IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
مجلة جامعة الكوت
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
js.uokut.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
عدد خاص - المؤتمر العلمي التاسع للعلوم الإدارية والاقتصادية - 2-3 مايو/ ايار 2026

المسؤولية الجزائية عن الجرائم السيبرانية في ظل التحول الرقمي للهيئات الاقتصادية

م. م. صباح محسن جلعوط [1]

انتساب الباحث
[1] كلية القانون، جامعة واسط، العراق، واسط، الكوت، 52001

[1] Sabah.m@uowasit.edu.iq

[1] المؤلف المراسل

معلومات البحث
تاريخ النشر: آب 2026

المستخلص
يتناول هذا البحث موضوع المسؤولية الجزائية عن الجرائم السيبرانية في ظل التحول الرقمي الذي تشهده المؤسسات الاقتصادية، مع التركيز على الإطار القانوني المعتمد في التشريع العراقي. فقد أسهم الاعتماد المتزايد على التقنيات الرقمية والأنظمة الإلكترونية في تطوير الأداء الاقتصادي وتحسين كفاءة المؤسسات، إلا أنه في المقابل أوجد بيئة خصبة لظهور جرائم سيبرانية تستهدف البيانات والمعلومات والأنظمة الإلكترونية، بما يشكل تهديدًا حقيقيًا للأمن الاقتصادي والاستقرار القانوني.
ويسعى البحث إلى بيان مفهوم الجرائم السيبرانية المرتبطة بالنشاط الاقتصادي وتحليل أركانها القانونية، مع تسليط الضوء على أساس المسؤولية الجزائية المترتبة عليها، سواء بالنسبة للأشخاص الطبيعيين أم المعنويين كما يناقش مدى كفاية النصوص الجزائية النافذة في العراق، ولا سيما أحكام قانون العقوبات العراقي والقوانين ذات الصلة، في مواجهة هذا النوع من الجرائم، ولا سيما في ظل غياب تشريع متكامل ينظم الجرائم السيبرانية بصورة شاملة.
كما يتطرق البحث إلى أبرز الإشكاليات القانونية والعملية التي تواجه تطبيق المسؤولية الجزائية في هذا المجال، ومن بينها صعوبة الإثبات، وتحديد الفاعل الحقيقي للجريمة، وتداخل الاختصاص القضائي، فضلًا عن التحديات المتعلقة بمساءلة المؤسسات الاقتصادية عن الأفعال الجرمية المرتكبة عبر أنظمتها الرقمية، ويخلص البحث إلى ضرورة تطوير التشريع الجزائي العراقي من خلال سن نصوص قانونية خاصة بالجرائم السيبرانية، بما يواكب التحول الرقمي، ويعزز الحماية الجنائية للمؤسسات الاقتصادية، ويحد من مخاطر الاستغلال غير المشروع للتكنولوجيا الحديثة.

الكلمات المفتاحية: المسؤولية الجزائية، الجرائم السيبرانية، التحول الرقمي، المؤسسات الاقتصادية، التشريع العراقي

Criminal Liability for Cyber Crimes in Light of the Digital Transformation of Economic Institutions

Asst. Lec. Sabah Mohsen Jalout [1]

Affiliation of Author
[1] College of Law, Wasit University, Iraq, Wasit, Al-Kut, 52001

[1] Sabah.m@uowasit.edu.iq

[1] Corresponding Author

Paper Info.
Published: Aug. 2026

Abstract
The Constitution of the Republic of Iraq of 2005 represents a significant historical milestone in the development of the modern Iraqi state, being the first permanent constitution drafted by a committee from an elected national assembly and ratified through a public referendum. This legal framework emerged in the context of a profound political transition following 2003, aiming to establish a new political system based on political pluralism, separation of powers, and the guarantee of public rights and freedoms.
Good governance is closely linked to achieving comprehensive development and accompanies contemporary efforts to rebuild democracy, implement economic reforms, and strengthen the role of the private sector. Despite its importance, the failure of development experiences in some developing countries has often resulted from unclear and ad hoc public policies. Good governance addresses fundamental societal demands, including sustainable development, freedom, human dignity, and peaceful living. Effective governance in Iraq requires continuous cooperation between the government and the private sector to enhance institutional performance and political system stability.
The study highlights that the absence of good governance leads to weakened performance of constitutional institutions and diminished development and citizen welfare. The research aims to identify the determinants of good governance to enhance institutional performance and achieve sustainable development. Findings reveal limited state experience in public-private partnerships, inadequate institutional readiness, the absence of a legislative framework, weak reform initiatives, and technical and administrative gaps. The study emphasizes the importance of strengthening institutional and legal capacities, combating corruption, developing human resources, raising electronic awareness, and fostering collaboration among government, private sector, and civil society organizations to ensure

effective governance and improve the performance of constitutional institutions and political stability.

Keywords: Governance, Political System, Sound Governance, Iraq

المقدمة

ان هذا الموضوع شهد تحولًا رقميًا متسارعًا انعكس على جميع القطاعات الاقتصادية والإدارية، بما في ذلك المؤسسات العراقية، إذ أصبحت تعتمد بشكل شبه كامل على التكنولوجيا الرقمية في إدارة أعمالها ومعاملاتها المالية والمعلوماتية هذا التحول الرقمي أتاح فرصًا كبيرة للنمو والتطور، لكنه في الوقت نفسه خلق بيئة خصبة للجرائم السيبرانية، والتي تتميز بالعالمية والاحترافية وسرعة التنفيذ، ما جعل من الصعب على التشريعات التقليدية أن تواجه هذه الظاهرة بكفاءة عالية.

تتضمن الجرائم السيبرانية الاقتصادية في المؤسسات اختراق الأنظمة، الاحتيال المالي، سرقة البيانات، وتعطيل سير الأعمال الرقمية، وهي أفعال تضر باستقرار المؤسسات وتقلل من ثقة العملاء والمستثمرين من هنا، أصبح لزامًا دراسة المسؤولية الجزائية للفاعلين في هذا المجال، وتحليل مدى قدرة التشريعات الحالية، مثل قانون العقوبات العراقي وقانون جرائم المعلوماتية رقم 56 لسنة 2017، على مواجهة هذه التحديات الرقمية، إضافة إلى تقييم السياسات العقابية ودورها في تعزيز الحوكمة الرقمية الآمنة.

يهدف البحث إلى تسليط الضوء على طبيعة الجرائم السيبرانية الاقتصادية في العراق، وتحديد أركان المسؤولية الجزائية، والتحديات التي تواجه إثبات المسؤولية، وتحليل فعالية السياسة العقابية العراقية في حماية المؤسسات الاقتصادية وسيتم استعراض هذه الجوانب من خلال دراسة المفاهيم القانونية، الإشكاليات العملية، وأمثلة واقعية ضمن المؤسسات الاقتصادية العراقية، مع الاستناد إلى المراجع الفقهية والقانونية الحديثة.

