ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المجلد التاسع – العدد الحادي والتسعون
تاريخ الإصدار: 2 – أيّار – 2026م
www.ajsp.net

"اركان الجرائم الإلكترونية الواقعة على سيادة الدولة"

(بحث مستل من أطروحة دكتوراه في القانون العام)

إعداد الباحث: عايد غازي جبر الخفاجي

بإشراف: الاستاذ الدكتور كمال حماد

١٤٤٧هـ/٢٠٢٦م

Received: 25/04/2026 | Revised: 26/04/2026 | Accepted: 01/05/2026 | Published: 02/05/2026

Abstract:

Cybercrimes affecting state sovereignty represent one of the most serious forms of modern criminal activity, as they pose a direct threat to national security, political and economic stability, and the integrity of governmental institutions and digital infrastructure. These crimes have evolved beyond traditional forms to include cyberattacks, unauthorized access to governmental systems, cyber espionage, dissemination of disinformation, and interference in electoral processes, all of which aim to undermine state authority or weaken its sovereign functions.

The danger of such crimes lies in their transnational nature, the difficulty of identifying perpetrators, and the rapid development of the techniques used to commit them. These factors create significant challenges for national legal systems and law enforcement agencies. Moreover, such crimes may be committed by individuals, organized groups, or even state-sponsored actors, further complicating legal and security responses.

This study aims to define cybercrimes affecting state sovereignty, analyze their forms and legal elements, and examine the position of national legislations, particularly Iraqi law, in criminalizing such acts. It also explores international efforts to combat these crimes, highlights the challenges in their prosecution, and proposes mechanisms to strengthen legal and technical protection against them.

Keywords: cybercrime, state sovereignty, cybersecurity, cyberattacks, criminal law, national security.

ملخص البحث

تُعدّ الجرائم الإلكترونية الواقعة على سيادة الدولة من أخطر صور الإجرام المعاصر، لما تنطوي عليه من تهديد مباشر لأمن الدولة واستقرارها السياسي والاقتصادي، فضلًا عن تأثيرها على البنية التحتية الرقمية والمؤسسات الحكومية. ولم تعد هذه الجرائم تقتصر على الأفعال التقليدية، بل تطورت لتشمل الهجمات السيبرانية، واختراق الأنظمة الحكومية، والتجسس الإلكتروني، ونشر المعلومات المضللة، والتدخل في العمليات الانتخابية، وغيرها من الأنشطة التي تستهدف تقويض سلطة الدولة أو إضعاف قدرتها على أداء وظائفها السيادية.

وتبرز خطورة هذه الجرائم في طبيعتها العابرة للحدود، وصعوبة تتبع مرتكبيها، وتطور وسائل ارتكابها، الأمر الذي يطرح تحديات كبيرة أمام التشريعات الوطنية وأجهزة إنفاذ القانون. كما أن هذه الجرائم قد تُرتكب من قبل أفراد أو جماعات منظمة أو حتى جهات مدعومة من دول، مما يزيد من تعقيد مواجهتها قانونيًا وأمنيًا.

ويهدف هذا البحث إلى بيان مفهوم الجرائم الإلكترونية الواقعة على سيادة الدولة، وتحليل صورها وأركانها القانونية، وبيان موقف التشريعات الوطنية، ولا سيما القانون العراقي، من تجريمها، فضلًا عن استعراض الجهود الدولية في مكافحتها. كما يتناول البحث التحديات التي تواجه ملاحقة هذه الجرائم، ويقترح سبل تعزيز الحماية القانونية والتقنية لمواجهة هذا النوع من الجرائم.

الكلمات المفتاحية: الجرائم الإلكترونية، سيادة الدولة، الأمن السيبراني، الهجمات الإلكترونية، القانون الجنائي، حماية الدولة.

المجلد التاسع – العدد الحادي والتسعون
تاريخ الإصدار: 2 – أيّار – 2026م
www.ajsp.net

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

How to Cite This Article
الخفاجي، ع. غ. ج. (2026). أركان الجرائم الإلكترونية الواقعة على سيادة الدولة (بحث مستل من أطروحة دكتوراه في القانون العام). المجلة العربية للنشر العلمي (AJSP)، 9(91)، (769 -783).
(Individual DOI)
رابط الأرشفة الدولية المباشر والمخصص لبحثكم: https://doi.org/10.36571/ajsp.91.32

AJSP | Vol. 9 | Issue 91 | DOI: https://doi.org/10.36571/ajsp.91 AJSP ORCID: https://orcid.org/0009-0005-8048-2082

المقدمة:

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات إلى اعتماد الدول بصورة واسعة على الأنظمة المعلوماتية في إدارة المرافق العامة والخدمات والقطاعات الأمنية والعسكرية والاقتصادية. ومع هذا التحول برزت الجرائم الإلكترونية الواقعة على سيادة الدولة بوصفها من أخطر صور الإجرام المعاصر، لأنها تستهدف الأنظمة الحكومية والبنية التحتية الرقمية بما قد يفضي إلى أضرار جسيمة تمس الأمن الوطني والاستقرار السياسي والاقتصادي.

