Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية

E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

الحماية السيبرانية في مواجهة جرائم الاختراق الإلكتروني للبيانات: دراسة تحليلية في التشريع الإماراتي

Cybersecurity Protection Against Electronic Data-Breach Crimes: An Analytical Study of UAE Legislation

[i,ii]*Mohammad Ahmad Saeed Alfalasi, [ii]Syahirah Abdul Shukor, & [i,iii]Mahmoud Mohamed Ali Mahmoud Edris

[i]Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Bandar Baru Nilai, Negeri Sembilan, Malaysia
[ii]General Directorate of Identity and Foreigners Affairs – Dubai, United Arab Emirates
[iii]Academic Advisor, Faculty of Shariah and Law, University of Dongola, Sudan.

*(Corresponding author) e-mail: m.bin7zaim@gmail.com

Article history:
Submission date: 6 March 2026
Received in revised form: 7 May 2026
Acceptance date: 7 June 2026
Available online: 5 August 2026

Keywords:
Cybersecurity; cyber intrusion; electronic data; cybercrime; UAE legislation

Funding:
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Alfalasi, M. A. S., Abdul Shukor, S., & Mahmoud Edris, M. A. M. (2026). Al-himayah al-sibraniyyah fi muwajahat jara'im al-ikhtiraq al-iliktruni li-al-bayanat: Dirasah tahliliyyah fi al-tashri' al-Imarati | Cybersecurity protection against electronic data breach crimes: An analytical study in UAE legislation. *Law, Policy, and Social Science*, *5*(1), 40-60. https://doi.org/10.55265/lpsjournal.v5i1.146

ABSTRACT

This study aims to demonstrate the role of cybersecurity in countering cyber intrusion crimes in light of the applicable UAE legislation, through analyzing the legal issues associated with the violation of personal and confidential data, whether through full or partial access without lawful authorization. The study adopted the descriptive, analytical, and inductive approach in order to examine the relevant legislative provisions and analyze the UAE legislator's position on criminalizing such acts, by reviewing Articles (2) and (3) of Federal Decree-Law No. (34) of 2021, which relate to intrusion and unlawful access offenses, as well as the aggravating provisions concerning data destruction and system disruption, thereby reaching objective findings that enhance the academic understanding of the nature of these crimes and their security and legal implications. The study found that cyber data intrusion crimes are characterized by rapid execution and the possibility of being committed remotely, which means that their material element is often limited to a simple technical act, without requiring technical complexity or the physical presence of the offender at the scene of the crime. This creates exceptional challenges for criminal detection and prosecution mechanisms. In light of these findings, the study recommends the adoption of a separate legal provision within the Federal Law on Combating Rumors and Cybercrimes that criminalizes the use of cyber intrusion systems as a means of committing the offense, along with the introduction of a specific penalty in the Penal Code concerning the intrusion of governmental information systems, thereby strengthening the legal and security protection of the national cyberspace and keeping pace with the rapid technological developments in the field of digital crimes.

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية

E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

الملخص

تهدف هذه الدراسة إلى بيان دور الحماية السيبرانية في التصدي لجرائم الاختراق الإلكتروني في ضوء التشريع الإماراتي النافذ، وذلك من خلال تحليل الإشكاليات القانونية المرتبطة بالاعتداء على البيانات الشخصية والسرية، سواء تم ذلك بالاطلاع الكلي عليها أو الجزئي عليها دون سند قانوني. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي الاستقرائي، بهدف استقراء نصوص التشريعات ذات الصلة، وتحليل موقف المشرع الإماراتي من تجريم هذه الأفعال، من خلال استقراء نصوص المادتين (2) و(3) من المرسوم بقانون اتحادي رقم (34) لسنة 2021، المتعلقتين بجريمتي الاختراق والدخول غير المشروع، ونصوص الفقرات المشددة الخاصة بإتلاف البيانات وتعطيل الأنظمة، وصولًا إلى نتائج موضوعية تعزز الفهم العلمي لطبيعة هذه الجرائم وتداعياتها الأمنية والقانونية. وتوصلت الدراسة إلى أن جرائم اختراق البيانات السيبرانية تتسم بسرعة التنفيذ وإمكانية ارتكابها عن بُعد، بما يجعل الركن المادي فيها يقتصر غالبًا على إجراء تقني بسيط، دون اشتراط تعقيد تقني أو حضور مادي للجاني في مسرح الجريمة، الأمر الذي يفرض تحديات استثنائية على آليات الضبط والملاحقة الجنائية. وفي ضوء هذه النتائج، أوصت الدراسة بضرورة تخصيص مادة قانونية مستقلة ضمن قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي، تُجرّم استخدام أنظمة الاختراق السيبراني كأداة لارتكاب الجريمة، مع استحداث عقوبة خاصة في قانون الجرائم والعقوبات تتعلق باختراق الأنظمة المعلوماتية الحكومية، بما يعزز مستويات الحماية القانونية والأمنية للفضاء السيبراني الوطني، ويواكب التطور التقني المتسارع في مجال الجرائم الرقمية.

المقدمة

يشهد الأمن السيبراني اهتمامًا متزايدًا على المستوى العالمي، نظرًا لما يمثله غيابه من تهديد للأفراد والمؤسسات والدول على حد سواء، حتى أصبح جزءًا أساسيًا من مفهوم الأمن القومي الحديث. ويُقصد به مجموعة التدابير التقنية والتنظيمية والإدارية التي تتخذ لحماية الفضاء الرقمي من الهجمات الإلكترونية، ومنع الوصول غير المشروع إلى المعلومات والبيانات واستغلالها على نحو مخالف للقانون، بما يضمن استمرارية الأنظمة المعلوماتية وسريتها وخصوصيتها.

