جريمة القرصنة الالكترونية في التشريع القطري
"دراسة تحليلية مقارنة"

الباحث

متعب محمد مسعود ال حباب الهاجري

الملخص:

يشكل تطور الجرائم الإلكترونية، وفي مقدمتها جريمة القرصنة الإلكترونية، أحد أبرز التحديات التي تواجه الأنظمة القانونية المعاصرة، نظرًا لما تتميز به هذه الجرائم من تعقيد تقني، وسرعة تطور، وقدرة على تجاوز الحدود الوطنية التقليدية. وقد جاءت هذه الدراسة لتسلّط الضوء على الإطار القانوني الناظم لجريمة القرصنة الإلكترونية في التشريع القطري، من خلال تحليل أركان الجريمة، واستعراض العقوبات المقررة لها، ومقارنة ذلك بالتشريعات المماثلة في بعض الدول العربية، كالإمارات ومصر والسعودية.

اعتمد البحث على منهجية قانونية متعددة، شملت المنهج التحليلي للنصوص القانونية القطرية، والمنهج المقارن مع التشريعات العربية الأخرى، إضافة إلى المنهج الوصفي لتأطير الظاهرة إجرائيًا وتقنيًا. وقد خلُصت الدراسة إلى أن القانون القطري رقم (14) لسنة 2014 يُمثل خطوة متقدمة في مواجهة الجرائم الإلكترونية، لكنه لا يزال يعاني من جوانب قصور أبرزها: غياب النصوص الخاصة بالشروع والمساهمة الجنائية، نقص العقوبات التكميلية، وضعف مواكبة صور الجريمة الرقمية الحديثة.

وقد قدم البحث عددًا من التوصيات الجوهرية، من أهمها: ضرورة تعديل القانون لتضمين نصوص صريحة حول الشروع والمشاركة في الجريمة، إدراج عقوبات تكميلية تتناسب مع طبيعة الجريمة الإلكترونية، تحديث نصوص القانون بشكل دوري لمواكبة التطورات التقنية، وتخصيص هيئات قضائية متخصصة في النظر في هذا النوع من الجرائم. إن هذه التوصيات تهدف إلى تعزيز فاعلية السياسة الجنائية القطرية، وتحقيق الحماية القانونية الكافية في الفضاء السيبراني، بما يتوافق مع المعايير التشريعية الحديثة.

الكلمات المفتاحية: القرصنة الإلكترونية، الجرائم الرقمية، القانون القطري، السياسة الجنائية، الأمن السيبراني، التشريع المقارن.

Abstract:

Cybercrimes, particularly cyber piracy, represent one of the most pressing legal challenges in the digital era. This research explores the legal framework governing the crime of cyber piracy under Qatari Law No. 14 of 2014 on Cybercrime, with a specific focus on analyzing its legal elements and associated penalties. The study also offers a comparative assessment with the legislative approaches of the United Arab Emirates, Egypt, and Saudi Arabia.

Adopting a multi-method legal approach—analytical, comparative, and descriptive—the research reveals that while the Qatari legislation marked an important step in criminalizing cyber activities, it still suffers from significant shortcomings. These include the absence of explicit provisions on attempt and complicity in cyber offenses, limited application of supplementary and preventive penalties, and insufficient coverage of modern forms of cyber piracy such as AI-based attacks and dark web crimes.

The study concludes with several critical recommendations: the necessity of amending the law to explicitly criminalize attempted and participatory cyber acts, introducing technologically tailored sanctions, establishing specialized prosecutorial and judicial units, and adopting a periodic legislative review mechanism. Such reforms are essential for enhancing Qatar's criminal policy and ensuring effective legal protection in the cyberspace, in line with contemporary legislative standards.

Keywords :Cyber piracy, Cybercrime, Qatari Law, Criminal Policy, Digital Security, Comparative Legislation**.**

المقدمة:

في بيئة قانونية تُبنى على مبادئ الشرعية واليقين، يواجه النظام الجنائي اليوم نوعًا مختلفًا من الجريمة؛ جريمة لا تطرق الأبواب، ولا تُرى بالأعين، ولا تخضع للحدود الجغرافية أو السيادة التقليدية. القرصنة الإلكترونية لم تعد مجرد فعل جنائي حديث، بل أصبحت معضلة قانونية حقيقية تُهدد البنية المعلوماتية للدول، وتُضعف هيبة الردع القانوني، وتُحرج أدوات العدالة الجنائية التقليدية.

لقد تجاوزت هذه الجريمة مرحلة "الفعل التقني "إلى كونها أداة سيطرة سياسية واقتصادية وأمنية. من سرقة البيانات السيادية إلى تعطيل البنية التحتية الرقمية للدول، أصبحت القرصنة الإلكترونية تمثل حربًا خفية تُدار من خلف الشاشات. أمام هذا الواقع، يُطرح سؤال جوهري: هل ما زالت النصوص الجنائية الحالية - ومنها القانون القطري رقم (14) لسنة 2014- قادرة على احتواء هذا الانفلات الإلكتروني؟

تكمن خطورة هذه الجريمة في ثلاث نقاط أساسية: أولًا، أنها جريمة عابرة للحدود، ما يجعل مسألة الاختصاص القضائي والملاحقة الجنائية موضع ارتباك دائم. ثانيًا، أنها تعتمد على أدوات تتطور أسرع من التشريعات ذاتها، مما يخلق فجوة خطيرة بين الواقع والردع. وثالثًا، أن مرتكبيها غالبًا ما يتمتعون بمهارات تقنية تفوق قدرات الأجهزة المكلفة بالمواجهة.

ورغم أن التشريع القطري أظهر اهتمامًا مبكرًا بمكافحة هذه الجرائم من خلال قانون مكافحة الجرائم الإلكترونية، فإن القراءة التحليلية لهذا القانون تكشف عن ثغرات في تحديد الأركان، وضعف في بناء العقوبات، وتكرار في الصياغة، إلى جانب غياب تنظيمي واضح لمسائل الشروع، والاشتراك، والمسؤولية عن البرامج المساعدة.

تهدف هذه الدراسة إلى تفكيك البنية القانونية لهذه الجريمة كما وردت في التشريع القطري، واستكشاف مدى كفايتها وفعاليتها، من خلال مقارنة علمية دقيقة مع أبرز التشريعات المقارنة، وعلى رأسها التشريع المصري والإماراتي. كما تسعى إلى بناء تصور تشريعي واقعي لمواجهة هذه الجريمة، بعيدًا عن اللغة الإنشائية، ومن خلال رصد الإشكاليات القانونية الحقيقية التي تواجه القضاة والمحققين والمشرعين. ولتحقيق ذلك، تعتمد الدراسة

على منهج تحليلي نقدي لنصوص القانون، ومنهج مقارن يرصد الفروقات الجوهرية في المعالجة، ومنهج واقعي يستند إلى ممارسات عملية وقضائية في هذا المجال.

أهمية البحث:

تكمن أهمية هذا البحث في عدة مستويات مترابطة:

أولًا: الأهمية القانونية: جريمة القرصنة الإلكترونية تمثل تحديًا مباشرًا لمبدأ الشرعية الجنائية، لأنها لا تخضع للتكييف القانوني التقليدي، ولا تنسجم مع مفاهيم الجريمة الكلاسيكية. هذا يفرض على التشريع القطري أن يُعيد النظر في بنيته القانونية لمواكبة تطور هذه الجريمة، سواء من حيث تحديد الأركان أو تنظيم العقوبات أو ضبط المسؤولية الجنائية. البحث يسعى لتقديم معالجة قانونية دقيقة تُسهم في سد هذه الفجوة التشريعية.

ثانيًا: الأهمية الأمنية والوطنية: القرصنة الإلكترونية لا تُهدد فقط الأفراد أو الكيانات التجارية، بل تمتد آثارها إلى البيانات السيادية، البنية التحتية للدولة، مؤسسات الأمن القومي، ما يجعل التصدي لها جزءًا من واجب الدولة في حماية أمنها الرقمي. وعليه، فإن تطوير الإطار القانوني لهذه الجريمة يُعد مسألة أمن وطني بالدرجة الأولى.

ثالثًا: الأهمية العلمية والبحثية: رغم مرور ما يقارب عقد على صدور القانون القطري رقم (14) لسنة 2014، ما زالت الدراسات العلمية المتخصصة في تحليل هذا القانون ومقارنته بتشريعات أكثر تطورًا محدودة. يأتي هذا البحث ليسد هذا النقص عبر معالجة تحليلية دقيقة، وتقديم مقارنة موضوعية تُثري الساحة البحثية القانونية الخليجية والعربية.

أهداف البحث:

يهدف هذا البحث إلى ما يلي:

1. تقديم تحليل قانوني دقيق لجريمة القرصنة الإلكترونية وفقًا للقانون القطري، من حيث التعريف، الأركان، والعقوبات.
2. تحديد مكامن القصور والثغرات التشريعية التي قد تعيق فعالية هذا القانون في ردع مرتكبي الجريمة.
3. مقارنة تشريعية عملية بين القانون القطري وعدد من التشريعات العربية، بهدف استخلاص نماذج تشريعية ناجحة يمكن الاستفادة منها.

4. تقديم رؤية نقدية واقعية تستند إلى الفقه والممارسة، من أجل تعزيز كفاءة المنظومة القانونية في مكافحة هذه الجريمة.
5. اقتراح توصيات تشريعية وتطبيقية قابلة للتنفيذ تساعد المشرّع وصنّاع القرار في تطوير أدوات المواجهة الجنائية الرقمية.

أشكالية البحث:

تُعاني التشريعات المعاصرة، ومنها التشريع القطري، من فجوة ملموسة بين التطور التقني المتسارع ومرونة النصوص الجنائية. وتتجلى مشكلة هذا البحث في محاولة تقييم مدى كفاية القانون القطري رقم (14) لسنة 2014 في مواجهة جريمة القرصنة الإلكترونية، ومدى قدرته على مجاراة التحديات التقنية والعملية التي تفرضها هذه الجريمة.

وينبثق من هذه المشكلة عدد من التساؤلات الجوهرية:

- ما مدى وضوح وتكامل النصوص القانونية القطرية في تعريف جريمة القرصنة الإلكترونية وتحديد أركانها؟
- هل تشكل العقوبات الواردة في القانون القطري رادعًا حقيقيًا في ضوء حجم التهديد؟
- ما أوجه النقص أو القصور مقارنة بالتشريعات العربية المقارنة (خاصة التشريع المصري والإماراتي)؟
- هل يتطلب الأمر تدخلاً تشريعيًا لتعديل أو تحديث قانون مكافحة الجرائم الإلكترونية في قطر؟

منهجية البحث:

من أجل الإجابة على الإشكالية المطروحة ولأجل تحقيق أهداف هذه الدراسة على الوجه الأفضل، ارتكزت الدراسة على **تعدد مناهجي** يحقق تغطية دقيقة للموضوع من مختلف الزوايا:

- **المنهج التحليلي**: تم من خلاله تفكيك نصوص القانون القطري ذات الصلة، وتحليل أبعادها الموضوعية والإجرائية.
- **المنهج المقارن**: لمقارنة التشريع القطري بنماذج عربية رائدة (التشريعات المصرية والإماراتية والسعودية) واستخلاص أوجه القوة والقصور.

- **المنهج الوصفي الواقعي**: لتوصيف طبيعة جريمة القرصنة الإلكترونية من حيث أساليبها وتطورها، وربط النصوص القانونية بالواقع العملي والتقني الذي تنشأ فيه الجريمة.

خطة البحث:

جاءت خطة البحث موزعة على ثلاثة فصول رئيسية تناولت بالدراسة والتحليل مختلف الجوانب القانونية لجريمة القرصنة الإلكترونية، بدءًا بالإطار المفاهيمي والنظري للجريمة، مرورًا بتحليل أركانها القانونية والعقوبات المقررة لها، وانتهاءً بتقييم شامل لمدى كفاية السياسة الجنائية القطرية في مواجهتها.

الفصل الأول: الإطار النظري لجريمة القرصنة الإلكترونية

- المبحث الأول: التعريف الفقهي والقانوني للقرصنة الإلكترونية.
- المبحث الثاني: صور وأشكال جريمة القرصنة الإلكترونية.
- المبحث الثالث: أسباب انتشار هذه الجريمة وخصائصها.

الفصل الثاني: الأركان القانونية لجريمة القرصنة الإلكترونية

- المبحث الأول: الركن المادي.
- المبحث الثاني: الركن المعنوي.
- المبحث الثالث: الركن الشرعي والمحل.

الفصل الثالث: العقوبات القانونية لجريمة القرصنة الإلكترونية

- المبحث الأول: العقوبات في التشريع القطري (قانون 2014/14).
- المبحث الثاني: العقوبات في التشريعات المقارنة (مصر – الإمارات – السعودية).
- المبحث الثالث: تقييم مدى كفاية العقوبات وتحليل فجوات التجريم والعقاب.
- المبحث الرابع: أوجه القوة والقصور في السياسة الجنائية القطرية.

الخاتمة: النتائج والتوصيات .

المراجع

الفصل الأول: الإطار النظري لجريمة القرصنة الإلكترونية

المبحث الأول: التعريف الفقهي والقانوني لجريمة القرصنة الإلكترونية

تمهيد:

مع تصاعد الاعتماد على الوسائط الإلكترونية في إدارة شؤون الأفراد والمؤسسات، برزت تهديدات مستحدثة تتجاوز الجريمة التقليدية، وتتطلب مقاربات قانونية جديدة. جريمة القرصنة الإلكترونية ليست مجرد فعل تقني غير مشروع، بل هي نموذج على تحوّل الجريمة إلى شكل جديد يهاجم البنى المعلوماتية للدول والأشخاص. من هنا، بات تحديد تعريف دقيق لها ضرورة علمية وتشريعية ملحّة، وهو ما يتطلب الجمع بين الرؤية الفقهية والتحليل القانوني المقارن.