وعلى المستوى الدولي، حظيت هذه الجرائم باهتمام متزايد بسبب طبيعتها العابرة للحدود، إذ قد يُرتكب الفعل من خارج إقليم الدولة المستهدفة. وقد أسهمت الاتفاقيات الدولية، ولا سيما اتفاقية بودابست لعام 2001، في وضع إطار قانوني للتجريم وتعزيز التعاون الدولي في التحقيق والملاحقة.

وانطلاقًا من ذلك، تقتضي دراسة الجرائم الإلكترونية الواقعة على سيادة الدولة تحليل أركانها القانونية، وذلك من خلال بيان الركن المفترض المتمثل في وجود نظام معلوماتي أو بنية رقمية تابعة للدولة، ثم الركن المادي الذي يتمثل في السلوك الإجرامي الماس بهذه الأنظمة، وأخيرًا الركن المعنوي القائم على توافر القصد الجنائي للإضرار بمصالح الدولة أو أمنها أو سيادتها.

أولًا: مشكلة البحث

شهد العالم في العقود الأخيرة تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى بروز أنماط جديدة من الجرائم تُرتكب عبر الفضاء الإلكتروني، ومن أخطرها الجرائم الإلكترونية التي تستهدف سيادة الدولة. فهذه الجرائم لم تعد تقتصر على الاعتداء على الأفراد أو الأموال، بل امتدت لتشمل المساس بالمصالح العليا للدولة، من خلال اختراق الأنظمة الحكومية، والتجسس الإلكتروني، وتعطيل البنى التحتية الحيوية، ونشر المعلومات المضللة بهدف زعزعة الاستقرار السياسي والأمني.

وتكمن الإشكالية في أن هذه الجرائم تتسم بطبيعة خاصة، من حيث صعوبة تحديد مرتكبيها، وطابعها العابر للحدود، وتطور وسائل ارتكابها، مما يجعل مواجهتها في إطار القواعد التقليدية للقانون الجنائي أمرًا بالغ التعقيد. كما أن التداخل بين القانون الوطني والقانون الدولي في هذا المجال يثير تساؤلات مهمة حول مدى كفاية التشريعات القائمة في حماية سيادة الدولة من هذه التهديدات المستحدثة.

ثانيا: أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف، من أبرزها:

بيان مفهوم الجرائم الإلكترونية الواقعة على سيادة الدولة وتحديد خصائصها.

تحليل صور هذه الجرائم وأركانها القانونية في ضوء التشريعات الوطنية.

دراسة موقف القانون العراقي من تجريم هذه الأفعال ومدى كفايته في مواجهتها.

تسليط الضوء على دور القانون الدولي والاتفاقيات الدولية في مكافحة هذه الجرائم.

اقتراح سبل تطوير الإطار القانوني والتقني لمواجهة الجرائم الإلكترونية التي تمس سيادة الدولة.

ثالثا: منهجية البحث

يعتمد هذا البحث على المنهج الوصفي التحليلي، من خلال دراسة النصوص القانونية المتعلقة بالجرائم الإلكترونية وتحليلها، وبيان مدى فعاليتها في حماية سيادة الدولة. كما يستعين بالمنهج المقارن في بعض المواضع، من خلال الإشارة إلى بعض التشريعات والاتفاقيات الدولية ذات الصلة، بهدف الوقوف على أوجه القصور وإمكانيات التطوير.

وسوف يتم تقسيم هذا البحث لمطلبين نتناول في المطلب الأول: الركن المفترض اما المطلب الثاني فنتناول فيه الركن المادي والركن المعنوي

المطلب الأول: الركن المفترض

يُقصد بالركن المفترض في الجرائم الإلكترونية الواقعة على سيادة الدولة وجود بيئة تقنية أو بنية معلوماتية تابعة للدولة تكون محل الاعتداء أو الوسيلة التي تُرتكب من خلالها الجريمة. ويتميز هذا الركن في الجرائم الإلكترونية الماسة بسيادة الدولة بارتباطه بالبنية التحتية الرقمية للمؤسسات الحكومية أو الأنظمة المعلوماتية التي تعتمد عليها الدولة في إدارة شؤونها السياسية والأمنية والاقتصادية. ولذلك فإن قيام هذا النوع من الجرائم يفترض وجود نظام معلوماتي أو شبكة إلكترونية أو قاعدة بيانات حكومية تُستخدم في إدارة المرافق العامة أو حفظ المعلومات السيادية للدولة.[1]

