Journal Of the Iraqia University (76-2) 31 – May (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at
https://iasj.rdd.edu.iq/journals/journal/view/247

ادلة الاثبات في جرائم الاحتيال والنصب الالكتروني

م.م اندلس عبدالرحمن فرج

جامعة الفراهيدي / كلية القانون

Research Title Evidence in Cases of Electronic Fraud and Deception

Andalus Abdulrahman Faraj

الملخص

أفرز التطور المتسارع في تقنيات المعلومات والاتصالات أنماطاً جديدة من الجرائم، كان أبرزها جرائم الاحتيال والنصب الإلكتروني التي تعتمد على الوسائط الرقمية كأداة رئيسة في ارتكاب السلوك الإجرامي. وقد أوجدت هذه الجرائم تحديات قانونية غير مسبوقة، لا سيما في مجال الإثبات الجنائي، إذ لم تعد الأدلة التقليدية كافية وحدها لإثبات الوقائع الإجرامية في البيئة الإلكترونية. ويسعى هذا البحث إلى دراسة أدلة الإثبات في جرائم الاحتيال والنصب الإلكتروني، من حيث مفهومها وأنواعها وحجيتها القانونية، مع بيان الإشكالات العملية التي تواجه جهات التحقيق والمحاكم عند التعامل مع الأدلة الرقمية.

الكلمات المفتاحية :الاحتيال الإلكتروني – الدليل الرقمي – الإثبات الجنائي – الجريمة المعلوماتية – الحجية القانونية

Abstract

The rapid development of information and communication technologies has given rise to new patterns of crime, most notably electronic fraud and scam offenses that rely on digital media as a primary tool for committing criminal behavior. These crimes have posed unprecedented legal challenges, particularly in the field of criminal evidence, as traditional evidence alone is no longer sufficient to prove criminal acts in the digital environment. This study aims to examine the evidentiary aspects of electronic fraud and scam crimes, focusing on their concept, types, and legal validity, while highlighting the practical challenges faced by investigative authorities and courts when dealing with digital evidence.

Keywords : Electronic fraud - Digital evidence - Criminal evidence - Cybercrime - Legal validity

المقدمة

أصبحت جرائم الاحتيال والنصب الإلكتروني من أخطر الجرائم المستحدثة نتيجة التطور المتسارع في وسائل التكنولوجيا والاتصال، حيث استُخدمت الشبكات الإلكترونية ووسائل التواصل الاجتماعي كأدوات لارتكاب أفعال احتيالية تستهدف الأفراد والمؤسسات على حد سواء. وتكمن خطورة هذه الجرائم في صعوبة اكتشافها وإثباتها، نظراً لاعتمادها على وسائل رقمية غير ملموسة وسهلة الإخفاء أو التلاعب. ويهدف هذا البحث إلى بيان مفهوم أدلة الإثبات في جرائم الاحتيال والنصب الإلكتروني، وبيان أنواعها وقيمتها القانونية، مع تسليط الضوء على التحديات التي تواجه سلطات التحقيق والقضاء في جمعها وتقديره.

اولا: اهمية البحث

تنبع أهمية هذا البحث من الأهمية المتزايدة لأدلة الإثبات في الجرائم الإلكترونية، ولا سيما جرائم الاحتيال والنصب، لما لها من دور محوري في الوصول إلى الحقيقة وتحقيق العدالة الجنائية. كما تبرز أهميته في توضيح الطبيعة الخاصة للأدلة الرقمية وتمييزها عن الأدلة التقليدية وإبراز الصعوبات القانونية والفنية المتعلقة بإثبات جرائم الاحتيال والنصب الإلكتروني وكذلك الإسهام في دعم الجهود التشريعية والقضائية لمواجهة هذا النوع من الجرائم.

ثانيا: مشكلة البحث

تتمثل مشكلة البحث في مدى كفاية القواعد العامة للإثبات الجنائي في مواجهة جرائم الاحتيال والنصب الإلكتروني، ومدى قدرة الأدلة الرقمية على إثبات هذه الجرائم أمام القضاء، في ظل ما تتسم به من سهولة المحو أو التعديل، وتعدد الفاعلين، وصعوبة إسناد الفعل الإجرامي إلى مرتكبه

الحقيقي. كما يثير البحث إشكالية حجية الدليل.

منهجية البحث

يعتمد البحث على المنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بالإثبات والجرائم الإلكترونية، والمنهج الوصفي لبيان ماهية جرائم الاحتيال والنصب الإلكتروني وأنواع الأدلة المستخدمة في إثباتها. كما يستعين البحث بـ المنهج المقارن في بعض الجوانب، عبر مقارنة التشريعات الوطنية ببعض التشريعات الأجنبية والاتفاقيات الدولية ذات الصلة، بهدف الوصول إلى رؤية قانونية متكاملة.

