أن هذا المفهوم يمثل الجيل الثالث من القصد الجنائي لأنه يربط الإرادة القانونية بمرحلة تصميم الأداة، لا باستخدامها فقط [٣٥].

رابعًا: التحليل المقارن والبعد التطبيقي: من خلال المقارنة يتبين أن القانون العراقي لا يميز بين الفاعل المادي والمبرمج التقني، بينما النظام السعودي يوسّع نطاق النية ليشمل مرحلة التحضير البرمجي. وهذا الفارق ليس تقنيًا فحسب، بل فلسفيًا أيضًا: إذ يعكس اختلافًا في تصور الإرادة ذاتها — فالعراق ما زال يراها قرارًا فرديًا آنياً، بينما تراها السعودية قدرة تقنية واعية تمتد مع الأداة الرقمية. وهو ما يتفق مع الاتجاه الحديث في القانون المقارن الذي يُقرّ بمسؤولية من يتحكم في الوسيلة التقنية حتى لو لم يُنفذ الجريمة بنفسه [٣٦].

يتبين من خلال ما تقدم أن العراق بحاجة إلى إدراج تعريف تشريعي جديد للقصد الجنائي في الجرائم الإلكترونية ينص على أن تتحقق النية الإجرامية إذا أنشأ أو استخدم أو فعّل نظامًا إلكترونيًا بقصد مباشر أو محتمل لتحقيق نتيجة غير مشروعة وهذا النص سيُدخل العراق ضمن دائرة التشريعات الحديثة التي تعترف بأن النية التقنية جزء من الركن المعنوي.

الفرع الثاني: الخطأ غير العمدي والإهمال التقني – دراسة مقارنة بين القانون العراقي والتشريع التونسي

أولاً: مفهوم الخطأ الإلكتروني: الخطأ في البيئة الرقمية يُعرّف بأنه الانحراف عن السلوك الواجب تقنيًا، أي إخلال الفاعل بواجبات الحذر التقنية المقررة في بيئة عمله أو مجاله المهني .[٣٧]وفي هذا السياق، يُصبح الخطأ غير العمدي في جرائم الدفع الإلكتروني معتمدًا على معيار موضوعي هو معيار الخبير التكنولوجي الحذر، لا الشخص العادي .فمدير النظام الإلكتروني الذي يُهمل تفعيل خاصية التشفير أو تحديث البرامج يُعتبر مقصرًا تقنيًا، لأن هذا السلوك يُمكّن الغير من ارتكاب الجريمة.

ثانيًا: الإهمال التقني في القانون العراقي: نصّ المشرّع العراقي في المادة (٣٤) من قانون العقوبات على أن الجريمة تكون غير عمدية إذا وقعت نتيجة الإهمال أو قلة الاحتراز أو عدم مراعاة القوانين والأنظمة. ورغم أن هذا النص عام، إلا أنه يشمل سلوكًا سلبيًا يُفضي إلى ضرر في البيئة المعلوماتية. وفي قرار محكمة جنايات الكرخ رقم (١٤٨/ج/٢٠٢٢)، أُدين مسؤول أمني في أحد المصارف لعدم اتخاذه إجراءات الحماية اللازمة لأنظمة الدفع، مما مكن جهة خارجية من الاختراق. واعتبرت المحكمة هذا التقصير خطأ جسيمًا يعادل الفعل المادي [٣٨].ويُعد هذا القرار تحولًا نوعيًا في الفقه القضائي العراقي، لأنه اعترف ضمنيًا بمفهوم الإهمال التقني. ويؤكد عمار الأنبار أن هذا الاتجاه حوّل الخطأ من مجرد إهمال مادي إلى إخلال بالتزام تقني قانوني واجب [٣٩].

ثالثًا: الإهمال التقني في التشريع التونسي: في المقابل، كان المشرّع التونسي سبّاقًا في ترسيخ مفهوم الخطأ المعلوماتي، إذ نصّ الفصل (١١) من القانون الأساسي عدد (٥) لسنة ٢٠٠٤ على أن كل من تسبب بخطئه في ضرر للنظام المعلوماتي يُسأل جزائيًا إذا كان قادرًا على تفاديه ولم يفعل. وهذا النص يجعل الإهمال التقني سببًا مستقلاً للمسؤولية حتى دون قصد، ويحوّل الواجب الفني إلى التزام قانوني.

كما تبنّت محكمة الاستئناف بتونس في قرارها رقم (٢١٧٩/ج/٢٠١٩) هذا الاتجاه عندما قضت بمسؤولية مؤسسة مالية عن ضرر ناجم عن ضعف في أنظمة الأمان، رغم عدم إثبات نية أو علم [٤٠].ويرى حاتم الباجي أن التشريع التونسي حوّل واجب الحماية الرقمية إلى واجب قانوني ذي طبيعة جنائية [٤١].

رابعًا: التحليل المقارن والاستنتاجات: تُظهر المقارنة أن القانون العراقي يسير نحو الاعتراف الضمني بالإهمال التقني من خلال الاجتهاد القضائي، بينما التونسي أقرّه صراحةً في نص تشريعي .ويرى الفقه أن إدراج الخطأ الإلكتروني كصورة من صور الجريمة غير العمدية يُعبّر عن تطور السياسة الجنائية الحديثة من العقوبة إلى الوقاية. كما أن التوسع في تجريم الإهمال التقني يعكس مبدأ الأمن القانوني للبيانات الذي يعدّ أحد ركائز الاقتصاد الرقمي [٤٢].يؤكد الباحث أن العراق بحاجة إلى نصوص واضحة تُقرّ بوجود مسؤولية جنائية عن الإهمال الإلكتروني، على غرار التشريع التونسي، لتفعيل حماية النظام المالي والمصرفي. ويقترح الباحث إدراج مادة في قانون الجرائم الإلكترونية العراقي تنص على أن:

يُعد مرتكبًا لجريمة الإهمال الإلكتروني كل من تسبب بإهماله أو تقصيره في حماية الأنظمة الرقمية أو بيانات الدفع في إلحاق ضرر بالغير أو بالنظام المالي

المبحث الثاني: المسؤولية الجنائية عن جرائم بطاقات الدفع الإلكتروني

تُعدّ جرائم بطاقات الدفع الإلكتروني من الجرائم المستحدثة التي أعادت تشكيل مفاهيم المسؤولية الجنائية في المجال المالي، إذ لم يعد الفعل الجرمي مقصورًا على السلوك المادي التقليدي، بل أصبح يرتبط بسلوك تقني يستند إلى بيئة رقمية متطورة. وبهذا، لم تعد المسؤولية مقتصرة على الفاعل الأصلي الذي يتعمد استخدام البطاقة أو بياناتها بصورة غير مشروعة، بل امتد نطاقها ليشمل المسؤولية غير

المباشرة الناشئة عن الإهمال أو ضعف الرقابة التقنية أو الامتناع عن اتخاذ تدابير الحماية، سواء من قبل التاجر أو المؤسسات المصرفية أو حامل البطاقة. ومن أجل ذلك، يتناول هذا المبحث الأساس القانوني لهذه المسؤولية في التشريع العراقي مقارنةً ببعض التشريعات العربية، من خلال بيان صور المسؤولية الجنائية المباشرة التي تقوم على القصد الجرمي، والمسؤولية غير المباشرة الناتجة عن الإهمال أو التقصير في الرقابة أو الإبلاغ، وذلك في ضوء التحولات التشريعية والقضائية التي فرضتها البيئة الرقمية.

المطلب الأول: المسؤولية الجنائية المباشرة عن الأفعال العمدية في جرائم بطاقات الدفع الإلكتروني

الفرع الأول: المسؤولية الجنائية المباشرة للتاجر عن أفعاله

تُعدّ المسؤولية الجنائية المباشرة للتاجر من الركائز الجوهرية في النظام القانوني الذي ينظم المعاملات التجارية الإلكترونية، لأنها تمثل الحدّ الفاصل بين حرية النشاط الاقتصادي ومساءلة التاجر عن إساءة استعمال أدوات الدفع الإلكتروني .فالمسؤولية هنا تقوم عندما يُرتكب الفعل الإجرامي مباشرة من التاجر بصفته الشخصية أو بصفته ممثلًا عن منشأته التجارية، سواء كان ذلك من خلال السلوك المادي الإجرامي كالتزوير والاحتيال، أو من خلال الإهمال الواعي الذي يؤدي إلى ذات النتيجة الإجرامية. وتمثل هذه المسؤولية تطبيقًا لمبدأ أصيل في الفقه الجنائي، وهو أن من يملك السلطة على المال والنظام يجب أن يتحمل تبعة انحرافهما، وهو مبدأ بات يكتسب أهمية خاصة في البيئة الرقمية التي تقوم على الثقة والمعالجة الآلية للبيانات [٤٣].**ويُثار التساؤل هنا: ما الأساس القانوني الذي تقوم عليه هذه المسؤولية في التشريع العراقي، وما أوجه المقارنة بينها وبين التشريعات العربية الأخرى التي واجهت الجرائم الاقتصادية الرقمية بصرامة.**

أولًا: الأساس القانوني للمسؤولية المباشرة في التشريع العراقي: تستند المسؤولية المباشرة للتاجر إلى ثلاثة مصادر رئيسية في القانون العراقي: قانون العقوبات العام، وقانون التجارة، وتعليمات البنك المركزي الخاصة بأنظمة الدفع.

أ. القواعد العامة في قانون العقوبات العراقي: أرسى قانون العقوبات رقم (١١١) لسنة ١٩٦٩ القاعدة العامة للمساءلة الجنائية في المادة (٣٣)، التي نصت على أن:

تكون الجريمة عمدية إذا ارتكب الجاني الفعل بإرادته وكان عالمًا بأنه مخالف للقانون.