وقد أدى التحول الرقمي في عمل الحكومات إلى اعتماد المؤسسات الحكومية على الأنظمة المعلوماتية في إدارة العديد من الأنشطة الحيوية، مثل إدارة البيانات الحكومية، وتشغيل شبكات الاتصالات الوطنية، وإدارة الأنظمة المالية والاقتصادية، وكذلك إدارة الأنظمة العسكرية والأمنية. ونتيجة لذلك أصبحت هذه الأنظمة هدفًا للعديد من الهجمات الإلكترونية التي تهدف إلى اختراقها أو تعطيلها أو الحصول على المعلومات السرية التي تحتويها. ومن ثم فإن الركن المفترض في الجرائم الإلكترونية التي تمس سيادة الدولة يتمثل في وجود هذه الأنظمة المعلوماتية الحكومية التي تُشكل البنية التحتية الرقمية للدولة.[2] وسوف نقسم هذا المطلب الى فرعين الأول الركن المفترض في التشريعات الوطنية اما الفرع الثاني الركن المفترض في التشريعات الدولية .

الفرع الأول : الركن المفترض في التشريعات الوطنية

وقد أدركت التشريعات الوطنية خطورة الاعتداء على الأنظمة المعلوماتية الحكومية، ولذلك اتجهت إلى تجريم الأفعال التي تستهدف هذه الأنظمة أو البيانات المرتبطة بها. فعلى سبيل المثال، نص قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 على

[1] عبد الفتاح بيومي حجازي، الجرائم المعلوماتية عبر الإنترنت (القاهرة: دار الفكر الجامعي، 2012)، ص 161.
[2] محمد أمين البكري، القانون الجنائي وتكنولوجيا المعلومات (الإسكندرية: دار الجامعة الجديدة، 2016)، ص 209.

تجريم الدخول غير المشروع إلى الأنظمة المعلوماتية أو المواقع الإلكترونية التابعة للدولة أو الأشخاص الاعتبارية العامة، وكذلك تجريم تعطيل هذه الأنظمة أو إتلاف البيانات الحكومية أو التلاعب بها. ويُظهر هذا النص أن وجود النظام المعلوماتي الحكومي يُعد عنصرًا مفترضًا لقيام الجريمة، لأن الاعتداء يقع على هذا النظام أو البيانات المرتبطة به.[3]

كما تضمنت بعض التشريعات العربية نصوصًا مشابهة تهدف إلى حماية الأنظمة المعلوماتية الحكومية من الاعتداءات الإلكترونية، ومن ذلك قانون مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة رقم 34 لسنة 2021، الذي جرم الأفعال التي تستهدف المواقع الإلكترونية الحكومية أو الأنظمة المعلوماتية التابعة للدولة أو التي تهدف إلى تعطيل الخدمات العامة أو الإضرار بالبنية التحتية الرقمية للدولة. ويُعد وجود هذه الأنظمة الحكومية شرطًا أساسيًا لقيام الجرائم الإلكترونية التي تمس سيادة الدولة.[4]

أما في التشريعات التي تعتمد على القواعد العامة في قانون العقوبات، فقد تم تطبيق النصوص المتعلقة بجرائم أمن الدولة أو التجسس أو الاعتداء على المرافق العامة على الأفعال التي تُرتكب عبر الوسائل الإلكترونية. ففي العراق مثلًا يمكن تطبيق أحكام قانون العقوبات رقم 111 لسنة 1969 المعدل المتعلقة بجرائم أمن الدولة أو الاعتداء على المصالح الحكومية على الأفعال التي تستهدف الأنظمة المعلوماتية الحكومية أو البيانات الرسمية، باعتبار أن هذه الأفعال تمثل اعتداءً على سيادة الدولة ومصالحها الأساسية.[5]

الفرع الثاني :الركن المفترض في التشريعات الدولية

وعلى الصعيد الدولي، فقد اهتمت الاتفاقيات الدولية بمكافحة الجرائم التي تستهدف الأنظمة المعلوماتية للدول، نظرًا لما قد تشكله من تهديد للأمن الدولي والاستقرار السياسي. ومن أبرز هذه الاتفاقيات اتفاقية بودابست للجرائم الإلكترونية لعام 2001 التي نصت على تجريم

[3] قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
[4] قانون مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة رقم 34 لسنة 2021.
[5] قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.