تمثل هذه الدراسة محاولة لفهم مدى ملاءمة التشريعات والسياسات الحالية للتعامل مع التحولات الرقمية، وتقديم توصيات عملية لتعزيز قدرة القضاء على مواجهة الجرائم السيبرانية وحماية استدامة المؤسسات الاقتصادية في العراق

إشكالية البحث

على الرغم من وجود تشريعات عراقية متقدمة، مثل قانون العقوبات العراقي وقانون التوقيع الالكتروني والمعاملات الالكترونية رقم 56 لسنة 2017، إلا أن الجرائم السيبرانية الاقتصادية تمثل تحديًا جديدًا ومعقدًا للمؤسسات الاقتصادية في العراق.

وتتمثل الإشكالية في السؤال الرئيس:

1- إلى أي مدى تكفي التشريعات والسياسات العقابية العراقية الحالية لضمان إثبات المسؤولية الجزائية للجرائم السيبرانية وحماية استدامة المؤسسات الاقتصادية في ظل التحول الرقمي؟

2- تنبع هذه الإشكالية من عدة جوانب: هشاشة الأدلة الرقمية، صعوبة إثبات الركنين المادي والمعنوي، تعدد أساليب الاختراق، والتحديات التقنية التي تواجه القضاء العراقي.

فرضية البحث

يفترض البحث أن: تشريعات العراق الحالية، رغم فعاليتها الجزئية، غير كافية وحدها لمواجهة الجرائم السيبرانية الاقتصادية بشكل كامل، وتحتاج إلى تعزيز السياسات العقابية ووجود دوائر قضائية متخصصة وفِرق تقنية متقدمة لضمان الحوكمة الرقمية الآمنة وحماية المؤسسات الاقتصادية.

أهداف البحث

1. تحليل ماهية الجرائم السيبرانية الاقتصادية وخصائصها في البيئة المؤسسية العراقية.
2. تحديد أركان المسؤولية الجزائية للجرائم الرقمية وصعوبات إثباتها باستخدام الأدلة الرقمية.
3. تقييم فعالية السياسة العقابية العراقية ودورها في تحقيق الحوكمة الرقمية الآمنة.
4. اقتراح توصيات عملية لتطوير التشريعات والآليات القضائية والفنية لتعزيز حماية المؤسسات الاقتصادية.

منهجية البحث يعتمد البحث على منهج تحليلي قانوني وأكاديمي، ويشمل:

1. المنهج الوصفي والتحليلي: لدراسة المفاهيم القانونية للجرائم السيبرانية وخصائصها، وتحليل التشريعات والسياسات العقابية.
2. المنهج المقارن: لمقارنة التشريعات العراقية مع التجارب الدولية في مجال مكافحة الجرائم السيبرانية وحماية

المؤسسات الرقمية.

3. المنهج الاستقرائي: لاستنتاج النتائج والتوصيات بناءً على تحليل النصوص القانونية والفقه العراقي والمصادر العلمية المحكمة.

هيكلية البحث

يتكون البحث من مقدمة عامة، ومبحثين رئيسيين، وخاتمة، مع قائمة مصادر ومراجع:

المبحث الأول: ماهية الجرائم السيبرانية وخصائصها في البيئة المؤسسية

المطلب الأول: التعريف القانوني للجريمة السيبرانية الاقتصادية.

المطلب الثاني: الخصائص الفنية والقانونية للإجرام الرقمي.

المطلب الثالث: أنماط الاعتداء الرقمي التي تهدد استدامة المؤسسات الاقتصادية.

المبحث الثاني: أركان المسؤولية الجزائية وتحديات المواجهة العقابية

المطلب الأول: الأركان المكونة للجريمة السيبرانية (الركن المادي والمعنوي في الفضاء الافتراضي).

المطلب الثاني: إشكالية إثبات المسؤولية الجزائية في ظل "الدليل الرقمي" الهش.

المطلب الثالث: تقييم السياسة العقابية العراقية ودورها في تحقيق الحوكمة الرقمية الآمنة.

الخاتمة: تتضمن أهم الاستنتاجات حول مدى كفاية القوانين الحالية، والتوصية بضرورة تخصيص دوائر قضائية تقنية متخصصة، مع اقتراح توصيات عملية لتعزيز الحوكمة الرقمية وحماية المؤسسات.

المبحث الاول: ماهية الجرائم السيبرانية وخصائصها في البيئة المؤسسية

مع تزايد الاعتماد على التكنولوجيا الرقمية في إدارة المؤسسات الاقتصادية، برزت الحاجة إلى فهم الجرائم السيبرانية التي تهدد استدامة هذه المؤسسات وأمنها المالي والقانوني. فقد أوجد التحول الرقمي بيئة اقتصادية تعتمد على الأنظمة الإلكترونية والتعاملات الرقمية، ما أدى إلى ظهور أشكال جديدة من الاعتداءات الإجرامية لم تكن موجودة في التشريعات التقليدية.

إن الجرائم السيبرانية الاقتصادية لا تقتصر على مجرد سرقة أموال أو بيانات، بل تمتد لتشمل الإضرار بالسمعة المؤسسية، تعطيل العمليات التشغيلية، وزعزعة الثقة في الأنظمة الرقمية، ما يجعل من الضروري دراسة طبيعتها القانونية والفنية وتأثيرها على المؤسسات

المطلب الاول: التعريف القانوني للجريمة السيبرانية الاقتصادية (في الفقه والتشريع العراقي)

أدى التحول الرقمي المتسارع الذي شهدته المؤسسات الاقتصادية إلى تغيّر جوهري في طبيعة النشاط الاقتصادي وآليات إدارته، إذ لم تعد المعاملات تُنجز بالوسائل التقليدية، بل أصبحت تعتمد بشكل أساسي على الأنظمة الإلكترونية وقواعد البيانات الرقمية وشبكات الاتصال. وقد رافق هذا التطور بروز أنماط إجرامية جديدة استغلت البيئة الرقمية، الأمر الذي أوجد تحديات قانونية غير مسبوقة، في مقدمتها مسألة تحديد مفهوم الجريمة السيبرانية الاقتصادية وضبط حدودها القانونية.

إن خطورة الجرائم السيبرانية الاقتصادية لا تكمن فقط في الأضرار المالية المباشرة التي تُلحقها بالمؤسسات، وإنما تمتد لتشمل الإخلال بالثقة في المعاملات الرقمية، وتهديد استقرار النظام الاقتصادي، وهو ما يجعل من التصدي لها ضرورة قانونية واقتصادية في آن واحد [1].

أولًا: التعريف الفقهي للجريمة السيبرانية الاقتصادية

لم يتمكن الفقه القانوني من الاتفاق على تعريف موحد للجريمة السيبرانية، بسبب التطور المستمر في الوسائل التقنية وتعدد صور السلوك الإجرامي في الفضاء الإلكتروني. فقد ركز اتجاه فقهي على الجانب التقني، معتبرًا أن الجريمة السيبرانية هي كل فعل غير مشروع يُرتكب باستخدام الحاسوب أو الشبكات المعلوماتية، ويستهدف البيانات أو الأنظمة الإلكترونية بصورة مباشرة أو غير مباشرة [2]، ويُلاحظ أن هذا الاتجاه يمنح الوسيلة التقنية دورًا محوريًا في تحديد طبيعة الجريمة.