خطة البحث

قسم البحث الى المبحث الأول: الإطار المفاهيمي لجرائم الاحتيال والنصب الإلكتروني وفي المبحث الثاني نبين ماهية أدلة الإثبات في الجرائم الإلكترونية وأنواعها اما المبحث الثالث: حجية ادلة الاثبات الإلكترونية ودور القضاء في إثبات جرائم الاحتيال والنصب. وفي الخاتمة نوضح النتائج والتوصيات

المبحث الأول الاطار المفاهيمي لجرائم الاحتيال والنصب الالكتروني

يُعدّ التطور التكنولوجي المتسارع وما رافقه من توسع في استخدام شبكة الإنترنت ووسائل الاتصال الحديثة سبباً رئيساً في ظهور أنماط جديدة من الجرائم، كان من أبرزها جرائم الاحتيال والنصب الإلكتروني. وقد اتخذت هذه الجرائم أشكالاً متعددة، مستغلة الثقة التي يمنحها الأفراد للبيئة الرقمية، مما أدى إلى زيادة مخاطرها واتساع نطاقها. وتكمن خطورة جرائم الاحتيال والنصب الإلكتروني في كونها تعتمد على وسائل غير تقليدية يصعب اكتشافها أو إثباتها، فضلاً عن كونها لا تترك آثاراً مادية واضحة كما هو الحال في الجرائم التقليدية. ومن هنا، تبرز أهمية تحديد الإطار المفاهيمي لهذه الجرائم، من حيث بيان مفهومها وخصائصها الأساسية وأركانها القانونية، لما لذلك من دور في فهم طبيعتها وتمييزها عن غيرها من الجرائم المشابهة.

المطلب الأول مفهوم الاحتيال والنصب الالكتروني

يتناول هذا المطلب بيان مفهوم جرائم الاحتيال والنصب الإلكتروني، من خلال التعريف بهذه الجرائم وبيان معناها العام، سواء في صورتها التقليدية أو الإلكترونية، تمهيداً لفهم طبيعتها القانونية.

الفرع الأول مفهوم الاحتيال والنصب الالكتروني في الاطار التقليدي:

يُقصد بالاحتيال والنصب في المفهوم التقليدي استعمال الجاني لوسائل احتيالية تهدف إلى خداع المجني عليه ودفعه إلى تسليم ماله أو منقولة أو منفعة مالية بغير وجه حق. ولا تقوم هذه الجريمة على مجرد الكذب (حسني، د.ت، ص ص. ١٢٠-١٣٠)، وإنما تتطلب استخدام أساليب من شأنها إظهار الكذب في صورة حقيقة، مما يؤدي إلى وقوع المجني عليه في الغلط. ويُعد وقوع المجني عليه في الغلط نتيجة مباشرة للوسائل الاحتيالية التي يستخدمها الجاني، حيث يترتب على ذلك تسليم المال أو المنفعة عن رضا ظاهري، بينما يكون هذا الرضا مشوباً بالخداع. كما يشترط لقيام الجريمة توافر القصد الجنائي لدى الجاني، أي علمه بطبيعة فعله غير المشروع واتجاه إرادته إلى الاستيلاء على مال الغير ويُشكّل هذا المفهوم التقليدي الأساس الذي انطلقت منه الدراسات القانونية لمعالجة صور الاحتيال المستحدثة، ومنها الاحتيال والنصب الإلكتروني(عودة، د.ت، ج. ٢، ص ص. ٤٥١-٤٥٤)ولا تتحقق جريمة الاحتيال بمجرد الكذب أو الادعاء غير الصحيح، لأن الكذب وحده لا يكفي لقيام الجريمة ما لم يُدعَّم بوسائل مادية أو معنوية تعطيه مظهراً من مظاهر الصدق. فالوسائل الاحتيالية قد تتمثل في ادعاء صفة كاذبة، أو استعمال مستندات مزورة، أو إيجاد ظروف توحي بصحة الادعاءات، الأمر الذي يؤدي إلى وقوع المجني عليه في الغلط ودفعه إلى التصرف في ماله (نجم، د.ت، ص ص. ١٤٥-١٤٨). ويُشترط لقيام جريمة الاحتيال أن يكون تسليم المال أو المنفعة نتيجة مباشرة للغلط الذي وقع فيه المجني عليه بسبب الوسائل الاحتيالية. فإذا انتفى هذا الترابط السببي، انتفت الجريمة. كما يجب أن يكون الجاني قد تصرف بسوء نية، أي أن يكون عالماً بعدم صحة ما يدّعيه، ومتجهاً بإرادته إلى الاستيلاء على مال الغير أو الحصول على منفعة غير مشروعة (سرور، د.ت، ص ص. ٢٢١-٢٢٤).

