الحماية الجنائية من القرصنة الرقمية

م.م داليا محمد عبد الواحد
dalia.m.abdul-wahid@nahrainuniv.edu.iq
جامعة النهرين

الملخص:-

تُعدّ القرصنة الرقمية من أخطر الجرائم التي تهدّد الحماية القانونية لحقوق الملكية الفكرية، إذ نقلت الاعتداء من المجال المادي إلى الفضاء الإلكتروني الذي يتجاوز الحدود الوطنية وقد تناول هذا البحث دراسة الحماية الجنائية من القرصنة الرقمية من خلال تحليل مفهومها وأركانها الأساسية وبيان العقوبات المقررة لها في التشريعات المقارنة.

اذ استعرض البحث موقف المشرّع الفرنسي الذي أقرّ بنظام عقابي متدرّج في قانون الملكية الفكرية، والمشرّع المصري الذي نصّ صراحة على تجريم القرصنة ضمن قانون حماية حقوق الملكية الفكرية رقم (٨٢) لسنة ٢٠٠٢و بين موقف المشرع العراقي، الذي لا زال يعتمد على قانون حق المؤلف رقم (٣) لسنة ١٩٧١ خاصة ان مشروع قانون الجرائم المعلوماتية لم يقر حتى هذه اللحظة، فلا نجد نصوصا صريحة تواجه خصوصية الجريمة الرقمية .

وانتهى بحثنا إلى أن غياب التنظيم القانوني الواضح أضعف الردع والعقاب، مما يستوجب إصلاحًا تشريعيًا يتضمّن نصوصًا محددة، وتدرجًا في العقوبات، وتعاونًا قضائيًا دوليًا لتحقيق حماية فعّالة للحقوق الرقمية

الكلمات المفتاحية: القرصنة الرقمية –حق المؤلف– مشروع قانون الجرائم المعلوماتية – الملكية الفكرية الرقمية

Digital Interconnection and Intellectual Property Rights

M.M. Dalia Mohamed Abdelwahed
Imam Jaafar Al-Sadiq University

Abstract:-

Digital piracy is among the most serious crimes that threaten the legal protection of intellectual property rights, as it has transferred acts of infringement from the physical domain to the electronic space that transcends national borders, This study examines the criminal protection against digital piracy through an analysis of its concept, essential elements, and the penalties prescribed in comparative legislations. The research reviewed the position of the French legislator, who adopted a graded system of penalties under the Intellectual Property Code, and the Egyptian legislator, who explicitly criminalized digital piracy under Law No. 82 of 2002 on the Protection of Intellectual Property Rights. It also addressed the stance of the Iraqi legislator, who still relies on the Copyright Law No. 3 of 1971, particularly since the draft Cybercrime Law has not yet been enacted; thus, there are no explicit provisions addressing the specific nature of digital crime.

The study concludes that the absence of a clear legal framework has weakened deterrence and punishment, which necessitates a legislative reform that includes precise legal provisions, a proportional scale of penalties, and international judicial cooperation to ensure effective protection of digital rights.

Keywords: **Digital piracy – Copyright – Cybercrime Bill – Digital Intellectual Property**

بسم الله الرحمن الرحيم

المقدمة

لقد أصبحت التكنولوجيا الرقمية جزءًا لا يتجزأ من البنية القانونية والاقتصادية المعاصرة، الأمر الذي أفرز أنماطًا جديدة من السلوك الإجرامي تجاوزت الأطر التقليدية للتجريم والعقاب، من أبرز هذه الأنماط جريمة القرصنة الرقمية ، إذ انها تقوم على الاعتداء على المصنفات الفكرية عبر الوسائط الإلكترونية بوسائل يصعب ضبطها أو إثباتها، مما يعني ان التطور ادى إلى إرباك التشريعات الوطنية في تحديد التكييف القانوني للجريمة الرقمية وتمييزها عن غيرها من الجرائم المعلوماتية،كما أفرزت هذه الظاهرة تحديات تتعلق بحدود المسؤولية والعقوبة ومدى كفاية النصوص التقليدية في مواكبة الواقع التقني المتغير.

أهمية البحث

تنبع أهمية هذا البحث من كونه يعالج موضوعًا مستحدثًا يتقاطع بين القانون الجنائي و المدني، في وقتٍ أصبحت فيه الحقوق الرقمية جزءًا من الأمن القانوني والاقتصادي للدولة، كما يسعى لتحديد أوجه القصور في التشريع العراقي واقتراح حلول إصلاحية واقعية بهدف المساهمة في تطوير السياسة العقابية لمواجهة الجرائم الحديثة.

إشكالية البحث

يمكننا ان نطرح إشكالية البحث بشكل تساؤلات تتمثل في ما يلي:

١. إلى أي مدى تكفي النصوص الجزائية التقليدية في القانون العراقي لمواجهة جريمة القرصنة الرقمية التي تتسم بطابع تقني عابر للحدود؟

٢. ما السبل التشريعية والجنائية الكفيلة بتطوير الحماية القانونية بما يحقق التوازن بين الردع الفعّال وحماية الحقوق الرقمية؟

منهجية البحث

نرى انه لا بد لنا من اتباع المنهج التحليلي المقارن القائم على تحليل النصوص القانونية الوطنية والدولية ذات الصلة، مع المقارنة بين المشرّع العراقي ونظيريه الفرنسي والمصري في مجال العقوبة على

القرصنة الرقمية كما سيتم توظيف المنهج الوصفي لتقويم النصوص القائمة واقتراح البدائل التشريعية المناسبة.

خطة البحث

المبحث الأول: مفهوم القرصنة الرقمية وأركانها

- **المطلب الأول:** تعريف القرصنة الرقمية وتمييزها عن غيرها.
- **المطلب الثاني:** اركان جريمة القرصنة الرقمية.