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

وقد أفرز التطور التكنولوجي المتسارع، ولا سيما في مجالي تكنولوجيا المعلومات والاتصالات والبنية التحتية الرقمية، تحديًا يتمثل في تعرّض البيانات الشخصية والسرية للاختراق والانتهاك دون سند قانوني. وقد باتت هذه الأفعال تمثل تهديدًا مباشرًا لأمن البيانات الحكومية والخاصة، الأمر الذي يفرض ضرورة توفير حماية قانونية فعالة للفضاء الإلكتروني. وقد تجلى هذا الاهتمام التشريعي في المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية في دولة الإمارات العربية المتحدة، وإن ظل بحاجة إلى مزيد من الدقة التشريعية على النحو الذي تكشفه هذه الدراسة.

وعليه، سيتناول هذا البحث تحليلًا تشريعيًا مباشرًا للمادتين (2) و(3) من المرسوم بقانون اتحادي رقم (34) لسنة 2021، من خلال ثلاثة محاور أساسية: تحديد المفهوم القانوني والأركان الجنائية لجريمة الاختراق، والتمييز بينها وبين جريمتي الدخول غير المشروع والإتلاف، ثم تقييم مدى كفاية الجزاءات الإجرائية في مواجهة تحديات الضبط والملاحقة عن بُعد.

تتمثل مشكلة الدراسة في أن جرائم الاختراق السيبراني للبيانات أصبحت من الجرائم العابرة للحدود التي تواجهها معظم دول العالم، الأمر الذي يجعل من الحماية السيبرانية أداة تقنية وقانونية أساسية للتصدي لها. وتبرز الإشكالية القانونية في أن جريمة الاختراق السيبراني تتداخل مع جرائم أخرى متقاربة من حيث المحل وبعض عناصر الركن المادي، وعلى رأسها جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية المحمية وجريمة إتلاف البيانات أو تعطيل الأنظمة، بما يثير صعوبة في التمييز بين الفعل المكوِّن للجريمة والفعل الذي يُعد صورة مستقلة أو نتيجة مشددة لها.

ولما كان المرسوم بقانون اتحادي رقم (34) لسنة 2021 لم يفصل تفصيلًا كافيًا في ضبط الحدود الفاصلة بين هذه الصور الجرمية، من حيث تحديد ما إذا كان السلوك المنسوب يعد اختراقًا مستقلًا، أو دخولًا غير مشروع، أو إتلافًا لاحقًا على ذلك، فإن ذلك يفرض بحثًا تحليليًا معمقًا لبيان الطبيعة القانونية لكل صورة، وأثر هذا التمييز في تحديد المسؤولية الجزائية ومدى كفاية الحماية التشريعية المقررة لها.

تهدف هذه الدراسة إلى التأصيل القانوني لجريمة الاختراق السيبراني للبيانات في التشريع الإماراتي من خلال تحديد مفهومها وخصائصها وأركانها القانونية، وتحليل موقف المرسوم بقانون اتحادي رقم (34) لسنة 2021 لتقييم مدى

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

فعاليته في تجريم هذه الأفعال، مع تمييزها وبيان أوجه التداخل بينها وبين جرائم الدخول غير المشروع والإتلاف المعلوماتي، وصولاً إلى استخلاص الحلول التشريعية الكفيلة بمواجهة التحديات التقنية والإجرائية التي تفرضها هذه الجرائم.

أهمية الدراسة

تنبع الأهمية النظرية لهذه الدراسة من كونها تُسهم في تأصيل المفهوم القانوني للحماية السيبرانية بوصفها أداة لمواجهة جرائم الاختراق الإلكتروني للبيانات، وذلك من خلال تحليل جريمة الاختراق السيبراني في التشريع الإماراتي، وبيان أركانها القانونية، وتمييزها عن جريمتي الدخول غير المشروع والإتلاف المعلوماتي. كما تقدم الدراسة إطارًا تحليليًا يوضح طبيعة الاعتداءات الواقعة على البيانات والأنظمة الرقمية في ظل التطور التقني المتسارع، بما يعزز الفهم العلمي للجرائم المعلوماتية المرتبطة بالاختراق.

أما من الناحية العلمية والعملية، فتتمثل أهمية الدراسة في أنها تُعد من الدراسات التي تتناول بصورة مباشرة جريمة الاختراق السيبراني في ضوء المرسوم بقانون اتحادي رقم (34) لسنة 2021، مع التركيز على الإشكالات الناتجة عن التداخل بين صور التجريم المختلفة، ومدى كفاية الجزاءات الجنائية والإجرائية في مواجهتها. وتزداد هذه الأهمية بالنظر إلى ما يمكن أن تسهم به الدراسة من فائدة للباحثين القانونيين، والقضاة، والمحامين، والعاملين في مجال الأمن السيبراني، من خلال تقديم نتائج وتوصيات تساعد في تعزيز الحماية القانونية للبيانات وتطوير الاستجابة التشريعية للتهديدات الرقمية المستحدثة.

حدود الدراسة

من حيث الحدود الموضوعية، فتقتصر الدراسة على تحليل جريمة الاختراق السيبراني للبيانات في التشريع الإماراتي، مع التركيز على أركانها القانونية، والتمييز بينها وبين جريمتي الدخول غير المشروع والإتلاف المعلوماتي، ومدى كفاية الجزاءات الإجرائية والجنائية المقررة لها. ولا تتناول الدراسة سائر صور الجرائم الإلكترونية إلا بالقدر الذي يخدم موضوع الاختراق ويُعين على ضبط حدوده القانونية.