ويمثل هذا المفهوم التقليدي الأساس الذي تُقاس عليه صور الاحتيال المستحدثة، ومنها الاحتيال والنصب الإلكتروني، حيث يظل جوهر السلوك الإجرامي واحداً، بينما تختلف الوسائل والأدوات المستخدمة في ارتكابه.

الفرع الثاني مفهوم جرائم الاحتيال والنصب الالكتروني

تعد جرائم الاحتيال والنصب الإلكتروني امتداداً للجرائم التقليدية، لكنها تختلف في الوسيلة والأدوات التي يستخدمها الجاني. ففي حين كان الاحتيال التقليدي يعتمد على التعامل المباشر مع المجني عليه، أصبحت الجرائم الإلكترونية تعتمد على الوسائط الرقمية مثل الإنترنت، البريد الإلكتروني،

تطبيقات الهواتف الذكية، ومنصات التواصل الاجتماعي ويهدف الجاني في هذه الجرائم إلى خداع المجني عليه لتحقيق مكاسب مالية أو الحصول على بيانات أو معلومات شخصية بطرق غير مشروعة (سرور، د.ت، ص ص. ٤٥-٤٨) . وتشمل وسائل الاحتيال الإلكتروني إنشاء مواقع وهمية، إرسال رسائل إلكترونية مضللة، انتحال هوية جهات رسمية أو تجارية، أو استغلال منصات التجارة الإلكترونية لجمع أموال أو معلومات بطرق احتيالية. وتتميز الجرائم الإلكترونية بعدة سمات تميزها عن الجرائم التقليدية (الطرابلسي، د.ت، ص ص. ٢٢-٢٦) ، منها:

١. غياب الاتصال المباشر بين الجاني والمجني عليه، ما يزيد صعوبة التعرف على الفاعل.

٢. الاعتماد على التقنيات الرقمية، مما يجعل أثر الجريمة قابلاً للمحو أو التلاعب بسهولة.

٣. الانتشار السريع، حيث يمكن أن يؤثر الفعل على عدد كبير من الضحايا في أماكن مختلفة.

ويشير الفقه إلى أن جوهر الجريمة لا يختلف عن الاحتيال التقليدي، إذ يظل عنصر الخداع والغرض المالي حاضراً، بينما تختلف الأدوات والوسائل المستخدمة. ومع هذا، فإن طبيعة البيئة الرقمية تستدعي تطوير أساليب الإثبات والتشريع لمواكبة هذه الظاهرة الجديدة، وضمان إمكانية إثبات الجرائم ومعاقبة مرتكبيها بفعالية (حجازي، د.ت، ص ص. ٣٣-٣٦).

المطلب الثاني خصائص جرائم الاحتيال والنصب الالكتروني

بعد التعرف على مفهوم جرائم الاحتيال والنصب الإلكتروني، يأتي هذا المطلب لتوضيح الخصائص التي تميز هذه الجرائم عن الاحتيال التقليدي، والتي تؤثر بشكل مباشر على طرق التحقيق والإثبات. ففهم هذه الخصائص يساعد على التعامل القانوني والعملي مع الجرائم الرقمية بفعالية.

الفرع الأول الطابع الرقمي وغير المادي لجرائم الاحتيال والنصب الالكتروني وسرعة الانتشار

تتميز هذه الجرائم بطابعها الرقمي وغير المادي، حيث يقوم الجاني باستخدام بيانات ومعلومات إلكترونية غير ملموسة لإتمام الفعل الاحتيالي، مثل إرسال رسائل مضللة أو إنشاء مواقع إلكترونية وهمية. هذا الطابع يجعل اكتشاف الجريمة وإثباتها أكثر صعوبة مقارنة بالاحتيال التقليدي الذي يترك آثاراً مادية واضحة. تتيح البيئة الرقمية ارتكاب الجرائم بسرعة فائقة، وقد تمتد آثارها لتشمل عددًا كبيرًا من الضحايا في أماكن متعددة، حتى عبر الحدود الوطنية. فالجرائم الإلكترونية يمكن أن تتم خلال دقائق، بعكس الاحتيال التقليدي الذي يستغرق وقتاً أطول ويقتصر على نطاق جغرافي محدود (الطرابلسي، د.ت، ص ص. ٢٢-٢٦) .