المبحث الثاني: السياسة العقابية في مواجهة جريمة القرصنة الرقمية

المطلب الأول: النماذج التشريعية المقارنة في تجريم القرصنة الرقمية ومعاقبتها

المطلب الثاني: التنظيم العقابي في التشريع العراقي والتحديات التطبيقية

المبحث الأول: مفهوم القرصنة الرقمية

يُعدّ فهم مفهوم القرصنة الرقمية الأساس الذي تُبنى عليه دراسة الحماية الجنائية منها، إذ إنّ تحديد ماهيتها وتمييزها عن غيرها من الأفعال المشابهة هو الخطوة الأولى لتكوين تصور قانوني دقيق عنها، لذلك خُصِّص المطلب الأول لتناول الإطار المفاهيمي للقرصنة الرقمية، من خلال بيان معناها اللغوي والاصطلاحي، واستعراض الفوارق الجوهرية التي تميزها عن الجرائم الإلكترونية الأخرى كالاختراق والاحتيال. أما المطلب الثاني فقد خُصِّص لتحليل أركان جريمة القرصنة الرقمية بوصفها المكونات التي يقوم عليها التجريم، متناولًا الركن ، والركن المعنوي الذي يعكس نية الفاعل في ارتكاب السلوك غير المشروع.

المطلب الأول: تعريف القرصنة الرقمية وتمييزها عن الجرائم

تُعَدّ القرصنة الرقمية من الجرائم المستحدثة التي تشترك مع غيرها من الجرائم المعلوماتية في الوسيلة التقنية، لكنها تختلف عنها في المحلّ والغاية القانونية، ولغرض الإحاطة بجوهرها وتمييزها بدقة يتناول هذا المطلب بيان أوجه المقارنة بين القرصنة الرقمية وكلا من الاختراق الإلكتروني والاحتيال الإلكتروني، للكشف عن نقاط الاختلاف بينها.

الفرع الأول: تعريف القرصنة الرقمية

سنعرف القرصنة الرقمية من ناحيتين و هما الناحية اللغوية و الناحية الاصطلاحية، لتحديد معناها الدقيق فالقرصنة في اللغة مأخوذة من الفعل قَرْصَنَ، وهي منسوبة إلى القرصان الذي يعني

المعتدي أو السارق الذي يستولي على أموال الغير بوسائل غير مشروعة، وقد استُخدم هذا المصطلح قديمًا للدلالة على من يمارس السطو في البحر دون إذنٍ أو ترخيص من دولةٍ معينة[1].

ومع التطور التكنولوجي واتساع استخدام الحاسوب وشبكات الإنترنت، انتقل لفظ القرصنة من دلالته الأصلية التي ارتبطت بالسطو على السفن والأموال في البحر، إلى دلالةٍ حديثةٍ تعبّر عن الاعتداء في الفضاء الإلكتروني اذ عرّف الاتحاد الدولي للاتصالات (ITU) القرصنة الرقمية بأنها: (كل دخول أو استخدام غير مصرح به لأنظمة الحاسوب أو الشبكات بما يؤدي إلى المساس بسرية أو سلامة أو توافر البيانات)[2]

كما تُعرّف القرصنة الرقمية بأنها: (الفعل غير القانوني المتمثل في استنساخ السلع الرقمية — كالبرامج، والمستندات الرقمية، والمقاطع الصوتية (بما في ذلك الموسيقى والصوت)، والمقاطع المرئية —لأي غرض غير النسخ الاحتياطي، ومن دون إذنٍ صريحٍ أو تعويضٍ لصاحب الحق).[3]

ويعرفها اخرون بأنها:(عملية إعادة إنتاج أو استخدام أو توزيع المنتجات المعلوماتية بصيغ رقمية أو باستخدام التقنيات الرقمية دون إذنٍ من أصحابها القانونيين).[4]

ومما تقدم يمكننا ان نعرف القرصنة الرقمية بأنها:

كل سلوك عمدي غير مشروع يُرتكب عبر الوسائط أو الأنظمة الإلكترونية و يهدف إلى الاستعمال أو النسخ أو النشر أو التوزيع غير المصرح به لمصنفاتٍ أو بياناتٍ رقميةٍ محميةٍ قانونًا بقصد الإضرار بصاحب الحق أو تحقيق منفعة غير مشروعة ، مما يشكل اعتداءً على النظام المعلوماتي والملكية الفكرية في الفضاء الرقمي.

الفرع الثاني: تمييز القرصنة الرقمية عن الجرائم المعلوماتية الأخرى

[1] المنجد في اللغة والإعلام، المطبعة الكاثوليكية، بيروت، ط٢٦، بدون سنة طبع، ص٦١٦.

[2] TU, Understanding Cybercrime: Phenomena, Challenges and Legal Response, Geneva, 2020, p.13

[3] Gopal, R. D., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. C., *The Economics and Policy of Digital Content*, Elsevier Publishing, 2004, p. 4.

[4] Paul Belleflamme & Martin Peitz, *Digital Piracy*, *Encyclopedia of Law and Economics*, Springer, 2014, p. 1.

تُعدّ القرصنة الرقمية من أبرز الجرائم التي نشأت في ظل التطور التقني المتسارع، وقد تشابهت في بعض صورها مع جرائم أخرى تقع في البيئة الرقمية، لاسيما جريمة الاختراق الإلكتروني (Hacking)وجريمة الاحتيال الإلكتروني (E-Fraud) لذلك، من الضروري بيان أوجه الاختلاف الجوهرية بين هذه الجرائم لتحديد نطاق التجريم والعقاب بدقة.

أولاً: القرصنة الرقمية والاختراق الإلكتروني

يشترك كل من القرصنة الرقمية والاختراق في الاعتماد على وسائل وتقنيات إلكترونية لكنهما يختلفان فيما يلي:

١- من حيث المحلّ القانوني للحماية

تحمي القرصنة الرقمية حقوق الملكية الفكرية للمصنفات الرقمية مثل البرامج والأفلام والكتب، بينما يهدف الاختراق الإلكتروني إلى حماية سلامة الأنظمة المعلوماتية وسرّية البيانات من الدخول أو التلاعب غير المشروع[١].