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

وتنحصر الحدود المكانية لهذه الدراسة في دولة الإمارات العربية المتحدة، باعتبارها الإطار التشريعي الذي تتناوله الدراسة بالتحليل. وتمتد الحدود الزمانية من عام 2021، وهو عام صدور المرسوم بقانون اتحادي رقم (34) بشأن مكافحة الشائعات والجرائم الإلكترونية، وحتى تاريخ إعداد هذه الدراسة، بما يتيح رصد التطورات التشريعية والمؤسسية ذات الصلة بموضوعها.

ومن حيث الحدود البشرية، فإن الدراسة موجهة أساسًا إلى الباحثين القانونيين، والقضاة، والمحامين، والعاملين في مجال الأمن السيبراني، والطلاب والمهتمين بالقانون الجنائي الرقمي. ويعكس هذا التحديد الطبيعة البينية للموضوع، بوصفه موضوعًا يجمع بين البعد القانوني والبعد التقني والمؤسسي.

الدراسات السابقة

تناولت دراسة الناصر (2023) بعنوان "أشكال انتهاك الفضاء السيبراني ووسائلها وآثارها"، المنشورة في مجلة الندوة للدراسات القانونية بالمغرب، موضوع أشكال انتهاك الفضاء السيبراني ووسائلها وآثارها، من خلال التعرف على مفهوم الفضاء السيبراني ومفهوم انتهاكه، وتحديد وسائل الإجرام فيه، وبيان تصنيف المنتهكين، معتمدة المنهج الوصفي الاستقرائي التحليلي. وتوصلت الدراسة إلى غياب لائحة تنفيذية واضحة في النظام السعودي، وضعف الوعي المجتمعي بالانتهاكات السيبرانية، وأن ازدواجية القانون الداخلي مع القانون الدولي تُفاقم من تنامي هذه الانتهاكات. وتُعد هذه الدراسة قريبة من موضوع الدراسة الحالية من حيث تناول أشكال الانتهاك السيبراني عموماً، إلا أنها لم تخصّ جريمة الاختراق السيبراني للبيانات بالتحليل التشريعي المفصل في ضوء التشريع الإماراتي.

وفي دراسة المري (2023) تناول في بحثه "الأمن السيبراني وحماية الأنظمة الإلكترونية: دراسة تحليلية تأصيلية"، المنشور في مجلة الدراسات القانونية والاقتصادية، ارتباط أمن المعلومات العضوي بالأمن القومي في معظم دول العالم، باعتبار أن الاعتداء على البنى التحتية للاتصالات والأنظمة الإلكترونية يؤثر على مصالح الدول ويهدد استقرارها. وتناول الباحث المشكلات الاجتماعية والقانونية التي أفرزتها البيئة الرقمية، كالجريمة السيبرانية والابتزاز والتنمر عبر الأنظمة الإلكترونية، مؤكداً الحاجة الملحة لاتخاذ إجراءات محلية ودولية لحماية الخصوصية ومجابهة تقنية المعلومات ضد أشكال الجريمة السيبرانية. وتلتقي هذه الدراسة مع الدراسة الحالية بشكل وثيق في التأصيل النظري لمفهوم الأمن

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

السيبراني وحماية الأنظمة الإلكترونية، إلا أنها جاءت بطابع تأصيلي عام دون التعمق في تحليل نصوص المرسوم بقانون اتحادي رقم (34) لسنة 2021 الإماراتي وتحديد أركان جريمة الاختراق تحديداً.

كما تناولت دراسة العوايشة (2022) بعنوان "المسؤولية المدنية لمزودي الخدمة في الأمن السيبراني"، المنشورة في مجلة جامعة عمان العربية للبحوث – سلسلة البحوث القانونية، المسؤولية المدنية لمزودي الخدمة من خلال أربعة فصول، معتمدة المنهجين الوصفي والتحليلي والمنهج المقارن. وانتهت إلى أن المشرّع الأردني لم يعالج في قانون الأمن السيبراني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث طبيعته وأثره وتصنيفه. وتتصل هذه الدراسة بالدراسة الحالية من زاوية تصنيف حادث الأمن السيبراني، غير أنها تناولت المسؤولية المدنية دون التعرض للمسؤولية الجزائية عن فعل الاختراق نفسه.

وهدفت دراسة مقارنة حديثة للباحث الأزرق (2021) بعنوان "محددات المسؤولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الضبط والردع في التشريعات العربية في العصر الرقمي" إلى رصد وتوصيف محددات المسؤولية الجنائية لجرائم الاختراق والاعتراض والانتحال كما وردت في نصوص التشريعات العربية، وتقييم الأطر التشريعية الضابطة في مصر والإمارات والسودان والأردن من حيث شمول النصوص وآليات الردع، مستندة إلى نظرية الردع الجنائي ومعتمدة المنهج الوصفي التحليلي والاستقرائي والمقارن. وتوصلت الدراسة إلى أن القانون المصري تميّز بتوضيح حالات ارتكاب الجريمة الإلكترونية المرتبة للمسؤولية الجنائية أكثر من القوانين الأخرى، وأن التشريعات العربية محل الدراسة خرجت من عباءة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. وتُعد هذه الدراسة من أقرب الدراسات إلى موضوع الدراسة الحالية، إذ تتناول مباشرة جريمة الاختراق في التشريع الإماراتي مقارنة بتشريعات عربية أخرى، إلا أنها تناولت الاختراق إلى جانب جريمتين أخريين (الاعتراض والانتحال) دون التعمق في التمييز الدقيق بين الاختراق والدخول غير المشروع والإتلاف المعلوماتي الذي تعالجه الدراسة الحالية بشكل مستقل ومحدد.