الفرع الثاني صعوبة تحديد هوية الجاني و الطابع العابر للحدود والاعتماد على الوسائل الرقمية

يستفيد مرتكبو الجرائم الإلكترونية من تقنيات إخفاء الهوية مثل الحسابات المزيفة أو الشبكات الافتراضية الخاصة، مما يزيد صعوبة التعرف على الفاعل مباشرة. وهذا يعقد عمليات التحقيق ويستلزم تقنيات متقدمة لتعقب الأثر الرقمي (حجازي، د.ت، ص ص. ٣٣-٣٦) .و غالباً ما تتجاوز الجرائم الإلكترونية الحدود الوطنية، مما يثير إشكالات قانونية مرتبطة بالاختصاص القضائي وتنازع القوانين. كما يفرض التعاون الدولي لتبادل المعلومات والتنسيق بين سلطات التحقيق ضرورة وجود تشريعات واتفاقيات دولية لمكافحة هذه الجرائم (حسني، د.ت، ص ص. ٣١٠-٣١٤) .ويعتمد ارتكاب هذه الجرائم على استخدام أجهزة الحاسوب، الهواتف الذكية، الإنترنت، والبرمجيات المختلفة، مما يجعلها مرتبطة ارتباطاً وثيقاً بالتطور التكنولوجي المستمر، ويستدعي تطوير مهارات التحقيق وتحديث النصوص القانونية لتواكب هذه التغيرات (عبد الستار، د.ت، ص ص. ٢٠٥-٢٠٩) .

المبحث الثاني ادلة الاثبات في جرائم الاحتيال والنصب الالكتروني

تُعد جرائم الاحتيال والنصب الإلكتروني من الجرائم الحديثة التي فرضت تحديات كبيرة على قواعد الإثبات الجنائي التقليدية، نظرًا لاعتمادها على الوسائط الرقمية والتقنيات الإلكترونية، مما استلزم الاعتراف بأدلة إثبات جديدة تتلاءم مع طبيعتها الخاصة، مع مراعاة الضمانات القانونية لسلامة الإجراءات وحقوق المتهم.

المطلب الأول الادلة الالكترونية والفنية في جرائم الاحتيال والنصب الالكتروني

تمثل الأدلة الإلكترونية والفنية الركيزة الأساسية في إثبات جرائم الاحتيال والنصب الإلكتروني، نظرًا لاعتماد هذه الجرائم في ارتكابها على الوسائط الرقمية والتقنيات الحديثة. وقد فرضت طبيعة هذه الأدلة خصوصية متميزة من حيث جمعها وتحليلها وتقديمها أمام القضاء، بما يستلزم بيان مفهومها وصورها وشروط قبولها، وهو ما سيتم تناوله في هذا المطلب.

الفرع الأول مفهوم الادلة الالكترونية وخصائصها

يقصد بالأدلة الإلكترونية كل بيانات أو معلومات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو إرسالها أو استقبالها بواسطة أنظمة ووسائط إلكترونية، ويُستدل بها على وقوع جريمة الاحتيال أو النصب الإلكتروني ونسبتها إلى الفاعل (منصور، ٢٠١٨، ص. ٤٥)وتتميز هذه الأدلة بخصائص خاصة، من أهمها عدم الملموسية، وسهولة النسخ، وقابليتها للتعديل أو الإتلاف بسرعة، فضلًا عن إمكانية انتقالها عبر الحدود الجغرافية، الأمر الذي يفرض اتباع إجراءات دقيقة في جمعها وحفظها لضمان سلامتها وحجيتها أمام القضاء (حسني، ٢٠١٤، ص. ٣١٢) .

الفرع الثاني صور الأدلة الإلكترونية والفنية

تتعدد صور الأدلة الإلكترونية والفنية في جرائم الاحتيال والنصب الإلكتروني، ومن أبرزها المراسلات الإلكترونية والبريد الإلكتروني، والمحادثات عبر تطبيقات التواصل الاجتماعي، وسجلات المكالمات الهاتفية والرسائل النصية، إضافة إلى البيانات المصرفية الإلكترونية والتحويلات المالية (سرور، د.ت، ص. ٥٢٩)كما تشمل الأدلة الفنية تقارير الخبراء المختصين في مجال التحليل الجنائي الرقمي، والتي تتعلق بفحص الأجهزة الإلكترونية، وتحليل البيانات المخزنة عليها، وتتبع عناوين بروتوكول الإنترنت (IP)، وتحديد أوقات ومواقع الدخول، الأمر الذي يسهم في ربط الجريمة بالمتهم ربطًا تقنيًا دقيقًا (عامر، ٢٠٢٠، ص. ٨٨) .