في المقابل، ذهب اتجاه فقهي آخر إلى توسيع نطاق التعريف، من خلال التركيز على البيئة الرقمية بوصفها مسرحًا للجريمة، إذ يرى أن الجريمة السيبرانية تتحقق كلما استُخدمت التقنيات الحديثة كوسيلة أو محل لارتكاب فعل مجرّم قانونًا، بغض النظر عن نوع الأداة المستخدمة [3]، ويُعد هذا الاتجاه أكثر مرونة، لكونه ينسجم مع التطور التقني المتسارع ويحد من ظاهرة الإفلات من العقاب.

أما الجريمة السيبرانية الاقتصادية، فقد أولى الفقه العراقي اهتمامًا خاصًا بها، نظرًا لما تمثله من تهديد مباشر للمؤسسات الاقتصادية. إذ عرّفها بعض الفقه بأنها كل سلوك غير مشروع يُرتكب عبر الوسائط الإلكترونية ويستهدف الأموال أو البيانات أو الأنشطة الاقتصادية للمؤسسات، ويؤدي إلى تحقيق منفعة غير مشروعة أو إلحاق ضرر بالغير [2]، ويُفهم من هذا التعريف أن الجريمة

السيبرانية الاقتصادية تتميز بارتباطها الوثيق بالمصالح الاقتصادية، فضلًا عن اعتمادها على الوسائل التقنية الحديثة.

وتكمن خصوصية هذا النوع من الجرائم في كونه غالبًا ما يرتكب في إطار من السرية والاحتراف التقني، مما يصعّب اكتشافه وإثباته، ويجعل من تحديد الفاعل الحقيقي أمرًا معقدًا، خاصة في حال تعدد الأطراف أو استخدام وسائل إخفاء الهوية الرقمية [1].

ثانيًا: موقف التشريع العراقي من الجريمة السيبرانية الاقتصادية

لم يتضمن قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل تعريفًا صريحًا للجريمة السيبرانية أو للجريمة السيبرانية الاقتصادية، وهو ما يُعد انعكاسًا لطبيعة المرحلة التاريخية التي صدر فيها القانون، حيث لم تكن الجرائم الرقمية قد ظهرت بالصورة التي نشهدها اليوم. ونتيجة لذلك، لجأ القضاء والفقه إلى تطبيق النصوص العامة المتعلقة بجرائم الاحتيال والتزوير والاعتداء على الأموال لتكييف بعض صور الجرائم السيبرانية الاقتصادية [4].

إلا أن هذا التكييف التقليدي يواجه انتقادات فقهية عديدة، لكونه لا يراعي الخصوصية التقنية للجريمة السيبرانية، ولا يعكس خطورتها الحقيقية، خاصة عندما يكون محل الجريمة بيانات أو معلومات ذات قيمة اقتصادية كبيرة. كما أن بعض الأفعال السيبرانية لا يمكن إدراجها بسهولة ضمن الجرائم التقليدية، مما يؤدي إلى فراغ تشريعي يضعف الحماية الجزائية للمؤسسات الاقتصادية [1].

أما قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لسنة 2012، فقد شكّل خطوة مهمة في تنظيم البيئة الرقمية في العراق، إلا أنه لم يُعالج الجوانب الجزائية للجرائم السيبرانية الاقتصادية بصورة شاملة، واقتصر على تنظيم المعاملات الإلكترونية وإضفاء الحجية القانونية عليها، دون أن يتضمن تعريفًا دقيقًا للأفعال الجرمية المرتكبة في هذا المجال [5].

ثالثًا: الأهمية القانونية لتحديد مفهوم الجريمة السيبرانية الاقتصادية

إن غياب تعريف تشريعي واضح للجريمة السيبرانية الاقتصادية ينعكس سلبًا على فعالية تطبيق المسؤولية الجزائية، إذ يؤدي إلى تباين في التكييف القانوني، ويحد من قدرة القضاء على مواجهة هذا النوع من الجرائم بفعالية. فالتحديد الدقيق لمفهوم الجريمة يُعد أساسًا ضروريًا لتحديد أركانها، وضبط نطاق التجريم، وتحديد المسؤولية الجزائية سواء بالنسبة للأشخاص الطبيعيين أم المعنويين داخل المؤسسات الاقتصادية [6].

وعليه، يرى جانب من الفقه العراقي ضرورة تبني تعريف تشريعي للجريمة السيبرانية الاقتصادية يأخذ بنظر الاعتبار طبيعتها التقنية والاقتصادية، ويواكب التحول الرقمي الذي تشهده المؤسسات الاقتصادية، بما يسهم في تعزيز الأمن القانوني وحماية النشاط الاقتصادي من المخاطر السيبرانية المتزايدة [7].

المطلب الثاني: الخصائص الفنية والقانونية للإجرام الرقمي

مع تزايد الاعتماد على التكنولوجيا الحديثة في النشاط الاقتصادي والإداري، ظهرت جرائم رقمية معقدة تتميز بخاصيات فنية وقانونية تختلف تمامًا عن الجرائم التقليدية. ولفهم طبيعة الإجرام الرقمي، من الضروري التركيز على أبرز خصائصه، التي تنعكس على صعوبة التصدي له قانونيًا، سواء في التشريع العراقي أو في الممارسة القضائية.

أولًا: الطابع العالمي للإجرام الرقمي

من أهم الخصائص التي تميز الجرائم الرقمية هي العالمية، إذ يمكن للفاعل ارتكاب الجريمة من أي مكان في العالم، مستغلاً الشبكات الرقمية والإنترنت لتجاوز الحدود الوطنية. وقد لاحظت الدراسات أن هذا الطابع يجعل من تحديد الاختصاص القضائي ومسؤولية الدولة تحديًا كبيرًا، إذ يتيح للفاعلين استهداف أنظمة مؤسساتية واقتصادية في دول متعددة دون مواجهة قيود جغرافية [8].

ويتجلى الطابع العالمي بشكل خاص في الجرائم التي تستهدف البنى التحتية الرقمية، مثل الأنظمة المصرفية الإلكترونية، والمنصات التجارية الرقمية، حيث يمكن تنفيذ عمليات اختراق من خارج الدولة، ما يفرض على التشريع العراقي، وفق بعض الفقهاء، ضرورة وضع نصوص قانونية تكفل التعاون الدولي في مكافحة الجرائم السيبرانية [9].

ثانيًا: الاحترافية التقنية للجريمة السيبرانية

تتميز الجرائم الرقمية بالـ احترافية العالية في استخدام الوسائل التقنية، سواء كانت برمجيات متطورة أو أدوات لإخفاء الهوية الرقمية أو تقنيات التشفير. وقد أشار الباحثون إلى أن احترافية الفاعل تجعل من عملية كشف الجريمة وإثباتها صعبة ومعقدة، إذ غالبًا ما يكون الفاعل ملمًا بكيفية إدارة المخاطر التقنية ويعرف كيفية استغلال الثغرات في الأنظمة الرقمية [10].