وفي دراسة الدويكات (2024) بعنوان "نطاق الحماية الجزائية للبيانات الشخصية الإلكترونية في القانون الأردني"، جرى تحديد المفهوم القانوني للبيانات الشخصية وبيان صور الجرائم الواقعة عليها كالتصيد الاحتيالي وسرقة الهوية والدخول غير المصرح به، في ضوء قانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023. وتوصلت الدراسة إلى أن المشرع الأردني لم يحدد نطاق الحماية الجزائية لبعض المعطيات المرتبطة بالبيانات الشخصية كرقم بطاقة الائتمان

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

والبيانات البيومترية. وتتقارب هذه الدراسة مع الدراسة الحالية في التركيز على الثغرات التشريعية المتعلقة بجرائم الاعتداء على البيانات الشخصية، إلا أنها تناولت التشريع الأردني دون التعرض للتشريع الإماراتي.

وتناولت رسالة ماجستير للشامسي (2022) بعنوان "حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي: دراسة تحليلية مقارنة"، جامعة الإمارات العربية المتحدة، مدى كفاية وشمولية الأطر القانونية المعاصرة -- وأبرزها اللائحة الأوروبية العامة لحماية البيانات والمرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية الإماراتي -- في توفير الحماية المرجوة لخصوصية الأفراد أمام تطبيقات الذكاء الاصطناعي. وخلصت الدراسة إلى وجود قصور تشريعي يتمثل في غياب قانون مستقل شامل لحماية الخصوصية وقواعد قانونية خاصة بالذكاء الاصطناعي في دولة الإمارات. وتُعد هذه الدراسة من الدراسات الإماراتية القريبة جداً من موضوع الدراسة الحالية من حيث تناول التشريع الإماراتي لحماية البيانات، إلا أنها ركّزت على سياق الذكاء الاصطناعي تحديداً، دون تحليل جريمة الاختراق السيبراني للبيانات في قانون مكافحة الشائعات والجرائم الإلكترونية بشكل مباشر.

وأخيراً، تناولت دراسة جزائرية حديثة لجيدول وعباس (2026) بعنوان "حماية الخصوصية والأمن الرقمي في القانون الجنائي" الجرائم الإلكترونية المرتبطة بالخصوصية والأمن الرقمي والإطار القانوني الذي يجرّمها، والتحديات التي تواجه تطبيق هذا الإطار. وخلصت الدراسة إلى ضرورة تطوير التشريعات وتعزيز التعاون الدولي ورفع وعي الأفراد والمؤسسات. وتلتقي هذه الدراسة مع الدراسة الحالية في التأكيد على ضرورة مواكبة التشريعات للتطور التقني المتسارع، إلا أنها جاءت بمنهج عام دون التعمق في تحليل نصوص التشريع الإماراتي وتحديد أركان جريمة الاختراق السيبراني بدقة، وهو ما تنفرد به الدراسة الحالية وتُميّزها عن جميع الدراسات السابقة.

التعقيب على الدراسات السابقة

تتفق الدراسات السابقة مع الدراسة الحالية في التأكيد على خطورة الجرائم السيبرانية واتساع آثارها على الأفراد والمؤسسات والدول، وفي الإقرار بأن التطور التقني المتسارع أفرز صورًا مستحدثة من الاعتداء على البيانات والأنظمة المعلوماتية، بما يستدعي تطوير الأطر القانونية المنظمة لها. كما تلتقي هذه الدراسات مع الدراسة الحالية في الإشارة

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

إلى وجود حاجة تشريعية مستمرة لمواكبة أنماط السلوك الإجرامي الرقمي، سواء في نطاق التشريعات العربية المقارنة أو في سياق حماية البيانات والخصوصية الرقمية بوجه عام.

ومع ذلك، فإن أغلب الدراسات السابقة اتجهت إلى معالجة موضوع الأمن السيبراني أو الفضاء الرقمي من منظور عام، أو تناولت بعض جوانب الحماية القانونية للبيانات والأنظمة في إطار مقارن أو جزئي، دون أن تُفرد جريمة الاختراق السيبراني للبيانات في التشريع الإماراتي بتحليل مستقل ومفصل. كما أن بعض هذه الدراسات ركّز على الحماية المدنية أو على الخصوصية الرقمية أو على صور متعددة من الجرائم الإلكترونية في آن واحد، الأمر الذي حال دون التعمق في البنية القانونية الخاصة بجريمة الاختراق ذاتها.

وتتميز الدراسة الحالية عن الدراسات السابقة بأنها تُوجِّه عنايتها مباشرة إلى جريمة الاختراق السيبراني بوصفها جريمة مستقلة ذات طبيعة خاصة، من خلال تحليل نصوص المرسوم بقانون اتحادي رقم (34) لسنة 2021، وبيان أركانها القانونية، وتمييزها عن الجرائم المتقاربة معها، ولا سيما جريمتي الدخول غير المشروع والإتلاف المعلوماتي. كما تتميز بأنها لا تقف عند التأصيل النظري العام للأمن السيبراني، وإنما تربطه ربطًا مباشرًا بالتحليل التشريعي الجزائي في دولة الإمارات العربية المتحدة.

الفجوة البحثية

تتمثل الفجوة البحثية التي تسعى هذه الدراسة إلى معالجتها في أن الدراسات السابقة، رغم أهميتها وتنوع موضوعاتها، لم تتناول جريمة الاختراق السيبراني للبيانات في التشريع الإماراتي بالتحليل المستقل والمفصل الذي يكشف طبيعتها القانونية وحدود التجريم المقررة لها. فقد تناولت معظم الدراسات الموضوع في إطار عام يتعلق بالأمن السيبراني أو الفضاء الرقمي أو حماية البيانات، أو في سياق مقارن لا يجعل من التشريع الإماراتي محلًا رئيسًا للتحليل.