أولًا: التعريف الفقهي لجريمة القرصنة الإلكترونية

اتفق الفقه الجنائي على أن مصطلح "القرصنة الإلكترونية" يُستخدم للإشارة إلى كل فعل عدواني يتم من خلال الوسائل التكنولوجية بهدف اختراق الأنظمة الرقمية دون وجه حق. ويكاد يجمع الفقهاء على أن جوهر هذه الجريمة يكمن في الدخول غير المشروع إلى نظام معلوماتي أو شبكة محمية بقصد الوصول إلى بيانات أو التلاعب بها أو إتلافها أو استغلالها. وقد عرفها بعض الباحثين بأنها: "عملية اختراق لأنظمة إلكترونية، تتم عبر الإنترنت غالبًا، ويقوم بها شخص أو مجموعة أشخاص يمتلكون مهارات تقنية تتيح لهم تجاوز نظم الحماية للوصول إلى المعلومات، سواء بقصد الإتلاف أو السرقة أو التجسس أو الابتزاز"[1].

ويُلاحظ من هذا التعريف الفقهي أن هذه الجريمة تتميز بعدة خصائص رئيسية، أولها أنها تقوم على التعدي غير المشروع على نظم تقنية محمية، حيث يتجاوز الجاني الحدود القانونية المقررة لحماية هذه الأنظمة. كما تتميز بوجود نية عدوانية أو إرادة إجرامية متعمدة تدفع الفاعل إلى ارتكاب هذا السلوك. ولا يُتصور قيام هذه الجريمة دون وجود وسيلة إلكترونية تُعد عنصرًا لازمًا في تنفيذ الفعل، كاستخدام الحواسيب أو الشبكات الرقمية. وأخيرًا، فإن

(1) رامي متولي القاضي: "المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون (175) لسنة 2018م مقارناً بالمواثيق الدولية والتشريعات المقارنة"، مجلة البحوث القانونية والاقتصادية، العدد 45، مارس 2021، كلية الحقوق، جامعة المنصورة، مصر، 2021، ص998 وما بعدها.

هذه الأفعال تؤدي إلى نتائج ضارة، سواء تمثلت في ضرر مباشر مثل إتلاف البيانات أو تعطيل النظام، أو ضرر غير مباشر يتمثل في المساس بالأمن المعلوماتي أو تهديد الخصوصية والسرية الرقمية[1].

وتذهب بعض الآراء الفقهية إلى تصنيف القرصنة ضمن "جرائم الاعتداء على الأموال الرقمية"، بينما يعتبرها آخرون "جرائم ضد أمن الدولة الرقمي" في حال استهدفت نظمًا سيادية أو مؤسسات حيوية[1].

ثانيًا: التعريف القانوني للقرصنة الإلكترونية

في التشريع القطري نص القانون رقم (14) لسنة 2014 بشأن مكافحة الجرائم الإلكترونية في مادته الثانية على تجريم الدخول غير المشروع إلى الأنظمة المعلوماتية: "الدخول عمدًا، دون وجه حق، بأي وسيلة، إلى موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية... أو تجاوز الدخول المصرح به، أو الاستمرار في التواجد بها بعد العلم بعدم أحقية البقاء"[2]. ويُلاحظ أيضًا أن المشرع القطري اعتمد على مفهوم الدخول غير المشروع كأساس لتعريف الجريمة، دون تقديم تعريف جامع لمفهوم "القرصنة الإلكترونية" بمفهومها المركب، مما يُعد من أوجه القصور التشريعي[3].

---

(1) سيف مجيد العاني: "مسئولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي دراسة مقارنة"، دروب المعرفة للنشر والتوزيع، الأسكندرية، مصر، 2022، ص79.

(2) قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014

المادة (2) من قانون مكافحة الجرائم الإلكترونية القطري تنص على:

"يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة، أو مؤسساتها، أو هيئاتها، أو الجهات، أو الشركات التابعة لها."

كما تنص المادة (3) على:

"يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات من الدخول بدون وجه حق إلى موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد العلم بعدم أحقية البقاء، وترتب على ذلك إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف، أو تغيير، أو نقل أو نسخ أو إعادة نشر البيانات أو المعلومات، أو تدمير أو تعطيل الموقع أو النظام أو تعديل محتوياته أو تصميماته.

"تنص المادة (4) على:

"يعاقب كل من التقط أو اعترض أو تنصت عمدًا، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور."

(3) عبد الله دغش العجمي: "المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2014، ص20.

في التشريع المصري استخدم قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018 [1] مصطلح "الدخول غير المشروع"، وجرّم في المادة (14) أفعال الدخول العمد أو غير العمد على مواقع أو أنظمة معلوماتية دون تصريح، مع تشديد العقوبة حال اقتران الدخول بإتلاف أو نسخ أو تعديل البيانات. إلا أن المشرع المصري تميز نسبيًا بتقديم تفصيلات أوسع لحالات التعدي الإلكتروني، وربط النص بالعقوبات بشكل أكثر وضوحًا، مما يساهم في وضوح التكييف القضائي للجريمة [1].

في التشريع الدولي، اعتمدت اتفاقية بودابست لمكافحة الجرائم الإلكترونية (2001) مفهوم "التدخل غير المشروع في البيانات أو النظم"، وعرّفت ذلك من خلال عدة مواد. فقد نصت المادة 2 على تجريم "الدخول، عند ارتكابه عمدًا، إلى النظام الحاسوبي أو أي جزء منه دون حق"، سواء تم ذلك باختراق تدابير الأمان أو بنية غير شريفة. كما نصت المادة 3 على تجريم "الاعتراض، عند ارتكابه عمدًا، دون حق، وبوسائل تقنية، للبيانات الحاسوبية غير العامة أثناء انتقالها". وفي المادة 4، اعتبرت الاتفاقية أن "الإضرار أو الحذف أو التدهور أو التعديل أو القمع للبيانات الحاسوبية دون حق، عند ارتكابه عمدًا"، يُعد جريمة تستوجب التجريم. أما المادة 5، فقد وسّعت دائرة الحماية القانونية لتشمل النظام ككل، بنصها على "تجريم الإعاقة الجدية، عند ارتكابها عمدًا، دون حق، لوظيفة نظام حاسوبي من خلال إدخال أو نقل أو إتلاف أو حذف أو تدهور أو تعديل أو قمع البيانات الحاسوبية"[2].

---

(1) قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

- تنص المادة (14): "يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه."

(2) اتفاقية بودابست لمكافحة الجرائم الإلكترونية (2001)

➢ المادة 2- الدخول غير المشروع (Illegal Access)

"يتعين على كل طرف أن يتخذ التدابير التشريعية وغيرها من التدابير اللازمة لتجريم الدخول، عند ارتكابه عمدًا، إلى النظام الحاسوبي أو أي جزء منه دون حق. يجوز للطرف أن يشترط أن تكون الجريمة قد ارتُكبت من خلال اختراق تدابير الأمان، أو بنية الحصول على بيانات حاسوبية أو بنية غير شريفة أخرى، أو فيما يتعلق بنظام حاسوبي متصل بنظام حاسوبي آخر."

- المادة 3- الاعتراض غير المشروع (Illegal Interception)

"يتعين على كل طرف أن يتخذ التدابير التشريعية وغيرها من التدابير اللازمة لتجريم الاعتراض، عند ارتكابه عمدًا، دون حق، وبوسائل تقنية، للبيانات الحاسوبية غير العامة أثناء انتقالها إلى أو من أو داخل نظام حاسوبي، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام حاسوبي يحمل مثل هذه البيانات. يجوز للطرف أن يشترط أن تكون الجريمة قد ارتُكبت بنية غير شريفة، أو فيما يتعلق بنظام حاسوبي متصل بنظام حاسوبي آخر."

- المادة 4- التدخل في البيانات (Data Interference)

1. "يتعين على كل طرف أن يتخذ التدابير التشريعية وغيرها من التدابير اللازمة لتجريم الإضرار، أو الحذف، أو التدهور، أو التعديل، أو القمع للبيانات الحاسوبية دون حق، عند ارتكابه عمدًا."

هذا التعريف الدولي يختلف عن بعض التعريفات العربية، كونه يربط بين السلوك التقني (كالاختراق أو التعديل) والنية العدوانية (العمدية)، ويوسّع من نطاق الحماية القانونية ليشمل البيانات ذاتها، وليس فقط النظام المعلوماتي.[1]

ثالثًا: تقييم وملاحظات تحليلية

عند المقارنة بين التعريفات الفقهية والقانونية، يمكن استخلاص النقاط التالية:

- غياب تعريف تشريعي صريح في القانون القطري: عدم وجود تعريف واضح لمصطلح "القرصنة الإلكترونية" في القانون القطري يفتح المجال أمام تضارب التفسير القضائي، خاصة في ظل تداخل المصطلحات مثل "الدخول غير المشروع"، "الاعتداء على سلامة الشبكة"، و"التنصت على البيانات" [4].
- الفقه القانوني أوسع وأعمق من النصوص القانونية: الفقه القانوني يقدم توصيفًا أكثر شمولية للجريمة، مما يستدعي من المشرع القطري استلهام الرؤية الفقهية لتعريف جامع يُسهل على القضاء والضبط القضائي التعامل مع الوقائع [1].
- اتفاقية بودابست كمرجع تشريعي مهم: تمثل اتفاقية بودابست مرجعًا تشريعيًا مهمًا، وقد آن الأوان لأن يُعدّل التشريع القطري بما يتوافق مع نصوصها، خاصة وأنها تُجسد المعايير الدولية في تعريف الجرائم الرقمية [7].
- ضرورة إعادة النظر في التعريفات القانونية السائدة: نستنتج أن جريمة القرصنة الإلكترونية تُشكّل نمطًا جديدًا من الإجرام المعقّد، يتطلب إعادة النظر في التعريفات القانونية السائدة. إن التعريف الفقهي للجريمة يقدّم رؤية دقيقة تفتقدها كثير من النصوص التشريعية، وعلى رأسها القانون القطري، مما يجعل تبني تعريف قانوني جامع، يجمع

2. "يجوز للطرف أن يحتفظ بالحق في اشتراط أن يؤدي السلوك الموصوف في الفقرة 1 إلى ضرر جسيم."

- المادة 5- التدخل في النظام (System Interference)

"يتعين على كل طرف أن يتخذ التدابير التشريعية وغيرها من التدابير اللازمة لتجريم الإعاقة الجدية، عند ارتكابها عمدًا، دون حق، لوظيفة نظام حاسوبي من خلال إدخال، أو نقل، أو إتلاف، أو حذف، أو تدهور أو تعديل أو قمع البيانات الحاسوبية."

[1] Council of Europe. (2001). Convention on Cybercrime (ETS No. 185).

بين الوضوح والمرونة، ضرورة لا ترفًا، وذلك لضمان تماسك النظام الجنائي الرقمي وقدرته على الاستجابة للتحديات المستحدثة.

المبحث الثاني: صور وأشكال جريمة القرصنة الإلكترونية

تمهيد:

تتمثل خطورة جريمة القرصنة الإلكترونية في تعدد صورها واختلاف طرائق ارتكابها، مما يجعل مكافحتها أكثر تعقيدًا من الجرائم التقليدية. فهذه الجريمة ليست محصورة في صورة واحدة أو قالب نمطي، بل تتنوع بتنوع أهداف القراصنة وقدراتهم التقنية. ومن هنا، فإن الإلمام بصورها يُعد شرطًا لازمًا لفهم أركان الجريمة، وتكييفها قانونيًا، والتصدي لها بفاعلية. وسوف يتم في هذا المبحث استعراض أبرز صور القرصنة الإلكترونية، وفقًا لما أوردته التشريعات المختلفة والفقه المقارن، وهي: الدخول غير المشروع، الاعتراض غير المشروع، الاعتداء على سلامة النظم، والقرصنة المتقدمة ذات الطابع السيادي أو التجاري.[1]

أولًا: الدخول غير المشروع إلى الأنظمة المعلوماتية

يُعد الدخول غير المشروع الصورة الأساسية والأكثر شيوعًا لجريمة القرصنة الإلكترونية، وهو ما يشكل نقطة الانطلاق في معظم عمليات القرصنة، سواء كانت تهدف لاحقًا إلى الإتلاف أو السرقة أو حتى مجرد الاستطلاع. وقد نص القانون القطري رقم (14) لسنة 2014 في مادته الثانية على تجريم هذا الفعل بعبارة صريحة، حيث عرّفه بأنه: "الدخول عمدًا، دون وجه حق، بأي وسيلة، إلى موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية، أو تجاوز الدخول المصرح به، أو الاستمرار في التواجد بها بعد العلم بعدم أحقية البقاء" ويماثله في ذلك القانون المصري رقم (175) لسنة 2018، الذي شدد العقوبة في حالة اقتران الدخول غير المشروع بأفعال أخرى كالإتلاف أو النسخ أو الحذف. وهذا الفعل يُعتبر من الجرائم الشكلية التي تكتمل بمجرد ارتكاب السلوك دون الحاجة إلى تحقق نتيجة ضارة، على خلاف بعض الصور الأخرى التي يُشترط فيها تحقق الضرر المادي أو المعنوي. وقد

(1) مرفت محمود طيب، "الجريمة الإلكترونية وأنواعها وأشكالها وأدواتها ودوافعها وطرق مكافحتها والعقوبات القانونية لها"، المركز العربي لأبحاث الفضاء الإلكتروني، نُشر في 12 نوفمبر 2017.

اعتبر الفقه أن هذه الصورة تُعبّر عن انتهاك مباشر للحق في حماية الأنظمة المعلوماتية من التسلل غير المشروع، حتى وإن لم يترتب عليه مساس فعلي بالبيانات، لأن مجرد التواجد غير المصرح به يُمثل خطرًا حقيقيًا على سلامة النظام.