الفرع الثالث شروط قبول الادلة الالكترونية والفنية

يشترط لقبول الأدلة الإلكترونية والفنية أن يتم الحصول عليها بطريق مشروع لا ينطوي على مساس بالحقوق والحريات الأساسية، وأن يتم توثيقها وحفظها وفق ضوابط فنية وقانونية تمنع العبث بها أو التشكيك في سلامتها (دستور جمهورية العراق، ٢٠٠٥، المادة ٣٧)كما يجب أن تكون هذه الأدلة قابلة للفحص والمناقشة أمام المحكمة، وأن تؤدي إلى اطمئنان القاضي إلى صحتها ونسبتها إلى المتهم، إذ تخضع في تقديرها لسلطة المحكمة الجنائية وفقًا لمبدأ الاقتناع القضائي (عودة، د.ت، ص. ٤١٢) .

المطلب الثاني الأدلة التقليدية ودورها في إثبات جرائم الاحتيال والنصب الإلكتروني

على الرغم من الطابع التقني لجرائم الاحتيال والنصب الإلكتروني، إلا أن وسائل الإثبات التقليدية لا تزال تؤدي دورًا مهمًا في الكشف عن الحقيقة الجنائية. إذ تتكامل هذه الأدلة مع الأدلة الإلكترونية والفنية، بما يعزز قناعة المحكمة ويحقق مبدأ الاقتناع القضائي في الإثبات الجنائي.

الفرع الأول الشهادة في جرائم الاحتيال والنصب الإلكتروني

تُعد الشهادة من وسائل الإثبات التقليدية المعتمدة في القانون الجنائي، وتتمثل في أقوال المجني عليه أو الشهود الذين عاصروا واقعة الجريمة أو كانت لهم صلة بها، كموظفي المصارف أو شركات الاتصالات أو مزودي خدمات الإنترنت (حسني، د.ت، ص. ٣٥٦) .وتخضع الشهادة لتقدير المحكمة، التي تزنها بميزان الدقة والموضوعية، وتستخلص قيمتها الإثباتية في ضوء مدى انسجامها وتكاملها مع الأدلة الإلكترونية والفنية المعروضة في الدعوى، إذ لا يكفي الاعتماد عليها منفردة ما لم تؤيدها قرائن أو أدلة أخرى (سرور، د.ت، ص. ٦١٢) .

الفرع الثاني الاعتراف في جرائم الاحتيال والنصب الإلكتروني

يعد الاعتراف من أقوى أدلة الإثبات متى صدر صحيحًا ومطابقًا للحقيقة، سواء كان اعترافًا تقليديًا أمام جهة التحقيق أو المحكمة، أم اعترافًا مثبتًا بوسائل إلكترونية، كالمراسلات أو التسجيلات الرقمية (منصور، ٢٠١٨، ص. ٩٧)غير أن قيمة الاعتراف تبقى خاضعة لسلطة المحكمة التقديرية، التي تتحقق من صدوره عن إرادة حرة دون إكراه مادي أو معنوي، ومن مدى توافقه مع الوقائع والأدلة الأخرى في الدعوى، إذ لا يُعتد بالاعتراف المجرد غير المؤيد بدليل (عودة، ٢٠٠٩، ص. ٤٢١) .

الفرع الثالث القرائن القضائية وأهميتها في الإثبات

تلعب القرائن القضائية دورًا بالغ الأهمية في إثبات جرائم الاحتيال والنصب الإلكتروني، نظرًا لما يحيط بهذه الجرائم من صعوبات إثباتية. ومن أمثلة هذه القرائن حيازة المتهم للجهاز المستخدم في ارتكاب الجريمة، أو سيطرته على الحساب الإلكتروني محل الاحتيال، أو تحقق منفعة مالية غير مشروعة نتيجة السلوك الإجرامي (عامر، ٢٠٢٠، ص. ١٣٤)ويشترط في القرائن القضائية أن تكون قوية ومتساندة ومترابطة، وأن تؤدي إلى استنتاج منطقي يقيني تطمئن إليه المحكمة، بما يكفي لإسناد التهمة إلى المتهم دون شك معقول (مرقس، ٢٠١٥، ص. ٢٨٩) .