٢-من حيث الركن المادي للجريمة

يتحقق الركن المادي في القرصنة من خلال النسخ أو النشر أو التوزيع غير المصرّح به للمصنفات الرقمية المحمية، في حين يتحقق في جريمة الاختراق من خلال الدخول غير المصرح به إلى النظام المعلوماتي عبر كسر الحماية التقنية أو استغلال ثغرات أمنية[٢].

٣- **من حيث الركن المعنوي** في القرصنة الرقمية، ينصرف القصد الجرمي إلى الاعتداء على حق المؤلف أو تحقيق كسب غير مشروع عبر استغلال المحتوى المحمي، أما في الاختراق الإلكتروني فيتجسد القصد في العلم بعدم الإذن و ارادة التعدي على سرّية النظام أو تعطيله أو تهيئته لارتكاب جرائم لاحقة[٣].

---

[1] ITU, opcit, p.45.

[٢] سلطان فياض محمد ، جريمة انتهاك سرية المعلومات عبر الوسائط الالكترونية، رسالة ماجستير، جامعة الشرق الاوسط، ٢٠٢١، ص٥٧.

[٣] د. عطية عبد السلام الفيتوري ، جريمة الدخول غير المشروع إلى اجهزة الحاسب الالي، مجلة الحق المجلة ، العدد ٦، ٢٠١٧، ص١٣٠-١٣٢.

ثانياً: القرصنة الرقمية والاحتيال الإلكتروني

يشترك كلٌ من القرصنة الرقمية والاحتيال الإلكتروني في كونهما جرائم معلوماتية تُرتكب باستخدام الوسائط أو الأنظمة الإلكترونية لكنهما يختلفان فيما يلي:

١- من حيث طبيعة الجريمة

نرى ان القرصنة الرقمية جريمة فكرية تستهدف الحقوق المعنوية والمالية للمؤلفين والمنتجين، بينما الاحتيال الإلكتروني جريمة مالية تهدف إلى الاستيلاء على أموال الغير من خلال وسائل رقمية قائمة على الخداع.[١].

٢-من حيث وسيلة التنفيذ

تُرتكب القرصنة باستخدام أدوات النسخ والمشاركة الرقمية دون إذنٍ من صاحب الحق، أما الاحتيال الإلكتروني فيُرتكب باستعمال وسائل احتيالية مثل رسائل التصيّد والمواقع المزيفة والبرمجيات الخبيثة لجمع بيانات مالية أو مصرفية[٢].

٣- من حيث المصلحة المحمية

نرى ان القرصنة الرقمية تحمي المصلحة الفكرية للمؤلف وحقوقه المعنوية والمادية في المصنفات الرقمية، في حين يحمي الاحتيال الإلكتروني الذمة المالية والمركز القانوني للضحايا ضد الأفعال الاحتيالية عبر الفضاء السيبراني[٣].

٤- من حيث الإثبات

نرى ان جريمة القرصنة بالأدلة الفنية مثل آثار النسخ أو التوزيع وسجلات المنصات الرقمية، بينما يُثبت الاحتيال الإلكتروني من خلال تتبع الإشعارات الإلكترونية و فحص ذاكرة الحاسوب و البرمجيات المخزونة و استعادتها[١].

---

[١] عبد الوهاب عبد الكريم محمد المبارك، "إشكالية المسؤولية القانونية عن جرائم النصب والاحتيال الإلكتروني الواقعة على عملاء البنوك"، المجلة القانونية ، مصر، ٢٠٢٣، ص ٨.

[٢] شيلان محمد شريف، *الأحكام الموضوعية والإجرائية في جريمة الاحتيال الإلكتروني*، أطروحة دكتوراه، كلية القانون، جامعة السليمانية، ٢٠١٩، ص ٢٢

[٣] عبد الوهاب عبد الكريم محمد المبارك، المصدر السابق، ص ١٩.

يتبيّن لنا مما تقدم أن القرصنة الرقمية جريمة فكرية تستهدف انتهاك حقوق الملكية للمصنفات الرقمية، بينما الاختراق الإلكتروني هو سلوك تقني يخرق الأنظمة دون إذن وغالبًا يُستخدم كوسيلة لجرائم أخرى، أما الاحتيال الإلكتروني فهو جريمة مالية تقوم على الخداع لتحقيق كسب غير مشروع مما يعني ان هذه الفروقات تستلزم تمييزًا واضحًا بينها لضمان فعالية الحماية الجنائية في الفضاء الرقمي.

المطلب الثاني: أركان جريمة القرصنة الرقمية

يتناول هذا المطلب ركني جريمة القرصنة الرقمية إذ يركّز أولاً على بيان السلوك المادي المكوّن للجريمة وما يتضمنه من فعل ونتيجة وعلاقة سببية في البيئة التقنية و هذا ما يتناوله الفرع الاول، ثم يتناول الركن المعنوي الذي يُعبّر عن القصد الجنائي الخاص لدى الفاعل و هذا ما يتناوله الفرع الثاني ومن خلال دراسة هذين الركنين تتضح الصورة الكاملة لبناء هذه الجريمة.

الفرع الأول: الركن المادي في جريمة القرصنة الرقمية

ان الركن المادي أساس لقيام اية جريمة ، إذ يمثّل **السلوك الخارجي الملموس** الذي تُترجم من خلاله الإرادة الإجرامية إلى فعل يعتدي على مصلحة يحميها القانون و من الثابت ان هذا الركن لا يتحقق إلا بتوافر السلوك والنتيجة وعلاقة السببية، بوصفها العناصر التي تُظهر الجريمة في شكلها الواقعي القابل للإثبات.[٢]

وبتطبيق هذا المفهوم على جريمة **القرصنة الرقمية**، يتضح أن الركن المادي فيها يتخذ **صورة سلوك تقنيٍّ إيجابي** يُمارَس من خلال الوسائط الرقمية، ويتمثل في أفعال النسخ أو النشر أو التوزيع أو الإتاحة غير المشروعة للمصنفات المحمية، مما يجعلها امتدادًا حديثًا لفكرة الفعل المادي التقليدي ولكن بوسائل رقمية ومعاصرة[٣].