هذا النص يُعدّ حجر الأساس في تحديد نية التاجر، إذ يُسأل جزائيًا إذا قام بفعل يعلم أنه غير مشروع ضمن نطاق عمله التجاري، سواء تمثل هذا الفعل في إدخال بيانات مزيفة في نظام الدفع أو تمرير معاملات مزوّرة.

كما أن المادة (٤٥٦) تُعدّ من النصوص التي يمكن تطبيقها مباشرة، لأنها تجرّم كل من يتوصل إلى تسلم أو نقل حيازة مال الغير لنفسه أو لغيره بإحدى وسائل الاحتيال، وهو ما ينطبق تمامًا على عمليات الدفع الإلكترونية غير المشروعة [٤٤].

ويؤيد الفقيه عبد الكريم الجبوري هذا الاتجاه بقوله: إن صور الاحتيال الحديثة لم تعد تقتصر على القول الكاذب أو الخداع المادي، بل امتدت إلى المجال الإلكتروني الذي يُمارَس فيه الإيهام بوسائل رقمية متقدمة.[٤٥]

ب . التزوير الإلكتروني والتلاعب بالبيانات: أضافت المادة (٢٨٦) من القانون ذاته بُعدًا آخر للمسؤولية الجنائية للتاجر، إذ وسّعت مفهوم التزوير ليشمل تحريف الحقيقة في محرر بأية وسيلة كانت. وبالتفسير الحديث، أصبح المحرر الإلكتروني مساويًا للمحرر الورقي من حيث الحماية الجنائية، استنادًا إلى قرار محكمة التمييز الاتحادية رقم (١٩/ج/٢٠١٩)، الذي اعتبر البيانات الإلكترونية محررات ذات قوة قانونية إذا كانت تنتج أثرًا في الواقع القانوني أو المالي [٤٦].وهكذا فإن التاجر الذي يُدخل بيانات مغايرة للحقيقة في نظام الدفع الإلكتروني أو يُعدّل سجل العمليات المالية يتحمل مسؤولية جنائية مباشرة بوصفه فاعلًا أصليًا .ويؤكد محمد الصغير في مؤلفه الإنترنت والقانون الجنائي أن إدخال بيانات خاطئة عمدًا في نظام إلكتروني مالي يمثل أخطر صور التزوير المعاصر لأنه يجمع بين الاحتيال والتقنية، ويُحدث أثرًا قانونيًا لحظيًا يصعب تداركه. [٤٧]

ج. الالتزامات القانونية المقررة بموجب تعليمات البنك المركزي: نصّت تعليمات البنك المركزي العراقي رقم (٣) لسنة ٢٠٢٠ بشأن أنظمة الدفع الإلكتروني على التزامات محددة للتجار، منها:

التحقق من هوية حامل البطاقة و حفظ السجلات الإلكترونية للعمليات لمدة لا تقل عن خمس سنوات و الإبلاغ عن أي معاملة مشبوهة أو متكررة تفوق الحدّ المعتاد. ويُعدّ الإخلال بهذه الالتزامات جريمة إذا كان مقترنًا بالقصد، أو إهمالًا جسيمًا متى نتج عنه ضرر مالي ويرى داوود عبد الكريم أن هذه الالتزامات تمثل إطارًا جنائيًا خاصًا لحماية المعاملات المصرفية، وأن مخالفتها تُعد سلوكًا ماديًا مخالفًا للقانون وإن لم يُذكر صراحة في نصوص التجريم التقليدية.[٤٨]

ثانيا: صور المسؤولية المباشرة للتاجر في جرائم الدفع الإلكتروني: تتجسد الأفعال الموجبة للمسؤولية المباشرة في ثلاث صور أساسية:

أ. الاحتيال التجاري الإلكتروني: ويتحقق عندما يتعمد التاجر استخدام بيانات غير صحيحة أو يُدخل معاملات وهمية بغرض الحصول على منفعة مالية غير مشروعة.

وقد قضت محكمة التمييز الاتحادية في قرارها رقم (١١٢/ج/٢٠٢٠) باعتبار أن قيام التاجر بتفعيل نظام إلكتروني لإجراء معاملات زائفة يمثل جريمة احتيال متكاملة الأركان [٤٩].ويرى فوزي عيسى أن هذه الصورة من الاحتيال تُعد امتدادًا طبيعيًا للاحتيال التقليدي، لكن خطورتها مضاعفة لأنها تُمارَس عبر بيئة رقمية تُخفي الدليل وتُسهّل الإفلات من العقاب [٥٠].

ب. تزوير البيانات والمستندات الرقمية: يتحقق التزوير عندما يُعدّل التاجر عمدًا في بيانات البطاقات أو السجلات الإلكترونية بهدف تضليل البنك أو العميل .وفي القانون المقارن، تُعتبر هذه الجريمة معاقبًا عليها بنص المادة (٦٠٧-٦) من القانون الجنائي المغربي، التي تجرّم إدخال أو حذف أو تعديل معطيات معلوماتية عن علم لخلق معطيات غير صحيحة [٥١].كما عالجها القانون الجزائري رقم (٠٩-٠٤)

لسنة ٢٠٠٩ في المادة (١٢)، التي جرّمت كل إدخال أو إتلاف متعمّد للبيانات أو البرامج الإلكترونية. وهذا الاتجاه المقارن يؤكد أن المشرع العربي يتعامل مع تغيير البيانات بوصفه عملاً ماديًا مُجرَّمًا بذاته، بغضّ النظر عن الوسيلة التقنية المستخدمة.

ج. إساءة استخدام المعلومات السرية للعميل: ويحدث هذا عندما يقوم التاجر بإفشاء بيانات العملاء أو استغلالها خارج إطار الغرض المخصص لها. وقد نصّت المادة (٤٣٩) من قانون العقوبات العراقي على تجريم إفشاء الأسرار المهنية، ويمكن تكييفها لتشمل الأسرار الإلكترونية.

وفي دراسة عبد الهادي عبد الحميد، أكد أن السرية المعلوماتية تمثل ركيزة أساسية للثقة المصرفية، والإفصاح عنها يُعد انتهاكًا مزدوجًا للحق في الخصوصية وللأمان المالي.[٥٢]

ثالثا: الركن المعنوي للمسؤولية المباشرة (القصد والنية التقنية): يتخذ الركن المعنوي هنا صورتين:

١. القصد الجنائي المباشر: أي أن يعلم التاجر بطبيعة فعله وأن يقصده لتحقيق منفعة غير مشروعة. ويتحقق هذا القصد في أفعال الاحتيال والتزوير عندما يُثبت أن التاجر تعمّد إدخال بيانات غير صحيحة أو تمرير معاملات وهمية.

٢. القصد الاحتمالي أو العلم التقني: ويكفي لتحققه أن يكون التاجر على علم بإمكان وقوع الجريمة نتيجة لإهماله في تأمين نظام الدفع أو مراقبة المعاملات .وقد أشار عبد العزيز عبد الجواد إلى أن النية التقنية الحديثة تُستخلص من سلوك الإعداد الرقمي وليس فقط من التنفيذ، لأن الفاعل في البيئة الإلكترونية يُرتكب فعله على مرحلتين: برمجة ثم تشغيل. [٥٣]وبذلك، يُصبح العلم الفني للنظام جزءًا من القصد الجنائي، لأن استخدام أدوات الدفع الإلكتروني يقتضي إلمامًا كافيًا بآلية عملها، ومن ثم يُفترض علم التاجر بالنتائج المحتملة لأفعاله.

٣. القصد البرمجي وفق الفقه المقارن بين الدول

أ. في المغرب: نصّ القانون الجنائي المغربي (الفصل ٦٠٧-٣) على تجريم الاستعمال الاحتيالي لنظام معالجة المعطيات الآلية.

ويمتاز هذا النص بأنه لا يشترط حدوث ضرر فعلي، بل يكفي مجرد استعمال النظام بشكل غير مشروع لتحقيق النية الإجرامية.

وهو ما يتفق مع الاتجاه الحديث الذي يرى أنّ مجرد استغلال البيئة المعلوماتية بنية غير مشروعة كافٍ لقيام الجريمة.[٥٤]

ب. في الجزائر: جاء القانون الجزائري رقم (٠٩-٠٤) لسنة ٢٠٠٩ أكثر دقة، إذ فرّق بين الولوج غير المشروع والتعديل العمدي للبيانات، مما يجعل السلوك التقني ذاته جريمة مستقلة حتى لو لم يتحقق الربح أو الضرر المالي [٥٥].

وهذا المفهوم أكثر شمولًا من النصوص العراقية الحالية، التي لا تجرّم مجرد الدخول أو التعديل إلا عند ثبوت النتيجة المادية.

ج. الاتجاه المقارن العام: يتجه الفقه المقارن إلى اعتبار أن التاجر أو المؤسسة المالية فاعل مباشر في الجريمة متى كانت لديه سلطة تحكم على النظام الإلكتروني واستخدمها عمدًا أو بإهمال لتحقيق غرض غير مشروع. ويؤكد رفيق مرادأن المعيار الحديث للمسؤولية لم يعد هو صدور الفعل مباشرة من الشخص، بل درجة تحكمه في الوسيلة الرقمية التي نتج عنها الفعل. [٥٦] يرى الباحث أن المسؤولية الجنائية المباشرة للتاجر في جرائم بطاقات الدفع الإلكتروني تمثل تطبيقًا حديثًا لمبدأ المساءلة عن إساءة استعمال التقنية .فالتاجر ليس مجرد مستخدم للنظام المالي، بل هو فاعل قانوني ومهني مسؤول عن حماية الثقة العامة في التعاملات الرقمية، ومن ثم، فإنّ الأفعال التي تُرتكب باستخدام النظام الإلكتروني لأغراض غير مشروعة تُعدّ جرائم عمدية، ولو تمت دون احتكاك مادي مباشر بالمال. ويقترح الباحث أن يتبنى المشرع العراقي نصًا خاصًا ضمن مشروع قانون الجرائم الإلكترونية على النحو الآتي:

ُعدّ مرتكبًا لجريمة الاستعمال الاحتيالي لأنظمة الدفع كل من استخدم أو عدّل أو فعّل نظام الدفع الإلكتروني أو بياناته بقصد الحصول على منفعة غير مشروعة، سواء تحقق الضرر أم لم يتحقق .بهذا النص، يُواكب التشريع العراقي التطورات التقنية ويغلق الثغرات القائمة في تجريم الأفعال الرقمية الحديثة.