ثانيًا: الاعتراض أو التنصت غير المشروع على البيانات

الاعتراض غير المشروع هو الصورة الثانية من صور القرصنة، وتتمثل في التقاط البيانات أو التنصت عليها أثناء انتقالها عبر الشبكة المعلوماتية، سواء كانت بيانات شخصية أو تجارية أو أمنية. وهي من أكثر الأفعال شيوعًا في جرائم التجسس والابتزاز. نصت المادة (4) من قانون الجرائم الإلكترونية القطري على أن: "يعاقب كل من التقط أو اعترض أو تنصت عمدًا، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور".

كما أورد القانون المصري في المادة (16) تجريمًا مشابهًا، واعتبر أن الاعتراض غير المشروع يُعد من الأفعال التي تمثل انتهاكًا للسرية الرقمية[1]. وتُعد هذه الجريمة من الجرائم ذات الطابع الإيجابي السلبي؛ أي أنها تُرتكب بوسائل سلبية (كالمراقبة الصامتة) لكنها تؤدي إلى نتائج بالغة الخطورة، خاصة في سياق التسريبات أو الابتزازات السياسية والإعلامية[2]

ثالثًا: الاعتداء على سلامة البيانات والنظم المعلوماتية

يُقصد به كل فعل يؤدي إلى تعطيل، أو إتلاف أو تشويه أو تعديل البيانات أو البرامج أو الأنظمة المعلوماتية، ويُعد من أكثر أشكال القرصنة ضررًا وتأثيرًا، خصوصًا إذا استهدف نظمًا حيوية (كأنظمة الصحة أو الطاقة أو البنوك). تُجرّم المادة (2/3) من القانون القطري هذا الفعل بوضوح، حيث شددت العقوبة في حال ترتب على الدخول غير المشروع أفعال

(1) قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، جمهورية مصر العربية، المادة (16): "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها."

(2) مريم بالطة، آسيا برغيت: "الأمن المعلوماتي في مواجهة القرصنة الالكترونية"، بحث منشور في مجلة دراسات حقوق الإنسان، المجلد 7، العدد 1، جوان 2022، جامعة كسكيدة، الجزائر، ص14.

مثل: "إلغاء، حذف، إضافة، إفشاء، إتلاف، تغيير، نقل، نسخ، أو إعادة نشر البيانات، أو تدمير أو تعطيل الموقع أو النظام، أو تعديل محتوياته أو تصميماته.

وتنص المادة (21) من القانون المصري على أن: "يعاقب كل من أوقف أو عطّل أو حدّ من كفاءة شبكة معلوماتية أو نظام معلوماتي عن العمل بدون وجه حق"[1]. وتقع هذه الجريمة غالبًا في سياق الهجمات المتعمدة ضد البنية التحتية الرقمية، وتُستخدم أحيانًا لأغراض إرهابية أو اقتصادية كبرى، كما في حالات "هجمات الفدية" أو "تخريب قواعد البيانات السيادية" [2]

رابعًا: القرصنة ذات الطابع المتقدم – (الهجمات السيادية أو التجارية)

وهذه الصورة لم تُنظَّم صراحة في معظم التشريعات العربية، رغم أنها تمثل اليوم أكثر صور القرصنة تقدمًا وخطورة. وتشمل:

- القرصنة الموجهة ضد أنظمة الدولة كاختراق نظم الجوازات أو الانتخابات أو البيانات الأمنية.
- القرصنة الصناعية والتجارية بهدف التجسس على براءات اختراع أو سرقة أسرار شركات أو بنوك.
- القرصنة الممولة دوليًا أو عسكريًا وهي التي تُدار من قبل جهات استخباراتية أو حكومات، غالبًا لأهداف استراتيجية.

ويرى بعض الفقهاء أن هذه الصورة من الجرائم تُصنف ضمن ما يُعرف بـ"العدوان الرقمي"، ويجب أن تُقابل ليس فقط برد جنائي، بل أيضًا بإجراءات سيادية وأمنية متقدمة. ويُلاحظ أن التشريع القطري لم يفرد تنظيمًا مستقلًا لهذه الصور المتقدمة، رغم أن الواقع

(1) (قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات المصري، المادة 21)
"يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمدًا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها."

(2) نجاة دحو، فاطمة أولاد على: "جريمة القرصنة الالكترونية في التشريع الجزائري"، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة غرداية، الجزائر، 2021-2022، ص7.

العملي بات يفرض ضرورة الاعتراف بها وتجريمها بنصوص صريحة، خاصة في ظل تزايد حالات استهداف الأنظمة السيادية في عدد من الدول الخليجية [1].

في الختام نستنتج أن تتعدد صور جريمة القرصنة الإلكترونية ما بين الدخول غير المشروع، الاعتراض، الإتلاف، والاختراق الاستراتيجي، وهو ما يستوجب أن يكون النظام القانوني مرنًا وشاملًا بما يكفي لتغطية كل هذه الصور. ويُلاحظ أن التشريع القطري، رغم تقدمه النسبي، لا يزال بحاجة إلى توسيع وتعميق نطاق التجريم لاحتواء الصور المستحدثة من الجريمة الرقمية، وخاصة تلك ذات الطابع المتقدم والعابر للحدود[2].

المبحث الثالث: أسباب انتشار جريمة القرصنة الإلكترونية وخصائصها

تمهيد:

إن فهم الدوافع والخصائص البنيوية لجريمة القرصنة الإلكترونية ليس ترفًا نظريًا، بل ضرورة حيوية لصياغة أدوات قانونية وتشريعية فعّالة. فكل جريمة لا تولد في فراغ، بل تنمو ضمن بيئة تقنية واجتماعية واقتصادية تغذيها وتمنحها أدوات النمو. والقرصنة الإلكترونية، على وجه الخصوص، تُعد نتاجًا مباشرًا لعصر الانفجار الرقمي، وتُمارس بطرق تتجاوز قدرة التشريعات التقليدية على الاستيعاب والردع. وعليه، يتناول هذا المبحث محورين أساسيين: أولًا، الأسباب الجوهرية لانتشار هذه الجريمة؛ وثانيًا، الخصائص التي تجعلها جريمة نوعية ومركبة وخطيرة من منظور قانوني وتشريعي.[3]

أولًا: أسباب انتشار جريمة القرصنة الإلكترونية

تتعدد الأسباب التي ساهمت في تفشي هذه الجريمة، إلا أن الفقه والواقع يُجمعان على وجود أربعة دوافع رئيسية وهما ضعف الوازع الأخلاقي والتربوي أشارت دراسات متخصصة إلى أن غياب الضوابط القيمية الداخلية عند بعض الأفراد – خاصة صغار السن أو المراهقين – يؤدي إلى تجاوز الخطوط القانونية والأخلاقية في البيئة الرقمية، سواء بدافع اللهو أو

(1) أحمد معاذ أحمد عبد الرازق: "أمن المعلومات ودوره في الحد من القرصنة الإلكترونية"، المركز القومي للمعلومات، رسالة ماجستير، معهد بحوث ودراسات العالم الإسلامي، جامعة أم درمان الإسلامية، السودان، 2016، ص23.

(2) فيصل بدري: "مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي: أطروحة مقدمة لنيل شهادة علوم تخصص قانون عام"، كلية الحقوق، جامعة الجزائر، 2018، ص29.

(3) خليل، محمد. (2020). السياسة الجنائية في مواجهة الجرائم الإلكترونية: دراسة مقارنة. القاهرة: دار النهضة العربية.

الفضول أو الانتقام. ويتجلى هذا العامل بوضوح في المجتمعات التي لم تُواكب التوسع الرقمي ببنية تربوية قائمة على ثقافة احترام الخصوصية الرقمية وحرمة البيانات.

الدوافع الاقتصادية وسهولة الربح غير المشروع تُعد القرصنة الإلكترونية وسيلة "مغرية" للكسب السريع دون مخاطرة مباشرة. فالجريمة يمكن أن تُنفّذ عن بُعد، من غرفة مغلقة، ضد هدف في دولة أخرى، مما يُضعف احتمالية الملاحقة القانونية، ويُضخم العائد المادي، وتزداد هذه الدوافع حدة في البيئات التي تعاني من ارتفاع معدلات البطالة أو ضعف التوعية القانونية.

التطور التقني وسهولة الوصول إلى أدوات الاختراق لم تعد أدوات الاختراق والقرصنة حكرًا على "العباقرة الرقميين"، بل أصبحت متاحة بسهولة عبر الإنترنت، إما مجانًا أو بثمن زهيد، بل إن بعض المواقع تُقدم "خدمات قرصنة مدفوعة" وفق طلب العميل. كما أن تطور البرامج الخبيثة وظهور ما يُعرف بـ"الهاكرز كخدمة" (Hacking-as-a-Service) ساهم في تحويل الجريمة إلى نشاط رقمي منظم وشبه احترافي.[1]

نقص الخبرة التقنية لدى الأجهزة الأمنية والقضائية تواجه معظم الدول تحديًا حقيقيًا يتمثل في الفجوة الواسعة بين قدرات القراصنة من جهة، والمهارات التقنية المتوفرة لدى جهات الضبط والتحقيق من جهة أخرى. هذا الخلل يجعل ملاحقة الجريمة أصعب، ويزيد من جرأة مرتكبيها. كما أن كثيرًا من الضحايا -أفرادًا ومؤسسات- لا يُبلّغون عن الجرائم الإلكترونية خوفًا من الفضيحة أو ضعف الثقة في جدوى الملاحقة.

ثانيًا: خصائص جريمة القرصنة الإلكترونية

تتمتع هذه الجريمة بجملة من الخصائص التي تجعلها فريدة في بنيتها القانونية والاجتماعية، وأبرزها جريمة عابرة للحدود الجغرافية تتم ممارستها عبر شبكة الإنترنت، ما يجعل تحديد

(1) الموسوي، أحمد حسن. (2021). الجرائم الإلكترونية وسبل مكافحتها في التشريع العربي المقارن. بيروت: المركز العربي للبحوث القانونية والقضائية.

الاختصاص القضائي معقدًا، ويُثير مشكلات حقيقية في التعاون الدولي، خاصة إذا كان الجاني في دولة لا تُجرّم الفعل أو لا تربطها مع الدولة المتضررة اتفاقيات تعاون قانوني[1].

جريمة ناعمة غير عنيفة ولكنها مدمّرة لا تتطلب هذه الجريمة استخدام العنف أو التواجد في مسرح مادي، ما يصعب اكتشافها ميدانيًا. فهي تُرتكب من خلال "نقرة زر"، ولكن قد تؤدي إلى نتائج كارثية، مثل تدمير بنوك بيانات، أو تعطيل أنظمة ملاحة، أو تسريب معلومات أمنية حساسة[2].

سرعة تطور وسائل ارتكابها مقارنة بسرعة تعديل القوانين الواقع يؤكد أن القوانين تتخلف دائمًا عن وتيرة تطور الجرائم الإلكترونية. فبينما يُطور القراصنة أدواتهم يومًا بعد يوم، تبقى النصوص القانونية جامدة، وتعتمد في الغالب على التوصيفات التقليدية التي قد لا تستوعب الصورة الجديدة للجريمة. هذا الفارق الزمني بين تطور الجريمة وتطور القوانين يجعل من الصعب على المشرعين مواكبة التغيرات السريعة في أساليب القرصنة.

صعوبة الإثبات وكثرة "الرقم المظلم" كثير من جرائم القرصنة لا تُكتشف أصلًا، أو تُكتشف متأخرة، أو لا يتم التبليغ عنها، مما يجعل الإحصائيات الرسمية أقل بكثير من الواقع الفعلي. وتُعرف هذه الفجوة في علم الإجرام بـ"الرقم المظلم"، وهي تحدٍ بارز أمام الباحثين والمشرعين[3]. هذه الظاهرة تعكس عدم الثقة في قدرة الأنظمة القانونية على حماية الأفراد والمؤسسات، مما يؤدي إلى تفشي الجريمة بشكل أكبر.

فى الختام نستخلص أن جريمة القرصنة الإلكترونية لا تنشأ فقط من خلل فردي، بل هي نتاج تفاعل اجتماعي وتقني واقتصادي وتشريعي معقد، يتطلب مقاربة قانونية متكاملة. كما أن طبيعتها الخاصة -من حيث الأدوات والخصائص- تجعلها واحدة من أكثر الجرائم حاجة

(1) "الجرائم الإلكترونية القرصنة الإلكترونية"، مجلة فضاء المعرفة القانونية، 15 نوفمبر 2023.

(2) سعاد شاكر بعيوي: "جريمة الابتزاز الالكتروني - دراسة مقارنة"، مجلة ميسان الدراسات القانونية المقارنة، كلية القانون، جامعة ميسان، المغرب، 2019م، ص126.

(3) حسون عبيد هجيج، صفاء كاظم غازي: "آثار جريمة قرصنة البريد الالكتروني"، مجلة القادسية للقانون والعلوم السياسية، جامعة القادسية، العراق، العدد الثاني، المجلد السابع، كانون الأول، 2016، ص171-212.

إلى تحديث تشريعي مستمر وتعاون دولي فعّال. وبدون إدراك هذه الأسباب والخصائص، تبقى المواجهة القانونية غير فعّالة ومحدودة التأثير[1].

الفصل الثاني: الأركان القانونية لجريمة القرصنة الإلكترونية

المبحث الأول: الركن المادي

تمهيد:

يُعد الركن المادي أحد الأركان الجوهرية في بناء الجريمة، إذ لا يُتصور قيام مسؤولية جنائية في غياب سلوك مادي يُشكل اعتداءً على القيم المحمية قانونًا. وفي جريمة القرصنة الإلكترونية، يتخذ هذا الركن طابعًا خاصًا نابعًا من طبيعة الوسيلة المستخدمة (الوسائل التقنية) وطبيعة المصلحة المعتدى عليها (البيانات الرقمية، النظم المعلوماتية، الخصوصية). لذا يُعد فهم طبيعة الركن المادي في هذه الجريمة شرطًا أساسيًا لضمان التكييف القانوني السليم ولإثبات الجريمة أمام القضاء.