ومن الثابت ان الفعل لا يكفي لتحقق الركن المادي بل يجب ان تكون هناك نتيجة إجرامية (تتمثل هنا في المساس الفعلي أو المحتمل بحقوق الملكية الفكرية أو بحرمان صاحب المصنف من عائد الاستغلال المشروع)،[٤]وان تقوم **علاقة السببية** يستدل منها على أن الفعل التقني المتمثل في

[١] شيلان محمد شريف، مصدر سابق، ص ١٧١

[٢] د. فخري الحديثي، *القانون الجنائي ، القسم العام*، ط٤، بغداد، ٢٠١٢، ص١١٢.

[3] OECD, *Piracy of Digital Content*, Paris, 2009, pp.12–15

[4] UNODC, *opcit*, pp.89–90.

النسخ أو الإتاحة غير المصرّح بها كان هو السبب المباشر في وقوع الضرر، لذا نرى ان خصوصية الركن المادي في الجريمة الرقمية، إذ يجري في فضاء غير مادي لكنه يُنتج آثارًا واقعية ملموسة تمسّ النظام القانوني للملكية الفكرية مما يعني أن الركن المادي في جريمة القرصنة الرقمية لا يقوم إلا إذا تحقق سلوك فعلي موجه نحو انتهاك الحماية الرقمية، وأنتج أثرًا غير مشروع في البيئة الإلكترونية[1].

و نرى أن الركن المادي في جريمة القرصنة الرقمية يُجسّد التحول من الفعل المادي التقليدي إلى السلوك التقني الحديث الذي يقع في بيئة غير مادية لكنه يُحدث أثرًا واقعيًا ، ويُبرز الحاجة إلى تطوير القواعد الجنائية لتواكب التطورات التقنية المستمرة .

الفرع الثاني: الركن المعنوي في جريمة القرصنة الرقمية

يُعدّ الركن المعنوي الأساس النفسي الذي يمنح جريمة القرصنة الرقمية طابعها الإجرامي، إذ يُبرز **علم الجاني بفعله وارادة** ارتكاب الفعلٍ و كما يلي:

أولًا: العلم بعدم المشروعية في السلوك الرقمي

يتحقق العلم في جريمة القرصنة الرقمية عندما **يدرك الجاني إدراكًا تامًا** أن المحتوى أو البيانات التي يتعامل معها خاضعة لحماية قانونية، وأن نسخها أو نشرها أو توزيعها دون ترخيص يُعد تعديًا على حقوق الغير، فالعلم في هذه الجريمة لا يقتصر على معرفة الفعل، بل يمتد إلى فهم نظام الحماية التقنية والقانونية الذي يحظر الوصول غير المصرح به[2].

ويُستفاد من الفقه أن عنصر العلم في البيئة الرقمية يُستدل عليه من **القرائن الفنية**، مثل استخدام برامج متخصصة لكسر الشفرات، أو الدخول إلى شبكات مغلقة، أو تجاوز شروط الترخيص البرمجي، وتُظهر هذه القرائن أن الجاني تصرف بوعيٍ كامل بمخالفته القانون، لا سيما في ظل التطور التشريعي الذي أصبح يُدرج هذه الأفعال ضمن الجرائم العمدية البحتة كما أن العلم في جريمة القرصنة الرقمية يمتد ليشمل إدراك الجاني لعواقب، إذ يعلم أن قرصنة البرامج أو المحتوى تؤدي إلى ضرر مالي للمؤلفين والشركات، وتُضعف الثقة في منظومات الحماية المعلوماتية، مما يعني

[1] د.محمد فؤاد الحريري، *الإطار القانوني لتجريم القرصنة الإلكترونية في مملكة البحرين*، مجلة القانون، العدد الثالث عشر، معهد الدراسات القضائية والقانونية، المنامة، ٢٠٢١، ص ٩٦.

[2] متعب محمد مسعود آل حباب الهاجري، *جريمة القرصنة الإلكترونية في التشريع القطري – دراسة تحليلية مقارنة*، مجلة كلية الحقوق، جامعة الإسكندرية، العدد (٤٠)، ٢٠٢٣، ص ٤٩١

ان العلم في الجرائم الرقمية أكثر عمقًا من نظيره في الجرائم التقليدية، لأنه يجمع بين الإدراك القانوني والفني معًا[1].

ثانيًا: الإرادة المتجهة إلى الاعتداء على الحق الرقمي

من المعلوم ان الإرادة تمثّل **الاختيار الحرّ في تنفيذ الفعل رغم العلم بعدم مشروعيته** ففي جريمة القرصنة الرقمية، تتحقق الإرادة عندما يختار الجاني عمداً كسر نظام الحماية أو نشر محتوى مقرصن أو إعادة بيعه على نحو غير قانوني. فهذه الأفعال لا يمكن أن تقع بغير تدخل إرادي، لأنها تتطلب معرفة تقنية وتحضيراً مسبقًا[2].

وتظهر الإرادة الإجرامية بصورة أوضح عندما يكون الهدف من الفعل **تحقيق مكسب اقتصادي أو شهرة رقمية**، إذ يسعى الجاني إلى استغلال الملكية الفكرية للغير لتحقيق منفعة خاصة، فالإرادة هنا ليست مجرد نية في ارتكاب الفعل، بل هي **إصرار متعمّد على تكراره أو توسيعه**، كما في حالة تشغيل مواقع أو قنوات تبث محتوى مقرصن على نطاق واسع، مما يكشف عن قصد خاص يميز هذه الجريمة عن غيرها[3].

نستنتج مما تقدم أن الركن المعنوي في جريمة القرصنة الرقمية يقوم على علمٍ متكاملٍ بطبيعة الفعل المجرَّم وإرادةٍ حرةٍ متجهةٍ نحو تحقيقه، كما يتطلب تحقيقها الى قصد جنائي خاصٍ يتمثل بنية الإضرار والاستغلال.