المبحث الثالث حجية ادلة الاثبات في جرائم الاحتيال والنصب الالكتروني ودور القضاء

ثير أدلة الإثبات في جرائم الاحتيال والنصب الإلكتروني إشكالات قانونية وقضائية متعددة، تتعلق بمدى حجيتها في الإثبات الجنائي، وحدود سلطة القاضي في تقديرها، فضلًا عن التحديات العملية التي تعترض سبيل إثبات هذا النوع من الجرائم، الأمر الذي يستوجب تسليط الضوء على هذه الجوانب لما لها من أثر مباشر في تحقيق العدالة الجنائية.

المطلب الأول حجية أدلة الإثبات الإلكترونية في الدعوى الجنائية

يركز هذا المطلب على الأدلة الإلكترونية والفنية باعتبارها الركيزة الأساسية لإثبات جرائم الاحتيال والنصب الإلكتروني، نظرًا لاعتماد هذه الجرائم على الوسائط الرقمية والتقنيات الحديثة. ويتناول المطلب تعريف الأدلة الإلكترونية وخصائصها، وأنواعها المختلفة، بالإضافة إلى الشروط القانونية والفنية التي يجب توافرها لقبولها أمام القضاء.

الفرع الأول مفهوم الأدلة الإلكترونية وخصائصها

يقصد بالأدلة الإلكترونية كل بيانات أو معلومات ذات قيمة إثباتية يتم إنشاؤها أو تخزينها أو إرسالها أو استقبالها عبر أنظمة ووسائط إلكترونية، ويُستدل بها على وقوع جريمة الاحتيال أو النصب الإلكتروني ونسبتها إلى الفاعل (منصور، ٢٠١٨، ص. ٤٥)وتتميز هذه الأدلة بعدة خصائص تجعلها مختلفة عن الأدلة التقليدية، من أهمها عدم الملموسية، وسهولة النسخ، وقابليتها للتعديل أو الإتلاف بسرعة، إضافة إلى إمكانية انتقالها عبر الحدود الجغرافية، الأمر الذي يفرض اتباع إجراءات دقيقة في جمعها وحفظها لضمان سلامتها وحجيتها أمام القضاء (حسني، ٢٠١٤، ص. ٣١٢) .

الفرع الثاني صور الأدلة الإلكترونية والفنية

تتعدد صور الأدلة الإلكترونية والفنية في جرائم الاحتيال والنصب الإلكتروني، وتشمل المراسلات الإلكترونية والبريد الإلكتروني، والمحادثات عبر تطبيقات ومواقع التواصل الاجتماعي، وسجلات المكالمات الهاتفية والرسائل النصية، إضافة إلى البيانات المصرفية الإلكترونية والتحويلات المالية (سرور، د.ت، ص. ٥٢٩)كما تشمل الأدلة الفنية تقارير الخبراء المختصين في مجال التحليل الجنائي الرقمي، التي تتعلق بفحص الأجهزة الإلكترونية وتحليل البيانات المخزنة عليها وتتبع عناوين بروتوكول الإنترنت (IP) وتحديد أوقات ومواقع الدخول، الأمر الذي يسهم في ربط الجريمة بالمتهم ربطًا تقنيًا دقيقًا (عامر، ٢٠٢٠، ص. ٨٨) .

الفرع الثالث شروط قبول الأدلة الإلكترونية والفنية

يشترط لقبول الأدلة الإلكترونية والفنية أمام القضاء أن يتم الحصول عليها بطريقة مشروعة لا تنتهك الحقوق والحريات الأساسية، وأن يتم توثيقها وحفظها وفق ضوابط فنية وقانونية تمنع العبث بها أو التشكيك في صحتها (دستور جمهورية العراق، ٢٠٠٥، المادة ٣٧)كما يجب أن تكون هذه الأدلة قابلة للفحص والمناقشة أمام المحكمة، وأن تؤدي إلى اطمئنان القاضي إلى صحتها ونسبتها إلى المتهم، إذ تخضع في تقديرها لسلطة المحكمة الجنائية وفقًا لمبدأ الاقتناع القضائي (عودة، ٢٠٠٩، ص. ٤١٢) .

المطلب الثاني لأدلة التقليدية ودورها في إثبات جرائم الاحتيال والنصب الإلكتروني

على الرغم من الطابع التقني لجرائم الاحتيال والنصب الإلكتروني، إلا أن الأدلة التقليدية ما تزال تلعب دورًا مهمًا في إثبات هذه الجرائم، إذ تتكامل مع الأدلة الإلكترونية والفنية لتعزيز قناعة المحكمة وتحقيق مبدأ الاقتناع القضائي في الإثبات الجنائي.