مجموعة من الأفعال المرتبطة باستخدام الأنظمة المعلوماتية، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية أو اعتراض البيانات أو تعطيل الأنظمة الإلكترونية. وقد شكلت هذه الاتفاقية إطارًا قانونيًا دوليًا لمكافحة الجرائم المرتكبة عبر شبكات الحاسوب والإنترنت، بما في ذلك الجرائم التي تستهدف الأنظمة المعلوماتية الحكومية.[6]

كما أن حماية سيادة الدول في الفضاء الإلكتروني أصبحت محل اهتمام متزايد في القانون الدولي المعاصر، حيث تسعى الدول والمنظمات الدولية إلى وضع قواعد قانونية تنظم استخدام الفضاء السيبراني وتمنع الاعتداء على البنية التحتية الرقمية للدول. ويعكس ذلك إدراك المجتمع الدولي لخطورة الجرائم الإلكترونية التي تستهدف الأنظمة المعلوماتية الحكومية، وما قد تسببه من أضرار تمس الأمن الوطني والسيادة الرقمية للدولة.[7]

وقد أكدت التطبيقات القضائية الحديثة أهمية الركن المفترض في الجرائم الإلكترونية التي تمس سيادة الدولة، حيث اعتبرت المحاكم أن استخدام الأنظمة المعلوماتية الحكومية أو استهدافها يمثل عنصرًا أساسيًا في تكوين هذا النوع من الجرائم. ففي حكم صادر عن إحدى المحاكم المصرية، اعتُبر اختراق موقع إلكتروني حكومي والحصول على بيانات رسمية منه جريمة يعاقب عليها القانون، نظرًا لكون الموقع الإلكتروني يمثل جزءًا من البنية المعلوماتية للدولة.[8]

كما أصدرت بعض المحاكم المقارنة أحكامًا تتعلق بالهجمات الإلكترونية التي تستهدف الأنظمة الحكومية، حيث اعتبرت أن تعطيل موقع حكومي أو التلاعب بالبيانات الرسمية يمثل اعتداءً على المصالح الأساسية للدولة. وقد قضت إحدى المحاكم في دولة الإمارات بإدانة متهم قام باختراق نظام معلوماتي تابع لجهة حكومية ومحاولة الحصول على بيانات سرية، معتبرة أن هذا الفعل يشكل جريمة إلكترونية تمس سيادة الدولة.[9]

[6] Council of Europe, Convention on Cybercrime (Budapest Convention), Budapest, 2001.
[7] Ahmad Abdel-Zaher, Cybercrime and the Law (Cairo: Dar Al-Nahda Al-Arabiya, 2018), 134.
[8] محكمة النقض المصرية، الطعن رقم 20458 لسنة 92 قضائية، جلسة 15 شباط 2023.
[9] حكم محكمة جنايات أبوظبي، القضية رقم 522 لسنة 2023 بشأن اختراق نظام معلوماتي حكومي...

ومن خلال ما تقدم يتضح أن الركن المفترض في الجرائم الإلكترونية الواقعة على سيادة الدولة يتمثل في وجود النظام المعلوماتي الحكومي أو البنية التحتية الرقمية التي تُشكل جزءًا من مؤسسات الدولة أو مرافقها العامة. ويُعد هذا الركن عنصرًا أساسيًا في تكوين الجريمة الإلكترونية التي تمس سيادة الدولة، لأنه يحدد محل الاعتداء الذي يقع على الأنظمة المعلوماتية الحكومية أو البيانات الرسمية، ويُميز هذه الجرائم عن غيرها من الجرائم الإلكترونية التي تستهدف الأفراد أو الأموال.

المطلب الثاني: الركن المادي والركن المعنوي

سوف يتم تقسيم هذا المطلب لفرعين نتناول في الفرع الاول الركن المادي اما الفرع الثاني فنتناول فيه الركن المعنوي

الفرع الاول : الركن المادي

يقصد بالركن المادي في الجرائم الإلكترونية الواقعة على سيادة الدولة السلوك الخارجي الذي يصدر عن الجاني ويترتب عليه الاعتداء على الأنظمة المعلوماتية الحكومية أو البنية التحتية الرقمية للدولة أو البيانات المرتبطة بها. ويتمثل هذا الركن في مجموعة الأفعال المادية التي تتم عبر الوسائل الإلكترونية أو الأنظمة الحاسوبية بقصد الإضرار بالمصالح الأساسية للدولة أو تعطيل مرافقها العامة أو المساس بأمنها المعلوماتي. ويتميز الركن المادي في هذا النوع من الجرائم بخصوصية ترتبط بطبيعة الوسائل المستخدمة في ارتكابها، إذ يتم تنفيذ السلوك الإجرامي عبر شبكات الحاسوب أو الإنترنت أو الأنظمة الرقمية المتصلة بالبنية التحتية للدولة، الأمر الذي يجعلها تختلف عن الجرائم التقليدية التي تعتمد على الوسائل المادية المباشرة.[10]

وتتخذ الأفعال التي تشكل الركن المادي لهذه الجرائم صورًا متعددة، من أبرزها الدخول غير المشروع إلى الأنظمة المعلوماتية الحكومية أو اختراق المواقع الإلكترونية الرسمية للدولة أو المؤسسات العامة، وكذلك تعطيل هذه الأنظمة أو إتلاف البيانات الحكومية أو التلاعب بها.