الفرع الثاني: المسؤولية غير المباشرة للتاجر عن أفعال العاملين أو الشركاء

إنّ التاجر في النظام القانوني المعاصر لم يعد مجرد شخص يمارس نشاطًا تجاريًا منفردًا، بل أصبح يدير منظومة متكاملة تتكون من موظفين، ومحاسبين، ومبرمجين، وشركاء تقنيين يتعاملون مع أنظمة الدفع الإلكتروني .وفي ظل هذه البنية المركّبة، قد تقع الجريمة من أحد العاملين أو من جهة متعاقدة خارجيًا، فتُطرح إشكالية قانونية دقيقة: هل يمكن مساءلة التاجر جنائيًا عن فعل لم يصدر منه شخصيًا؟

لقد تجاوز الفقه الجنائي الحديث مفهوم المسؤولية الفردية الصرفة، ليقرّ بمبدأ المسؤولية بالرقابة التقنية أو المؤسسية، التي تُحمّل صاحب العمل أو مدير المنشأة مسؤولية أفعال العاملين متى كان قادرًا على منعها أو اكتشافها ولم يفعل [٥٧]

.هذا التحول يعكس تطور فلسفة العقوبة من الجزاء الشخصي إلى الحماية الوقائية للنظام الاقتصادي الرقمية ونبينه في ما يلي.

أولًا: الأساس القانوني للمسؤولية غير المباشرة في القانون العراقي: يُعدّ قانون التجارة العراقي رقم (٢١) لسنة ٢٠٢١ هو النص الأبرز الذي وضع قاعدة عامة للمساءلة غير المباشرة في البيئة التجارية الرقمية. فالمادة (٣٨٦) تنصّ صراحة على أنّ: يُسأل البائع جنائيًا عن الأفعال الإجرامية المرتكبة في نطاق نشاطه التجاري إذا كان على علم بها أو كان بإمكانه منعها ولم يفعل. هذا النص يؤسس لمبدأ المسؤولية عن الإهمال في الرقابة، بحيث يُسأل التاجر إذا توفرت ثلاثة شروط متلازمة:

- أن تقع الجريمة ضمن نطاق النشاط التجاري.
- أن تكون لديه سلطة فعلية أو تقنية تمكّنه من الرقابة أو المنع.
- أن يثبت أنه تقاعس عن أداء واجب الإشراف أو سمح ضمنيًا بوقوع الجريمة.

ويرى محمد الداودي أنّ هذه المادة تمثل انتقالًا نوعيًا من فكرة "النية الإجرامية" إلى فكرة "الواجب الإشرافي"، لأن التاجر لم يعد يُسأل فقط إذا شارك، بل أيضًا إذا أهمل السيطرة على أدواته التقنية [٥٨].

كما يُستفاد من المادة (٣٥) من قانون العقوبات رقم (١١١) لسنة ١٩٦٩ أنّ الإهمال أو قلة الاحتراز سبب للمساءلة متى ترتب عليه ضرر، وهي قاعدة عامة تشمل صور الإهمال المؤسسي أو التقني، إذ لا فرق بين الإهمال في العمل المادي والإهمال في النظام الإلكتروني الذي يملك التاجر حق السيطرة عليه [٥٩].

ثانيًا: مفهوم الإخلال بالرقابة التقنية كأساس للمسؤولية: تتحقق المسؤولية غير المباشرة عندما يكون التاجر قد أخلّ بواجب الإشراف، أي لم يضع نظامًا فعالًا للرقابة الداخلية يمنع العاملين من استغلال صلاحياتهم أو ارتكاب الجرائم ويُعدّ هذا الإخلال فعلاً إيجابيًا من حيث أثره، لأنه يؤدي إلى تمكين الجريمة أو تسهيلها.

ويُظهر التطبيق العملي أنّ هذه المسؤولية تتحقق غالبًا في ثلاث حالات:

١. **ضعف نظام المراقبة الداخلية:** كعدم وجود فصل في المهام بين الموظفين أو غياب التحقق المزدوج للعمليات المالية.

٢. **الإهمال في تأمين النظام الإلكتروني:** مثل ترك كلمات المرور العامة، أو عدم تحديث أنظمة الحماية، مما يسمح بالاختراق.

٣. **عدم الإبلاغ عن الشبهات المالية:** وهي من الالتزامات المفروضة بموجب تعليمات البنك المركزي رقم (٩) لسنة ٢٠٢٠، التي تُلزم التاجر بالإبلاغ عن أي عملية مشبوهة فورًا [٦٠].ويرى نجيب خالد أنّ هذه الصور الثلاث تُكوّن ما يُعرف في الفقه الحديث بـ الخطأ التنظيمي المؤسسي، وهو خطأ يقوم مقام الفعل المادي في تأسيس المسؤولية الجنائية [٦١].

ثالثًا: التطبيقات القضائية للمسؤولية غير المباشرة: أكد القضاء العراقي الاتجاه نحو إقرار هذه المسؤولية في حكم محكمة التمييز الاتحادية رقم (٥٧/ج/٢٠٢١)، الذي جاء فيه:

إنّ عدم اتخاذ صاحب العمل للتدابير التقنية اللازمة للرقابة على موظفيه يشكل إهمالًا جزائيًا موجبًا للمساءلة إذا ترتب عليه ضرر للغير.

وفي هذا الحكم، تم تحميل التاجر المسؤولية عن اختراق النظام المالي لمتجره بسبب تقصيره في متابعة سجلات الدخول الإلكتروني للموظفين .وهذا التوجه يُظهر أنّ القضاء العراقي بدأ يتعامل مع الإهمال التقني كفعل إجرامي مستقل، وليس مجرد مخالفة مهنية.

كما يُلاحظ اتجاه مشابه في حكم محكمة جنايات الكرخ رقم (٨٨/ج/٢٠٢٢)، الذي قرر أنّ صاحب المتجر الذي لم يؤمّن الأجهزة الإلكترونية المخصصة للدفع مسؤول جزائيًا عن الأضرار التي نتجت عن استخدام تلك الأجهزة في تحويلات غير مشروعة.[٦٢]ويرى فاضل الشاوي أنّ هذا التطور في الاجتهاد القضائي العراقي يُعدّ تأصيلًا لفكرة الرقابة الإلكترونية بوصفها واجبًا قانونيًا وليس مجرد التزام إداري، وهو ما يعكس وعيًا تشريعيًا بخصوصية الجريمة الرقمية [٦٣].

رابعًا: المقارنة التشريعية بين العراق وبعض الدول العربية

١. **تونس:** تُعدّ القانون الأساسي عدد (٥) لسنة ٢٠٠٤ من التشريعات العربية الرائدة في هذا المجال، فقد نصّ الفصل (١٣) منه على أنّ: تُسند المسؤولية إلى كل من أتاح أو لم يمنع استخدام نظامه المعلوماتي في ارتكاب الجريمة إذا كان قادرًا على تفاديها ويتميّز النص التونسي بأنه لا يشترط العلم الفعلي بالجريمة، بل يكتفي بوجود القدرة المفترضة على المنع .ويرى حاتم الباجي أنّ هذا المعيار يعكس مبدأ "العناية التقديرية الذي يقيس الإهمال بمدى الالتزام بالمعايير التقنية لا بالنية [٦٤].

٢. **فرنسا:** كرّس القانون الجنائي الفرنسي في المادة (١٢١-٢) مبدأ المسؤولية المؤسسية (Responsabilité pénale des personnes morales)، حيث تكون الشركة مسؤولة عن الجرائم التي تُرتكب باسمها أو لمصلحتها من قبل ممثليها أو أجهزتها الإدارية.[٦٥]وقد فسّر القضاء الفرنسي هذا النصّ في قضايا مصرفية ليشمل الإهمال في الرقابة المعلوماتية، معتبرًا أن ترك النظام دون تدقيق أو إشراف يوازي السماح بارتكاب الجريمة.

٣. **المغرب:** أدخل المشرع المغربي تعديلًا عام ٢٠١٨ أقرّ في الفصل (٦٠٧-٧) من القانون الجنائي مسؤولية الأشخاص المعنويين عن الجرائم المعلوماتية متى أخلّوا بواجب حماية البيانات أو الرقابة على العاملين. ويُعدّ هذا التوجه أكثر تقاربًا مع الاتجاه العراقي، إذ يجعل الإهمال في الرقابة الإلكترونية مناطًا للمساءلة [٦٦].

خامسًا: التحليل الفقهي المقارن: يتبيّن من المقارنة أنّ الأساس الفقهي للمسؤولية غير المباشرة يقوم على فكرة الإخلال بواجب الرقابة الذي تحوّل في البيئة الإلكترونية إلى التزام قانوني إيجابي. فالقانون العراقي، رغم عموميته أقرّ هذا الاتجاه ضمنيًا في المادة (٣٨٦) من قانون التجارة، في حين تبنّته التشريعات التونسية والمغربية صراحة. ويشير عبد الله الزعبي إلى أنّ المسؤولية بالرقابة في الجرائم المعلوماتية هي تطور طبيعي لمفهوم الحراسة في القانون المدني، إذ أصبح من يملك السيطرة التقنية على النظام مطالبًا قانونيًا بضمان عدم انحرافه. [٦٧]

أما سعاد خلف والشاوي فترى أن إسناد المسؤولية لصاحب المشروع لا يُخلّ بمبدأ شخصية العقوبة، لأنّ الإهمال في الرقابة يُعتبر فعلاً إيجابيًا قائمًا بذاته. [٦٨]وهذا التحليل ينسجم مع مبدأ العدالة الجنائية الحديثة التي تُساوي بين الفاعل بالإهمال والفاعل بالفعل متى تساوت النتيجة الاجتماعية للجريمة.