كما لم تُفرد الدراسات السابقة معالجة دقيقة للتمييز بين جريمة الاختراق السيبراني وجريمتي الدخول غير المشروع والإتلاف المعلوماتي، رغم ما يثيره هذا التداخل من إشكالات قانونية تتصل بتحديد الركن المادي للجريمة، والنتيجة الإجرامية المترتبة عليها، وحدود المسؤولية الجزائية الناشئة عنها. وإلى جانب ذلك، لم تُقيِّم هذه الدراسات على نحو تفصيلي مدى كفاية نصوص المرسوم بقانون اتحادي رقم (34) لسنة 2021 في استيعاب صور الاختراق المتطورة ومواجهة ما تفرضه من تحديات في الضبط والملاحقة عن بُعد.

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ومن ثم، تأتي هذه الدراسة لسد هذه الفجوة من خلال تحليل تشريعي مباشر لجريمة الاختراق السيبراني في القانون الإماراتي، وبيان أركانها، وتمييزها عن الجرائم المشابهة، وتقييم مدى كفاية النصوص القانونية المنظمة لها، بما يحقق إضافة علمية متخصصة في هذا المجال.

منهج الدراسة

اعتمد الباحث المنهج الوصفي التحليلي الاستقرائي، بهدف استقراء نصوص التشريعات ذات الصلة، وتحليل موقف المشرع الإماراتي من تجريم أفعال الاختراق السيبراني للبيانات. وقد جرى ذلك من خلال استقراء نصوص المواد (1)، و(2)، و(3) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 بصورة تفصيلية، وتفكيكها لفظيًا وفقهيًا، بما يتيح تحديد أركان هذه الجريمة وبيان طبيعتها القانونية وأوجه تمييزها عن الجرائم المشابهة. كما تسعى الدراسة إلى تقييم مدى كفاية النصوص القانونية النافذة في مواجهتها، وصولًا إلى نتائج وتوصيات موضوعية تعزز الفهم العلمي لهذه الجرائم وتسهم في تطوير الإطار القانوني المنظم لها.

الإطار النظري لدور الأمن السيبراني في مواجهة جرائم الاختراق

يُقدّم هذا الإطار النظري الأساس المفاهيمي والتشريعي لدور الأمن السيبراني في مواجهة جرائم الاختراق في دولة الإمارات العربية المتحدة، بما يتوافق مع مشكلة الدراسة التي تتمثل في تحديد مدى كفاية التشريع الإماراتي في تجريم وضبط فعل الاختراق السيبراني، وبيان الأركان القانونية ذات الصلة، وتمييزه عن الصور الجرميّة المتقاربة معه. وقد اعتمدت الدراسة المنهج الوصفي التحليلي الاستقرائي، من خلال استقراء النصوص التشريعية ذات الصلة وتحليلها في ضوء المرسوم بقانون اتحادي رقم (34) لسنة 2021، مع الاستئناس بالإطار المؤسسي للأمن السيبراني في الدولة. ويحدد بالمطالب التالية:

المطلب الأول: الأمن السيبراني والجهود الإماراتية في تعزيز الأمن السيبراني

أولاً: الأمن السيبراني بوصفه إطارًا وقائيًا وتشريعيًا

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ظهر الأمن السيبراني بوصفه مجالًا بحثيًا وتطبيقيًا مع بدايات استخدام الشبكات الحاسوبية في سبعينيات القرن العشرين، حين برزت محاولات مبكرة لمواجهة البرمجيات المتحركة ذاتيًا وحماية الأنظمة من الاختراق غير المشروع، ثم تطور المفهوم تدريجيًا مع اتساع الاعتماد على الحواسيب والشبكات وازدياد إدراك الحكومات والمؤسسات البحثية لخطورة الوصول غير المصرح به إلى البيانات والأنظمة (Lynn, 2011 ;Tomlinson, 1984). ومع تصاعد الهجمات الإلكترونية في الثمانينات، وما رافقها من معايير حماية مؤسسية وبرامج مكافحة الفيروسات، انتقل الأمن السيبراني من مجرد استجابة تقنية إلى منظومة متكاملة تجمع بين الوقاية التقنية والتنظيم القانوني والحماية المؤسسية (Sladek, 1989 ;McAfee Associates, 1988 ;Department of Defense, 1985). ويُبرز هذا التطور أن جرائم الاختراق ووسائل مكافحتها تتطوران بصورة متلازمة، بما يفرض على المشرّع مواكبة هذا التحول تشريعيًا على نحو مستمر، وهو ما ينسجم مع هدف هذه الدراسة في تحليل كفاية الإطار الإماراتي في مواجهة الاختراق السيبراني.

وأصبح الأمن السيبراني جزءًا أساسيًا من منظومة الأمن الحديث، إذ لم يعد مقتصرًا على الحماية التقنية للأنظمة والشبكات، بل اتسع ليشمل حماية البيانات والبرامج والبنى الرقمية من أي وصول غير مشروع أو عبث أو تعطيل، الأمر الذي يجعله إطارًا وقائيًا وتشريعيًا متكاملًا لحماية المصالح الرقمية للأفراد والمؤسسات والدول (UAE Government Official Portal, 2024; Al-Marri, 2023). وتزداد أهمية هذا المفهوم في ظل الاعتماد المتنامي على الوسائط الإلكترونية في إدارة المرافق العامة والأنشطة الخاصة، بما يجعل أي اختراق للبيانات أو الأنظمة تهديدًا مباشرًا للاستقرار المؤسسي والخصوصية الرقمية (Al-Marri, 2023). ومن هذا المنطلق، فإن الأمن السيبراني لا يُنظر إليه باعتباره تدبيرًا تقنيًا صرفًا، بل باعتباره أحد مرتكزات الحماية القانونية والتنظيمية في البيئة الرقمية (Al-'Awayshah, 2022; UAE Government Official Portal, 2024).