المبحث الثاني: التنظيم العقابي في التشريع العراقي والتحديات التطبيقية

تمثل السياسة العقابية الركيزة الأساسية التي تُترجم بها الدول موقفها من الجريمة ووسائل الردع المناسبة لها، لاسيما في المجال الرقمي الذي يتسم بتطور تقني متسارع وتنوع في أنماط السلوك الإجرامي، وقد اتجهت بعض التشريعات إلى تبنّي تنظيمات خاصة لمواجهة القرصنة الرقمية تراعي خصوصيتها التقنية وطابعها العابر للحدود، ويهدف هذا المبحث إلى تقييم فاعلية النصوص الوطنية في ضوء التجارب التشريعية الحديثة ،لذا سنقسم هذا المبحث إلى مطلبين، نتناول في الأول النماذج التشريعية المقارنة في تجريم القرصنة الرقمية ومعاقبتها، وفي الثاني التنظيم العقابي في التشريع العراقي والتحديات التطبيقية ،

[1] متعب محمد مسعود آل حباب الهاجري ، المصدر السابق ، ص ٤٩٣

[2] Ajoy P. B., Developing an Analytical Definition of Cybercrime, IOSR Journal of Humanities and Social Science, Vol. 29, Issue 1, Series 6, January 2024, p. 14..

[3] Ahmed Awda, *Cybercrime and Criminal Intent: A Comparative Analysis*, , 2021, p.6

المطلب الأول: النماذج التشريعية المقارنة في تجريم القرصنة الرقمية ومعاقبتها

تُظهر التجارب القانونية المقارنة تباينًا في معالجة جريمة القرصنة الرقمية بين التشريعات المتقدمة والأنظمة العربية، من حيث تحديد الأفعال المجرّمة وتقدير العقوبات المقررة لها ويُعدّ هذا التنوع انعكاسًا لاختلاف فلسفة التجريم والردع في مواجهة الجرائم المعلوماتية. ولذا سنقسم هذا المطلب إلى **فرعين**، نتناول في **الأول** التنظيم القانوني للعقوبة في الأنظمة المقارنة المتقدمة، وفي **الثاني** الأسس العامة للعقوبة في التشريعات العربية ذات الصلة.

الفرع الأول :التنظيم القانوني للعقوبة في الأنظمة المقارنة المتقدمة

يُعدّ التشريع الفرنسي من أوائل الأنظمة القانونية التي تصدّت صراحةً لجريمة القرصنة الرقمية، إذ عالجها ضمن قانون الملكية الفكرية الفرنسي وقد ميّز المشرّع الفرنسي بين الأفعال التي تشكّل مجرد مخالفة مدنية وبين الأفعال التي ترقى إلى جريمة جزائية تستوجب العقاب، مؤكدًا على أن كل نسخ أو توزيع أو بثّ لمصنف محمي عبر الإنترنت دون إذنٍ من صاحبه يُعدّ جريمة تزييف رقمي[1]

وحدّد المشرّع الفرنسي العقوبات المقررة لهذه الجريمة في المادة (L.335-2) من القانون المذكور، إذ نصّت على أن من يرتكب فعل التزييف الرقمي يُعاقب بحبسٍ لا يتجاوز ثلاث سنوات وغرامة تصل إلى ٣٠٠،٠٠٠ يورو، مع مضاعفة العقوبة في حالة التكرار أو ارتكاب الفعل ضمن نطاق جماعي منظم ،كما أجاز القانون للمحكمة أن تقضي بـ **مصادرة الأجهزة والبرمجيات** المستخدمة في تنفيذ الفعل الإجرامي، و**إغلاق المواقع الإلكترونية** التي تمارس نشاطًا مخالفًا للقانون وقد دعم هذا الإطار التشريعي بإصدار قانون خاص هو **قانون HADOPI لعام ٢٠٠٩**، الذي أنشأ هيئة إدارية مختصة و منحها صلاحية مراقبة الشبكات وتوجيه **إنذارات إلكترونية تدريجية** للمستخدمين المخالفين وفق نظام الإنذار الثلاثي، قبل إحالة المخالف المتكرّر إلى القضاء الجزائي[2].

ويُظهر أن المشرّع الفرنسي لم يكتفِ بالعقوبات التقليدية المتمثلة في الحبس والغرامة، بل اعتمد فلسفة تشريعية تقوم على **التدرّج في الجزاء والتكامل بين العقوبة والإدارة**، فالمخالفة البسيطة تُواجه بالإنذار، بينما الفعل المتكرر أو المقصود تجاريًا يُعاقب بالعقوبات الجنائية المشددة وهذه السياسة تُبرز

[1] Code de la Propriété Intellectuelle – 2023

[2] Loi n°2009-669 relative à la diffusion et à la protection de la création sur internet (HADOPI) – 2009.

توازنًا بين حماية حقوق المؤلف من جهة، وضمان حرية تداول المعلومات من جهة أخرى، مما جعل التجربة الفرنسية نموذجًا متقدّمًا في مجال مكافحة القرصنة الرقمية[1].

الفرع الثاني: الأسس العامة للعقوبة في التشريعات العربية ذات الصلة

انطلق المشرّع المصري في تنظيمه لعقوبة القرصنة الرقمية من مبدأ حماية حقوق الملكية الفكرية بوصفها من الحقوق ذات الطبيعة المزدوجة، تجمع بين الحق المالي والحق الأدبي للمؤلف، وقد تضمّن **قانون حماية حقوق الملكية الفكرية رقم (٨٢) لسنة ٢٠٠٢** نصوصًا صريحة تجرّم الأفعال التي تشكّل اعتداءً رقمياً على هذه الحقوق، سواءً تمثلت في استنساخ المصنفات الإلكترونية أو نشرها أو تداولها بوسائل رقمية دون إذن صاحب الحق، واعتبر ذلك صورة من صور "الاعتداء المادي" على المصنفات المحمية[2].