وعلى المستوى القانوني، يفرض هذا الاحتراف على القضاء التكيف مع التحديات التقنية، من خلال تدريب المحققين والقضاة على الأساليب الرقمية الحديثة، وتطوير النصوص القانونية لتغطية

الجوانب الفنية التي تتعلق بالبرمجيات والبيانات الرقمية، بما يضمن فعالية المسؤولية الجزائية ضد الفاعل.

ثالثًا: صعوبة الإثبات في الجرائم السيبرانية

تعتبر صعوبة الإثبات أحد أبرز الخصائص القانونية للإجرام الرقمي، إذ يعتمد هذا النوع من الجرائم على بيانات إلكترونية يمكن التلاعب بها أو حذفها أو تشفيرها. وقد بينت الدراسات أن التوثيق الرقمي للجرائم، والحفاظ على الأدلة الإلكترونية، يمثل تحديًا كبيرًا أمام السلطات القضائية، وهو ما يزيد من احتمالية الإفلات من العقاب [11].

كما أن الجرائم الرقمية غالبًا ما تكون غير مرئية للعين المجردة، مما يجعل من الضروري تطوير آليات فنية وإجرائية مثل تقنيات التحليل الرقمي، والتدقيق في سجلات الدخول، وتعقب الأنشطة الإلكترونية للفاعلين، لضمان إمكانية إثبات الفعل الجرمي. ويشير الفقه العراقي إلى أن عدم وضوح الأركان المادية والمعنوية للجريمة الرقمية يجعل من صعوبة الإثبات مسألة أساسية يجب التعامل معها في التشريع [7].

رابعًا: أهمية إدراك الخصائص في التشريع العراقي

تفرض الخصائص الثلاث (العالمية، الاحترافية، وصعوبة الإثبات) تحديات واضحة على التشريع العراقي، خاصة أن القانون الحالي لم يُواكب بالكامل طبيعة الجرائم السيبرانية المعاصرة. ووفق بعض الباحثين، فإن إدراج نصوص واضحة تحدد إجراءات التحري، وجمع الأدلة الرقمية، ومسؤولية الفاعل، إضافة إلى التعاون الدولي، يعتبر خطوة أساسية لتعزيز فاعلية القانون الجزائي العراقي في مواجهة الجرائم السيبرانية [1].

المطلب الثالث: أنماط الاعتداء الرقمي التي تهدد استدامة المؤسسات الاقتصادية

مع التحول الرقمي المتسارع، أصبحت المؤسسات الاقتصادية تعتمد بشكل متزايد على الأنظمة الإلكترونية والتطبيقات الرقمية لإدارة عملياتها اليومية. هذه البيئة الرقمية، رغم ما تقدمه من تسهيل وتحسين الأداء، فقد فتحت الباب أمام ظهور أنماط متنوعة من الاعتداء الرقمي التي تهدد استدامة المؤسسات الاقتصادية، سواء من الناحية المالية، أو السمعة، أو استمرارية العمل. ويمكن تصنيف هذه الأنماط وفق الدراسات والفقه العراقي إلى ثلاثة محاور رئيسية: الاعتداء على البيانات والمعلومات، الجرائم المالية الإلكترونية، والاعتداء على البنية التحتية الرقمية للمؤسسات.

أولًا: الاعتداء على البيانات والمعلومات

يُعد استهداف البيانات والمعلومات أهم وأخطر أشكال الاعتداء الرقمي على المؤسسات الاقتصادية، إذ تُعتبر البيانات الرقمية العمود الفقري لعمل المؤسسات، وتشمل قواعد البيانات الخاصة بالعملاء، المعلومات المالية، والمعاملات التجارية. وقد أوضح الفقه العراقي أن أي اختراق لهذه البيانات أو سرقتها أو تعديلها بدون إذن يُشكل جريمة سيبرانية اقتصادية تهدد الاستدامة المالية والتشغيلية للمؤسسة [6].

ومن الأمثلة الواقعية على هذا النوع من الاعتداء، تعرض بعض الشركات العراقية لمحاولات اختراق قواعد البيانات الخاصة بعملائها بهدف سرقة معلومات بطاقة الدفع، أو تعديل سجلات المخزون، ما يؤدي إلى خسائر مباشرة وغير مباشرة.

ثانيًا: الجرائم المالية الإلكترونية

تشمل الجرائم المالية الإلكترونية جميع الأفعال الإجرامية التي تستهدف الأموال أو المعاملات المالية للمؤسسات باستخدام الوسائل الرقمية، مثل الاحتيال المالي عبر الإنترنت، سرقة الحسابات البنكية، وتحويل الأموال دون إذن قانوني. وأكد الفقه العراقي أن هذه الجرائم تمثل تهديدًا مباشرًا لاستدامة المؤسسات الاقتصادية لأنها تؤدي إلى خسائر مالية كبيرة، وتضعف الثقة بين العملاء والمؤسسات [10].

على سبيل المثال، قام أحد الهاكرز باختراق نظام تحويل الأموال لشركة عراقية متعددة الجنسيات، وتحويل مبالغ كبيرة إلى حسابات خارجية، مما اضطر المؤسسة لتعليق عملياتها مؤقتًا، وإعادة تقييم الأنظمة الأمنية الرقمية.

ثالثًا: الاعتداء على البنية التحتية الرقمية للمؤسسات

يشمل هذا النوع الاعتداء على الأنظمة والبرمجيات والخوادم التي تشغل المؤسسات الاقتصادية، سواء عبر تعطيل الأنظمة (هجمات الحرمان من الخدمة – DDoS)، أو زرع برمجيات خبيثة تؤثر على سير العمل. ويشير الفقه العراقي إلى أن هذا النوع من الاعتداء الرقمي يهدد استمرارية العمل ويؤدي إلى توقف العمليات الاقتصادية، ويصعب التعامل معه إذا لم تكن هناك آليات قانونية وتقنية واضحة لمواجهة هذه المخاطر [11].

كمثال على ذلك، تعرضت إحدى شركات الاتصالات العراقية لهجوم DDoS أدى إلى توقف خدماتها لعدة ساعات، ما أثر على العمليات التجارية وتعاملات العملاء، وأظهر ضعف الحماية الرقمية على الرغم من وجود بروتوكولات أمان.

رابعًا: أنماط هجينة ومتعددة الأهداف

تتصف الجرائم الرقمية الحديثة أحيانًا بأنها هجينة، حيث يجمع الهجوم الواحد بين سرقة البيانات، الاحتيال المالي، وتعطيل الأنظمة، بهدف تحقيق أكبر ضرر ممكن للمؤسسة. وبهذا الشكل، تصبح الجرائم الرقمية متعددة الأبعاد، مما يزيد من صعوبة التكييف القانوني وملاحقة الجناة [8].