ثانياً: جهود دولة الإمارات في تعزيز الأمن السيبراني

أولت دولة الإمارات العربية المتحدة اهتمامًا مؤسسيًا واضحًا بالأمن السيبراني من خلال تطوير استراتيجيات وطنية متخصصة وإنشاء أطر تنظيمية ومؤسساتية مكرسة لحماية الفضاء الرقمي، وهو ما يعكس إدراكًا رسميًا مبكرًا لخطورة التهديدات السيبرانية على المرافق الحيوية والبيانات والأنظمة الإلكترونية (Telecommunications and

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

(Digital Government Regulatory Authority, 2019; Cabinet, 2020). كما يعزز هذا التوجه المؤسسي ما تقرره المنصة الرسمية للحكومة من أن قانون مكافحة الشائعات والجرائم الإلكترونية يمثل جزءًا من الإطار الوطني لحماية المجتمع والأنظمة من الجرائم الرقمية (UAE Government Official Portal, 2024). غير أن هذه الجهود، على أهميتها، لا تغني عن ضرورة وجود تنظيم جزائي دقيق يحدد صور الأفعال المجرّمة وحدود المسؤولية المترتبة عليها، وهو ما يتجلى في المرسوم بقانون اتحادي رقم (34) لسنة 2021 (Official Gazette, 2021).

ويؤسس هذا المحور المؤسسي والاستراتيجي لفهم البيئة التي تعمل فيها التشريعات الجزائية محل الدراسة، ويُظهر أن التفوق التقني والمؤسسي لا يكفي بمفرده لمواجهة جرائم الاختراق ما لم يواكبه إطار تشريعي جزائي دقيق ومحدد، وهو ما تسعى هذه الدراسة إلى تحليله وتقييمه.

المطلب الثاني: المفهوم القانوني والأركان الجنائية لجريمة الاختراق السيبراني

يُستفاد من المادة الأولى من المرسوم بقانون اتحادي رقم (34) لسنة 2021 أن المشرّع الإماراتي قد وسّع من نطاق مفهوم الاختراق السيبراني، بحيث لم يقتصر على الدخول غير المرخص فحسب، بل امتد ليشمل الدخول المخالف لأحكام الترخيص، والدخول بطريقة غير مشروعة، والبقاء غير المشروع في نظام معلوماتي أو شبكة معلوماتية (Official Gazette, 2021). ويكشف هذا التنظيم عن اتجاه تشريعي يرمي إلى استيعاب صور متعددة من السلوك الإجرامي الرقمي، وعدم حصره في قالب تقني ضيق قد لا يواكب التطور المستمر في أساليب الاعتداء على الأنظمة المعلوماتية (Al-Azraq, 2021).

وقد جاءت المادة الثانية من المرسوم لتضع الإطار العقابي الأساسي لهذه الجريمة، فنصت على معاقبة كل من اخترق موقعًا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلومات أو وسيلة تقنية معلومات بالحبس والغرامة، مع تشديد العقوبة إذا اقترن الفعل بإتلاف أو إفشاء أو حصول غير مشروع على البيانات أو المعلومات (Official Gazette, 2021). ويُفهم من ذلك أن المشرّع تعامل مع جريمة الاختراق في صورتها الأساسية باعتبارها من جرائم الخطر أو الجرائم الشكلية، التي يكتمل ركنها المادي بمجرد تحقق السلوك الإجرامي ذاته، دون اشتراط وقوع ضرر لاحق. ويتفق هذا التكييف مع الطبيعة الخاصة للجرائم السيبرانية، إذ قد يكفي مجرد الولوج غير المشروع لتهديد المصلحة المحمية قانونًا (Al-Azraq, 2021; Official Gazette, 2021).

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ولا يقف التنظيم التشريعي عند هذه الصورة، بل يمتد إلى تشديد العقوبة متى اقترن الاختراق بنتيجة أكثر جسامة. فقد نصت الفقرة الثانية من المادة الثانية من المرسوم بقانون اتحادي رقم (34) لسنة 2021 على تشديد العقوبة إلى الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن 150,000 درهم ولا تزيد على 500,000 درهم إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل الموقع أو النظام، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها (Official Gazette, 2021). أما إذا اتجهت إرادة الجاني إلى الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع، فإن العقوبة ترتفع إلى الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن 200,000 درهم ولا تزيد على 500,000 درهم (Official Gazette, 2021). ويُظهر هذا التدرج أن المشرّع الإماراتي أقام بناءً عقابيًا متدرجًا يراعي جسامة الفعل والنتيجة والقصد المصاحب له، وهو ما يتفق مع ما قررته الدراسات الفقهية من أن جرائم الاختراق لا تُعالج بعقوبة واحدة جامدة، بل بعقوبات تتفاوت تبعًا لدرجة الخطر والضرر المتحقق.

ويؤكد هذا الاتجاه الفقهي كذلك أن تشديد الجزاء في جرائم الاختراق يجد مبرره في الطبيعة المركبة لهذه الجرائم، إذ قد يبدأ الفعل بدخول غير مشروع، ثم يتطور إلى عبث بالبيانات أو تعطيل للنظام أو إفشاء للمعلومات، بما يقتضي استجابة تشريعية مرنة ومتدرجة.