الفرع الأول الشهادة في الجرائم الإلكترونية

تُعد الشهادة من وسائل الإثبات التقليدية في القانون الجنائي، وتتمثل في أقوال المجني عليه أو الشهود الذين عاصروا واقعة الجريمة أو كانت لهم صلة بها، مثل موظفي المصارف أو شركات الاتصالات أو مزودي خدمات الإنترنت (حسني، ٢٠١٤، ص. ٣٥٦)وتخضع الشهادة لتقدير المحكمة، التي توازن بين مصداقيتها وملاءمتها للأدلة الإلكترونية والفنية الأخرى، فلا يكفي الاعتماد على الشهادة وحدها ما لم تؤيدها قرائن أو دلائل إضافية (سرور، د.ت، ص. ٦١٢) .

الفرع الثاني لاعتراف في جرائم الاحتيال والنصب الإلكتروني

يُعد الاعتراف من أقوى الأدلة متى صدر صحيحًا ومطابقًا للواقع، سواء كان اعترافًا تقليديًا أمام جهة التحقيق أو المحكمة، أم مثبتًا بوسائل إلكترونية (منصور، ٢٠١٨، ص. ٩٧)غير أن قيمته تبقى خاضعة لسلطة المحكمة التقديرية، التي تتحقق من صدوره عن إرادة حرة ودون أي إكراه، ومن مدى توافقه مع الوقائع والأدلة الأخرى (عودة، ٢٠٠٩، ص. ٤٢١) .

الفرع الثالث لقرائن القضائية وأهميتها في الإثبات

تلعب القرائن القضائية دورًا مهمًا في إثبات جرائم الاحتيال والنصب الإلكتروني، لا سيما في الحالات التي يصعب فيها الحصول على أدلة مباشرة. ومن أمثلة هذه القرائن: حيازة المتهم للجهاز المستخدم في ارتكاب الجريمة، أو سيطرته على الحساب الإلكتروني محل الاحتيال، أو تحقق منفعة مالية غير مشروعة نتيجة الفعل الجرمي (عامر، ٢٠٢٠، ص. ١٣٤)ويشترط في هذه القرائن أن تكون قوية ومتساندة ومترابطة، بحيث تؤدي إلى

استنتاج منطقي يقيني يقنع المحكمة بوقوع الجريمة ونسبتها للمتهم دون شك معقول (مرقس، ٢٠١٥، ص. ٢٨٩) .

الخاتمة

وفي ختام بحثنا توصلنا الى نتائج وتوصيات:

النتائج :-

١- أظهرت الدراسة أن جرائم الاحتيال والنصب الإلكتروني تُعد من الجرائم المستحدثة التي فرضها التطور التكنولوجي، مما جعل إثباتها أكثر تعقيدًا مقارنة بالجرائم التقليدية.

٢- تبيّن أن الأدلة الرقمية تمثل الوسيلة الأساسية لإثبات هذا النوع من الجرائم، ولا سيما الرسائل الإلكترونية، وسجلات الاتصالات، وبيانات الحسابات الإلكترونية، وتقارير الخبرة الفنية.

٣- أثبت البحث أن الأدلة التقليدية، كالشهادة والاعتراف والقرائن، ما زالت تحتفظ بأهميتها، إلا أنها غالبًا ما تأتي مكملة للأدلة الإلكترونية وليست بديلة عنها.

٤- كشفت الدراسة عن وجود صعوبات عملية في جمع الأدلة الرقمية، أهمها سهولة إتلافها أو التلاعب بها، والحاجة إلى خبرات فنية متخصصة للتعامل معها.

٥- تبيّن أن عدم وجود تنظيم تشريعي دقيق وصريح لحجية الدليل الإلكتروني يؤدي إلى تباين في التطبيق القضائي ويؤثر على تحقيق العدالة.

التوصيات:-

١- ضرورة دعم أجهزة التحقيق بوسائل تقنية حديثة وكوادر فنية متخصصة قادرة على جمع وتحليل الأدلة الرقمية وفقًا للأصول القانونية.

٢- التوصية بتكثيف برامج التدريب والتأهيل للقضاة وأعضاء الادعاء العام في مجال الجرائم الإلكترونية وأساليب الإثبات الحديثة.

٣- الدعوة إلى تعزيز التعاون بين الجهات القضائية والأمنية ومزودي خدمات الاتصالات والإنترنت، بما يسهم في تسهيل الوصول إلى الأدلة الرقمية

٤- ضرورة تحديث التشريعات الجزائية العراقية ولاسيما قانون العقوبات رقم (١١١) لسنة ١٩٦٩، أو سنّ قانون خاص بالجرائم الإلكترونية، بما يواكب التطور التقني ويُجرّم صراحة صور الاحتيال والنصب الإلكتروني.