وقد أشار بعض الباحثين إلى أن هذه الأنماط الهجينة تجعل المؤسسات أكثر عرضة للتهديد، لأنها تتطلب تدخلًا قانونيًا وتقنيًا متكاملًا، يشمل التحقيق الرقمي، وتأمين البيانات، والتعاون الدولي في حال ارتكاب الجريمة عبر الحدود [9].

خامسًا: الأثر على استدامة المؤسسات الاقتصادية

إن تعرض المؤسسات لهذه الاعتداءات الرقمية لا يقتصر أثره على خسائر مالية فورية، بل يمتد إلى إضعاف الثقة في المؤسسة، تشويه سمعتها، تعطيل العمليات، وزيادة تكاليف الأمان الرقمي. ويرى الفقه العراقي أن حماية المؤسسات الاقتصادية من هذه المخاطر تتطلب وضع أطر قانونية واضحة، تشمل تعريف الجرائم، تحديد المسؤولية الجزائية، وتطوير العقوبات، مع اعتماد آليات التحقيق الرقمي وإجراءات الاستجابة للطوارئ [12].

بالتالي، يمكن القول إن فهم أنماط الاعتداء الرقمي والتصدي لها ليس مجرد مسألة تقنية، بل هو ضرورة قانونية واقتصادية لضمان استدامة المؤسسات وحماية الاستثمارات والمصالح العامة.

المبحث الثاني: أركان المسؤولية الجزائية وتحديات المواجهة العقابية

يشكل المبحث الثاني قلب البحث في دراسة المسؤولية الجزائية للجرائم السيبرانية، إذ يركز على الأركان القانونية والعملية التي تحدد مسؤولية الجاني، وكذلك التحديات العملية التي تواجه تطبيق النصوص الجزائية في بيئة رقمية متطورة. ففي حين تعتمد الجرائم التقليدية على أركان معروفة مثل الركن المادي والمعنوي، تأتي الجرائم السيبرانية لتعقّد عملية إثبات المسؤولية الجزائية بسبب طبيعتها التقنية، وسرعة انتشارها، وحماية مرتكبيها لأنفسهم عبر أساليب رقمية متقدمة.

يهدف هذا المبحث إلى تحليل الركن المادي والمعنوي للجريمة في الفضاء الافتراضي، وبيان الصعوبات المتعلقة بـ إثبات المسؤولية الجزائية باستخدام الأدلة الرقمية الهشة، بالإضافة إلى تقييم السياسة العقابية العراقية ودورها في تعزيز الحوكمة الرقمية الآمنة. ويعد هذا التحليل ضروريًا لفهم كيف يمكن للقوانين الحالية والآليات التنفيذية أن تواجه التحديات التي تفرضها الجرائم الإلكترونية على المؤسسات الاقتصادية.

كما يسعى المبحث إلى توضيح أن توافر الأدلة الرقمية وحده لا يكفي لإثبات الجريمة، بل يجب أن يُكملها إطار تشريعي وعقابي واضح، وخبرة فنية متخصصة، لضمان أن تكون المسؤولية الجزائية متحققة فعليًا، بما يحافظ على استدامة المؤسسات ويعزز الثقة في النظام الرقمي. ومن خلال هذا المبحث، سيتم الانتقال بسلاسة من دراسة الأركان القانونية إلى الإشكاليات الواقعية في الإثبات، ثم إلى تقييم السياسات العقابية، بما يوفر صورة شاملة لمواجهة الجرائم السيبرانية في العراق

المطلب الأول: الأركان المكوّنة للجريمة السيبرانية (الركن المادي والمعنوي في الفضاء الافتراضي)

تُعدّ دراسة الأركان المكوّنة للجريمة السيبرانية من الموضوعات الجوهرية في نطاق المسؤولية الجزائية، ولاسيما في ظل توسّع الفضاء الافتراضي وتحوله إلى بيئة خصبة لارتكاب أفعال إجرامية تمس المصالح الاقتصادية للمؤسسات والأفراد. فالجرائم السيبرانية، وإن اختلفت في وسيلتها عن الجرائم التقليدية، إلا أنها تخضع من حيث المبدأ للقواعد العامة لنظرية الجريمة، المتمثلة بتوافر الركن المادي والركن المعنوي، مع مراعاة خصوصية البيئة الرقمية التي تُرتكب فيها.

أولًا: الركن المادي للجريمة السيبرانية في الفضاء الافتراضي

يُقصد بالركن المادي للجريمة السيبرانية ذلك النشاط الخارجي الملموس الذي يصدر عن الجاني، ويأخذ في البيئة الرقمية صورة أفعال تقنية تُنفذ عبر الحاسوب أو الشبكات الإلكترونية. ويذهب جانب من الفقه العراقي إلى أن الفعل المادي في الجرائم السيبرانية لا يُشترط فيه التماس المادي المباشر، بل يكفي تحقق السلوك الإجرامي الإلكتروني الذي يؤدي إلى المساس بمصلحة يحميها القانون [13].

ويظهر الركن المادي للجريمة السيبرانية من خلال عدة صور، من أبرزها: الدخول غير المشروع إلى الأنظمة المعلوماتية، التلاعب بالبيانات الإلكترونية، تعطيل البرامج أو إتلافها، أو استخدام الوسائل التقنية لتنفيذ عمليات احتيال أو تحويل أموال دون وجه حق. وتتميز هذه الأفعال بأنها تتم في فضاء افتراضي عابر للحدود، ما يجعل تحديد مكان ارتكاب الجريمة مسألة إشكالية من الناحية القانونية [14].

كما أن الضرر الناتج عن الركن المادي في الجرائم السيبرانية قد يكون ضررًا غير مباشر، كالإضرار بالثقة في المؤسسة الاقتصادية أو تعطيل نشاطها، وهو ما يستوجب من القضاء الأخذ

بمفهوم الضرر الواسع، وعدم حصره بالأضرار المادية التقليدية[15].

ثانيًا: الركن المعنوي للجريمة السيبرانية

أما الركن المعنوي، فيتمثل بالقصد الجنائي، أي اتجاه إرادة الجاني إلى ارتكاب الفعل مع علمه بعدم مشروعيته. وتبرز أهمية هذا الركن في الجرائم السيبرانية بسبب الطبيعة التقنية المعقدة للأفعال المرتكبة، والتي غالبًا ما تتطلب مستوى معينًا من المعرفة والخبرة الرقمية، ما يدل على توافر عنصر العمد في أغلب الحالات .

ويرى الفقه العراقي أن القصد الجنائي في الجرائم السيبرانية يتحقق متى ما ثبت أن الجاني كان مدركًا لطبيعة الفعل الإلكتروني الذي يقوم به، ومدركًا للنتائج المترتبة عليه، سواء تمثلت تلك النتائج في تحقيق منفعة غير مشروعة أو إلحاق ضرر بالمؤسسة أو النظام المعلوماتي [16].