سادسًا: نحو تأصيل المفهوم في القانون العراقي: رغم التطور القضائي، لا يزال المشرّع العراقي بحاجة إلى نصّ صريح يُقرّ بمسؤولية التاجر عن الإهمال الرقابي في أنظمة الدفع الإلكتروني.

ويقترح الباحث إضافة مادة جديدة إلى قانون الجرائم الإلكترونية أو قانون التجارة تنصّ على الآتي: يُسأل جزائيًا التاجر أو المدير المسؤول عن كل فعل يُرتكب في نطاق منشأته التجارية إذا ثبت أن الجريمة قد وقعت نتيجة لإهماله أو تقصيره في الرقابة التقنية، سواء علم بها أو لم يعلم، متى كان في موقع يسمح له بالمنع أو الاكتشاف. فهذا النصّ يُجسّد مبدأ المسؤولية المؤسسية الوقائية، التي تهدف إلى تعزيز الأمن المالي قبل وقوع الجريمة، وتفرض على التاجر التزامًا بالمتابعة اليومية للأنظمة الإلكترونية.

يرى الباحث أن المسؤولية غير المباشرة للتاجر ليست خروجًا على مبدأ شخصية المسؤولية، بل تطويرًا له في ضوء طبيعة المعاملات الإلكترونية فالتاجر الذي يملك نظامًا إلكترونيًا متقدمًا دون أن يؤمنه أو يراقبه يمارس خطأً إيجابيًا في صورة إهمال تقني جسيم، كما أن منح القضاء سلطة تقدير مدى التزام التاجر بالمعايير الفنية (كالمعايير الدولية PCI DSS الخاصة بحماية بيانات البطاقات) يُعدّ خطوة ضرورية لتقدير المسؤولية على أسس موضوعية. ويخلص الباحث إلى أنّ إقرار هذه المسؤولية يعزّز الثقة العامة في النظام المصرفي، ويُسهم في وقاية الاقتصاد الرقمي من الجرائم المستحدثة التي لا يمكن مكافحتها بوسائل التشريع التقليدية إنّ المسؤولية غير المباشرة للتاجر في جرائم بطاقات الدفع الإلكتروني تُجسد تحولًا جوهريًا في المفهوم الجنائي التقليدي، حيث لم تعد المساءلة قاصرة على الفعل الشخصي، بل امتدت إلى الإهمال الرقابي المؤسسي، الذي يُعدّ في البيئة المعلوماتية الحديثة فعلاً إجراميًا كامل الأركان.

المطلب الثاني: حالات قيام المسؤولية الجنائية في جرائم بطاقات الدفع الإلكتروني

تُعدّ حالات قيام المسؤولية الجنائية في جرائم بطاقات الدفع الإلكتروني من الموضوعات الحديثة التي تجمع بين الجانب التقني والجانب القانوني، إذ أصبح النشاط الإجرامي في هذا المجال يتخذ صورًا متعددة تتراوح بين الأفعال العمدية كالاستعمال غير المشروع والتزوير والاحتيال الإلكتروني، وبين الأفعال غير العمدية التي تقوم على الإهمال أو التقصير في أداء واجب الإبلاغ أو الرقابة على الأنظمة المالية.

وتكمن أهمية هذا المطلب في بيان الأساس القانوني لكل صورة من صور المسؤولية، وتحليل مدى كفاية النصوص العراقية في مواجهة تلك الأفعال مقارنةً بالتشريعات العربية والأوروبية التي طوّرت قواعد خاصة لحماية وسائل الدفع الحديثة.

وبذلك، سيتناول هذا المطلب في فرعه الأول المسؤولية الجنائية الناشئة عن الأفعال العمدية، وفي فرعه الثاني المسؤولية الناشئة عن الإهمال أو التقصير في الإبلاغ أو الرقابة التقنية.

الفرع الأول: المسؤولية الجنائية الناشئة عن الأفعال العمدية

تتحقق المسؤولية الجنائية العمدية متى توافرت إرادة الجاني وعلمه بعدم مشروعية فعله، وهي الأساس في أغلب الجرائم الإلكترونية الخاصة بوسائل الدفع، إذ تقوم على نشاط تقني واعٍ موجّه نحو غاية مالية محددة.

وقد تبلورت ثلاث صور رئيسية لهذه المسؤولية في الواقع العملي: الاستخدام غير المشروع للبطاقة، والتزوير الإلكتروني، والاحتيال في المعاملات المصرفية، وكلها تمثل أفعالًا عمدية يتحقق بها القصد الجرمي في الجريمة المالية الرقمية[٦٩].

أولًا: الاستخدام غير المشروع لبطاقات الدفع الإلكتروني: يُعد الاستخدام غير المشروع لبطاقات الدفع الإلكتروني من أبرز صور الجرائم المعلوماتية في البيئة المصرفية الحديثة، ويتحقق هذا الفعل عندما يستعمل الجاني البطاقة أو بياناتها دون إذنٍ من صاحبها، سواء بالاستيلاء المادي عليها أو بسرقة بياناتها عبر وسائل إلكترونية كالاختراق أو التصيد الاحتيالي.

ويُعتبر هذا الفعل من قبيل الاحتيال وفق المادة (٤٥٦) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، التي تُعاقب على من يتوصل إلى تسلم أو نقل مالٍ مملوكٍ للغير بإحدى وسائل الاحتيال[٧٠].

وقد قضت محكمة التمييز الاتحادية العراقية في قرارها رقم (١٤١/ج/٢٠٢١) بأن استعمال البطاقة المصرفية للغير دون إذنه يشكل احتيالًا معلوماتيًا متكامل الأركان، لأن الوسيلة التقنية تحقق عنصر الخداع المطلوب قانونًا[٧١].

ويرى الدكتور محمد نجيب أن هذا النوع من الأفعال يمثل تحويلًا افتراضيًا للملكية، إذ يُستخدم النظام المالي ذاته كوسيلة احتيال بديلة عن التعامل النقدي[٧٢].

ويضيف الدكتور عبد الكريم الجبوري أن الثقة بالنظام المصرفي الإلكتروني أصبحت محل الحماية الجنائية بذاتها، لأن أي استخدام غير مأذون به يُعدّ إخلالًا بالائتمان المالي للدولة[٧٣].وفي المقارنة العربية، نصّت المادة (٤) من نظام مكافحة الجرائم المعلوماتية السعودي لعام ٢٠٠٧ على تجريم الاستيلاء على مالٍ منقول أو سند بطرقٍ احتيالية أو انتحال هوية الغير عبر الوسائل التقنية، كما نصّت المادة (١٨) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨على تجريم الاستيلاء الإلكتروني ولو لم يتحقق ضرر فعلي[٧٤].أما التوجيه الأوروبي رقم (٧١٣/٢٠١٩) فقد ذهب أبعد من ذلك، إذ عاقب على محاولة الاستخدام غير المصرّح بها باعتبارها جريمة قائمة بذاتها حتى قبل تحقق النتيجة[٧٥].من الواضح أن المشرع العراقي لم يواكب التطور التقني في معالجة هذه الجريمة، فبينما نصّت القوانين الحديثة على تجريم الفعل الإلكتروني ذاته، ما زالت النصوص العراقية عامة ومقيدة بمفاهيم مادية، مما يؤدي إلى تفاوت في التكييف القضائي ويتضح أن الحل التشريعي الأمثل يكمن في إدراج نص خاص بعنوان "الاستعمال الاحتيالي لبطاقات الدفع الإلكتروني"، لتجريم كل استعمال غير مشروع للبيانات أو الأوامر المصرفية ولو لم يتحقق ضرر فعلي.

ثانيًا: التزوير الإلكتروني في بطاقات الدفع: يقوم التزوير الإلكتروني على تحريف الحقيقة في البيانات الرقمية أو إنشاء بطاقات مزيفة بوسائل تقنية كبرامج النسخ أو التعديل، بقصد الحصول على منفعة مالية, وقد نصّت المادة (٢٨٦) من قانون العقوبات العراقي على أن يعد تزويرًا كل تغييرٍ للحقيقة في محررٍ بإحدى الطرق المبيّنة قانونًا بقصد استعماله كمحررٍ صحيح متى كان من شأنه إحداث ضرر بالغير[٧٦].إلا أن النص لم يشمل البيانات الإلكترونية كمحل للجريمة، ما أوجد فراغًا تشريعيًا ملحوظًا وقد سعت محكمة التمييز الاتحادية إلى معالجة ذلك في قرارها رقم (١٩/ج/٢٠١٩)، حيث اعتبرت البيانات الإلكترونية المعتمدة في الأنظمة المصرفية محررات قانونية ذات أثر مالي، وبذلك مدّت الحماية الجنائية إلى المحررات الرقمية[٧٧].ويرى الدكتور عبد الهادي عبد الحميد أن التحريف الرقمي للحقيقة يُعدّ صورة حديثة للتزوير المعنوي، لأن البيانات تمثل مضمونًا ذا حجية قانونية، وإن اختلفت وسيلة التعبير عنه[٧٨].كما يرى الدكتور فهمي عبد الحافظ أن الجرائم الرقمية ألغت الفاصل بين الورقي والإلكتروني، وأصبح الأصل في الحماية هو الأثر القانوني لا شكل الوسيلة[٧٩].