[10] عبد الفتاح بيومي حجازي، الجرائم المعلوماتية عبر الإنترنت (القاهرة: دار الفكر الجامعي، 2012)، ص 168.

كما قد يتمثل الركن المادي في اعتراض البيانات المتبادلة عبر الشبكات الحكومية أو نشر المعلومات السرية التي تتعلق بأمن الدولة أو مصالحها الاستراتيجية. وقد يؤدي ارتكاب هذه الأفعال إلى تعطيل الخدمات العامة أو إلحاق أضرار جسيمة بالبنية التحتية الرقمية للدولة، الأمر الذي يبرر تدخل القانون الجنائي لحماية هذه المصالح الحيوية.[11]

وقد اهتمت التشريعات الوطنية بتجريم هذه الأفعال، فنصت العديد من القوانين على معاقبة كل من يقوم بالدخول غير المشروع إلى الأنظمة المعلوماتية الحكومية أو تعطيلها أو إتلاف البيانات المرتبطة بها. ففي مصر نص قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على تجريم الدخول غير المشروع إلى موقع أو حساب أو نظام معلوماتي مملوك للدولة أو لإحدى الجهات العامة، كما جرم تعطيل الأنظمة المعلوماتية أو إتلاف البيانات أو البرامج المرتبطة بها، وفرض عقوبات مشددة إذا كان الاعتداء موجّهًا إلى جهة حكومية أو يمس الأمن القومي للدولة. ويعكس هذا التشريع إدراك المشرع لخطورة الأفعال التي تستهدف الأنظمة المعلوماتية الحكومية باعتبارها جزءًا من سيادة الدولة وأمنها الرقمي.[12]

كما اتجهت بعض التشريعات العربية إلى تجريم الأفعال التي تؤدي إلى تعطيل البنية التحتية الرقمية للدولة أو المساس بالمصالح العامة عبر الوسائل الإلكترونية. ومن ذلك قانون مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة رقم 34 لسنة 2021، الذي جرم الأفعال التي تؤدي إلى تعطيل المواقع الحكومية أو الأنظمة المعلوماتية التابعة للمؤسسات العامة أو الإضرار بالخدمات العامة عبر الوسائل الرقمية، وفرض عقوبات صارمة على مرتكبي هذه الأفعال نظرًا لما قد تسببه من تهديد للأمن الوطني.[13]

أما في التشريعات التي لم تعتمد قوانين خاصة بالجرائم الإلكترونية، فقد تم تطبيق القواعد العامة في قانون العقوبات على الأفعال التي تُرتكب عبر الوسائل الإلكترونية إذا كانت تمس أمن الدولة أو مصالحها الأساسية. ففي العراق مثلًا يمكن تطبيق النصوص المتعلقة بجرائم

[11] محمد أمين البكري، القانون الجنائي وتكنولوجيا المعلومات (الإسكندرية: دار الجامعة الجديدة، 2016)، ص 215.
[12] قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
[13] قانون مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة رقم 34 لسنة 2021.

أمن الدولة المنصوص عليها في قانون العقوبات رقم 111 لسنة 1969 المعدل على الأفعال التي تستهدف الأنظمة المعلوماتية الحكومية أو البيانات الرسمية، مثل جرائم التجسس أو إفشاء الأسرار أو الاعتداء على المرافق العامة، وذلك إذا تم ارتكاب هذه الأفعال عبر الوسائل الإلكترونية أو الشبكات المعلوماتية.[14]

وعلى الصعيد الدولي، فقد سعت الاتفاقيات الدولية إلى تحديد الأفعال التي تشكل جرائم إلكترونية وتوفير إطار قانوني للتعاون بين الدول في مجال مكافحة هذه الجرائم. ومن أبرز هذه الاتفاقيات اتفاقية بودابست للجرائم الإلكترونية لعام 2001 التي نصت على تجريم مجموعة من الأفعال المرتبطة باستخدام الأنظمة المعلوماتية، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، واعتراض البيانات، والتدخل غير المشروع في الأنظمة أو البيانات، وكذلك إساءة استخدام الأجهزة أو البرامج التي تُستخدم في ارتكاب الجرائم الإلكترونية. وقد شكلت هذه الاتفاقية خطوة مهمة نحو توحيد الجهود الدولية في مواجهة الجرائم السيبرانية التي قد تستهدف الدول أو مؤسساتها الحكومية.[15]

كما أكدت بعض المبادرات الدولية الحديثة أهمية حماية البنية التحتية الرقمية للدول من الهجمات السيبرانية، نظرًا لما قد تسببه هذه الهجمات من أضرار خطيرة تمس الأمن الدولي والاستقرار السياسي. وقد اعتبر العديد من الفقهاء أن الهجمات الإلكترونية التي تستهدف الأنظمة الحكومية أو البنية التحتية الحيوية قد ترقى في بعض الحالات إلى مستوى الأعمال العدائية التي تهدد الأمن الدولي، خاصة إذا أدت إلى تعطيل الخدمات الأساسية أو الإضرار بالاقتصاد الوطني للدولة.[16]