أولًا: مفهوم الركن المادي في الجريمة الإلكترونية

الركن المادي هو السلوك الإجرامي الظاهر الذي يتجسد في أفعال أو امتناعات تمثل الاعتداء الجنائي. ويتكوّن – في عموم الجرائم – من ثلاثة عناصر رئيسية: السلوك الإجرامي، الذي يتمثل في الفعل أو الامتناع؛ والنتيجة الإجرامية، التي تعبر عن الأثر الضار الذي يترتب على السلوك؛ وعلاقة السببية، التي تمثل الرابط بين الفعل والنتيجة. غير أن هذا التصور الثلاثي قد لا ينطبق دائمًا بنفس الكيفية على الجرائم الإلكترونية، وخصوصًا جريمة القرصنة، التي قد تتحقق بمجرد السلوك – أي الدخول غير المشروع – حتى دون أن تتحقق نتيجة ضارة مادية. لذلك، تُعد من الجرائم الشكلية أو الجرائم ذات النتيجة المفترضة في بعض صورها[2].

---

[1] شيرين دبابنة: "الجرائم الالكترونية، القرصنة الالكترونية"، مجلة الدراسات المالية والمصرفية، مجلد 23، ع1، مجلد الأكاديمية العربية للعلوم المالية والمصرفية، مركز البحوث المالية والمصرفية، الأردن، 2015، ص19.

[2] خالد سليمان عبد الله الحمادي: جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة قطر، 2019.

ثانيًا: صور السلوك المكون للركن المادي في جريمة القرصنة

السلوك المجرّم الذي يُكوّن الركن المادي في القرصنة الإلكترونية يتخذ صورًا متنوعة، وقد نص القانون القطري رقم (14) لسنة 2014 على أبرزها، ومنها:

1. الدخول غير المشروع إلى النظام المعلوماتي: يُعتبر الدخول غير المشروع إلى النظام المعلوماتي الصورة الكلاسيكية التي تتأسس عليها أغلب جرائم القرصنة. وهو يُعد فعلًا ماديًا قائمًا بذاته، لا يُشترط فيه أن يترتب عليه ضرر لاحق. وقد نصت المادة الثانية من القانون القطري على أن الجريمة تتحقق إذا تم الدخول عمدًا، دون وجه حق، بأي وسيلة إلى موقع إلكتروني أو نظام معلوماتي، أو تجاوز الدخول المصرح به. ويعكس ذلك أن السلوك المادي هنا هو فعل إيجابي يتمثل في "الدخول أو البقاء" غير المشروع في بيئة رقمية محمية. وقد أكد الفقه أن هذه الصورة من السلوك لا تتطلب تحقق نتيجة ضارة، وتُعد جريمة شكلية يعاقب فيها القانون على الفعل ذاته، وهو ما يجسد فلسفة "الردع الوقائي" في الجرائم الرقمية[1].
2. التعدي على سلامة البيانات أو النظام: يأخذ السلوك المادي هنا صورة أفعال مثل الحذف، الإتلاف، النقل، التعديل، أو النشر غير المشروع للبيانات. وقد ورد هذا في الفقرة الثانية من المادة (3) من القانون القطري، واعتبر المشرّع أن هذه الأفعال تمثل ظروفًا مشددة إذا اقترنت بالدخول غير المشروع. ويُعد هذا النوع من السلوك أكثر خطورة من مجرد الدخول، لأنه يُفضي إلى نتيجة إجرامية ملموسة، ويُعد من الجرائم ذات النتيجة، وتُشترط فيه علاقة سببية بين الفعل والأثر.
3. الاعتراض أو التنصت على البيانات: تأخذ هذه الصورة شكل التقاط بيانات أثناء انتقالها في الشبكة، سواء بالنسخ أو التنصت أو التصنت الإلكتروني. وقد نصت عليها المادة (4) من القانون القطري، باعتبارها أفعالًا إيجابية تشكل تدخلًا غير مشروع في حق الغير بالخصوصية. كما أشار بعض الباحثين إلى أن هذا السلوك يشبه من حيث البناء

[1] الرواشدة، سامي حمدان. (2019). "جريمة الدخول غير المشروع للأنظمة المعلوماتية في القانون الجنائي القطري: دراسة مقارنة". مجلة كلية القانون الكويتية العالمية.

القانوني "جريمة اعتراض المراسلات التقليدية"، لكن بوسائل رقمية حديثة، مما يستوجب تكييفًا قانونيًا يراعي خصوصية الوسيلة والبيئة الرقمية.

ثالثًا: النتيجة الإجرامية وعلاقتها بالسلوك

كما سبق الإشارة، فإن النتيجة ليست عنصرًا لازمًا في جميع صور جريمة القرصنة. ففي صورة الدخول غير المشروع، تُعد النتيجة مفترضة، لأن الجريمة تُعاقب عليها لمجرد وقوع السلوك، دون اشتراط تحقق ضرر فعلي أما في الصور الأخرى، مثل الإتلاف أو التعديل أو النشر، فإن تحقق نتيجة ضارة مادية - كتعطيل النظام، تلف البيانات، أو تسريب المعلومات - يشكل شرطًا لقيام الجريمة، ويرتبط به تشديد العقوبة وهنا يتطلب الأمر إثبات علاقة سببية مباشرة بين الفعل والسلوك الضار، وهو ما يعتبر تحديًا تقنيًا يصعب تحقيقه إلا بواسطة خبراء متخصصين وبتقنيات تحقيق متقدمة[1].

رابعًا: تقييم موقف القانون القطري

يرى الباحث أن القانون القطري - على الرغم من كونه من أوائل القوانين في الخليج التي صدّت للقرصنة الإلكترونية - ما زال تصور الركن المادي فيه بحاجة إلى مزيد من الدقة والتفصيل. فلم يتم تفصيل وتعريف كل سلوك مجرّم على حدة، كالدخول غير المشروع والاعتراض والتعديل غير المشروع. كما أن الحدود الفاصلة بين الجرائم الشكلية وتلك ذات النتائج المادية غير واضحة، وبذلك فإن التكييف القضائي قد يواجه صعوبات في التطبيق.

بناء على ذلك، يدعو بعض الفقهاء إلى تعديل المواد 2 و3 و4 من قانون 14 لسنة 2014 لتصبح أوضح وأكثر اتساقًا مع الأساليب المتغيرة للجرائم الرقمية، بما يعزز من فعالية الملاحقة القانونية.[2]

كما يُظهر تحليل الركن المادي في جريمة القرصنة الإلكترونية تعدده وتعقيده، حيث يتضمن أفعالًا شكلية لا تستلزم وجود ضرر مباشر، وأفعالًا أخرى تستلزم تحقق أضرار ملموسة

(1) بشرى حسين الحمداني، القرصنة الإلكترونية: أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، عمان، 2014

(2) الديب، محمد خميس. (2021). الحماية الجنائية للمعلومات في مواجهة الجرائم الإلكترونية: دراسة تحليلية للقانون القطري رقم 14 لسنة 2014. مجلة دراسات الخليج والجزيرة العربية، جامعة الكويت، العدد 185، ص. 144–147.

مع إثبات علاقة سببية. ورغم أن القانون القطري وضع الأسس اللازمة لتجريم هذه الأفعال، إلا أنه لا يزال بحاجة إلى تطوير وتفصيل لضمان التكييف القانوني الدقيق، وتسهيل إثبات الجرائم، مما يضمن حماية فعالة للنظم المعلوماتية والبيانات الرقمية.

المبحث الثاني: الركن المعنوي

تمهيد:

لا يكفي في التجريم تحقق الركن المادي فقط، بل لا بد من قيام الركن المعنوي، وهو العنصر الداخلي الذي يعبر عن الدافع والنية واللهجة النفسية التي تصاحب السلوك الإجرامي. في جوهر الأمر، الركن المعنوي أو القصد الجنائي يتطلب أن يكون لدى الجاني علمٌ بركني الفعل والنتيجة، وإرادة في تحقيقهما. وهذه الضرورة تزداد أهمية في الجرائم الرقمية المعقدة مثل جريمة القرصنة الإلكترونية التي تتميز باستخدام وسائل تقنية عالية التعقيد، والتي تتطلب إثبات توافر الوعي والإرادة لدى الجاني. فبدون تحقق الركن المعنوي لا يمكن مساءلة المتهم جنائياً، حيث يُعد الركن المعنوي قاعدة أساسية تميز الجريمة عن الخطأ أو الفعل العارض غير المُتعمد. كما أن جريمة القرصنة الإلكترونية، على الرغم من طبيعتها التقنية، تخضع لهذه القاعدة وتستوجب توفر إرادة واعية ومدركة للسلوك الجاني وعواقبه القانونية.

أولًا: طبيعة الركن المعنوي في القرصنة الإلكترونية

جريمة القرصنة الإلكترونية تصنف ضمن جرائم العمد؛ أي لا يقع التجريم إلا مع توافر القصد الجنائي العام، والذي يشمل العلم والإرادة. فالقانون القطري رقم (14) لسنة 2014 يؤكد ضرورة أن يكون الفعل قد ارتكب "عمدًا" أو "بقصد"، وهو ما يعني أن الجاني يجب أن يكون على علم بالفعل الذي يقوم به وأن يكون له الإرادة الحرة في تنفيذه.[3]

العلم حيث يتعين أن يكون الفاعل مدركًا بأن النظام المعلوماتي أو البيانات التي يتدخل فيها خاصة أو محمية عليه، وأنه يتصرف بغير إذن قانوني. العلم بهذا الواقع فقهيًا وقانونيًا يُعتبر شرطًا جوهريًا، إذ لا تغطي المسؤولية حالات الخطأ غير الواعي أو الجهل بالخصوصية، بينما الإرادة تعني سلوك الفاعل بفعل إرادي ومدروس، دون تعرضه لأي إكراه أو إجبار خارجي، ما يضمن وقوع الفعل بصورة حرة غير قسرية، ووفقاً للمشرعات والقضاء، فإن

غياب أي من هذين العنصرين يُبطل توافر القصد الجنائي ويُسقط مسؤولية الجاني. على سبيل المثال، في حالات الدخول العرضي إلى نظام غير محمي أو عدم معرفة الفاعل بطبيعة النظام، لا تُعتبر جريمة. .[1]

ثانيًا: القصد الجنائي الخاص وأهميته في القرصنة

بعض صور القرصنة تشمل بقصد أو نية معينة، تعرف بالقصد الجنائي الخاص. وهذا النوع من القصد يحدد الدافع الأساسي للعمل، كأن يكون الاستحواذ على معلومات سرية، الإضرار بسمعة أو أمن جهة معينة، أو الاستفادة ماديًا عبر الابتزاز أو الاحتيال. في هذه الحالات، لا يُعاقب الفاعل على مجرد الدخول أو التسلل، بل على القصد والإرادة الموجهة لاستغلال الدخول في أفعال ضارة أخرى. توضح الدراسات الفقهية أن غياب الباعث الإجرامي المرتبط بالضرر يجعل العقوبة أخف أو ينفي الجريمة، حيث يختلف التقاضي بين الفضولي الذي يزور نظامًا بدافع التجربة، وبين المخطط والمنفذ بغاية إحداث ضرر مقصود.

ثالثًا: التحديات العملية في إثبات الركن المعنوي

إثبات الركن المعنوي في الجرائم الإلكترونية يُعد من المهام المعقدة التي تواجه الهيئات القانونية، حيث تنبع هذه الصعوبة من طبيعة الجريمة ذاتها التي تتم عبر الشبكات الافتراضية، مما يؤدي إلى غياب الشهود المباشرين، الأمر الذي يحرم الجهات القضائية من أحد أهم أدوات الإثبات التقليدية. ويُضاف إلى ذلك تعقيد الأدلة الرقمية، حيث يعتمد المحققون على قرائن تقنية مثل سجلات الدخول (Log Files) وبرامج التتبع وتحليل البيانات، وهي أدوات تتطلب خبرات تخصصية دقيقة لضمان صحتها القانونية وإمكانية قبولها أمام المحكمة. كما تزداد التحديات تعقيدًا باستخدام الجناة لتقنيات التمويه والإخفاء مثل البرمجيات الخبيثة والتشفير والشبكات المظلمة، والتي تهدف إلى إخفاء الهوية ومنع التتبع، مما يصعّب من مهمة إثبات القصد الجنائي أو الإرادة الحرة في ارتكاب الفعل. ومن ثمّ، فإن التعامل مع هذه القضايا يتطلب تنسيقًا عالي المستوى بين الجوانب الفنية والقانونية، مما

[1] الحمادي، خالد. (2018). "جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة". رسالة ماجستير، كلية القانون، جامعة قطر.

يجعل من أدوات التحقيق الرقمي جسرًا أساسيًا لا غنى عنه لإثبات الركن المعنوي في مثل هذه الجرائم.

ختاما يتضح أن الركن المعنوي في جريمة القرصنة الإلكترونية هو العمود الفقري الذي يقوم عليه إثبات المسؤولية الجنائية، ويُميز بين الجريمة المتعمدة والخرق العرضي أو غير المقصود. ورغم التحديات الفنية والقانونية، فإن التطور المستمر في أدوات التحقيق الجنائي الرقمي، وتحديث التشريعات بما يضمن ضم الأدلة الرقمية والتقنية، يشكل ركيزة أساسية لتعزيز فعالية مكافحة هذه الجريمة وحماية الأمن السيبراني. ولا غنى عن تكامل الجهود الفنية والقانونية لضمان تحقيق العدالة والردع القانوني الفعال في مواجهة الجرائم الرقمية الحديثة.