وقد نصّت المادة (١٨١) من القانون المذكور على :(كل من ارتكب عمداً أحد الأفعال الآتية يعاقب بالحبس مدة لا تقل عن شهرين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرة آلاف جنيه، أو بإحدى هاتين العقوبتين، وذلك إذا قام دون إذن المؤلف أو من يخلفه باستنساخ أو نشر أو توزيع مصنف من المصنفات المحمية بأي وسيلة كانت)[3] ويتضح لنا من هذا النص أن المشرّع المصري أخذ بمبدأ **الجمع بين العقوبتين** كوسيلة لتحقيق الردع العام، وأنه لم يقصر الحماية على النشر الورقي بل وسّعها لتشمل الوسائل الرقمية كافة .

كما أقرّ القانون في المادة (١٨٤) منه **تشديد العقوبة في حالة العود**، بحيث تضاعف عقوبة الحبس والغرامة مع جواز الحكم بإغلاق المنشأة أو مصادرة الأجهزة المستخدمة في ارتكاب الفعل[4] ويعكس هذا النص إدراك المشرّع المصري لطبيعة الجريمة الرقمية، إذ تتطلب وسائلها التقنية الحديثة تشديد الردع الجزائي وتوسيع نطاق المصادرة ليشمل الأدوات الإلكترونية. ويرى الفقه المصري أن السياسة العقابية في هذا القانون تقوم على **مبدأ التناسب بين جسامة الضرر وطبيعة الفعل**، فالقرصنة التي تهدف إلى الربح التجاري أو التي تتم عبر شبكات منظمة تستوجب عقوبة الحبس مع الغرامة، بينما الأفعال البسيطة ذات الطابع غير التجاري يمكن الاكتفاء فيها

[1] Pierre Yves Gautier, *Propriété littéraire et artistique*, Dalloz, Paris, 2021, p. 412.

[2] ينظر في المادة (١٤٠) والمادة (١٨١) من قانون حماية حقوق الملكية الفكرية المصري رقم (٨٢) لسنة ٢٠٠٢.

[3] ينظر في المادة (١٨١) من قانون حماية حقوق الملكية الفكرية المصري رقم (٨٢) لسنة ٢٠٠٢.

[4] ينظر في المادة (١٨٤) من قانون حماية حقوق الملكية الفكرية المصري رقم (٨٢) لسنة ٢٠٠٢.

بالغرامة فقط. وهذا الاتجاه يحقق مرونة في التطبيق ويمنح القاضي سلطة تقديرية تراعي تطور صور الجريمة الرقمية[1].

.وبذلك يتضح أن المشرّع المصري قد أدرك مبكرًا خطورة القرصنة الرقمية على الاقتصاد الوطني والثقافة الرقمية، فاستحدث نظامًا عقابيًا مزدوجًا يجمع بين **العقوبة الأصلية (الحبس والغرامة)** و**العقوبات التبعية (المصادرة والإغلاق)**، دون أن يفصل بين الوسائط المادية والرقمية وتُعد هذه المقاربة خطوة متقدمة في البيئة العربية، كونها جسّدت التكييف القانوني الدقيق للقرصنة بوصفها اعتداءً جنائيًا على الحقوق الفكرية في الفضاء الإلكتروني[2].

المطلب الثاني التنظيم العقابي في التشريع العراقي والتحديات التطبيقية

يُعدّ التشريع العراقي من الأنظمة التي لم تُواكب بعد التطور التقني الحاصل في مجال الجرائم المعلوماتية، إذ ما زالت النصوص العقابية المتعلقة بالقرصنة الرقمية متفرقة في قوانين عامة كقانون حق المؤلف رقم (٣) لسنة ١٩٧١، دون أن تتضمن معالجة خاصة لهذه الجريمة، وتثير هذه المحدودية التشريعية تساؤلات حول مدى كفاية القواعد القائمة لمواجهة السلوك الرقمي الإجرامي وضمان حماية فعالة للحقوق الرقمية، وسنقسم هذا المطلب إلى فرعين، نتناول في الأول الإطار القانوني للعقوبة في العراق ومشروع قانون الجرائم المعلوماتية، وفي الثاني التحديات العملية في تطبيق العقوبات على جريمة القرصنة الرقمية.

الفرع الأول: الإطار القانوني للعقوبة في العراق ومشروع قانون الجرائم المعلوماتية

لم يخصّص المشرّع العراقي حتى الآن نصًا نافذًا يُجرّم القرصنة الرقمية بشكل مباشر، غير أنه أدرج بعض صورها ضمن القواعد العامة لقانون حق المؤلف رقم (٣) لسنة ١٩٧١ المعدّل بالأمر (٨٣) لسنة ٢٠٠٤، إذ نصّت المادة (٤٥) منه على اذ نصت على:

(١- يعتبر اي فعل يرتكب مما يأتي من اعمال القرصنة التي يعاقب عليه بغرامة لا تقل عن ٥,٠٠٠,٠٠٠ دينار ولا تتجاوز ١٠,٠٠٠,٠٠٠ دينار ٢-من عرض للبيع او للتداول او للإيجار مصنفا مقلدا او نسخا منه ونقله الى الجمهور بأية وسيلة واستخدمه صلحة مادية وادخله الى العراق او اخرجه منه سواء اكان عالما او لديه سبب كافي للاعتقاد بان ذلك المصنف غير مرخص ٣- في حالة الادانة لمرة ثانية سيعاقب الجاني السجن لمدة لا تقل عن خمس سنوات ولا تزيد على عشر سنوات وبغرامة لا

[1] د. أحمد عودة، *الركن المعنوي في الجريمة المعلوماتية دراسة مقارنة*، جامعة دمشق، ٢٠٢١، ص٧٤

[2] د. مروى السيد السيد ، *الحماية الجنائية من جرائم الاعتداء على الملكية الفكرية للمصنفات الرقمية*،مجلة مستقبل العلوم الاجتماعية، العدد الثامن، ٢٠٢٢، ص١٣٥

تقل عن ١٠٠,٠٠٠,٠٠٠ دينار ولا تزيد على ٢٠٠,٠٠٠,٠٠٠دينار أو بإحدى هاتين العقوبتين وللمحكمة في حالة الادانة لمرة ثانية الحكم بغلق المؤسسة التي استخدمت من قبل المقلدين او شركاؤهم في ارتكاب الجرم لمدة معينة او الى الابد.