إلا أن إثبات الركن المعنوي في الفضاء الافتراضي يواجه صعوبات عملية، لاسيما مع استخدام الجناة لوسائل إخفاء الهوية الرقمية أو العمل عبر وسطاء تقنيين. ولهذا يؤكد الباحثون على ضرورة الاعتماد على الأدلة الرقمية، كتحليل سجلات الدخول، وتتبع عناوين الشبكات، وربط السلوك الإجرامي بسلسلة من الأفعال المتكررة التي تدل على توافر النية الإجرامية.

ثالثًا: التكامل بين الركنين وأثره في قيام المسؤولية الجزائية

إن قيام المسؤولية الجزائية عن الجريمة السيبرانية لا يتحقق إلا بتكامل الركن المادي مع الركن المعنوي، إذ لا يكفي مجرد حدوث اختراق أو فعل تقني ما لم يُثبت أن الفاعل قد قصده بإرادة واعية. ويُعد هذا التكامل من أبرز التحديات التي تواجه تطبيق النصوص الجزائية التقليدية على الجرائم السيبرانية، خصوصًا في ظل قصور بعض التشريعات عن مواكبة التطور التقني [17].

ومن هنا، تبرز الحاجة إلى تطوير آليات الإثبات الجزائي، بما ينسجم مع خصوصية الفضاء الافتراضي، ويضمن عدم إفلات الجناة من العقاب، وفي الوقت ذاته يحافظ على ضمانات المحاكمة العادلة.

المطلب الثاني: إشكالية إثبات المسؤولية الجزائية في ظل "الدليل الرقمي" الهش

في العصر الرقمي، أصبحت الجرائم السيبرانية من أكبر التحديات القانونية التي تواجه السلطات القضائية، لاسيما في المؤسسات الاقتصادية التي تعتمد بشكل كامل على الأنظمة الرقمية لإدارة عملياتها. ويمثل الدليل الرقمي الهش أحد أبرز التحديات التي تواجه إثبات المسؤولية الجزائية، لما له من طبيعة متقلبة وسهلة التلاعب أو الحذف، الأمر الذي يضع القضاء في موقف صعب عند محاولة الربط بين الجريمة ومرتكبها.

أولًا: طبيعة الدليل الرقمي الهش

الدليل الرقمي يشمل كل السجلات الإلكترونية، قواعد البيانات، البريد الإلكتروني، ملفات النظام، وسجلات المعاملات الرقمية. ويتميز هذا النوع من الأدلة بأنه قابل للتعديل أو الحذف أو التشفير بسهولة، خلاف الأدلة التقليدية الورقية أو المادية التي يصعب تغييرها دون أثر واضح [4].

لهذا السبب، يواجه القضاء صعوبة في الاعتماد على هذه الأدلة وحدها لإثبات الركن المادي والمعنوي للجريمة، فالهاكر أو مرتكب الجريمة الرقمية يمكنه، على سبيل المثال، تغيير سجلات التحويلات المالية، أو مسح ملفات الدخول، أو استخدام برامج للتعتيم على أثره الرقمي، ما يجعل من الصعب التأكد من هوية الفاعل ونواياه.

ثانيًا: تحديات الركن المادي في الإثبات الرقمي

الركن المادي للجريمة السيبرانية يعتمد على الفعل الإجرامي الملموس في الفضاء الرقمي، مثل اختراق الأنظمة، تعديل أو حذف البيانات، أو تعطيل سير العمليات الرقمية. ويواجه القضاء العراقي صعوبة في إثبات هذا الركن لعدة أسباب:

1. غياب الأدلة المادية التقليدية، فالجرائم الرقمية غالبًا لا تترك أثرًا ملموسًا يمكن عرضه أمام المحكمة.
2. الطابع العابِر للحدود، إذ يمكن ارتكاب الجريمة من خارج العراق، ما يستلزم تعاونًا دوليًا لإثبات الفعل.
3. تعدد الوسائل التقنية المستخدمة، والتي قد تشمل شبكات مخفية، برامج تشفير، أو استغلال الثغرات الأمنية [18].

وهذا يعقد مهمة المحققين في ربط الفعل المادي بالفاعل بشكل مباشر.

ثالثًا: تحديات الركن المعنوي والإثبات الجنائي

الركن المعنوي، أي النية الجنائية، يمثل أحد أصعب الأركان إثباتًا في الفضاء الرقمي. فالفاعلين غالبًا ما يستخدمون أساليب لإخفاء الهوية، مثل البروكسي أو VPN، أو انتحال هوية موظفين داخل المؤسسة، ما يجعل إثبات قصدهم الجنائي تحديًا كبيرًا.

ويشير الفقه العراقي إلى أن إثبات القصد الجنائي في الجرائم السيبرانية يتطلب:

- تحليل الأدلة التقنية: مثل سجلات الدخول، مسارات الشبكة، وأثر البرمجيات الخبيثة.
- ربط الفعل بالنتائج المحققة: أي توضيح كيف أن الفعل أدى إلى ضرر محدد أو منفعة غير مشروعة [19].
- توثيق الأدلة بطريقة قانونية: بحيث يمكن تقديمها أمام المحكمة دون إمكانية الطعن في مصداقيتها.

رابعًا: آثار هشاشة الدليل الرقمي على استدامة المؤسسات

هشاشة الأدلة الرقمية لا تؤثر فقط على التحقيقات القضائية، بل تمتد لتؤثر على استدامة المؤسسات الاقتصادية. إذ أن عدم القدرة على إثبات المسؤولية الجزائية:

1. يتيح للفاعلين الإفلات من العقاب، ويزيد من احتمالية تكرار الجرائم.
2. يضعف الثقة بين العملاء والمؤسسات، خصوصًا إذا تم اختراق بيانات حساسة.
3. يزيد من تكاليف الأمن الرقمي للمؤسسات، والتي تصبح مضطرة لاستثمار مبالغ كبيرة في حماية أنظمتها [20].

خامسًا: مقترحات لمواجهة إشكالية إثبات المسؤولية

لمواجهة هذه الإشكالية، يشير الفقه العراقي إلى ضرورة اعتماد استراتيجيات متكاملة تشمل:

- تطوير التشريعات الخاصة بالجرائم السيبرانية، بما يضمن تعريف واضح للأفعال الإجرامية وطرق جمع الأدلة الرقمية.
- تدريب فرق التحقيق الرقمي المتخصصة، لضمان القدرة على تتبع العمليات الإلكترونية وتحليلها بشكل علمي.
- تطبيق آليات حماية الأدلة الرقمية، مثل النسخ الاحتياطية المشفرة، وتوثيق السجلات لحفظها من العبث أو التغيير.
- تعزيز التعاون الدولي، خصوصًا في الجرائم العابرة للحدود، لضمان مصداقية الأدلة وربطها بالفاعل الحقيقي.