وعلى الصعيد المقارن، نصّ الفصل (٦٠٧-٦) من القانون الجنائي المغربي المعدّل ٢٠١٨ على تجريم إدخال أو حذف أو تعديل البيانات عن علم في نظام المعالجة الآلية للمعطيات ،في حين نصّ القانون الجزائري رقم (٠٩-٠٤) لسنة ٢٠٠٩ في المادة (١١) على معاقبة كل إدخال أو تعديل متعمد للبيانات الإلكترونية في نظام محمي[٨٠].وفي القانون الفرنسي، عاقبت المادة (٤٤١-١) على "كل من غيّر أو شوّه بيانات إلكترونية ترتب أثرًا قانونيًا" واعتبرت ذلك تزويرًا معاصرًا,[٨١]وبما إنّ نطاق الحماية في التشريع العراقي ما زال ضيقًا، لأن المشرّع لم يعترف بعد بالمحرر الإلكتروني كمحل لجريمة التزوير ,أما القوانين المقارنة، فاعتمدت معيار الأثر القانوني للبيانات بدلًا من ماديتها، وهو ما ينسجم مع التطور الرقمي في التعامل المالي.

ومن خلال ما تم ذكره ينبغي تعديل المادة (٢٨٦) بإضافة فقرة تنص على: ويُعد تزويرًا أيضًا كل تحريفٍ للحقيقة في بيانات إلكترونية ذات أثر مالي أو قانوني، لتغطية الواقع التقني المعاصر وتوحيد التفسير القضائي.

ثالثًا: الاحتيال الإلكتروني في المعاملات المصرفية: يُعد الاحتيال الإلكتروني أخطر صور جرائم الدفع، لأنه يستهدف النظام المالي ذاته وليس الأفراد فحسب، ويقوم على إدخال بيانات أو أوامر إلكترونية مضللة تؤدي إلى تحويل أموالٍ من حسابٍ إلى آخر دون وجه حق.

وتنطبق على هذا الفعل المادة (٤٥٦/ثانيًا) من قانون العقوبات العراقي التي تُجرّم من يتوصل إلى مال الغير بوسائل احتيالية، لكن النص لم يذكر الوسائل التقنية تحديدًا[٨٢].وفي قرار محكمة التمييز الاتحادية رقم (١٤١/هيئة جزائية/٢٠٢١)، عُدّ إنشاء موقعٍ إلكترونيٍ شبيه بموقع مصرفٍ رسمي وسحب أموال العملاء "احتيالًا إلكترونيًا"، إذ تحققت أركان الجريمة من خلال الخداع المعلوماتي بدل الخداع اللفظي. ويرى الدكتور مجيد عبد الرضا أن الاحتيال الإلكتروني يختلف عن التقليدي من حيث موضوع الجريمة، لأن الخداع موجّه نحو النظام البرمجي نفسه، مما يستوجب نصوصًا خاصة تنظم علاقة الجاني بالأنظمة المعلوماتية[٨٣].وقد أخذ التوجيه الأوروبي رقم (٧١٣/٢٠١٩) بهذا المفهوم حين اعتبر أن "الاحتيال يتحقق بمجرد إدخال أوامر غير مشروعة في نظام المعالجة المالية"، حتى لو لم يتحقق تحويل فعلي[٨٤].وفي القانون الفرنسي، نصّت المادة (٣٢٣-٣-١) على معاقبة "كل من يُدخل أوامر إلكترونية بقصد تحويل الأموال بطريقة احتيالية"، وهي صيغة تتفق مع الاتجاه الأوروبي في توسيع نطاق الحماية وإنّ معالجة هذه الجريمة في القانون العراقي لا تزال تقليدية، إذ لم يُميز المشرّع بين الاحتيال الموجه إلى الأشخاص والاحتيال الموجه إلى الأنظمة، وهو ما يؤدي إلى قصور في الردع.

بينما اعتمدت التشريعات المقارنة تمييزًا دقيقًا بين "الاحتيال التقني" و"الاحتيال التقليدي"، مما يوفر حماية أوسع للنظام المصرفي.

يتبين من خلال ما تم ذكره بضرورة استحداث مادة بعنوان "خداع الأنظمة المعلوماتية المالية" ،التي تُجرّم إدخال أوامر إلكترونية مضللة بقصد تحويل الأموال أو الحصول على منافع مالية غير مشروعة،

وتُعد مكملة للمادتين (٢٨٦) و(٤٥٦) في القانون العراقي تضح من تحليل صور الأفعال العمدية أن القانون العراقي ما زال قاصرًا عن مواكبة التطور التقني الذي يشهده القطاع المالي، إذ يُطبّق نصوصًا وضعت لمعالجة سلوك مادي على أفعال ذات طبيعة رقمية.

أما التشريعات المقارنة العربية والأوروبية، فقد تبنّت نصوصًا جزائية متخصصة تُجرّم الوسائل التقنية ذاتها وتفصل بين الاحتيال والتزوير الإلكترونيين، مما حقق وضوحًا تشريعيًا وردعًا فعالًا.

لذلك، فإن الإصلاح التشريعي في العراق يجب أن يتجه نحو وضع قانون خاص بجرائم الدفع الإلكتروني، يتضمن نصوصًا صريحة تجرّم الأفعال التقنية وتحمي الثقة العامة بالنظام المصرفي

الفرع الثاني: المسؤولية الجنائية الناشئة عن الإهمال أو التقصير في الإبلاغ أو الرقابة التقنية

تُعدّ المسؤولية الجنائية الناشئة عن الإهمال أو التقصير في مجال بطاقات الدفع الإلكتروني من أهم المسائل القانونية المستحدثة، إذ لم تعد المسؤولية الجنائية مقصورة على الأفعال الإيجابية التي تتم عن قصدٍ وعلم، بل امتدت لتشمل الأفعال السلبية المتمثلة في الامتناع أو الإهمال متى ترتب عليه ضرر مالي أو خطر فعلي على النظام المصرفي. فقد بات الإهمال في الإبلاغ عن فقدان البطاقة أو التقصير في تطبيق إجراءات الرقابة التقنية يوفّر بيئة خصبة لوقوع الجرائم المالية الإلكترونية، ويُعد في ذاته سلوكًا مخالفًا لواجب الحيطة المصرفية التي تفرضها القوانين الحديثة[٨٥].

ويُقسّم هذا الفرع إلى محورين رئيسيين:

١. الإهمال في الإبلاغ عن الفقدان أو الاختراق.

٢. التقصير في الرقابة التقنية والإدارية على أنظمة الدفع الإلكتروني.

أولاً: الإهمال في الإبلاغ عن الفقدان أو الاختراق: يُعتبر الإبلاغ الفوري عن فقدان البطاقة أو تعرّض الحساب للاختراق واجبًا قانونيًا أساسيًا في نظام الدفع الإلكتروني، لأنه يُمثل خط الدفاع الأول ضد الاحتيال. وقد نصّت المادة (٥) من تعليمات البنك المركزي العراقي رقم (٩) لسنة ٢٠٢٠ بشأن أنظمة الدفع الإلكتروني على أن :يلتزم حامل البطاقة بإبلاغ الجهة المصدرة فور علمه بفقدان البطاقة أو استخدامها دون إذنه، ويتحمّل المسؤولية عن التأخير في الإبلاغ[٨٦].وتتجلى أهمية هذا النص في كونه أول تنظيم صريح يحمّل المستخدم مسؤولية الامتناع عن الإبلاغ، باعتباره سلوكًا مخالفًا لواجب العناية المصرفية المفترضة. كما تنص المادة (٣٥) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ على أن الخطأ أو الإهمال سبب للمسؤولية متى كان الجاني قادرًا على توقع النتيجة الضارة وتفاديها[٨٧].وفي حكم محكمة جنايات الكرخ رقم (١٠١/ج/٢٠٢٢)، قضت المحكمة بمسؤولية أحد المستخدمين لعدم تبليغه عن فقدان بطاقته خلال (٤٨) ساعة، مما أدى إلى استخدامها من قبل مجهولين في تحويل أموال، واعتبرت المحكمة هذا الامتناع إهمالاً جسيمًا ترتب عليه ضرر فعلي يستوجب العقاب[٨٨].ويرى الدكتور عبد الحميد طارق أن الإبلاغ في المجال الإلكتروني لم يعد مجرد التزام إداري أو مصرفي، بل هو واجب قانوني ذي طبيعة جزائية، لأن الامتناع عنه يؤدي إلى تمكين الجريمة من الاستمرار[٨٩].ويُشاركه الرأي

الدكتور فاضل الشاوي في تأكيده أن الإهمال في الإبلاغ عن المخاطر الإلكترونية يمثل مشاركة غير مباشرة في الجريمة، لأنه يُخلّ بواجب الوقاية الذي يفرضه القانون على جميع المتعاملين في البيئة المالية الرقمية[٩٠].أما في المقارنة العربية، فقد نصّ الفصل (١٤) من القانون التونسي رقم (٥) لسنة ٢٠٠٤ بشأن أمن النظم المعلوماتية على أن: كل من علم بفقدان وسيلة تؤدي إلى الولوج إلى نظام معلوماتي ولم يُبلغ فورًا السلطات المختصة يُعاقب بالحبس والغرامة[٩١].

ويُعد هذا النص من أوضح الأمثلة على تجريم الامتناع عن الإبلاغ كجريمة قائمة بذاتها ذات طابع وقائي. أما في القانون الفرنسي، فقد تبنّى مفهوم الواجب الإيجابي بالإخطار (Obligation de signalement)، حيث تُلزم المادة (L.561-15) من قانون النقد والمال الفرنسي المؤسسات المصرفية والأفراد بالإبلاغ عن أي عملية مالية مشبوهة فورًا إلى السلطات المختصة، ويُعدّ التأخر في ذلك إخلالًا مهنيًا وجنائيًا معًا[٩٢].