ومن ناحية أخرى، تبرز المادة الثالثة من المرسوم بقانون اتحادي رقم (34) لسنة 2021 أهم صور الحماية المشددة التي أولاها المشرّع الإماراتي للأنظمة المعلوماتية الخاصة بالدولة، إذ قررت عقوبة السجن المؤقت والغرامة التي لا تقل عن 200,000 درهم ولا تزيد على 500,000 درهم لكل من اخترق موقعًا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لجهة حكومية. كما ترتفع العقوبة إلى السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن 250,000 درهم ولا تزيد على 1,500,000 درهم إذا ترتب على الاختراق إحداث أضرار أو تدمير أو تعطيل أو إيقاف عن العمل، وتصل إلى السجن مدة لا تقل عن سبع سنوات إذا كان الاختراق بقصد الحصول على بيانات أو معلومات خاصة بالجهات الحكومية (Official Gazette, 2021). ويعكس هذا التدرج العقابي اتجاهًا تشريعيًا واضحًا نحو تشديد الحماية الجنائية كلما اتصل فعل الاختراق بالأنظمة الحكومية أو بالمعلومات ذات الطبيعة العامة، وهو ما ينسجم مع ما تؤكده الدراسات الفقهية من أن جرائم

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

الاختراق تتطلب بناءً عقابيًا متدرجًا يراعي جسامة الفعل والنتيجة والقصد الإجرامي المصاحب له (Al-Azraq, 2021).

كما يكشف هذا التنظيم عن أن المشرّع الإماراتي لم يتعامل مع الاختراق باعتباره مجرد سلوك تقني عارض، بل بوصفه اعتداءً ينال من بنيان الأمن الرقمي ذاته، وهو ما ينسجم مع الاتجاه الفقهي الذي ينظر إلى الأمن السيبراني باعتباره منظومة حماية متكاملة لا تقتصر على الوقاية التقنية، بل تمتد إلى الإسناد التشريعي والتحصين الجزائي والتنسيق المؤسسي (Al-Marri, 2023). ومن ثم، فإن تشديد العقوبة في هذه الصورة لا يعد مجرد وسيلة ردعية، بل يمثل ترجمة قانونية لطبيعة الخطر الذي يهدد البيانات والأنظمة الحكومية، وما يترتب عليه من آثار تمس الثقة العامة واستقرار المرافق الحيوية.

الأركان الجنائية للجريمة:

يتمثل الركن المادي لجريمة الاختراق السيبراني في فعل الدخول غير المرخص، أو تجاوز حدود الترخيص، أو البقاء غير المشروع في النظام المعلوماتي، وذلك بصرف النظر عن تحقق نتيجة إضافية كالإتلاف أو الإفشاء. ومن ثم، فإن الجريمة في صورتها الأساسية تُعد من قبيل جرائم الخطر أو الجرائم الشكلية، التي يكتمل ركنها المادي فيها بمجرد ارتكاب الفعل، دون توقف على تحقق ضرر فعلي لاحق (Official Gazette, 2021). وتنبع أهمية هذا التكييف من كونه ينسجم مع الطبيعة الخاصة للجرائم السيبرانية، التي قد يكون مجرد الولوج غير المشروع فيها كافيًا لتهديد المصلحة المحمية قانونًا.

أما الركن المعنوي، فيقوم على توافر القصد الجنائي العام، المتمثل في علم الجاني بعدم مشروعية دخوله أو بقائه في النظام، وانصراف إرادته إلى ارتكاب هذا الفعل. وقد يتعزز هذا القصد العام بقصد خاص يؤدي إلى تشديد العقوبة، كما في حالة استهداف الحصول على بيانات أو معلومات لتحقيق غرض غير مشروع، أو المساس ببيانات الجهات الحكومية أو أنظمتها (Official Gazette, 2021). ويؤكد ذلك أن المشرّع الإماراتي لم يكتفِ بتجريم السلوك المادي، بل ربط بين طبيعة الإرادة الإجرامية وبين مقدار الجزاء المترتب عليها.

ويخلص مما تقدم إلى أن المشرّع الإماراتي قد أقام تنظيمًا تشريعيًا متدرجًا لجريمة الاختراق السيبراني، يميّز بين صورتها البسيطة وصورها المشددة المرتبطة بالإتلاف أو الإفشاء أو القصد غير المشروع أو استهداف الأنظمة الحكومية.

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ويُعد هذا التنظيم أساسًا تحليليًا مهمًا يساعد على تحديد ماهية الجريمة وأركانها وحدودها، ويعكس في الوقت نفسه استجابة تشريعية دقيقة لطبيعة الخطر الذي تمثله الجرائم السيبرانية على الأمن المعلوماتي والمصلحة العامة.

المطلب الثالث: التمييز بين الاختراق السيبراني وجريمتي الدخول غير المشروع والإتلاف

يقتضي التحليل الدقيق لأحكام المرسوم بقانون اتحادي رقم (34) لسنة 2021 التمييز بين ثلاث صور جرمية متقاربة في ظاهرها، متباينة في طبيعتها القانونية وأثرها الجزائي، وهي: الاختراق السيبراني، والدخول غير المشروع، وإتلاف المعلومات أو الأنظمة. فهذه الصور، وإن اشتركت في اتصالها بالبيئة الرقمية وفي مساسها بالأنظمة المعلوماتية، إلا أن لكل منها بنيانًا قانونيًا خاصًا يوجب الفصل بينها من حيث الركن المادي، والنتيجة الإجرامية، ومدى تشديد العقوبة (Official Gazette, 2021). كما تؤكد الدراسات المقارنة أن الخلط بين هذه الصور يؤدي إلى اضطراب في التكييف القانوني، ويؤثر في تحديد المسؤولية الجنائية وآليات الردع المناسبة (Al-Azraq, 2021).