سادسًا: الخلاصة التحليلية

يتضح أن إشكالية إثبات المسؤولية الجزائية في الجرائم السيبرانية تمثل تحديًا جوهريًا للقضاء العراقي، وذلك بسبب هشاشة الدليل الرقمي وصعوبة إثبات الركنين المادي والمعنوي. ويؤكد الفقه العراقي على ضرورة الجمع بين الأدوات القانونية والفنية الحديثة لتجاوز هذا التحدي، بما يضمن حماية المؤسسات الاقتصادية واستمرارية أعمالها، وتحقيق العدالة بشكل فعّال.

ثالثاً: تقييم السياسة العقابية العراقية ودورها في تحقيق الحوكمة الرقمية الآمنة

أصبحت الجرائم السيبرانية تهديدًا حقيقيًا لاستقرار المؤسسات الاقتصادية في العراق، مع تزايد الاعتماد على الأنظمة الرقمية في إدارة الأعمال والمعاملات المالية. لذلك، لم يعد كافيًا وجود تشريعات فقط، بل أصبح من الضروري تقييم السياسة العقابية العراقية ومدى فعاليتها في تحقيق الحوكمة الرقمية الآمنة، أي إنشاء بيئة رقمية آمنة تضمن حماية البيانات، استمرارية العمليات، وثقة العملاء والمستثمرين في المؤسسات.

أولًا: الإطار القانوني والسياسة العقابية في العراق

تستند السياسة العقابية العراقية إلى قانون جرائم المعلوماتية رقم 56 لسنة 2017، الذي جرّم الأفعال المرتكبة باستخدام الوسائل الرقمية وحدد العقوبات لكل نوع من الجرائم السيبرانية. كما نص القانون على مسؤولية المؤسسات عن حماية البيانات وتأمين أنظمتها ضد الاختراقات والهجمات الرقمية [21].

مع ذلك، يشير الفقه العراقي إلى أن التشريعات وحدها لا تكفي لضمان الحوكمة الرقمية، لأن طبيعة الجرائم الرقمية عالمية، سريعة، ومعقدة تقنيًا. لذا، تحتاج الدولة إلى سياسة عقابية متكاملة تجمع بين العقوبات القانونية، الإجراءات التنفيذية، وآليات الرقابة التقنية [22].

ثانيًا: مكونات السياسة العقابية الرقمية

يمكن تصنيف عناصر السياسة العقابية الفعالة في العراق كما يلي:

1. العقوبات الرادعة: وضع عقوبات محددة لكل نوع من الجرائم السيبرانية، مثل الاختراق غير المشروع للأنظمة، الاحتيال المالي الرقمي، وتعطيل البنية التحتية الرقمية.
2. التحقيق الرقمي المتخصص: الاعتماد على خبراء وتقنيات متقدمة لجمع الأدلة وتحليلها لضمان سلامتها.
3. التنسيق بين الجهات القضائية والأمنية والمؤسسات: تعزيز التعاون بين وزارة الداخلية، القضاء، والقطاع الخاص لضمان رصد الجرائم الرقمية واستجابتها سريعًا.
4. التوعية والتثقيف القانوني والتقني: نشر ثقافة الأمن الرقمي لدى موظفي المؤسسات، وتوضيح مسؤولياتهم القانونية تجاه حماية البيانات [23].

ثالثًا: دور السياسة العقابية في الحوكمة الرقمية الآمنة

تلعب السياسة العقابية دورًا محوريًا في تحقيق الحوكمة الرقمية، من خلال:

- تعزيز الردع القانوني: العقوبات الرادعة تقلل من احتمالية ارتكاب الجرائم الرقمية.
- ضمان المساءلة: توثيق المخالفات ومعاقبة الفاعلين يحمي المؤسسات ويدعم الثقة العامة في النظام الرقمي.
- تحفيز المؤسسات على تطوير أنظمة الحماية: تطبيق العقوبات يشجع المؤسسات على الاستثمار في الأمن الرقمي ومنع الاختراقات [24].

رابعًا: التحديات التي تواجه السياسة العقابية العراقية

رغم أهمية السياسات العقابية، تواجه العراق عدة تحديات رئيسية:

1. تأخر تحديث التشريعات لمواكبة التطورات التقنية السريعة.
2. نقص الخبرات الفنية لدى المحققين والقضاة للتعامل مع الأدلة الرقمية.
3. الجرائم العابرة للحدود، حيث يمكن ارتكاب الفعل من خارج العراق، ما يتطلب تنسيقًا دوليًا.
4. ضعف التعاون بين القطاعين العام والخاص في تبادل المعلومات الأمنية.

خامسًا: مقترحات لتعزيز الحوكمة الرقمية الآمنة

لتعزيز فعالية السياسة العقابية، يقترح الفقه العراقي:

- تحديث التشريعات بشكل دوري لتواكب التقنيات الجديدة.
- إنشاء فرق متخصصة للتحقيق الرقمي داخل القضاء والأمن.
- فرض عقوبات رادعة وموثقة على المخالفين.
- تعزيز التعاون الدولي والإقليمي لملاحقة الجرائم العابرة للحدود.
- نشر برامج توعية قانونية وتقنية لموظفي المؤسسات الاقتصادية.

سادسًا: الخلاصة التحليلية

تؤكد الدراسة أن السياسة العقابية العراقية تعد أداة مهمة لتحقيق الحوكمة الرقمية الآمنة، لكنها تحتاج إلى تطوير مستمر من حيث التشريعات والآليات التنفيذية. الجمع بين العقوبات القانونية والإجراءات التقنية والفنية يضمن حماية المؤسسات الاقتصادية، تعزيز الثقة الرقمية، ورفع مستوى الردع القانوني ضد الجرائم السيبرانية.

خاتمة البحث

خلص هذا البحث حول موضوع المسؤولية الجزائية عن الجرائم السيبرانية في ظل التحول الرقمي للهيئات الاقتصادية، لما تمثله هذه الجرائم من تهديد حقيقي للأمن الاقتصادي، وبسبب ما تثيره من إشكالات قانونية تتعلق بإثبات الجريمة وتحديد المسؤولية الجزائية في البيئة الرقمية.

الاستنتاجات

1. أظهرت الدراسة أن الجرائم السيبرانية ذات الطابع الاقتصادي تتسم بالاحترافية والانتشار العابر للحدود، مما يجعل ملاحقتها الجزائية أكثر تعقيدًا، ولا سيما في ظل هشاشة الأدلة الرقمية وسهولة العبث بها.
2. تبيّن تعدد صور الاعتداءات الرقمية التي تستهدف الهيئات الاقتصادية، كالاختراق المالي والاحتيال الإلكتروني وسرقة البيانات وتعطيل الأنظمة، وهو ما ينعكس سلبًا على استقرار هذه الهيئات واستدامة نشاطها.
3. خلص البحث إلى أن إثبات أركان الجريمة السيبرانية، سواء المادية أو المعنوية، يواجه صعوبات عملية واضحة داخل البيئة الرقمية، رغم وجود نصوص قانونية عراقية تُجرّم هذه الأفعال.
4. ثبت أن فعالية تطبيق التشريعات الجزائية القائمة ترتبط ارتباطًا وثيقًا بكفاءة التعامل مع الأدلة الرقمية وتوفر الخبرة الفنية المتخصصة في تحليلها.
5. بيّنت الدراسة أن السياسة العقابية العراقية تسهم في دعم الحوكمة الرقمية، إلا أن محدودية الخبرات التقنية لدى الجهات القضائية وضعف التنسيق المؤسسي يقللان من أثر الردع الجزائي.