إنّ المشرّع العراقي لا يزال يعالج الإهمال في الإبلاغ من خلال النصوص العامة لقانون العقوبات، رغم أنه سلوك ذو خصوصية رقمية تستوجب تنظيماً جزائياً مستقلاً .ففي البيئة التقنية، لا يترتب على الإهمال ضرر شخصي فقط، بل يتعداه إلى النظام المالي ككل، مما يجعل المسؤولية ذات طابع اجتماعي وقائي لا فردي .يتعين على المشرّع العراقي إدراج مادة خاصة بعنوان "الإخلال بواجب الإبلاغ عن الفقدان أو الاختراق الإلكتروني"، تُعاقب على التأخير غير المبرر متى ترتب عليه ضرر فعلي أو محتمل، مع تحديد المدة الزمنية التي يُعدّ تجاوزها إهمالاً جزائياً.

ثانيًا: التقصير في الرقابة التقنية والإدارية على أنظمة الدفع الإلكتروني: تتجسد الرقابة التقنية في الإجراءات التي تتخذها المؤسسات المصرفية والتجارية لحماية أنظمة الدفع من الاختراق أو سوء الاستخدام، مثل تحديث الأنظمة الأمنية، ومراقبة العمليات المشبوهة، والتدقيق المستمر للبيانات.

ويُعدّ التقصير في هذه الرقابة سببًا مباشرًا في وقوع الجريمة الإلكترونية أو استمرارها، مما يجعل صاحب العمل أو المؤسسة مسؤولًا جنائيًا متى ثبت أن الإهمال في الرقابة كان سببًا في تحقق النتيجة الضارة.

وقد نصّت المادة (٣٨٧) من قانون التجارة العراقي رقم (٢١) لسنة ٢٠٢١على أن:

وفي المقارنة، نصّ التوجيه الأوروبي رقم (٧١٣/٢٠١٩) على مسؤولية الجهات المقدمة لخدمات الدفع في حال فشلها في اتخاذ التدابير الوقائية المعقولة لمنع الاحتيال الإلكتروني، وعدّ ذلك إخلالًا بمبدأ الرقابة المؤسسية الإلزامية.[٩٣]

كما أقرّ القانون الفرنسي في المادة (٣٢٣-٤-١)مسؤولية الأشخاص المعنويين عن الإهمال في مراقبة الأنظمة المعلوماتية متى ترتب عليه تسهيل ارتكاب الجريمة أو الإضرار بالغير[٩٤].من الملاحظ أن القانون العراقي قد خطا خطوة إيجابية بإدراج مبدأ الرقابة في قانون التجارة لعام ٢٠٢١، لكنه لم يمنحه بعد الصفة الجزائية الصريحة. بينما اتجهت التشريعات المقارنة إلى تأصيل هذا الالتزام في صلب المسؤولية الجنائية للمؤسسات والأشخاص المعنويين، لما له من أثر مباشر على الأمن الاقتصادي

الوطني. إنّ غياب نصّ جزائي واضح يحمّل المؤسسات مسؤولية التقصير في الرقابة يجعل الممارسة القضائية العراقية عرضة للتباين في التكييف .وعليه، يُقترح تعديل قانون التجارة أو العقوبات لإضافة نص صريح يقضي بمساءلة الأشخاص الطبيعيين والمعنويين عن الإهمال التقني والإداري الذي يؤدي إلى المساس بسلامة النظام المالي.

إنّ الإهمال في الإبلاغ أو الرقابة يُشكّل أحد أخطر مظاهر القصور في البنية التشريعية العراقية لمواجهة الجرائم الإلكترونية. ففي حين أن التشريعات الأوروبية والعربية قد جرّمت هذه الأفعال بوصفها تهديدًا للأمن المالي، ما زال القانون العراقي يعالجها ضمن القواعد العامة دون نصوص خاصة . ويستنتج من ذلك أن السياسة الجنائية العراقية بحاجة إلى تبني نموذج تشريعي وقائي، يجعل الإبلاغ والرقابة التقنية التزامين جزائيين إلزاميين، لضمان سرعة الاستجابة ومنع تفاقم الخطر المالي في البيئة الإلكترونية.

خاتمة

يتضح من خلال الدراسة أن جرائم بطاقات الدفع الإلكتروني تمثل تحديًا تشريعيًا مستحدثًا لا تزال النصوص العراقية التقليدية عاجزة عن استيعابه، سواء على مستوى التجريم أو المسؤولية أو الإثبات. وهو ما يفرض ضرورة الانتقال من مرحلة المعالجة الجزئية إلى بناء إطار قانوني متكامل يواكب التطور الرقمي ويحمي الثقة بالنظام المالي. وفي ضوء ما سبق، يمكن استخلاص أهم النتائج والتوصيات الآتية:

أولاً: أهم النتائج

١. تبيّن أن القانون العراقي لا يتضمن نصوصًا جزائية خاصة بجرائم بطاقات الدفع الإلكتروني، وأن الاعتماد على مواد الاحتيال والتزوير التقليدية (مثل المادة ٤٥٦ و٢٨٦ عقوبات) لا يكفي لتجريم السلوك الرقمي المستحدث، ما يؤدي إلى ضعف الحماية الجنائية للمعاملات الإلكترونية.

٢. أثبت البحث أن الركن المادي في جرائم الدفع الإلكتروني يقوم على سلوك تقني غير مادي (اختراق، استعمال غير مشروع، تزوير بيانات، أوامر برمجية)، وهو ما يخرج عن نطاق التعريف التقليدي للجريمة في قانون العقوبات العراقي، الذي صيغ لجرائم مادية محسوسة.

٣. أظهر البحث أنّ الركن المعنوي في هذه الجرائم لم يعد يقتصر على القصد الجرمي التقليدي، بل يتطلب الاعتراف بما يُسمّى "القصد البرمجي" أو "الإرادة التقنية"، أي النية المتحققة عبر تصميم أو تفعيل الأداة الرقمية قبل ارتكاب الجريمة، وهو ما لا يعالجه المشرع العراقي إطلاقًا.

٤. أثبتت الدراسة أن المسؤولية الجزائية لا تقتصر على الفاعل الأصلي، بل تمتد إلى المسؤولية غير المباشرة الناشئة عن الإهمال الرقابي أو التقني داخل المؤسسات المصرفية والتجارية، وهو ما غاب عنه التشريع العراقي بخلاف بعض التشريعات العربية (كالقانون الإماراتي والمغربي).

ثانياً: أهم التوصيات

١. استحداث فصل خاص في قانون العقوبات العراقي بعنوان: "الجرائم المتعلقة بوسائل الدفع الإلكتروني"، يتضمن نصًا يُجرّم كل استعمال غير مشروع لبطاقة الدفع أو بياناتها، ولو لم يتحقق ضرر مالي فعلي.

٢. تعديل المادة (٢٨٦) عقوبات الخاصة بالتزوير بإضافة فقرة تنص على: "ويُعد تزويرًا كذلك كل تغيير أو تحريف في البيانات الإلكترونية ذات الأثر المالي أو المصرفي وبذلك يصبح التزوير الرقمي مجرّماً صراحةً لا قياسًا.

٣. إضافة مادة جديدة بعد المادة (٤٥٦) عقوبات بعنوان :"الاحتيال عبر الأنظمة الإلكترونية"، تجرّم إدخال أوامر أو بيانات رقمية بقصد تحويل أو الاستيلاء على الأموال.

٤. تعديل المادة (٣٤) من قانون العقوبات لتشمل الإهمال التقني، وذلك بإضافة نص يقرر المسؤولية الجزائية عن :"التقصير في حماية الأنظمة الإلكترونية أو بيانات الدفع متى أدى إلى وقوع جريمة أو تسهيلها".

٥. تضمين تعليمات البنك المركزي نصًا جزائيًا ملزمًا يفرض على التجار والمؤسسات مزوّدة خدمة الدفع الإلكتروني اعتماد أنظمة حماية معتمدة دوليًا (PCI DSS)، ويقرر مساءلة جزائية عند الإخلال بواجب الرقابة أو الإبلاغ عن الاختراق.

الهوامش:

(١) ينظر قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، المواد (٤٥٥–٤٥٦).

(٢) ينظر قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المادة (١٣).

(٣) ينظر القانون الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات، المادة (٢).

(٤) انظر قرار محكمة التمييز الاتحادية العراقية رقم (٧٤/هيئة جزائية/٢٠٢١).

(٥) ينظر محكمة القاهرة الاقتصادية، القضية رقم ٣٨٤ لسنة ٢٠٢٠.

(٦) ينظر القانون الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢، المادة (١٠).

(٧) ينظر قرار محكمة جنايات الكرخ رقم (٨٨/ج/٢٠٢٢).

(٨) ينظر قرار محكمة النقض المصرية، الطعن رقم ١٧٦ لسنة ٢٠١٩ اقتصادي.

(٩) ينظر قرار محكمة بداية عمان، قرار بتاريخ ٢٠٢٠/٩/١٤.

(١٠) ينظر محكمة دبي الابتدائية، القرار رقم (١١٢/ج/٢٠٢٠).

(١١) ينظر محمود حسن، التحقيق الجنائي في الجرائم الرقمية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١، ص٩٧.

(١٢) ينظر قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المادة (٢٧).

(١٣) ينظر قانون المعاملات الإلكترونية الأردني رقم ٨٥ لسنة ٢٠٠١، المادة (٢٦).

(١٤) ينظر القانون الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢، المادة (٣٥).

(١٥) ينظر محمد الصغير، القانون الجنائي والإنترنت، دار النهضة العربية، القاهرة، ٢٠١٨، ص١٣٤.

(١٦) ينظر قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، المادة (٦).

(١٧) ينظر قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المادة (٢٩).

(١٨) ينظر قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠، المادة (٣).

(١٩) ينظر، عبد الهادي عبد الحميد، القانون الجنائي للتقنيات الحديثة، دار النهضة العربية، القاهرة، ٢٠٢٠، ص٩٧.