٥- تنظيم حجية الدليل الإلكتروني وإجراءات جمعه وضبطه في قانون أصول المحاكمات الجزائية العراقي، مع ضمان حماية الحقوق والحريات الشخصية.

٦- تعزيز الدور الفني لأجهزة التحقيق والادعاء العام من خلال توفير الخبرات التقنية والتدريب المتخصص في مجال الأدلة الرقمية.

٧- توحيد الاتجاه القضائي العراقي بشأن الإثبات في الجرائم الإلكترونية عبر مبادئ قضائية صادرة عن محكمة التمييز الاتحادية لضمان استقرار الأحكام.

المصادر :

١- حجازي، عبد الفتاح بيومي . (٢٠١٣) .الدليل الجنائي في الجرائم المعلوماتية .دار الكتب القانونية.

٢- حسني، محمود نجيب . (٢٠١٤) .شرح قانون الإجراءات الجنائية .دار النهضة العربية.

٣- حسني، محمود نجيب.(د.ت) .الوسيط في قانون العقوبات: القسم الخاص .دار النهضة العربية.

٤- سرور، أحمد فتحي . (٢٠١٣) .الوسيط في قانون العقوبات: القسم الخاص .دار الشروق.

٥- سرور، أحمد فتحي.(٢٠١٥) . الجرائم الإلكترونية وأدلة إثباتها .دار الشروق.

٦- الطرازي، محمد شريف .(د.ت) .الجرائم المعلوماتية: المفهوم والعناصر والتجريم .دار الفكر الجامعي.

٧- عامر، عادل.(٢٠١٠) . الجرائم المعلوماتية وأدلة إثباتها الرقمية .دار الفكر الجامعي.

٨- عبد الستار، توفيق .(د.ت) .شرح قانون العقوبات: القسم الخاص .دار النهضة العربية.

٩- عودة، عبد القادر.(٢٠١٠) . التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي (ج. ٢). دار الكتاب العربي.

١٠- قهوجي، محمد عبد القادر(د.ت) .الجرائم المعلوماتية: المفهوم والعناصر والتجريم .دار الفكر الجامعي.

١١- مرقس، سليمان.(٢٠١٥) . أصول الإثبات وإجراءاته في المواد الجنائية .دار الكتب القانونية.

١٢- منصور، محمد حسين.(٢٠١٨) . الإثبات الجنائي في الجرائم الإلكترونية .دار الجامعة الجديدة.

١٣- نجم، محمد صبحي .(د.ت) .الجرائم الواقعة على الأموال .دار الثقافة للنشر والتوزيع.

الدساتير:

١- دستور جمهورية العراق ٢٠٠٥

References:

1- Hijazi, Abdel Fattah Bayoumi. (2013). Criminal Evidence in Cybercrimes. Dar Al-Kutub Al-Qanuniyya.
2- Hosni, Mahmoud Najib. (2014). Explanation of the Criminal Procedure Code. Dar Al-Nahda Al-Arabiya.
3- Hosni, Mahmoud Najib. (n.d.). The Intermediate Guide to Penal Law: Special Section. Dar Al-Nahda Al-Arabiya.
4- Sorour, Ahmed Fathi. (2013). The Intermediate Guide to Penal Law: Special Section. Dar Al-Shorouk.
5- Sorour, Ahmed Fathi. (2015). Cybercrimes and Their Evidence. Dar Al-Shorouk.
6- Al-Tarazi, Muhammad Sharif. (n.d.). Cybercrimes: Concept, Elements, and Criminalization. Dar Al-Fikr Al-Jami'i.
7- Amer, Adel. (2010). Cybercrimes and Their Digital Evidence. Dar Al-Fikr Al-Jami'i.
8- Abdel Sattar, Tawfiq. (n.d.). Explanation of the Penal Code: Special Section. Dar Al-Nahda Al-Arabiya.
9- Awda, Abdul Qadir. (2010). Islamic Criminal Legislation Compared to Positive Law (Vol. 2). Arab Book House.
10- Qahwaji, Muhammad Abdul Qadir (n.d.). Cybercrimes: Concept, Elements, and Criminalization. University Thought House.
11- Marqas, Sulaiman. (2015). Principles and Procedures of Evidence in Criminal Matters. Legal Books House.
12- Mansour, Muhammad Hussein. (2018). Criminal Evidence in Cybercrimes. New University House.
13- Najm, Muhammad Subhi. (n.d.). Crimes Against Property. Culture House for Publishing and Distribution.

Constitutions:

1- Constitution of the Republic of Iraq 2005