وقد عكست التطبيقات القضائية الحديثة خطورة الركن المادي في الجرائم الإلكترونية التي تمس سيادة الدولة، حيث أصدرت العديد من المحاكم أحكامًا تتعلق باختراق المواقع الحكومية أو تعطيل الأنظمة المعلوماتية التابعة للدولة. ففي حكم صادر عن محكمة النقض

[14] قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
[15] Council of Europe, Convention on Cybercrime (Budapest Convention), Budapest, 2001.
[16] Ahmad Abdel-Zaher, Cybercrime and the Law (Cairo: Dar Al-Nahda Al-Arabiya, 2018), 141.

المصرية اعتُبر اختراق أحد المواقع الإلكترونية الحكومية ونشر بيانات رسمية دون إذن جريمة إلكترونية يعاقب عليها القانون، نظرًا لما يشكله هذا الفعل من اعتداء على النظام المعلوماتي للدولة.[17]

كما قضت إحدى المحاكم في دولة الإمارات العربية المتحدة بإدانة متهم قام بتنفيذ هجوم إلكتروني أدى إلى تعطيل أحد المواقع الحكومية لفترة زمنية محددة، معتبرة أن هذا الفعل يشكل اعتداءً على البنية التحتية الرقمية للدولة ويستوجب العقوبة المقررة في قانون الجرائم الإلكترونية. وقد أكدت المحكمة في حكمها أن استخدام الوسائل الإلكترونية لتعطيل الخدمات الحكومية يمثل خطرًا جسيمًا على الأمن الوطني ويستوجب مواجهة قانونية صارمة.[18]

ومن خلال ما تقدم يتضح أن الركن المادي في الجرائم الإلكترونية الواقعة على سيادة الدولة يتمثل في مجموعة الأفعال الإجرامية التي تستهدف الأنظمة المعلوماتية الحكومية أو البيانات الرسمية أو البنية التحتية الرقمية للدولة. ويشمل ذلك الاختراق الإلكتروني، وتعطيل الأنظمة المعلوماتية، وإتلاف البيانات الحكومية أو التلاعب بها، وكذلك نشر المعلومات السرية أو اعتراضها عبر الشبكات الإلكترونية. وتُعد هذه الأفعال من أخطر صور الجرائم الإلكترونية نظرًا لما قد تسببه من أضرار تمس الأمن الوطني والسيادة الرقمية للدولة.

الفرع الثاني: الركن المعنوي

يُعد الركن المعنوي أحد الأركان الأساسية في قيام الجرائم الإلكترونية الواقعة على سيادة الدولة، إذ لا يكفي لقيام الجريمة أن يتحقق السلوك المادي المتمثل في الاعتداء على الأنظمة المعلوماتية الحكومية أو البيانات الرسمية، بل يجب أن يكون هذا السلوك قد صدر عن إرادة واعية لدى الجاني مصحوبة بقصد جنائي يهدف إلى تحقيق نتيجة غير مشروعة. ويقصد بالركن المعنوي في هذا السياق الحالة النفسية التي يكون عليها الجاني وقت ارتكاب

[17] محكمة النقض المصرية، الطعن رقم 20458 لسنة 92 قضائية، جلسة 15 شباط 2023.
[18] حكم محكمة جنايات أبوظبي، القضية رقم 522 لسنة 2023 بشأن تعطيل نظام معلوماتي حكومي...

الفعل الإجرامي، والتي تتمثل في علمه بطبيعة فعله غير المشروع واتجاه إرادته إلى ارتكابه رغم علمه بما قد يترتب عليه من آثار تمس مصالح الدولة أو أمنها أو سيادتها.[19]

ويتخذ الركن المعنوي في الجرائم الإلكترونية الماسة بسيادة الدولة غالبًا صورة القصد الجنائي العمدي، حيث يكون الجاني على علم بطبيعة النظام المعلوماتي الذي يستهدفه وبكونه تابعًا لجهة حكومية أو مؤسسة رسمية، ومع ذلك يتجه بإرادته إلى اختراق هذا النظام أو تعطيله أو الحصول على البيانات المرتبطة به. ويستلزم تحقق القصد الجنائي في هذه الجرائم عنصرين أساسيين هما العلم والإرادة؛ فالعلم يتمثل في إدراك الجاني أن الفعل الذي يقوم به يشكل اعتداءً على نظام معلوماتي حكومي أو بيانات ذات طبيعة سيادية، أما الإرادة فتتمثل في اتجاه إرادته الحرة إلى ارتكاب هذا الفعل وتحقيق النتيجة الإجرامية المترتبة عليه.[20]