التوصيات

1. ضرورة مراجعة التشريعات الجزائية العراقية وتحديثها بما ينسجم مع التطور المتسارع في أساليب الجرائم السيبرانية.
2. استحداث محاكم أو دوائر قضائية متخصصة بالجرائم الرقمية تضم قضاة وخبراء في الجوانب القانونية والتقنية.
3. تعزيز التعاون بين الجهات القضائية والأمنية والهيئات الاقتصادية لمواجهة الجرائم السيبرانية بشكل أكثر فاعلية.
4. العمل على رفع مستوى الوعي القانوني والتقني لدى العاملين في المؤسسات الاقتصادية، بما يسهم في الحد من المخاطر الرقمية.
5. دعم السياسة العقابية بآليات فنية حديثة تسهم في حماية الأدلة الرقمية وضمان سلامة الإجراءات الجزائية.

المصادر

[1] الجبوري، أحمد حسن. "الجرائم الإلكترونية وأثرها على الأمن الاقتصادي"، مجلة العلوم القانونية، كلية القانون، جامعة بغداد؛ 2019؛ العدد (2).

[2] السامرائي، محمد كريم. "تكييف الجرائم الإلكترونية في قانون العقوبات العراقي"، مجلة القضاء، مجلس القضاء الأعلى؛ 2018؛ العدد (3).

[3] العلواني، حسين عبد الرزاق. "التنظيم القانوني للمعاملات الإلكترونية في العراق"، مجلة الدراسات القانونية، كلية القانون، جامعة بابل؛ 2022؛ العدد (4).

[4] العلواني، حسين عبد الرزاق. "تحديات الإثبات في الفضاء الافتراضي وتأثيرها على المسؤولية الجزائية"، مجلة القانون المعاصر، كلية القانون، جامعة بابل؛ 2021؛ العدد (6).

[5] البهاء، رائد كريم. "إثبات المسؤولية الجزائية في الجرائم السيبرانية العراقية"، مجلة القانون والتكنولوجيا، كلية القانون، جامعة بغداد؛ 2022؛ العدد (13).

[6] الزرفي، قاسم عبد الله. "الحماية الجزائية للمعاملات الإلكترونية في القانون العراقي"، مجلة القانون، كلية القانون، جامعة بغداد؛ 2021؛ العدد (15).

[7] الحسني، محمود عبد الله. "الجرائم الإلكترونية وخصوصية الاختصاص القضائي"، مجلة الدراسات القانونية، كلية القانون، جامعة الكوفة؛ 2020؛ العدد (10).

[8] النعيمي، كريم حسين. "التعاون الدولي في مكافحة الجرائم السيبرانية"، مجلة العلوم القانونية والاقتصادية، كلية القانون، جامعة تكريت؛ 2019؛ العدد (8).

[9] الشريف، سامي علي. "الاحترافية التقنية للجرائم الرقمية وتحديات الإثبات"، مجلة القانون والتكنولوجيا، كلية القانون، جامعة بغداد؛ 2021؛ العدد (12).

[10] الدليمي، أحمد كاظم. "صعوبة الإثبات في الجرائم السيبرانية"، مجلة القضاء والحقوق، مجلس القضاء الأعلى؛ 2022؛ العدد (5).

[11] الزوبعي، رائد عبد الرحمن. "الأركان القانونية للجرائم السيبرانية في التشريع العراقي"، مجلة القانون المعاصر، كلية القانون، جامعة الموصل؛ 2020؛ العدد (7).

[12] الحميدي، كريم فاضل. "الدليل الرقمي بين الإثبات القانوني والهشاشة التقنية"، مجلة القضاء والحقوق، مجلس القضاء الأعلى؛ 2021؛ العدد (4).

[13] العلواني، حسين عبد الرزاق. "الركن المادي للجريمة الإلكترونية وأثره على المسؤولية الجزائية"، مجلة القانون المعاصر، كلية القانون، جامعة بابل؛ 2020؛ العدد (5).

[14] المهدي، عبد الحسين. "تطبيق أركان الجريمة في الفضاء الافتراضي: دراسة مقارنة"، مجلة الدراسات القانونية، كلية القانون، جامعة الكوفة؛ 2020؛ العدد (11).

[15] السعدون، ماجد عبد الله. "الركن المعنوي في الجرائم الرقمية: دراسة تحليلية"، مجلة العلوم القانونية والاقتصادية، كلية القانون، جامعة تكريت؛ 2021؛ العدد (9).

[16] الحميدي، كريم فاضل. "الأركان المكونة للجريمة السيبرانية في القانون العراقي"، مجلة القضاء والحقوق، مجلس القضاء الأعلى؛ 2019؛ العدد (2).

[17] المهدي، عبد الحسين. "إثبات المسؤولية الجزائية في الفضاء الرقمي: دراسة مقارنة للتشريع العراقي"، مجلة الدراسات القانونية، كلية القانون، جامعة الكوفة؛ 2021؛ العدد (12).

[18] السعدون، ماجد عبد الله. "إشكاليات الإثبات الرقمي في الجرائم السيبرانية العراقية"، مجلة العلوم القانونية والاقتصادية، كلية القانون، جامعة تكريت؛ 2022؛ العدد (11).

[19] البهاء، رائد كريم. "التحقيق الرقمي وحماية الأدلة في الجرائم السيبرانية"، مجلة القانون والتكنولوجيا، كلية القانون، جامعة بغداد؛ 2022؛ العدد (14).

[20] الزركوش، علياء حسين خلف. "السياسة العقابية لمواجهة الجرائم الرقمية في العراق"، مجلة الفتح للعلوم القانونية، جامعة ديالى؛ 2021؛ العدد (14).

[21] الغزي، فلاح عبد الله. "الجرائم السيبرانية وتأثيرها على الحوكمة الرقمية في المؤسسات العراقية"، مجلة القانون والاقتصاد الرقمي، كلية القانون، جامعة بغداد؛ 2022؛ العدد (3).

[22] البهادلي، مهند كاظم. "العقوبات الرادعة والحوكمة الرقمية في العراق"، مجلة الدراسات القانونية المعاصرة، كلية القانون، جامعة الكوفة؛ 2021؛ العدد (10).

[23] الشمري، سهيل عبد الرحمن. "فعالية التشريعات العراقية في مكافحة الجرائم الإلكترونية"، مجلة القانون والتكنولوجيا، كلية القانون، جامعة تكريت؛ 2020؛ العدد (8).

[24] القيسي، حسن فاضل. "دور السياسة العقابية في تحقيق الأمن الرقمي للمؤسسات العراقية"، مجلة القضاء والحقوق، مجلس القضاء الأعلى؛ 2022؛ العدد (5).