المبحث الثالث: الركن الشرعي والمحل في جريمة القرصنة الإلكترونية

أولًا: الركن الشرعي: مبدأ الشرعية الجنائية

الركن الشرعي يُعتبر أحد الأركان الأساسية التي تقوم عليها الجريمة، حيث يُعبر عن وجود نص قانوني يُجرّم الفعل محل الاتهام. يُعد هذا الركن تجسيدًا لمبدأ شرعي أصيل يُعرف بمبدأ "لا جريمة ولا عقوبة إلا بنص"، والذي يُعتبر حجر الزاوية في الأنظمة القانونية الحديثة. هذا المبدأ يضمن عدم معاقبة الأفراد على أفعال لم يُحددها القانون كجرائم، مما يعكس أهمية حماية الحقوق الفردية ويعزز من مبدأ العدالة. في سياق جريمة القرصنة الإلكترونية، لا يمكن اعتبار أي فعل من أفعال القرصنة جريمة إلا إذا كان هناك نص قانوني صريح يُجرّمه.

في القانون القطري، تم تحديد العديد من الأفعال التي تُعتبر قرصنة إلكترونية، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية (المادة 2)، الاعتراض على البيانات (المادة 4)، والتعديل أو الإتلاف للبيانات (المادة 3).

كما حدد القانون العقوبات المناسبة لكل من هذه الأفعال، مما يُعزز من الإطار القانوني الذي يحكم الجرائم الإلكترونية. ومع ذلك، يُشير بعض الفقهاء إلى أن النصوص القانونية الحالية قد لا تغطي كافة صور القرصنة الحديثة، خاصة تلك التي تعتمد على تقنيات متقدمة مثل الذكاء الاصطناعي أو القرصنة التي تتم عبر شبكات مجهولة الهوية. هذا النقص في

النصوص القانونية يُعتبر تحديًا كبيرًا، حيث يفتح الباب لتوسيع النصوص أو تعديلها لتتناسب مع تطور الجريمة، مما يستدعي ضرورة تحديث التشريعات بشكل دوري لمواكبة التغيرات السريعة في عالم التكنولوجيا.

ثانيًا: المحل القانوني للجريمة – محل الحماية الجنائية

المحل في الجريمة يُشير إلى الحق أو المصلحة التي يحميها القانون ويُعتدى عليها بفعل الجريمة. في جريمة القرصنة الإلكترونية، تتعدد هذه المحال بحسب نوع الفعل المرتكب. على سبيل المثال، يُعتبر انتهاك خصوصية الأفراد من خلال اختراق البريد الإلكتروني أو التنصت على الرسائل اعتداءً على حق الأفراد في الخصوصية، وهو حق محمي بموجب القوانين المحلية والدولية. كما أن سرية البيانات تُعتبر من المحال المهمة، حيث يُعد سرقة أو نشر معلومات شخصية أو تجارية اعتداءً على حقوق الملكية الفكرية والمعلوماتية، مما يُؤثر سلبًا على الأفراد والشركات على حد سواء.

علاوة على ذلك، فإن سلامة النظام المعلوماتي تُعتبر محلًا آخر للحماية، حيث إن الإتلاف أو التعطيل لأنظمة المعلومات يُؤثر على كفاءة وأمان هذه الأنظمة، مما يُعرض المؤسسات لمخاطر كبيرة. كما أن الاقتصاد الرقمي يُعتبر من المحال الحيوية التي تتعرض للتهديد من خلال قرصنة أنظمة الدفع أو الاحتيال الإلكتروني، مما يُشكل خطرًا على الاستقرار المالي والاقتصادي للدول.

يتميز محل الحماية في جريمة القرصنة بأنه غير مادي وغير محسوس، إذ لا يتعلق بشيء مادي ملموس، بل بمنظومة رقمية تمثل قيمة معنوية وقانونية عالية. هذا الأمر يُصعّب من تقييم الضرر الناتج عن الجريمة، حيث قد يكون من الصعب قياس الأثر الفعلي للقرصنة على الأفراد أو المؤسسات. لذلك، يُعتبر وجود تشريع صريح يحمي هذه المحال أمرًا بالغ الأهمية، حيث يُسهم في تعزيز الحماية القانونية للبيانات والمعلومات الرقمية.

نستخلص أن أركان جريمة القرصنة تكتمل بوجود نص قانوني واضح يُجرم الفعل (الركن الشرعي)، ووجود محل قانوني يتمثل في مصلحة محمية تم الاعتداء عليها. يُلاحظ أن التشريع القطري، رغم تغطيته لنطاق واسع من أفعال القرصنة، لا يزال بحاجة إلى تطوير الصياغات وتوسيع التجريم ليواكب تطورات الجريمة الرقمية المتسارعة. إن تحديث

التشريعات وتوسيع نطاق الحماية القانونية يُعتبر أمرًا ضروريًا لمواجهة التحديات التي تطرأ على عالم الجرائم الإلكترونية، مما يُعزز من قدرة النظام القانوني على حماية الحقوق والمصالح الرقمية للأفراد والمؤسسات.

الفصل الثالث: العقوبات القانونية لجريمة القرصنة الإلكترونية

المبحث الأول: العقوبات في التشريع القطري (قانون 2014/14)

تمهيد:

يمثّل قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014 الإطار التشريعي الأبرز الذي نظّم العقوبات الخاصة بالأفعال المكوّنة لجريمة القرصنة الإلكترونية[3]. وقد تبنى المشرّع القطري في هذا القانون نهجًا تدريجيًا في العقوبات، يراعي جسامة الفعل، وخطورته، والآثار المترتبة عليه، مع تشديد واضح للعقوبة في حال اقتران الجريمة بظروف مشددة كالمساس بالأمن القومي أو تعطيل أنظمة الدولة الحيوية. في هذا المبحث، سيتم تحليل العقوبات الواردة في القانون، وتصنيفها وفقًا لأنواع الأفعال الإجرامية المختلفة، ثم تقييم مدى كفايتها في تحقيق الردع العام والخاص.

أولًا: عقوبة الدخول غير المشروع إلى النظام المعلوماتي

نصت المادة (2) من القانون على أن: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) ريال قطري، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، دون وجه حق، بأي وسيلة، إلى موقع إلكتروني، أو نظام معلوماتي، أو شبكة معلوماتية...". يُلاحظ هنا أن المشرّع اعتبر مجرد الدخول دون إذن – ولو دون إضرار أو اختراق بيانات – جريمة قائمة بذاتها، ويُعاقب عليها بعقوبة مقيدة للحرية ومالية. يُعد هذا التوجه مهمًا في الردع الوقائي، إذ يقرّر العقوبة حتى قبل وقوع الضرر، وهو ما ينسجم مع طبيعة الجرائم الإلكترونية التي يصعب أحيانًا ضبطها بعد وقوع الفعل الإجرامي الكامل.

ثانيًا: العقوبات المشددة عند إتلاف البيانات أو التعديل أو الإفشاء

نصت المادة (2/3) من القانون على ما يلي: "تكون العقوبة الحبس مدة لا تجاوز خمس سنوات، والغرامة التي لا تزيد على (1,000,000) ريال قطري، أو إحدى هاتين العقوبتين، إذا ترتب على الدخول ارتكاب أي من الأفعال الآتية: إلغاء أو حذف أو إضافة أو إفشاء أو

تغيير أو نقل أو نسخ أو إعادة نشر البيانات، أو تدمير أو تعطيل الموقع...". هذه الفقرة تُظهر أن القانون القطري ميّز بين الجريمة الأساسية (الدخول فقط)، والجريمة المشددة التي يقترن فيها الدخول بإضرار فعلي في البيانات أو النظم. هنا ارتفعت العقوبة من ثلاث إلى خمس سنوات، والغرامة من نصف مليون إلى مليون ريال، وهو ما يعكس مراعاة المشرّع لجسامة النتيجة الإجرامية. ويرى بعض الباحثين أن هذا التدرج في العقوبة يُعد تطبيقًا سليمًا لمبدأ "التناسب بين الجريمة والعقوبة" في القانون الجنائي.

ثالثًا: الاعتراض أو التنصت على البيانات

جاءت المادة (4) لتعالج صورة أخرى من صور القرصنة، وهي التنصت على البيانات أو اعتراضها أثناء انتقالها، فنصت على أن: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، والغرامة التي لا تزيد على (500,000) ريال قطري، أو بإحدى هاتين العقوبتين، كل من التقط أو اعترض أو تنصت عمدًا، دون وجه حق، على أية بيانات مرسلة...". وتُعد هذه العقوبة متناسبة مع طبيعة الفعل، رغم أن بعض الفقه يرى أنها معتدلة نسبيًا مقارنة بخطورة ما قد ينجم عن التنصت الرقمي من جرائم لاحقة، كالتشهير أو الابتزاز أو التجسس.

رابعًا: العقوبات المرتبطة بالمساس بالأمن القومي أو الأنظمة السيادية

خصص المشرع القطري مواد مستقلة للعقوبات المشددة حال المساس بالبنية المعلوماتية السيادية، كما ورد في المادة (9)، التي نصت على أن: "يعاقب بالحبس مدة لا تجاوز عشر سنوات، والغرامة التي لا تزيد على (2,000,000) ريال قطري، إذا وقعت الجرائم المنصوص عليها على أنظمة معلوماتية تخص إحدى الجهات السيادية"[1]. يُعد هذا النص من أقوى ما جاء في قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014، حيث يعكس التشديد في العقوبات أهمية وحساسية المساس بأمن الدولة الرقمي والنظم السيادية التي تؤثر على استقرار ومصالح الدولة العليا. ويشير هذا التوجه إلى إدراك المشرّع

[1] قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014، المادة 9:
"يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص لحمله على القيام بعمل أو الامتناع عنه."

لخطورة الأفعال الموجهة ضد البنى التحتية الرقمية التي تُعد العمود الفقري لعمل المؤسسات السيادية والخدمية للدولة، ويُعزز من الردع القانوني والجنائي لهذه الجرائم باهظة الأثر.

خامسًا: تقييم شامل للعقوبات في القانون القطري

رغم أن قانون 14 لسنة 2014 وضع أساسًا تشريعيًا متقدمًا لتنظيم الجرائم الإلكترونية والعقوبات المقررة لها، إلا أن هناك ملاحظات جوهرية تؤكد الحاجة إلى المزيد من التطوير والتفصيل، وهي:

- غياب الحد الأدنى للعقوبة مما قد يتيح للقضاة مجالًا واسعًا في تقدير العقوبة، ويؤدي إلى تفاوت في الأحكام وعدم استقرارها، خاصة في قضايا القرصنة التي تتطلب حزمًا قانونيًا.
- استخدام مصطلحات فضفاضة مثل عبارة "دون وجه حق" التي تُستخدم في عدة مواد بدون تحديد دقيق أو تعريف قانوني واضح مما يُسبب غموضًا في فهم النصوص وتطبيقها.
- غياب العقوبات التكميلية مثل مصادرة الأجهزة الإلكترونية المستخدمة في الجريمة، أو فرض حظر على ممارسة أنشطة تقنية لفترة محددة، وهي عقوبات فعالة جدًا في مواجهة الجرائم السيبرانية.
- عدم تناول الشروع والمساهمة حيث لا يحتوي القانون على نصوص واضحة للتعامل مع حالات الشروع في جريمة القرصنة أو مساهمة أطراف أخرى، وهي حالات متكررة في فضاء الجرائم الرقمية مما يستوجب ضمها في النصوص القانونية.

في الختام يمكن القول أن يشكل قانون الجرائم الإلكترونية القطري رقم 14 لسنة 2014 خطوة متقدمة وهامة في مكافحة جريمة القرصنة الإلكترونية من خلال وضع هيكل قانوني متكامل للعقوبات يتناسب مع جسامة الأفعال المرتكبة. كما تبنت نصوصه مبدأ التدرج في العقوبات بالتناسب مع نوع الفعل وخطورته، خصوصًا في حالات المساس بالأمن السيبراني أو الأنظمة السيادية. ومع ذلك، لازال القانون بحاجة إلى تعزيز بعض الجوانب الفنية

والتشريعية، من خلال تبني تعريفات دقيقة وشاملة، وإدخال عقوبات تكميلية، وتوسيع نطاق التجريم ليشمل الشروع والمساهمة، مع ضرورة تطوير آليات التحقيق والإثبات بما يتلاءم مع طبيعة الجريمة الإلكترونية المعقدة والمتجددة، لضمان تحقيق الردع العام والخاص بشكل فعّال.

المبحث الثاني: العقوبات في التشريعات المقارنة (مصر – الإمارات – السعودية)

تمهيد:

أصبحت مسألة تجريم أفعال القرصنة الإلكترونية محل اهتمام تشريعي متزايد في الدول العربية، التي سعت إلى إصدار قوانين خاصة لمواجهة الجرائم الإلكترونية بما في ذلك جريمة القرصنة. وفي هذا السياق، صدرت قوانين متقدمة نسبيًا في كل من مصر والإمارات والسعودية. ويهدف هذا المبحث إلى استعراض وتحليل العقوبات الواردة في تلك التشريعات، ومقارنتها بمثيلتها في التشريع القطري، بهدف الوقوف على أفضل الممارسات التشريعية في هذا المجال.[1]

أولًا: العقوبات في التشريع المصري (قانون رقم 175 لسنة 2018)

صدر قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، كأول تشريع متخصص في مواجهة الجريمة الرقمية في مصر، وتضمّن مواد عديدة تُجرّم أفعال القرصنة الإلكترونية وتُحدد عقوباتها.

الدخول غير المشروع: نصت المادة (14) على أن: "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا أو بغير وجه حق... إلى موقع أو نظام معلوماتي محمي" يُلاحظ أن المشرع المصري حدد حدًا أدنى للعقوبة، مما يُسهم في تقليل التفاوت القضائي، ويُحقق درجة أعلى من الحزم مقارنة بالقانون القطري الذي لم ينص على حد أدنى صريح.

---

[1] حمزة، سامي محمد. (2020). الحماية الجنائية من الجرائم الإلكترونية في التشريعات العربية: دراسة مقارنة بين القانون المصري والإماراتي والسعودي. مجلة الدراسات القانونية المعاصرة، جامعة عين شمس، العدد 12، ص. 155–192.