وقد تتخذ الجرائم الإلكترونية التي تمس سيادة الدولة صورًا متعددة من القصد الجنائي، فقد يكون القصد مباشرًا إذا كان الهدف من ارتكاب الجريمة هو الإضرار بالمصالح الأساسية للدولة أو الحصول على معلومات سرية تتعلق بأمنها القومي، كما قد يكون القصد غير مباشر إذا كان الجاني يتوقع النتيجة الإجرامية المحتملة لفعله ويقبل بها. وفي بعض الحالات قد يكون الدافع وراء ارتكاب هذه الجرائم سياسيًا أو أيديولوجيًا، مثل الجرائم التي ترتكبها بعض الجماعات الإلكترونية بهدف التأثير في السياسات الحكومية أو إضعاف المؤسسات الرسمية للدولة.[21]

وقد اهتمت التشريعات الوطنية بتحديد الركن المعنوي في الجرائم الإلكترونية، فنصت العديد من القوانين على ضرورة توافر القصد الجنائي لدى الجاني لقيام الجريمة. فعلى سبيل المثال نص قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 على معاقبة كل من يدخل عمدًا إلى موقع أو نظام معلوماتي تابع للدولة دون وجه حق، أو يقوم بتعطيل هذا

[19] عبد الفتاح بيومي حجازي، الجرائم المعلوماتية عبر الإنترنت (القاهرة: دار الفكر الجامعي، 2012)، ص 173.
[20] محمد أمين البكري، القانون الجنائي وتكنولوجيا المعلومات (الإسكندرية: دار الجامعة الجديدة، 2016)، ص 221.
[21] أحمد عبد الظاهر، الجرائم المعلوماتية (القاهرة: دار النهضة العربية، 2017)، ص 145.

النظام أو إتلاف البيانات المرتبطة به، مما يدل على أن المشرع يشترط توافر القصد الجنائي لقيام هذه الجرائم. كما شدد المشرع العقوبة في الحالات التي يكون فيها القصد متجهًا إلى الإضرار بالأمن القومي أو المصالح العليا للدولة.[22]

وفي العراق، وعلى الرغم من عدم وجود قانون خاص شامل لمكافحة الجرائم الإلكترونية حتى وقت قريب، إلا أن القواعد العامة في قانون العقوبات رقم 111 لسنة 1969 المعدل يمكن تطبيقها على الأفعال التي تُرتكب عبر الوسائل الإلكترونية إذا كانت تمس أمن الدولة أو مصالحها الأساسية. وقد نص القانون على معاقبة الأفعال التي تهدف إلى الإضرار باستقلال الدولة أو وحدتها أو سلامة أراضيها، وكذلك الجرائم المتعلقة بالتجسس أو إفشاء الأسرار، وهي نصوص يمكن تطبيقها على الجرائم الإلكترونية إذا تم ارتكابها بقصد الإضرار بسيادة الدولة أو مصالحها الحيوية.[23]

أما على الصعيد الدولي، فقد تناولت الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونية مسألة القصد الجنائي في هذه الجرائم، حيث نصت اتفاقية بودابست للجرائم الإلكترونية لعام 2001 على ضرورة أن تكون الأفعال المرتبطة بالاختراق الإلكتروني أو تعطيل الأنظمة المعلوماتية قد ارتُكبت عمدًا حتى تُعد جرائم يعاقب عليها القانون. ويعكس هذا النص اتجاه القانون الدولي إلى اشتراط توافر القصد الجنائي لدى الجاني لضمان عدم تجريم الأفعال التي قد تقع نتيجة الخطأ أو الإهمال غير المقصود في استخدام الأنظمة المعلوماتية.[24]

وقد أكدت التطبيقات القضائية الحديثة أهمية الركن المعنوي في الجرائم الإلكترونية التي تستهدف الأنظمة الحكومية أو البنية التحتية الرقمية للدولة. ففي حكم صادر عن محكمة النقض المصرية اعتُبر أن اختراق أحد المواقع الحكومية ونشر البيانات الموجودة فيه يشكل جريمة إلكترونية إذا ثبت أن الجاني كان على علم بطبيعة الموقع وبكونه تابعًا لجهة

[22] قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
[23] قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
[24] Council of Europe, Convention on Cybercrime (Budapest Convention), Budapest, 2001.