٤- للمحكمة ان تامر كذلك بمصادرة وتدمير جميع النسخ او التسجيلات الصوتية محل الاعتداء وكل الادوات والآلات او المعدات المستعملة في صنع هذه النسخ او التسجيلات الصوتية محل الاعتداء)[١] .

ولكون التشريع المذكور لا يكفي لمعالجة القرصنة الرقمية عمد المشرع الى لسدّ هذا الفراغ بإعداد **مشروع قانون الجرائم المعلوماتية** الذي طُرح بعدة صيغ و الذي تم التعديل على نصوصه عدة مرات و لكن لم يقر .

و نرى ان السياسة العقابية في العراق تتراوح بين **التقنين الجزئي التقليدي** في قانون حق المؤلف **والتجريم الحديث الموسّع** في مشروع قانون الجرائم المعلوماتية وهذا التباين يعكس مرحلة انتقالية لم تكتمل بعد نحو إطار عقابي رقمي متكامل، على خلاف التشريعات المقارنة كفرنسا ومصر التي حسمت الموقف بتجريم صريح ومفصّل للقرصنة الرقمية .

الفرع الثاني :التحديات العملية في تطبيق العقوبات على جريمة القرصنة الرقمية

تواجه القرصنة الرقمية تحديات كبيرة تتمثل في ما يلي:

أولًا: ضعف البنية الإجرائية والقضائية

ان غياب محاكم متخصصة في الجرائم المعلوماتية يجعل تطبيق العقوبات يخضع لاجتهاد المحاكم الجزائية العادية التي لا تمتلك الخبرة التقنية الكافية كما ان نقص الكوادر الفنية (الخبراء الرقميين، المحققين التقنيين) يضعف من قيمة الأدلة الإلكترونية ويؤدي إلى صعوبة إثبات الجريمة أمام القضاء[٢].

ثانيًا: قصور التنظيم القانوني للإثبات الرقمي

[١] ينظر في المادة (45) قانون حق المؤلف العراقي رقم (٣) لسنة ١٩٧١ المعدّل بالأمر (٨٣) لسنة ٢٠٠٤.

[٢] د. خالد المشهداني، *الجرائم المعلوماتية في التشريع العراقي – دراسة مقارنة*، مجلة القانون، جامعة بغداد، ٢٠٢٢، ص٩٣.

ان قانون أصول المحاكمات الجزائية العراقي لا يتضمن نصوصًا خاصة تنظم إجراءات جمع الأدلة الرقمية أو حفظها، يؤدي هذا القصور إلى فقدان حجية الدليل الإلكتروني مما يُفلت معه الجناة من العقاب رغم وجود آثار رقمية واضحة[1].

ثالثًا: التحديات المرتبطة بالطبيعة الديناميكية للأدلة الرقمية:

يتميز الدليل الرقمي بسرعة انتقاله عبر الشبكات وإمكانية تعديله أو محوه بسهولة، مما يجعل من الصعب تعقبه وضبطه، ولا سيما عند ارتكاب الجريمة عبر الحدود باستخدام أنظمة حاسوب في دول مختلفة. وتؤدي هذه الطبيعة المتغيرة إلى تعقيد إجراءات جمع الأدلة وتقديرها، الأمر الذي يستدعي تعاوناً دولياً فعالاً لضمان سلامة الإثبات وسيادة الدولة في مواجهة الجرائم الإلكترونية العابرة للحدود.[2]

رابعًا: نقص المعرفة التقنية

يُعدّ نقص المعرفة التقنية لدى رجال القانون من أبرز معوقات مكافحة الجرائم الإلكترونية، نظراً للطبيعة المعقدة للأدلة الرقمية التي تتطلب فهماً خاصاً لتقنيات الحاسوب والشبكات فالكشف عن هذه الجرائم يستوجب اعتماد أساليب واستراتيجيات متقدمة تتناسب مع طبيعتها التقنية، الأمر الذي يفرض تدريب المحققين وأفراد الأجهزة الأمنية على اكتساب المهارات الرقمية اللازمة. [3]

الخاتمة

اولا: الاستنتاجات

١. إن جريمة القرصنة الرقمية تمثل تطوراً نوعيًا للجريمة التقليدية، إذ انتقلت من المجال المادي إلى الفضاء الإلكتروني مما فرض واقعًا تشريعيًا جديدًا يتطلب معالجة قانونية خاصة.

٢. أظهر التحليل أن المشرّع الفرنسي والمصري تبنّيا تنظيمًا تشريعيًا واضحًا يتضمن نصوصًا صريحة تحدد الأركان والعقوبات، في حين ظل المشرّع العراقي يعتمد على القواعد العامة دون معالجة دقيقة لخصوصية الجريمة الرقمية.

[1] د. رائد كاظم، *الحماية الجنائية للبيئة الرقمية في القانون العراقي – دراسة مقارنة*، جامعة الكوفة، ٢٠٢١، ص٥٨.

[2] د اسامة حسين محي الدين، حجية الدليل الرقمي في الاثبات الجنائية للجرائم المعلوماتية، دراسة تحليلية مقارنة ، مجلة البحوث القانونية و الاقتصادية ، العدد ٧٦ ، ٢٠٢١ ، ص٧٠٨ .

[3] د اسامة حسين محي الدين ، المصدر نفسه ، ص ٧١١ .