إتلاف البيانات أو تعديلها: المادة (23) قررت الحبس مدة لا تقل عن سنتين وغرامة تبدأ من 100,000 جنيه، حال إتلاف أو تعديل أو نسخ أو نشر بيانات أو معلومات إلكترونية، وهو ما يمثل تصعيدًا للعقوبة في حالة وقوع نتيجة ضارة[1]

اختراق الأنظمة السيادية: نصت المادة (29) على الحبس مدة لا تقل عن ثلاث سنوات وغرامة تصل إلى 500,000 جنيه لمن اخترق مواقع تخص الدولة، مع عقوبات مشددة حال وجود قصد الإضرار بالأمن القومي أو البيانات السيادية.[2] وهذه المادة تُظهر وعيًا تشريعيًا بخصوصية البنية التحتية الرقمية للدولة، وهو ما يتوافق مع الاتجاه القطري في المادة (9) من قانون 2014/14.

ثانيًا: العقوبات في التشريع الإماراتي (القانون الاتحادي رقم 5 لسنة 2012 وتعديلاته)

يُعد القانون الإماراتي من أكثر القوانين العربية تقدمًا من حيث الصياغة الدقيقة للعقوبات وتفصيلها وفقًا لكل صورة من صور الجريمة الإلكترونية.

الدخول غير المشروع: نصت المادة (2) على: "يعاقب بالحبس والغرامة التي لا تقل عن 100,000 درهم ولا تجاوز 300,000 درهم، أو بإحدى هاتين العقوبتين، كل من دخل موقعًا إلكترونيًا أو نظام معلوماتي دون تصريح أو بطريقة غير مشروعة"[3]. وتُشدد العقوبة إذا تم المساس بسرية البيانات، لتصل إلى السجن المؤقت والغرامة التي قد تبلغ مليون درهم.

---

(1) (قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 المادة 23): "يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أوعطل أو حذف، أو غيّر، أو نسخ، أو نشر بيانات، أو معلومات إلكترونية... دون وجه حق، فإذا ترتب على ذلك ضرر، تكون العقوبة الحبس مدة لا تقل عن ثلاث سنوات وغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه".

(2) (قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 المادة 29):

"يعاقب بالحبس مدة لا تقل عن ثلاث سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، كل من دخل عمدًا، أو بغير وجه حق، أو تجاوز حدود الحق المصرح له به إلى موقع أو نظام معلوماتي يدار بمعرفة أو لحساب الدولة أو أحد أجهزتها أو الهيئات أو المؤسسات العامة أو وحدات الإدارة المحلية أو مملوك لها، فإذا كان الدخول بهدف تعطيل الموقع أو النظام أو إتلاف ما به من بيانات أو معلومات أو تغييرها أو محوها أو نسخها أو إعادة نشرها، تكون العقوبة الحبس مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه، وإذا كان ذلك بقصد الإضرار بالأمن القومي أو تعريضه للخطر، تكون العقوبة السجن المشدد".

(3) القانون الاتحادي الاماراتي رقم 5 لسنة 2012

- المادة (2):

"يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكتروني أو شبكة معلوماتية دون تصريح أو بطريقة غير مشروعة، وتكون العقوبة

التعدي على البيانات الحكومية أو السيادية: أفردت المادة (4) نصًا خاصًا لمن يدخل أنظمة معلوماتية تخص الدولة، حيث تصل العقوبة إلى السجن المؤبد إذا كان القصد الإضرار بالأمن القومي أو المصالح العليا للدولة. وهذا يُظهر أن التشريع الإماراتي لا يتعامل مع الجرائم الرقمية فقط كجرائم تقنية، بل يدمجها في الأمن القومي السيبراني، وهو توجه متقدم نسبيًا مقارنة بالتشريعات الأخرى.

ثالثًا: العقوبات في التشريع السعودي (نظام مكافحة جرائم المعلوماتية الصادر عام 2007)

رغم قدم القانون السعودي نسبيًا، إلا أنه شكّل خطوة رائدة في المنطقة، إذ كان من أوائل التشريعات العربية التي تناولت الجريمة الإلكترونية بشكل منهجي.

الدخول غير المشروع: نصت المادة (3) على أن: "يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على 500,000 ريال، أو بإحدى العقوبتين، كل من دخل إلى موقع إلكتروني أو نظام معلوماتي دون تصريح".[1] ويُلاحظ هنا أن القانون لم يضع حدًا أدنى للعقوبة، لكنه شدد على المساس بسلامة البيانات أو النظام في المادة (5)، لترتفع العقوبة إلى السجن لمدة أربع سنوات وغرامة تصل إلى 3,000,000 ريال.

الإضرار بالأنظمة السيادية: المادة (6) من القانون السعودي نصت على أن: "كل من تسبب في تعطيل خدمات عامة أو ارتكب أفعالًا تمس الأمن الوطني من خلال الوسائل الإلكترونية، يعاقب بالسجن حتى عشر سنوات". وتقارب هذه العقوبة في شدتها المادة (9) من القانون

الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم إذا ترتب على الدخول حذف، أو كشف، أو إعادة نشر البيانات، أو المعلومات الخاصة بأي وسيلة كانت".

- المادة (4):

"يعاقب بالسجن المؤقت كل من دخل دون تصريح إلى أي موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية تخص إحدى الجهات الحكومية، أو المؤسسات العامة، أو الهيئات الاتحادية، أو المحلية، أو أي جهة أخرى تابعة للدولة. وإذا كان القصد من الدخول الإضرار بالدولة، أو تعطيل عمل الموقع، أو النظام، أو الحصول على بيانات حكومية أو معلومات تتعلق بأمن الدولة أو مصالحها العليا، تكون العقوبة السجن المؤبد أو السجن المؤقت الذي لا يقل عن عشر سنوات".

(1) نظام مكافحة جرائم المعلوماتية، المملكة العربية السعودية، 2007.

- المادة (3): "يعاقب بالسجن مدة لا تزيد عن سنة، وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع إلكتروني أو نظام معلوماتي دون تصريح".
- نصت المادة (5) على: "يعاقب بالسجن لمدة لا تزيد عن أربع سنوات، وبغرامة تصل إلى ثلاثة ملايين ريال، كل من قام بتغيير، أو حذف أو تلف البيانات أو المعلومات المخزنة أو المسترجعة إلكترونيًا في الأنظمة المعلوماتية أو تعرض للأمن المعلوماتي بأي وسيلة كانت".
- المادة (6): "كل من تسبب في تعطيل خدمات عامة أو ارتكب أفعالًا تمس الأمن الوطني أو تضر بمصلحة الدولة من خلال الوسائل الإلكترونية يعاقب بالسجن لمدة لا تزيد عن عشر سنوات".

القطري والمادة (4) من القانون الإماراتي، ما يدل على تقارب النهج التشريعي في الجرائم ذات الطابع السيادي.[1]

رابعًا: المقارنة العامة بين التشريعات الثلاثة

يتسم التشريع المصري بتحديد حد أدنى للعقوبات، وهو ما يساهم بشكل كبير في تقليص التفاوت القضائي ويسهم في إرساء العدالة الجنائية من خلال تقديم إطار قانوني صارم. في المقابل، يفتقر كل من التشريع القطري والتشريع السعودي إلى هذا التوجه، مما قد يؤدي إلى تفاوت في تطبيق العقوبات، وتنوع في مدى الردع القانوني بناءً على تقديرات المحاكم. من جانب آخر، يُظهر التشريع الإماراتي أعلى درجات التشديد في العقوبات، لاسيما في الحالات التي تتعلق بالمساس بالأمن القومي، حيث تصل العقوبات إلى السجن المؤبد في حال وقوع جريمة تمس المصالح العليا للدولة. بينما تظل التشريعات المصرية والسعودية أقل شدة في بعض الحالات، رغم ما تتضمنه من عقوبات رادعة تهدف إلى ردع الجريمة الإلكترونية.

من حيث التنظيم القانوني، يتميز التشريع الإماراتي بتفصيل دقيق وشامل للعقوبات وفقًا للنوع الدقيق للجريمة الإلكترونية، مما يسهل عملية تطبيق القانون ويعزز فعاليته. أما التشريع المصري، ورغم حداثته وتنظيمه، إلا أنه يحتاج إلى مزيد من التفصيل في بعض الجوانب المتعلقة بالجريمة الرقمية ذات الطابع السيادي. في المقابل، يُظهر التشريع القطري فهمًا متقدمًا لأهمية حماية الأمن السيبراني، إذ يتم التعامل مع الجرائم الإلكترونية كجزء من الأمن القومي، وهو ما يعكس التوجه الاستراتيجي المتكامل لحماية مصالح الدولة العليا. بينما التشريع السعودي، على الرغم من كونه من أوائل التشريعات التي تناولت الجريمة الإلكترونية بشكل منهجي، لا يزال بحاجة إلى تحديثات قانونية لتواكب التطورات السريعة في هذا المجال الحيوي.

(1) المملكة العربية السعودية. (2007). نظام مكافحة جرائم المعلوماتية، الصادر بموجب المرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ.

علاوة على ذلك، يُظهر التشريع الإماراتي مرونة أكبر في التعامل مع الجرائم الإلكترونية، إذ يوفر إمكانية تشديد العقوبات استنادًا إلى الظروف المحيطة بالجريمة، مثل المساس بسرية البيانات أو الأضرار التي قد تلحق بالأمن القومي. في حين يفتقر التشريع القطري والتشريع السعودي إلى هذه المرونة في تطبيق العقوبات، وهو ما قد يؤثر سلبًا على فعالية الردع في الحالات التي تتطلب مرونة قانونية للتعامل مع الجريمة الإلكترونية.

في الختام، يمكننا الاستنتاج أن هناك توجهًا عامًا بين التشريعات العربية نحو تشديد العقوبات على أفعال القرصنة الإلكترونية، وخاصة تلك التي ترتبط بأمن الدولة أو تمس مصالحها العليا. إلا أن التشريع الإماراتي يبرز بتفصيله الدقيق والعقوبات الرادعة والمتدرجة التي تزيد من فعالية القانون في مواجهة الجرائم الإلكترونية. في حين أن التشريع المصري يعد منظمًا وحديثًا، لكنه يتطلب مزيدًا من التفصيل في بعض الأبعاد القانونية. أما التشريع السعودي فيظل بحاجة إلى تحديثات شاملة لضمان مواكبته للتطورات السريعة في أساليب وتقنيات الجرائم الإلكترونية. وأما التشريع القطري، على الرغم من تقدمه في بعض الجوانب، فإنه يحتاج إلى توسيع نطاق النصوص القانونية وتنقيح الصياغات وتحديد الحد الأدنى للعقوبة لضمان تحقيق العدالة الجنائية المتوازنة في هذا المجال.

المبحث الثالث: تقييم مدى كفاية العقوبات وتحليل فجوات التجريم والعقاب

العقوبة ليست فقط أداة للرد على الجريمة، بل هي في جوهرها وسيلة للردع والوقاية المجتمعية، وهي بذلك تمثل ركيزة جوهرية في النظام الجنائي. وفي ظل تزايد معدلات الجريمة الإلكترونية، وعلى رأسها جريمة القرصنة، فإن تقييم مدى كفاية العقوبات القانونية المقررة لهذه الجرائم يُعد اختبارًا حقيقيًا لجدوى التشريعات وحداثتها وقدرتها على المواجهة الفعلية. هذا المبحث يُعالج ما إذا كانت العقوبات الواردة في قانون مكافحة الجرائم الإلكترونية القطري كافية وفعّالة، ويُسلّط الضوء على أبرز الثغرات في التجريم أو قصور العقاب مقارنة بالتطور الواقعي للجريمة.[1]

[1] سعيد، عبد الله. (2019). تقييم فعالية التشريعات الجنائية في مكافحة الجرائم الإلكترونية: دراسة مقارنة بين الدول العربية. دار الكتب القانونية.

أولًا: مدى كفاية العقوبات من حيث الردع العام والخاص

تمثل العقوبات في قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014 محاولة من المشرع لتحقيق توازن بين الفعل الجرمي والعقوبة المقررة. حيث تبدأ العقوبات من الحبس والغرامة في الجرائم البسيطة مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، وتتصاعد بشكل تدريجي في حال توافر ظروف مشددة، مثل تعديل أو إتلاف أو إفشاء البيانات، أو في حالة استهداف الأنظمة السيادية والحساسة. غير أن الردع الفعلي لا يتمثل فقط في النصوص العقابية، بل يتطلب ضمانات في التطبيق العملي لهذه العقوبات.

إحدى الملاحظات الجوهرية التي أشار إليها العديد من الفقهاء هي غياب الحد الأدنى للعقوبة، مما يؤدي إلى تعزيز قدرة القضاء على اتخاذ قرارات متفاوتة استنادًا إلى تقدير القاضي، وهو ما قد يساهم في التفاوت الكبير في الأحكام القضائية وقد يؤدي إلى التساهل في تطبيق العقوبات في بعض الحالات. كما أن التدرج العقابي الذي يعتمد عليه القانون ليس محكومًا بضوابط دقيقة، مما قد يخلق نوعًا من الضبابية في تفسير الأفعال الإجرامية وتحديد العقوبات المناسبة لها، وهو ما يعكس إشكالية قانونية في تكييف النصوص القانونية مع الوقائع الفعلية.[1]

علاوة على ذلك، تفتقر بعض الجرائم الإلكترونية إلى العقوبات التبعية الفعّالة التي تُعتبر ضرورية لمواجهة الجرائم الرقمية، مثل حرمان المتهمين من ممارسة الأنشطة الرقمية أو مصادرة الأدوات المستخدمة في ارتكاب الجريمة. هذه العقوبات التبعية تُعد من الأدوات الضرورية في ردع الجريمة الإلكترونية، حيث تسهم في تقليل فرص تكرار الجريمة من قبل الأفراد المتورطين. بناءً على ذلك، يتضح أن القانون القطري، رغم تقدمه، لا يزال بحاجة إلى مزيد من التدقيق والتنقيح لتلبية متطلبات الردع العام والخاص بصورة أكثر فعالية.