(٢٠) ينظر، مجيد عبد الرضا، الجرائم المستحدثة في القانون الجنائي، دار الفكر الجامعي، بغداد، ٢٠٢٠، ص٨٠.

(٢١) ينظر، مجيد عبد الرضا، الجرائم المستحدثة في القانون الجنائي، دار الفكر الجامعي، بغداد، ٢٠٢٠، ص٨٠.

(٢٢) د، فاضل الشاوي، النظام الجنائي للجريمة المعلوماتية، دار الثقافة، بغداد، ٢٠١٩، ص٩١.

(٢٣) د، عبد الحميد أحمد، التوقيع الإلكتروني وحجيته القانونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٨، ص١٢١.

(٢٤) د. يوسف فرج، القانون الجنائي للتكنولوجيا الحديثة، دار الثقافة، عمان، ٢٠٢١، ص١٠٤.

(٢٥) د. محمود حسن، التحقيق الجنائي في الجرائم الرقمية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١، ص٩٩

(٢٦) د. بدر محمد، الخصوصية وحماية البيانات في القانون الجنائي، دار الفكر العربي، بيروت، ٢٠٢٠، ص٨٣.

(٢٧) د. عبد الكريم داوود، القانون الجنائي الدولي والجرائم عبر الحدود الإلكترونية، دار الفكر العربي، القاهرة، ٢٠٢١، ص١٥٥.

(٢٨) د. خالد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة، عمان، ٢٠١٦، ص١٢٤.

(٢٩) د. قاسم الجبوري، المسؤولية الجنائية في الجرائم المعلوماتية، دار ابن الأثير، الموصل، ٢٠١٩، ص٧٥.

(٣٠) د. قاسم الجبوري، المسؤولية الجنائية في الجرائم المعلوماتية، دار ابن الأثير، الموصل، ٢٠١٩، ص٧٥.

(٣١) د. عبد العزيز عبد الجواد، القصد الجنائي في الجريمة المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٢، ص٥٨

(٣٢) ينظر. قرار محكمة جنايات الرصافة رقم (٢١٧/ج/٢٠٢٠)، مجلة القضاء العراقي، العدد ٤، ٢٠٢١، ص١٤٣.

(٣٣) د. فاضل الشاوي، النظام الجنائي للجريمة المعلوماتية، دار الثقافة، بغداد، ٢٠١٩، ص١٤٢.

(٣٤) ينظر. نظام مكافحة الجرائم المعلوماتية السعودي لعام ٢٠٠٧، المادة (٣).

(٣٥) ينظر. حكم المحكمة الجزائية بالرياض، القضية رقم (٣٤٢/ق/٢٠٢١)، مجلة القضاء السعودي، العدد ١٢، ٢٠٢٢، ص٢٠٧.

(٣٦) د. عبد الله الأنصاري، القصد في الجرائم المعلوماتية، مركز القانون العربي، الرياض، ٢٠٢١، ص٨١.

(٣٧) د. فوزي عيسى، المسؤولية الجنائية عن الأفعال الإلكترونية، دار الثقافة، عمان، ٢٠٢١، ص٩٤.

(٣٨) ينظر. قرار محكمة جنايات الكرخ رقم (١٤٨/ج/٢٠٢٢)، مجلة العدالة، العدد ٣، بغداد، ٢٠٢٢، ص١٩٢.

(٣٩) د. عمار الأنباري، تطور المسؤولية الجنائية في الجريمة الرقمية، دار الفكر الجامعي، بغداد، ٢٠٢١، ص١١٨.

(٤٠) ينظر، حكم محكمة الاستئناف بتونس رقم (٢١٧٩/ج/٢٠١٩)، مجلة القضاء التونسي، العدد ٣، ٢٠٢٠، ص٢١٣.

(٤١) ينظر. حاتم الباجي، المسؤولية الجنائية في الجرائم المعلوماتية، دار سحر للنشر، تونس، ٢٠٢١، ص١٠٣.

(٤٢) د. رفيق مراد، النية الجنائية في القانون المقارن، دار النهضة العربية، بيروت، ٢٠٢٠، ص١٠٥.

(٤٣) د. عبد الرحمن المناعسة، الجرائم المعلوماتية في الفقه الجنائي المعاصر، دار الثقافة، عمان، ٢٠٢١، ص٤٥.

(٤٤) ينظر. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، المادة (٤٥٦).

(٤٥) د. عبد الكريم الجبوري، المسؤولية الجنائية لجرائم الأخلاق باستخدام التقنيات الحديثة، دار ابن الأثير، الموصل، ٢٠٢٠، ص٩٢.

(٤٦) ينظر. قرار محكمة التمييز الاتحادية العراقية رقم (١٩/ج/٢٠١٩)، مجلة القضاء العراقي، العدد ٢، ٢٠٢٠، ص١١٧.

(٤٧) د. محمد الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠١٧، ص٨٤.

(٤٨) د. عبد الكريم داوود، القانون الجنائي الدولي والجرائم عبر الحدود الإلكترونية، دار الفكر العربي، القاهرة، ٢٠٢١، ص١١٥.

(٤٩) ينظر. قرار محكمة التمييز الاتحادية رقم (١١٢/ج/٢٠٢٠)، مجلة العدالة، العدد ٤، ٢٠٢١، ص١٤١.

(٥٠) د. فوزي عيسى، المسؤولية الجنائية عن الأفعال الإلكترونية، دار الثقافة، عمان، ٢٠٢١، ص١٣٣.

(٥١) ينظر. القانون الجنائي المغربي (تعديل ٢٠١٨)، الفصل (٦٠٧-٦).

(٥٢) د. عبد الهادي عبد الحميد، القانون الجنائي للتقنيات الحديثة، دار النهضة العربية، القاهرة، ٢٠٢٠، ص١٠٤.

(٥٣) د. عبد العزيز عبد الجواد، القصد الجنائي في الجريمة المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٢، ص٧١.

(٥٤) د. خالد المناصرة، الجرائم الإلكترونية وأمن المعاملات المالية، دار الفكر الجامعي، عمان، ٢٠٢١، ص١٢١.

(٥٥) ينظر. القانون الجزائري رقم (٠٩-٠٤) لسنة ٢٠٠٩، المادة (١٢).

(٥٦) د. رفيق مراد، النية الجنائية في القانون المقارن، دار النهضة العربية، بيروت، ٢٠٢٠، ص٩٧.

(٥٧) د. عبد الرزاق السنهوري، النظام القانوني للمسؤولية التجارية في البيئة الرقمية، دار الفكر العربي، القاهرة، ٢٠٢٠، ص ٦٧.

(٥٨) د. محمد الداودي، المسؤولية الجنائية لمورد خدمة الإنترنت، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦، ص ٩٢.

(٥٩) ينظر. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، المادة (٣٥).

(٦٠) ينظر. قرار محكمة التمييز الاتحادية رقم (٥٧/ج/٢٠٢١)، مجلة القضاء العراقي، العدد ٥، ٢٠٢١، ص ١٨٨.

(٦١) د. نجيب خالد، جرائم الدفع الإلكتروني في القانون المقارن، دار الثقافة، بغداد، ٢٠٢٢، ص ١٤٢.

(٦٢) ينظر. قرار محكمة جنايات الكرخ رقم (٨٨/ج/٢٠٢٢)، مجلة العدالة، العدد ٣، بغداد، ٢٠٢٢، ص ٢١٤.

(٦٣) د. فاضل الشاوي، النظام الجنائي للجريمة المعلوماتية، دار الثقافة، بغداد، ٢٠١٩، ص ١٧٣.

(٦٤) د. حاتم الباجي، المسؤولية الجنائية في الجرائم المعلوماتية، دار سحر للنشر، تونس، ٢٠٢١، ص ١١٩.

(65) Code pénal français, Article 121-2, modifié par Loi n°2016-1691 du 9 décembre 2016

(٦٦) ينظر. القانون الجنائي المغربي، الفصل (٦٠٧-٧)، تعديل ٢٠١٨.

(٦٧) د. عبد الله الزعبي، التحول الوقائي في السياسة الجنائية المعلوماتية، دار الثقافة، عمان، ٢٠٢٢، ص ١٢١.

(٦٨) د. سعاد خلف والشاوي، المبادئ العامة في قانون العقوبات، دار الثقافة، عمان، ٢٠١٧، ص ٢٠٤.

(٦٩) د. فاضل الشاوي، التحول الرقمي والمسؤولية الجنائية في العراق، مجلة القانون والاقتصاد العراقية، العدد (٤)، ٢٠٢١، ص ٤٥.

(٧٠) ينظر. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، المادة (٤٥٦).

(٧١) ينظر. قرار محكمة التمييز الاتحادية رقم (١٤١/ج/٢٠٢١)، مجلة القضاء العراقي، العدد ٦، ٢٠٢٢.

(٧٢) د. محمد نجيب، جريمة الدفع الإلكتروني في القانون العراقي، دار الثقافة، بغداد، ٢٠١٩، ص ٩١.

(٧٣) د. عبد الكريم الجبوري، المسؤولية الجنائية لجرائم الأخلاق باستخدام التقنيات الحديثة، دار ابن الأثير، الموصل، ٢٠٢٠، ص ١١٨.

(٧٤) ينظر. نظام مكافحة الجرائم المعلوماتية السعودي لعام ٢٠٠٧، المادة (٤)؛ قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨، المادة (١٨).

(75) European Union Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, Article 4.

(٧٦) ينظر. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، المادة (٢٨٦).

(٧٧) د. عبد الهادي عبد الحميد، القانون الجنائي للتقنيات الحديثة، دار النهضة العربية، القاهرة، ٢٠٢٠، ص ١٤٤.