٣. إن الفراغ التشريعي في القانون العراقي أدى إلى ضعف الردع وصعوبة الملاحقة، خاصة في ظلّ الجرائم ذات الطابع العابر للحدود.

٤. ضعف البنية المؤسسية والقضائية في مجال التحقيق الرقمي يمثل أحد أهم معوقات التطبيق الفعلي للعقوبات المقرّرة.

٥. ان الحماية الجنائية الفعالة لا تقوم فقط على النص العقابي، بل تتطلب بيئة قانونية متكاملة تشمل التشريع، والإثبات، والتعاون الدولي، والتدريب القضائي.

ثانيا:المقترحات

١. استحداث قانون خاص بالجرائم المعلوماتية يتضمن نصوصًا صريحة تُعرّف جريمة القرصنة الرقمية وتحدّد أركانها وعقوباتها بشكل دقيق و بما ينسجم مع مبدأ الشرعية الجنائية.

٢. تعديل قانون حق المؤلف العراقي رقم (٣) لسنة ١٩٧١ ليتضمن بابًا خاصًا بالحماية الرقمية للمصنفات الفكرية، أسوة بالتشريعات المقارنة.

٣. إنشاء محاكم أو دوائر قضائية متخصصة بالنظر في الجرائم الإلكترونية، مع تدريب القضاة والمحققين على آليات الإثبات الرقمي وحفظ البيانات.

٤. تعزيز التعاون الدولي لضمان الملاحقة العابرة للحدود للجناة الرقميين.

٥. تطوير الوعي القانوني والمجتمعي بمخاطر القرصنة الرقمية عبر حملات تثقيفية ومناهج أكاديمية تُبرز الأبعاد القانونية والاقتصادية لهذه الجريمة.

قائمة المصادر

اولا:المعاجم و الكتب اللغوية

١- المنجد في اللغة والإعلام، المطبعة الكاثوليكية، بيروت، ط٢٦، بدون سنة طبع.

ثانيا: الكتب

١. أحمد عودة، *الركن المعنوي في الجريمة المعلوماتية – دراسة مقارنة*، جامعة دمشق، ٢٠٢١.

٢. رائد كاظم، *الحماية الجنائية للبيئة الرقمية في القانون العراقي – دراسة مقارنة*، جامعة الكوفة، ٢٠٢١.

٣. فخري الحديثي، *القانون الجنائي ، القسم العام*، ط٤، بغداد، ٢٠١٢.

ثانيًا: الرسائل والأطاريح

سلطان فياض محمد، *جريمة انتهاك سرية المعلومات عبر الوسائط الإلكترونية*، رسالة ماجستير، جامعة الشرق الأوسط، ٢٠٢١.

شيلان محمد شريف، *الأحكام الموضوعية والإجرائية في جريمة الاحتيال الإلكتروني*، أطروحة دكتوراه، كلية القانون، جامعة السليمانية، ٢٠١٩.

ثالثًا: البحوث والمقالات العلمية

١. أسامة حسين محي الدين، *حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية – دراسة تحليلية مقارنة*، مجلة البحوث القانونية والاقتصادية، العدد ٧٦، ٢٠٢١.

٢. خالد المشهداني، *الجرائم المعلوماتية في التشريع العراقي – دراسة مقارنة*، مجلة القانون، جامعة بغداد، ٢٠٢٢.

٣. عبد الوهاب عبد الكريم محمد المبارك، *إشكالية المسؤولية القانونية عن جرائم النصب والاحتيال الإلكتروني الواقعة على عملاء البنوك*، المجلة القانونية، مصر، ٢٠٢٣.

٤. عطية عبد السلام الفيتوري، *جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلي*، مجلة الحق، العدد ٦، ٢٠١٧.

٥. متعب محمد مسعود آل حباب الهاجري، *جريمة القرصنة الإلكترونية في التشريع القطري – دراسة تحليلية مقارنة*، مجلة كلية الحقوق، جامعة الإسكندرية، العدد (٤٠)، ٢٠٢٣.

٦. محمد فؤاد الحريري، *الإطار القانوني لتجريم القرصنة الإلكترونية في مملكة البحرين*، مجلة القانون، العدد الثالث عشر، معهد الدراسات القضائية والقانونية، المنامة، ٢٠٢١.

٧. مروى السيد السيد، *الحماية الجنائية من جرائم الاعتداء على الملكية الفكرية للمصنفات الرقمية*، مجلة مستقبل العلوم الاجتماعية، العدد الثامن، ٢٠٢٢.

رابعًا: القوانين

١. قانون حق المؤلف العراقي رقم (٣) لسنة ١٩٧١ المعدّل بالأمر (٨٣) لسنة ٢٠٠٤، المادة (45).
قانون حماية حقوق الملكية الفكرية المصري رقم (٨٢) لسنة ٢٠٠٢

2. *Code de la Propriété Intellectuelle* 2023.
3. *Loi n°2009-669 relative à la diffusion et à la protection de la création sur internet (HADOPI)* 2009.

خامسًـــا: المصـــادر الأجنبيـــة

١-Ahmed Awda, *Cybercrime and Criminal Intent: A Comparative Analysis*, 2021.

٢-Ajoy P. B., *Developing an Analytical Definition of Cybercrime*, *IOSR Journal of Humanities and Social Science*, Vol. 29, Issue 1, Series 6, January 2024.

٣-Belleflamme, Paul & Peitz, Martin, *Digital Piracy*, *Encyclopedia of Law and Economics*, Springer, 2014.

٤-Gopal, R. D., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. C., *The Economics and Policy of Digital Content*, Elsevier Publishing, 2004.

٥-ITU, *Understanding Cybercrime: A Guide for Developing Countries*, Geneva, 2012.

٦-OECD, *Piracy of Digital Content*, Paris, 2009

٧-Pierre-Yves Gautier, *Propriété littéraire et artistique*, Dalloz, Paris, 2021.

٨-TU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, Geneva, 2020.

٩-UNODC, *Comprehensive Study on Cybercrime*, Vienna, 2013.