[1] العتيبي، فهد. (2017). تحليل فعالية التشريعات العقابية في مواجهة الجرائم الإلكترونية: دراسة مقارنة بين قوانين الدول العربية. مؤسسة الفكر العربي للنشر.

ثانيًا: غياب النصوص الخاصة بالشروع في الجريمة

من أبرز الثغرات في قانون 14 لسنة 2014 عدم وجود معالجة صريحة لمسألة الشروع في الجريمة الإلكترونية. في حين أن أغلب الجرائم التقليدية يجرّم فيها الشروع، فإن الجرائم الرقمية، التي غالبًا ما تُكتشف في منتصف تنفيذها، تحتاج لنصوص خاصة تُجرّم الشروع. ففي حالة اكتشاف محاولة اختراق قبل تحقق الضرر، لا توجد مادة صريحة تعاقب على الشروع، مما يُفقد أجهزة الضبط فرصة التدخل المبكر. وقد نص القانون المصري في المادة (45) من قانون 175 لسنة 2018 على تجريم الشروع في أغلب الجرائم المعلوماتية، وهو ما يُعد نموذجًا متقدمًا يُحتذى[1].

ثالثًا: ضعف المعالجة التشريعية للمساهمة الجنائية الإلكترونية

لم يُفرد القانون القطري تنظيمًا دقيقًا لمسؤولية الشركاء أو المحرّضين أو المساعدين في الجرائم الإلكترونية. وهذا أمر بالغ الخطورة، إذ إن كثيرًا من جرائم القرصنة تتم من خلال شبكات منظمة يعمل فيها أكثر من فاعل: أحدهم يخطط، وآخر ينفذ، وآخر يُسهل أو يُخفي الأدلة. الاقتصار على معاقبة الفاعل المباشر يُفرغ النص القانوني من مضمونه في مواجهة الجرائم المنظمة عبر الإنترنت، خاصة في ظل ازدياد استخدام "البرمجيات الوسيطة" و"أدوات الاختراق الجاهزة" التي يبيعها طرف ثالث.

رابعًا: قصور النصوص في مواكبة تطورات الجريمة التقنية

تتسم الجرائم التقنية بكونها متغيرة بطبيعتها، حيث تتطور أدواتها وأساليب تنفيذها بوتيرة متسارعة، ما يفرض تحديًا تشريعيًا دائمًا في سبيل الإبقاء على فعالية النصوص القانونية. إلا أن التشريع القطري، منذ صدور القانون رقم 14 لسنة 2014 بشأن مكافحة الجرائم

---

[1] (قانون رقم 175 لسنة 2018 مادة 45): "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم حسابًا إلكترونيًا أو شبكة معلوماتية أو أي وسيلة إلكترونية أخرى لنشر أو ترويج أو نشر أخبار أو بيانات أو معلومات غير صحيحة عن شخص أو مجموعة أشخاص أو جهة ما، وإذا كانت الجريمة قد تم ارتكابها باستخدام وسيلة من وسائل الإعلام أو الصحافة أو إذا كانت قد ارتكبت ضد جهة عامة، تكون العقوبة الحبس مدة لا تقل عن سنة."

الإلكترونية، لم يشهد أي تعديلات جوهرية تستوعب هذه التحولات، رغم التحول النوعي في أنماط الجرائم الإلكترونية الحديثة. ومن أبرز هذه الأنماط[1]:

1. استخدام تقنيات الذكاء الاصطناعي في تنفيذ الهجمات السيبرانية (AI-Powered Cyber Attacks)،
2. توظيف الشبكات المظلمة (Dark Web) كبيئة خفية لتبادل البيانات والبرمجيات الخبيثة،
3. استغلال الأجهزة الذكية وتقنيات إنترنت الأشياء (IoT) في أنشطة القرصنة والاختراق.

غياب تحديثات تشريعية لمواجهة هذه التحديات يؤدي إلى وجود فراغ تشريعي حقيقي، يُصعّب مهمة جهات إنفاذ القانون ويُلقي بعبء ثقيل على القضاة في تأويل النصوص الحالية بشكل يتماشى مع تلك الوقائع المستحدثة. وفي بعض الحالات، قد يؤدي غياب النصوص الصريحة إلى نتائج قانونية غير مُرضية، مثل ضعف الحماية الجنائية أو حتى الحكم بالبراءة استنادًا إلى قاعدة "لا جريمة ولا عقوبة إلا بنص"

خامسًا: الحاجة إلى العقوبات التكميلية في الجرائم السيبرانية

على الرغم من أهمية العقوبات الأصلية (كالسجن والغرامة) في الحد من الجرائم المعلوماتية، إلا أن التشريعات الحديثة في مجال مكافحة الجريمة السيبرانية لم تكتفِ بها، بل عمدت إلى إدراج عقوبات تكميلية تهدف إلى تحقيق الردع العام والخاص، وإصلاح الخلل الناتج عن الجريمة. إلا أن القانون القطري أغفل النص على هذه العقوبات التكميلية، مما يُعد ثغرة تشريعية ينبغي معالجتها. ومن أبرز صور هذه العقوبات: مصادرة الأجهزة أو البرمجيات التي استُخدمت في ارتكاب الجريمة، الحرمان المؤقت من استخدام تقنيات محددة قد تُستخدم لأغراض ضارة، الإلزام بالتعويض المالي للضحايا عن الأضرار الناجمة، نشر الحكم القضائي في وسائل الإعلام الإلكترونية لتعزيز الردع العام.[2]

---

[1] اللجنة الدائمة للتوعية الأمنية – وزارة الداخلية القطرية. (2019). التوعية بمخاطر الجرائم الإلكترونية.

[2] European Commission. (2021). Cybersecurity: EU strengthens rules to ensure more secure and resilient digital infrastructure. Retrieved from

تعكس هذه العقوبات طبيعة الجريمة المعلوماتية التي لا تقتصر آثارها على الجانب الجنائي فقط، بل تمتد إلى أبعاد اقتصادية وأمنية واجتماعية. كما أن تطبيق هذه العقوبات يُسهم في معالجة الآثار العملية للجريمة، وهو ما تنص عليه العديد من التشريعات المقارنة كالقانون الأوروبي الموحد لمكافحة الجريمة السيبرانية والقانون الأمريكي المعروف بـ Computer Fraud and Abuse Act (CFAA) (12).[1]

المبحث الرابع: أوجه القوة والقصور في السياسة الجنائية القطرية

تمهيد:

تُجسّد السياسة الجنائية الإطار العام الذي تُحدّد من خلاله الدولة رؤيتها في مواجهة الظاهرة الإجرامية، ليس فقط عبر سنّ النصوص العقابية، وإنما من خلال رسم فلسفة التجريم، واختيار العقوبات المناسبة، وبناء مؤسسات إنفاذ القانون، وتكييفها مع التحولات الاجتماعية والتقنية. وفي ظل تصاعد الجرائم الإلكترونية وعلى رأسها جريمة القرصنة، أضحى من الضروري إعادة النظر في الأسس التقليدية للسياسة الجنائية، بما يضمن فعاليتها في عصر رقمي متسارع. وقد جاء القانون القطري رقم (14) لسنة 2014 بشأن مكافحة الجرائم الإلكترونية كمبادرة تشريعية مهمة تُشكّل أساسًا لهذه المواجهة. غير أن التطبيق العملي والتطور المستمر في أساليب الجريمة التقنية كشفا عن جوانب قوة في القانون تستحق التقدير، وأوجه قصور تتطلب التعديل والتطوير.

أولاً: أوجه القوة في السياسة الجنائية القطرية

مثّل إصدار القانون رقم (14) لسنة 2014 خطوة رائدة من المشرّع القطري، حيث جاء في وقت لم تكن فيه معظم دول الخليج قد تبنّت تشريعًا متخصصًا في الجرائم الإلكترونية. وقد أسهم ذلك في ملء فراغ تشريعي حرج، ووفّر مرجعية قانونية واضحة تُمكن الجهات القضائية والأمنية من التصدي للجريمة الرقمية في أطر قانونية دقيقة[3]. ومن أبرز مزايا القانون القطري شمولية نصوصه، إذ اشتمل على تجريم صور متعددة من أفعال القرصنة، مثل الدخول غير المشروع، والتعديل أو الحذف أو الإتلاف العمدي للمعلومات، والتنصت

[1] United States Congress. (1986). Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

أو اعتراض البيانات أثناء نقلها، والتعدي على النظم المعلوماتية السيادية، مما يُظهر محاولة المشرّع لإحاطة الجريمة الرقمية من مختلف جوانبها[1].

ومن ملامح القوة الأخرى في السياسة العقابية لهذا القانون اعتماده على العقوبات المركبة، حيث قرن الحبس بالغرامة المالية في أغلب صوره التجريمية. ويعكس هذا التوجه وعيًا تشريعيًا بطبيعة مرتكبي هذه الجرائم الذين غالبًا لا ينتمون إلى الفئات الإجرامية التقليدية، مما يجعل العقوبة المالية ذات أثر ردعي فعّال[21]. ويُحسب للمشرع القطري كذلك اهتمامه الواضح بحماية البنية المعلوماتية ذات الطابع السيادي، حيث شددت المادة (9) العقوبة إذا وقعت الجريمة على نظم تابعة لجهات أمنية أو عسكرية، في اعتراف ضمني بأن الأمن السيبراني يشكل امتدادًا مباشرًا للأمن القومي للدولة.

ثانياً: أوجه القصور في السياسة الجنائية القطرية:

رغم الإيجابيات التي تحققت بفضل القانون، إلا أن هناك عددًا من أوجه القصور التي تقلل من فعاليته، لعل أبرزها غياب النصوص الصريحة التي تُجرّم الشروع في الجريمة الإلكترونية، أو المشاركة فيها بالتحريض أو المساعدة أو توفير الأدوات التقنية. وتُعد هذه الثغرة مؤثرة للغاية، خاصة أن الجرائم الرقمية غالبًا ما تُرتكب في سياق جماعي منظم، وتُوزّع فيها الأدوار الفنية والقانونية بين عدة أطراف، وهو ما يستدعي توسيع نطاق التجريم ليشمل هذه الأدوار غير المباشرة[2].

ويُلاحظ أيضًا أن القانون لم ينص على العقوبات التكميلية أو الوقائية، رغم أهميتها الكبيرة في البيئة السيبرانية. فغياب أدوات مثل المصادرة الإلزامية للأجهزة المستخدمة، أو المنع من استخدام الإنترنت لفترة، أو النشر الرقمي للحكم، يضعف من فاعلية العقوبة في ردع الجريمة، خاصة عند مقارنتها بالتشريع الإماراتي الذي نص بوضوح على هذه العقوبات التكميلية ضمن أحكامه. كما أن القانون القطري لم يتناول الهجمات السيبرانية المتقدمة التي تُستخدم فيها تقنيات الذكاء الاصطناعي، أو تلك التي تتم عبر "الويب المظلم"، أو باستخدام

---

[1] وفاء محمد صافي، الحماية الجنائية لجريمة القرصنة الإلكترونية، مركز الدراسات العربية، 2023.

[2] جاسم محمد جندل: الجرائم الالكترونية، الطبعة الأولى، دار معتز للنشر والتوزيع، عمان، الأردن، 2022.

إنترنت الأشياء، ما يُنتج فجوة تشريعية يصعب سدّها بالقياس أو الاجتهاد القضائي، ويُعرّض بعض الصور المستحدثة من الجريمة للفراغ القانوني.

أما من حيث التجديد التشريعي، فلم يشهد القانون أي تعديل جوهري منذ صدوره عام 2014، رغم التغير الجذري في طبيعة وأساليب الجريمة الرقمية. وفي المقابل، نجد أن الدول التي نجحت نسبيًا في مواجهة هذه الجرائم، مثل مصر والإمارات، قد تبنت سياسة تشريعية مرنة تعتمد على التحديث المستمر وتكييف النصوص مع المستجدات الرقمية.

نستنتج من العرض السابق أن القانون القطري بشأن مكافحة الجرائم الإلكترونية يُشكّل قاعدة تشريعية متقدمة على مستوى المنطقة، إلا أن استمرارية فاعليته تظل رهينة بقدرته على مواكبة التحولات التقنية والتشريعية. فغياب النصوص الخاصة بالشروع والمساهمة، وضعف منظومة العقوبات التكميلية، وغياب تنظيم خاص للجريمة السيبرانية المعقدة، فضلًا عن الجمود التشريعي، كلّها عوامل تُضعف من أثر القانون في تحقيق الردع العام والخاص.

ومن ثمّ، فإن تطوير السياسة الجنائية في هذا المجال يتطلب إعادة النظر في الهيكل القانوني الحالي، وتبني مقاربة مرنة تُراعي خصوصية الجريمة الرقمية، بما في ذلك تحديث القانون بشكل دوري، وتجريم الأفعال المستحدثة، وتوسيع نطاق العقوبات، لضمان الحماية القانونية الفعالة في الفضاء السيبراني.

الخاتمة

في ضوء ما سبق من تحليل علمي مفصل لجريمة القرصنة الإلكترونية من حيث المفهوم، الأركان، العقوبات، وأوجه المعالجة التشريعية المقارنة، يمكن القول إن هذه الجريمة لم تعد مجرد سلوك إجرامي فردي محدود، بل أصبحت ظاهرة جنائية متطورة تتسم بالتنظيم، والتمويه، والتقنيات المعقّدة. إنها تعكس وجهًا جديدًا للجريمة في القرن الحادي والعشرين، حيث تتداخل العوامل التقنية والقانونية والاجتماعية والأمنية، وتفرض على النظم القانونية تحديات لا يمكن تجاوزها بالأدوات التقليدية.