(٧٨) ينظر. فهمي عبد الحافظ، التزوير الرقمي وحدود التجريم، مجلة الحقوق الكويتية، العدد (٢)، ٢٠١٩، ص ٨٧.

(٧٩) ينظر. القانون الجنائي المغربي (تعديل ٢٠١٨)، الفصل (٦٠٧-٦)؛ القانون الجزائري رقم (٠٩-٠٤) لسنة ٢٠٠٩، المادة (١١).

(80) Code pénal français, Article 441-1 (modifié 2016

(٨١) ينظر. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، المادة (٤٥٦/ثانيًا).

(٨٢) د. مجيد عبد الرضا، الجرائم المستحدثة، دار الفكر الجامعي، بغداد، ٢٠١٨، ص ١٥٧.

(83) European Union Directive (EU) 2019/713, Article 3.

(٨٤) ينظر. قرار محكمة التمييز الاتحادية رقم (١٩/ج/٢٠١٩)، مجلة القضاء العراقي، العدد ٢، ٢٠٢٠.

(٨٥) ينظر . د. فاضل الشاوي، التحول الرقمي والمسؤولية الجنائية في العراق، مجلة القانون والاقتصاد العراقية، العدد (٤)، ٢٠٢١، ص ٥٥.

(٨٦) ينظر. تعليمات البنك المركزي العراقي رقم (٩) لسنة ٢٠٢٠ بشأن أنظمة الدفع الإلكتروني، المادة (٥).

(٨٧) ينظر. قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، المادة (٣٥).

(٨٨) ينظر. قرار محكمة جنايات الكرخ رقم (١٠١/ج/٢٠٢٢)، مجلة العدالة العراقية، العدد (٢)، ٢٠٢٢.

(٨٩) د. عبد الحميد طارق، واجب الإبلاغ كآلية للوقاية الجنائية، مجلة الدراسات القانونية – جامعة الإسكندرية، العدد (٣)، ٢٠٢٠، ص ٦٥.

(٩٠) ينظر. دزفاضل الشاوي، المرجع السابق، ص ٦٠.

(٩١) ينظر. القانون التونسي رقم (٥) لسنة ٢٠٠٤ بشأن أمن النظم المعلوماتية، الفصل (١٤).

(92) Code Monétaire et Financier, Article L. 561-15, France.

(93) European Union Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, Article 5.

(94) Code pénal français, Article 323-4-1 (modifié 2018).

المصادر

الكتب

١) خالد المناعسة، جرائم نظم المعلومات الإلكترونية دار الثقافة، عمان، ٢٠١٦.

٢) رفيق مراد، النية الجنائية في القانون المقارن، دار النهضة العربية، بيروت، ٢٠٢٠.

٣) عبد العزيز عبد الجواد، القصد الجنائي في الجريمة المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٢.

٤) عبد العزيز عبد الجواد، القصد الجنائي في الجريمة المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٢.

٥) عبد الكريم داوود، القانون الجنائي الدولي والجرائم عبر الحدود الإلكترونية، دار الفكر العربي، القاهرة، ٢٠٢١.

٦) عبد الله الأنصاري، القصد في الجرائم المعلوماتية، مركز القانون العربي، الرياض، ٢٠٢١.

٧) عبد الله الزعبي، التحول الوقائي في السياسة الجنائية المعلوماتية، دار الثقافة، عمان، ٢٠٢٢.

٨) فاضل الشاوي، النظام الجنائي للجريمة المعلوماتية، دار الثقافة، بغداد، ٢٠١٩.

٩) فوزي عيسى، المسؤولية الجنائية عن الأفعال الإلكترونية، دار الثقافة، عمان، ٢٠٢١.

١٠) مجيد عبد الرضا، الجرائم المستحدثة، دار الفكر الجامعي، بغداد، ٢٠١٨.

١١) محمد الداودي، المسؤولية الجنائية لمورد خدمة الإنترنت، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦.

١٢) محمد نجيب، جريمة الدفع الإلكتروني في القانون العراقي، دار الثقافة، بغداد، ٢٠١٩.

١٣) نجيب خالد، جرائم الدفع الإلكتروني في القانون المقارن، دار الثقافة، بغداد، ٢٠٢٢.

١٤) بدر محمد، الخصوصية وحماية البيانات في القانون الجنائي، دار الفكر العربي، بيروت، ٢٠٢٠ .

١٥) حاتم الباجي، المسؤولية الجنائية في الجرائم المعلوماتية، دار سحر للنشر، تونس، ٢٠٢١.

١٦) خالد المناصرة، الجرائم الإلكترونية وأمن المعاملات المالية، دار الفكر الجامعي، عمان، ٢٠٢١.
١٧) رفيق مراد، النية الجنائية في القانون المقارن، دار النهضة العربية، بيروت، ٢٠٢٠.
١٨) سعاد خلف والشاوي، المبادئ العامة في قانون العقوبات، دار الثقافة، عمان، ٢٠١٧.
١٩) عبد الحميد أحمد، التوقيع الإلكتروني وحجيته القانونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٨
٢٠) عبد الرحمن المناعسة، الجرائم المعلوماتية في الفقه الجنائي المعاصر، دار الثقافة، عمان، ٢٠٢١، ص٤
٢١) عبد الرزاق السنهوري، النظام القانوني للمسؤولية التجارية في البيئة الرقمية، دار الفكر العربي، القاهرة، ٢٠٢٠.
٢٢) عبد الكريم الجبوري، المسؤولية الجنائية لجرائم الأخلاق باستخدام التقنيات الحديثة، دار ابن الأثير، الموصل، ٢٠٢٠.
٢٣) عبد الكريم داوود، القانون الجنائي الدولي والجرائم عبر الحدود الإلكترونية، دار الفكر العربي، القاهرة، ٢٠٢١.
٢٤) عبد الهادي عبد الحميد، القانون الجنائي للتقنيات الحديثة، دار النهضة العربية، القاهرة، ٢٠٢٠.
٢٥) عمار الأنباري، تطور المسؤولية الجنائية في الجريمة الرقمية، دار الفكر الجامعي، بغداد، ٢٠٢١.
٢٦) فاضل الشاوي، النظام الجنائي للجريمة المعلوماتية، دار الثقافة، بغداد، ٢٠١٩.
٢٧) فوزي عيسى، المسؤولية الجنائية عن الأفعال الإلكترونية، دار الثقافة، عمان، ٢٠٢١.
٢٨) قاسم الجبوري، المسؤولية الجنائية في الجرائم المعلوماتية، دار ابن الأثير، الموصل، ٢٠١٩.
٢٩) مجيد عبد الرضا، الجرائم المستحدثة في القانون الجنائي، دار الفكر الجامعي، بغداد، ٢٠٢٠.
٣٠) محمد الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠١٧.
٣١) محمود حسن، التحقيق الجنائي في الجرائم الرقمية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١.
٣٢) يوسف فرج، القانون الجنائي للتكنولوجيا الحديثة، دار الثقافة، عمان، ٢٠٢١

المجلات

١) فهمي عبد الحافظ، التزوير الرقمي وحدود التجريم، مجلة الحقوق الكويتية، العدد (٢)، ٢٠١٩.
٢) عبد الحميد طارق، واجب الإبلاغ كآلية للوقاية الجنائية، مجلة الدراسات القانونية – جامعة الإسكندرية، العدد (٣)، ٢٠٢٠.
٣) فهمي عبد الحافظ، التزوير الرقمي وحدود التجريم، مجلة الحقوق الكويتية، العدد (٢)، ٢٠١٩.

القوانين والتعليمات

١) قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠
٢) قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩
٣) قانون المعاملات الإلكترونية الأردني رقم ٨٥ لسنة ٢٠٠١
٤) القانون التونسي رقم (٥) لسنة ٢٠٠٤.

٥) القانون الجزائري رقم (٠٩-٠٤) لسنة ٢٠٠٩
٦) القانون الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢
٧) قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨
٨) القانون الجنائي المغربي، الفصل (٦٠٧-٧)، تعديل ٢٠١٨
٩) تعليمات البنك المركزي العراقي رقم (٩) لسنة ٢٠٢٠
١٠) قانون التجارة العراقي رقم (٢١) لسنة ٢٠٢١.

القرارات

١) قرار محكمة التمييز الاتحادية رقم (١٩/ج/٢٠١٩)، مجلة القضاء العراقي، العدد ٢، ٢٠٢٠.
٢) قرار محكمة جنايات الرصافة رقم (٢١٧/ج/٢٠٢٠)، مجلة القضاء العراقي، العدد ٤، ٢٠٢١
٣) قرار محكمة التمييز الاتحادية رقم (٥٧/ج/٢٠٢١)، مجلة القضاء العراقي، العدد (٦)، ٢٠٢١.
٤) قرار محكمة جنايات الرصافة رقم (٢١٧/ج/٢٠٢٠)، مجلة القضاء العراقي، العدد ٤، ٢٠٢١
٥) قرار محكمة جنايات الكرخ رقم (١٠١/ج/٢٠٢٢)، مجلة العدالة العراقية، العدد (٢)، ٢٠٢٢
٦) قرار محكمة التمييز الاتحادية رقم (١٤١/ج/٢٠٢١)، مجلة القضاء العراقي، العدد ٦، ٢٠٢٢.
٧) قرار محكمة جنايات الكرخ رقم (٨٨/ج/٢٠٢٢)، مجلة العدالة، العدد ٣، بغداد، ٢٠٢٢.

المواقع الالكترونية الاجنبية

1) Code Monétaire et Financier, Article L.561-15, France
2) Code pénal français, Article 121-2, modifié par Loi n°2016-1691 du 9 décembre 2016
3) Code pénal français, Article 323-4-1 (modifié 2018
4) Code pénal français, Article 441-1 (modifié 2016
5) European Union Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, Article 4
6) European Union Directive (EU) 2019/713, Article 3
7) European Union Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, Article 5