حكومية، وأنه قام بالفعل بقصد الحصول على البيانات أو نشرها دون إذن قانوني. وقد أكدت المحكمة أن توافر القصد الجنائي يُعد شرطًا أساسيًا لقيام الجريمة الإلكترونية.[25]

كما قضت إحدى المحاكم في دولة الإمارات العربية المتحدة بإدانة متهم قام بمحاولة اختراق نظام معلوماتي تابع لجهة حكومية بهدف الحصول على معلومات سرية، حيث اعتبرت المحكمة أن توافر القصد الجنائي لدى المتهم المتمثل في علمه بطبيعة النظام المعلوماتي وإرادته في الوصول إلى البيانات السرية يشكل الركن المعنوي للجريمة الإلكترونية التي تمس مصالح الدولة.[26]

ومن خلال ما تقدم يتضح أن الركن المعنوي في الجرائم الإلكترونية الواقعة على سيادة الدولة يتمثل في القصد الجنائي الذي يتوافر لدى الجاني عند ارتكاب الفعل الإجرامي عبر الوسائل الإلكترونية، سواء كان ذلك بهدف اختراق الأنظمة المعلوماتية الحكومية أو تعطيلها أو الحصول على البيانات المرتبطة بها. ويُعد توافر هذا الركن شرطًا أساسيًا لقيام المسؤولية الجنائية، إذ يميز بين الأفعال التي تُرتكب عمدًا بقصد الإضرار بالمصالح الأساسية للدولة وبين الأفعال التي قد تقع نتيجة الخطأ أو الإهمال في استخدام الأنظمة المعلوماتية.

الخاتمة

في ضوء ما تقدّم، يتضح أن الجرائم الإلكترونية الواقعة على سيادة الدولة تمثل أحد أخطر التحديات التي تواجه النظم القانونية المعاصرة، لما تنطوي عليه من تهديد مباشر للأمن الوطني والاستقرار السياسي والاقتصادي، فضلًا عن تعقيداتها التقنية والقانونية. وقد أفرزت هذه الجرائم واقعًا جديدًا تجاوز حدود المفاهيم التقليدية للجريمة، مما يستدعي تطوير أدوات المواجهة القانونية والإجرائية بما يتلاءم مع طبيعتها المتغيرة والعابرة للحدود.

[25] محكمة النقض المصرية، الطعن رقم 20458 لسنة 92 قضائية، جلسة 15 شباط 2023.
[26] حكم محكمة جنايات أبوظبي، القضية رقم 522 لسنة 2023 بشأن محاولة اختراق نظام معلوماتي حكومي...

كما أن حماية سيادة الدولة في الفضاء الإلكتروني لم تعد مسؤولية داخلية فحسب، بل أصبحت مسألة ذات بعد دولي تتطلب تعاونًا قانونيًا وتقنيًا بين الدول، وتكاملًا بين التشريعات الوطنية والاتفاقيات الدولية. وعليه، فإن مواجهة هذه الجرائم تستلزم تبني سياسة جنائية حديثة تقوم على التوازن بين الفعالية في المكافحة وضمان احترام الحقوق والحريات.

أولًا: الاستنتاجات

1. تبيّن أن الجرائم الإلكترونية التي تستهدف سيادة الدولة تمثل تطورًا نوعيًا في مفهوم الجريمة، حيث تنتقل من الاعتداء على الأفراد إلى المساس المباشر بالمصالح العليا للدولة.
2. أظهرت الدراسة أن هذه الجرائم تتسم بخصائص مميزة، أهمها الطابع العابر للحدود، وصعوبة تحديد مرتكبيها، والتطور المستمر في وسائل ارتكابها.
3. كشفت الدراسة أن التشريعات الوطنية، ومنها القانون العراقي، لا تزال تواجه تحديات في مواكبة التطور السريع للجرائم الإلكترونية، سواء من حيث التجريم أو من حيث الإجراءات.
4. تبيّن أن التعاون الدولي يمثل عنصرًا أساسيًا في مكافحة الجرائم الإلكترونية، نظرًا لطبيعتها العابرة للحدود، إلا أن هذا التعاون ما زال يواجه تحديات قانونية وسياسية.
5. كشفت الدراسة أن هناك حاجة ملحة إلى تطوير مفهوم السيادة ليشمل البعد الرقمي، بما يتلاءم مع طبيعة التهديدات الإلكترونية المعاصرة.

ثانيًا: المقترحات

1. ضرورة تحديث التشريعات الوطنية، ولا سيما في العراق، لتشمل نصوصًا واضحة ومحددة تجرّم مختلف صور الجرائم الإلكترونية التي تمس سيادة الدولة.
2. سنّ قانون متكامل للجرائم الإلكترونية يتضمن تعريفات دقيقة، وأحكامًا خاصة بالإجراءات والتحقيق والأدلة الرقمية.

3. تعزيز قدرات الجهات المختصة، من خلال تدريب الكوادر القانونية والفنية على التعامل مع الأدلة الرقمية والتحقيق في الجرائم السيبرانية .
4. تعزيز التعاون الدولي من خلال الانضمام إلى الاتفاقيات الدولية ذات الصلة، وتفعيل آليات تبادل المعلومات والخبرات بين الدول.
5. تطوير سياسات وطنية للأمن السيبراني تهدف إلى حماية البنية التحتية الرقمية والمؤسسات الحكومية من الهجمات الإلكترونية.