وقد بيّن هذا البحث أن المشرّع القطري، رغم ريادته في إصدار قانون مكافحة الجرائم الإلكترونية سنة 2014، إلا أنه لم يعد قادرًا – بصورته الحالية – على مواجهة أشكال الجريمة الرقمية المتطورة، خصوصًا في ظل غياب التحديث الدوري، وتطور أدوات الجريمة بشكل يفوق التوقعات. فالنصوص الجنائية الثابتة، مهما كانت قوتها، تبقى قاصرة ما لم تُصاحبها رؤية تشريعية ديناميكية قابلة للتطور المستمر، واستجابة واعية للتحولات التقنية.

كما كشف البحث، عبر التحليل المقارن، أن التشريعات في بعض الدول العربية مثل الإمارات ومصر استطاعت أن تُنتج نماذج أكثر مرونة واتساقًا مع البيئة الرقمية، من خلال تجريم الشروع والمساهمة، وتنظيم العقوبات التكميلية، وتحديث النصوص بصفة دورية. وتُعد هذه التجارب مرجعًا مهمًا يمكن للمشرع القطري الاستفادة منها دون إخلال بالخصوصية القانونية للدولة.

ويمكن التأكيد في ضوء ما سبق أن مواجهة جريمة القرصنة الإلكترونية لا تقتصر فقط على إصدار النصوص، بل تتطلب منظومة شاملة تشمل تحديثًا مستمرًا للقانون وبنية مؤسسية متخصصة في التحقيق والقضاء بالإضافة الى منظومة إثبات رقمية متقدمة وتعاونًا دوليًا فعالًا ووعيًا مجتمعيًا بخطورة الجريمة الرقمية.

في هذا البحث لم نقم فقط بتوصيف واقع قانوني، بل كنا نسعى إلى تقديم رؤية إصلاحية متكاملة قابلة للتنفيذ، تُسهم في بناء سياسة جنائية قطرية أكثر فاعلية، وأكثر تماشيًا مع التحولات التكنولوجية المتسارعة. وإذ نأمل أن تكون هذه الورقة لبنة في صرح الدراسات

القانونية الرقمية، ونقطة انطلاق لمزيد من الأبحاث المتخصصة التي تسهم في حماية المجتمع من الجريمة السيبرانية، وترتقي بالنظام العدلي لمستوى التحديات الرقمية الراهنة والمستقبلية.

النتائج:

وتأسيسًا على ما سبق، خلص البحث إلى النتائج التالية:

1. أن جريمة القرصنة الإلكترونية تُعد من الجرائم المركّبة والمتطورة تقنيًا، وتتسم بطابع عابر للحدود، مما يجعل مكافحتها تتطلب أدوات قانونية مرنة ومحدثة باستمرار، تتجاوز النمط التقليدي في التجريم والعقاب.
2. رغم أن المشرّع القطري بادر بإصدار قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، إلا أن هذا القانون يفتقر إلى عدد من المقومات الجوهرية اللازمة لمجابهة الجريمة الرقمية المعاصرة، خاصة من حيث شمول التجريم وحداثة الصور المغطاة قانونًا.
3. اتضح من الدراسة أن التشريع القطري لم ينص صراحة على تجريم الشروع في الجريمة الإلكترونية أو المساهمة الجنائية التقنية، رغم شيوع هذه الصور في الواقع العملي، الأمر الذي يُشكل فراغًا تشريعيًا مؤثرًا في فاعلية الملاحقة الجنائية.
4. أن القانون يركز على العقوبات الأصلية، لكنه يُغفل تمامًا العقوبات التكميلية ذات الطابع الوقائي، مثل المصادرة الإلكترونية، وحظر استخدام الوسائل التقنية، ونشر الأحكام القضائية عبر الوسائط الرقمية، وهي أدوات باتت ضرورية لتحقيق الردع في البيئة السيبرانية.
5. يُلاحظ ضعف استجابة القانون القطري لتطور صور القرصنة الحديثة، مثل الجرائم المرتبطة بالذكاء الاصطناعي، وإنترنت الأشياء، والعملات المشفرة، والشبكات المظلمة، وهو ما يحدّ من فاعليته ويجعل التكييف القضائي في بعض الحالات محل اجتهاد غير مضمون النتائج.
6. أظهرت مقارنة القانون القطري بنظيره الإماراتي والمصري أن بعض الدول العربية خطت خطوات متقدمة في مواجهة القرصنة الإلكترونية، خاصة في ما

يتعلق بتفصيل الصور المجرّمة، وتبني العقوبات التكميلية، وتضمين نصوص خاصة بالشروع والمشاركة.

7. أن السياسة الجنائية القطرية، وإن كانت متقدمة على مستوى المبادرة التشريعية، إلا أنها تعاني من جمود في التحديث، وعدم وجود آلية واضحة لإعادة تقييم القانون ومراجعته في ضوء التحولات التقنية والمجتمعية المتسارعة.
8. أخيرًا، خلص البحث إلى أن تعزيز فاعلية القانون القطري في مواجهة جريمة القرصنة الإلكترونية يتطلب إصلاحًا تشريعيًا ومؤسسيًا متكاملًا، لا يقتصر على تعديل النصوص، بل يشمل تطوير آليات التطبيق وتخصيص جهات متخصصة في التحقيق والفصل في هذا النوع من الجرائم.

التوصيات:

وبناء على هذه النتائج، يوصي البحث بما يلي:

1. تعديل القانون رقم (14) لسنة 2014 لإدراج نصوص صريحة تُجرّم الشروع في الجرائم الإلكترونية، باعتباره من الأفعال الشائعة في هذا النوع من الجرائم، لا سيما مع الطابع الرقمي الذي يسمح برصد المحاولة قبل تحقق النتيجة.
2. إدراج أحكام واضحة تتعلق بالمساهمة الجنائية في الجرائم الإلكترونية، تشمل التحريض، والمساعدة، وتوفير الأدوات التقنية، أسوة بما ورد في التشريعين المصري والإماراتي، وذلك لتفادي الإفلات من العقاب في الحالات الجماعية أو الشبكية للجريمة.
3. إضافة عقوبات تكميلية ذات طابع تقني إلى منظومة العقوبات الحالية، كالمصادرة الإلكترونية، أو المنع المؤقت من استخدام وسائل تقنية محددة، أو النشر الإلكتروني للأحكام القضائية، بما يتلاءم مع طبيعة الجريمة وبيئتها الرقمية.
4. تحديث نطاق التجريم ليشمل صور الجريمة المستحدثة، مثل الجرائم المرتبطة بالذكاء الاصطناعي، وإنترنت الأشياء، والعملات الرقمية، والقرصنة عبر

الشبكات المظلمة، من خلال إعادة صياغة المواد المتعلقة بأركان الجريمة الإلكترونية.

5. إصدار لوائح تنفيذية مفصلة تواكب النصوص القانونية، تحدد فيها آليات التحقيق الرقمي، ووسائل الإثبات الإلكتروني، وضوابط استخدام الأدلة التقنية أمام القضاء، بما يحقق الأمن القانوني ويوفر ضمانات المحاكمة العادلة.
6. إنشاء نيابة عامة ودوائر قضائية متخصصة في الجرائم الإلكترونية، تتولى حصريًا التحقيق والفصل في هذا النوع من القضايا، مع تدريب مستمر للكفاءات القانونية على المستجدات التقنية في بيئة الجريمة الرقمية.
7. إقرار آلية دورية لمراجعة وتحديث قانون مكافحة الجرائم الإلكترونية، من خلال تشكيل لجنة وطنية دائمة تُكلّف بمراجعة التحديات التقنية والمستجدات الإجرامية كل ثلاث سنوات، وتقديم مقترحات بالتعديلات اللازمة.
8. تعزيز التعاون القضائي الدولي والإقليمي في مجال الجرائم السيبرانية، والانضمام إلى الاتفاقيات الدولية ذات الصلة، وفي مقدمتها اتفاقية بودابست، لضمان تبادل المعلومات، وملاحقة الجناة عبر الحدود بكفاءة أكبر.
9. دعم البحث العلمي القانوني في مجال الجرائم الرقمية، وتشجيع الجامعات ومراكز الدراسات القانونية في قطر على إنتاج بحوث تطبيقية تساهم في تطوير التشريع والسياسات الجنائية المرتبطة بالأمن السيبراني.
10. إطلاق حملات توعية رقمية قانونية للمجتمع، تستهدف نشر الثقافة القانونية حول الجرائم الإلكترونية والعقوبات المقررة لها، بهدف الوقاية والردع المجتمعي قبل وقوع الجريمة.

المراجع

أولاً: المصادر الأولية

1. قانون العقوبات المصري رقم 58 لسنة 1937م.
2. قانون العقوبات القطري رقم 11 لسنة 2004.
3. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
4. قانون مكافحة الجرائم الإلكترونية القطري رقم 14 لسنة 2014.
5. نظام مكافحة جرائم المعلوماتية السعودي، مرسوم ملكي رقم م/17 بتاريخ 1428/3/8هـ.
6. قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
7. قانون مكافحة جرائم تكنولوجيا المعلومات الكويتي رقم 63 لسنة 2015.
8. قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021.

ثانياً: الكتب

1. بشرى حسين الحمداني، القرصنة الإلكترونية: أسلحة الحرب الحديثة، دار أسامة، عمان، 2014.
2. جاسم محمد جندل، الجرائم الإلكترونية، دار معتز، عمان، 2022.
3. حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، جامعة السادات، مصر، 2021.
4. حنان ريحان المضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2014.
5. خالد الغثبر ومحمد القحطاني، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، الرياض، 1429هـ.
6. فهد العتيبي، تحليل فعالية التشريعات العقابية في مواجهة الجرائم الإلكترونية: دراسة مقارنة، مؤسسة الفكر العربي، 2017.
7. سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي، دروب المعرفة، الإسكندرية، 2022.

8. مداوي سعيد القحطاني، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون، 2016.
9. عمر سالم، نحو قانون جنائي للصحافة، دار النهضة العربية، القاهرة، 1998.
10. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع للإنترنت، دار النهضة العربية، القاهرة، 2009.
11. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008.
12. وفاء محمد صافي، الحماية الجنائية لجريمة القرصنة الإلكترونية للملكية الفكرية الإلكترونية: دراسة مقارنة، مركز الدراسات العربية، 2023.

ثالثاً: الرسائل العلمية

1. أحمد، معاذ أحمد عبد الرازق، أمن المعلومات ودوره في الحد من القرصنة الإلكترونية، ماجستير، جامعة أم درمان الإسلامية، السودان، 2016.
2. بشير محمد الفيتوري كندي، الجرائم المعلوماتية في التشريع الليبي: دراسة مقارنة، دكتوراه، جامعة القاهرة، 2016–2017.
3. خالد سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، ماجستير، جامعة قطر، 2019.
4. سامي صالح الكعبي، مفهوم الأمن القومي في ظل العولمة: النظام الإقليمي العربي نموذجاً، ماجستير، جامعة الشرق الأوسط، 2014.
5. عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، ماجستير، جامعة الشرق الأوسط، 2014.
6. فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة، جامعة الجزائر، 2018.
7. نجاة دحو، فاطمة أولاد علي، جريمة القرصنة الإلكترونية في التشريع الجزائري، ماجستير، جامعة غرداية، 2021–2022.

8. محمد خليل، السياسة الجنائية في مواجهة الجرائم الإلكترونية: دراسة مقارنة، دار النهضة العربية، 2020.
9. سعيد عبد الله، تقييم فعالية التشريعات الجنائية في مكافحة الجرائم الإلكترونية: دراسة مقارنة بين الدول العربية، دار الكتب القانونية، 2019.
10. حمزة سامي محمد، الحماية الجنائية من الجرائم الإلكترونية في التشريعات العربية: دراسة مقارنة، مجلة الدراسات القانونية المعاصرة، جامعة عين شمس، العدد 12، 2020.

رابعاً: المجلات والندوات

1. حسون عبيد هجيج، صفاء كاظم غازي، "آثار جريمة قرصنة البريد الإلكتروني"، مجلة القادسية للقانون والعلوم السياسية، العدد 2، المجلد 7، 2016.
2. خالد حامد مصطفى، "المسؤولية الجنائية لناشري الخدمات التقنية"، مجلة رؤى استراتيجية، الإمارات، 2013.
3. رامي متولي القاضي، "المواجهة الجنائية لجرائم تقنية المعلومات في مصر"، مجلة البحوث القانونية والاقتصادية، العدد 45، جامعة المنصورة، 2021.
4. سعاد شاكر بعيوي، "جريمة الابتزاز الإلكتروني"، مجلة ميسان للدراسات القانونية المقارنة، جامعة ميسان، 2019.
5. سيناء عبد الله محسن، "المواجهة التشريعية للجرائم المتصلة بالكمبيوتر"، ندوة إقليمية، الدار البيضاء، 2007.
6. شيرين دبابنة، "الجرائم الإلكترونية، القرصنة"، مجلة الدراسات المالية والمصرفية، الأردن، 2015.
7. مريم بالطة، آسيا برغيت، "الأمن المعلوماتي في مواجهة القرصنة الإلكترونية"، مجلة دراسات حقوق الإنسان، المجلد 7، العدد 1، 2022.
8. هشام فريد رستم، "أصول التحقيق الفني"، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، 2000.

9. أنور محمد صدقي، "إضاءات حول قانون الجرائم الإلكترونية القطري"، المجلة القانونية والقضائية، وزارة العدل القطرية، 2015.
10. مرفت محمود طيب، "الجريمة الإلكترونية: الأنواع والأدوات والعقوبات"، المركز العربي لأبحاث الفضاء الإلكتروني، 2017.
11. "الجرائم الإلكترونية: القرصنة الإلكترونية"، مجلة فضاء المعرفة القانونية، 15 نوفمبر 2023.
12. سامي حمدان الرواشدة، "جريمة الدخول غير المشروع في القانون الجنائي القطري"، مجلة كلية القانون الكويتية العالمية، 2019.
13. الموسوي، أحمد حسن. الجرائم الإلكترونية وسبل مكافحتها في التشريع العربي المقارن. بيروت: المركز العربي للبحوث القانونية والقضائية. (2021)

خامساً: المصادر الدولية

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Budapest Convention.