أولًا: الاختراق السيبراني بوصفه جريمة خطر مستقلة

يتجلى الاختراق السيبراني، وفق ما يُستفاد من المادة الثانية من المرسوم، في فعل الدخول غير المرخص إلى الموقع أو النظام أو الشبكة المعلوماتية، بصرف النظر عن تحقق أثر لاحق على البيانات أو الأنظمة (Official Gazette, 2021). ومن ثم، فإن المشرّع لم يربط قيام الجريمة في صورتها الأساسية بتحقق ضرر مادي محدد، بل اكتفى بمجرد الولوج غير المشروع، وهو ما يجعلها من الجرائم الشكلية أو جرائم الخطر المجرد، التي يكتمل ركنها المادي بمجرد ارتكاب الفعل، دون توقف على وقوع نتيجة ضارة مستقلة. أما ما يترتب على هذا الاختراق من إتلاف أو إفشاء أو تعطيل، فإنه لا يغير من طبيعة الجريمة الأساسية، بل ينهض سببًا لتشديد العقوبة وفقًا لصورها المشددة (Official Gazette, 2021; Al-Azraq, 2021).

ثانيًا: الدخول غير المشروع بوصفه فعلًا تأسيسيًا

أما الدخول غير المشروع، فهو ليس جريمة مستقلة بذاته في البنيان القانوني للاختراق، بقدر ما يُعد الفعل التأسيسي الذي يقوم عليه هذا الاختراق. وقد عرّفه المشرّع في المادة الأولى بأنه الدخول إلى نظام معلوماتي بأي وسيلة دون تصريح، أو الدخول بموجب تصريح ثم تجاوز حدوده، أو البقاء في النظام بعد العلم بزوال الحق في الاستعمال

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

(Official Gazette, 2021). ويؤدي هذا التعريف إلى نتيجة مهمة، مؤداها أن الدخول غير المشروع يشكل الحلقة الأولى في سلسلة التجريم، بينما يظل الاختراق هو الوصف القانوني الأشمل الذي يستوعب هذا الفعل ويمد نطاقه إلى ما قد يتبعه من صور أشد. ومن ثم، فإن التمييز بينهما ليس ترفًا اصطلاحيًا، بل ضرورة تحليلية تكشف الطبيعة الحقيقية للركن المادي وتضبط مجال المسؤولية الجزائية (Al-Azraq, 2021).

ثالثًا: الإتلاف بوصفه جريمة نتيجة

في المقابل، تمثل جريمة إتلاف المعلومات أو الأنظمة صورة من صور جرائم النتيجة، إذ يشترط القانون لقيامها تحقق أثر مادي ملموس يتمثل في إحداث أضرار أو تدمير أو إيقاف النظام عن العمل أو تعطيله أو حذف البيانات أو تغييرها أو نشرها (Official Gazette, 2021). وعلى هذا الأساس، فإن الإتلاف لا يُعد وصفًا مرادفًا للاختراق، بل نتيجة لاحقة عليه، وقد لا يتحقق الاختراق في صورته البسيطة معه، لكنه إذا وقع ارتقى بالفعل الجرمي إلى صورة أشد تستوجب العقوبة المشددة. كما أن هذا الإتلاف لا يمكن فصله عن الفعل السابق عليه، إذ غالبًا ما يكون ثمرة دخول غير مشروع أو اختراق تمهيدي، الأمر الذي يبرز الطبيعة التدرجية للبناء التشريعي الذي اعتمده المشرّع الإماراتي في مواجهة هذه الأفعال (Official Gazette, 2021; Jaydul & 'Abbas, 2026).

رابعًا: خلاصة التمييز بين الصور الثلاث

يُظهر هذا التمييز أن المشرّع الإماراتي لم يتعامل مع هذه الأفعال باعتبارها مترادفات قانونية، بل بنى لها نسقًا تشريعيًا متدرجًا يربط بين الفعل الأصل، والوصف الجرمي، والنتيجة المشددة (Official Gazette, 2021). فالاختراق جريمة خطر مستقلة في صورتها الأساسية، والدخول غير المشروع فعل تأسيسي يدخل في تكوينها، والإتلاف جريمة نتيجة تشدد العقوبة عند تحققها. ويُعد هذا التصنيف أساسًا تحليليًا بالغ الأهمية، لأنه يرفع الالتباس بين المصطلحات، ويستجيب مباشرة لملاحظة المحكّم بشأن ضرورة التمييز الدقيق بين هذه الصور وعدم الاكتفاء بالإشارات العامة (Al-Azraq, 2021).

جدول التمييز بين الصور الثلاث

وجه التمييز	الاختراق السيبراني (المادة 2/1)	الدخول غير المشروع (المادة 1)	إتلاف المعلومات (المادة 2/2)
طبيعة الجريمة	جريمة خطر/شكلية	ركن مادي تأسيسي ضمن الاختراق	جريمة نتيجة

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

وجه التمييز	الاختراق السيبراني (المادة 1/2)	الدخول غير المشروع (المادة 1)	إتلاف المعلومات (المادة 2/2)
الركن المادي	الدخول أو البقاء غير المرخص	الدخول دون تصريح أو تجاوزه	إحداث ضرر أو تعطيل أو حذف فعلي
اشتراط النتيجة	غير مشترط لقيام الجريمة الأساسية	غير مشترط، فعل تمهيدي محض	مشترط لتشديد العقوبة
العلاقة بين الصور	وصف جرمي شامل	حلقة أولى في التجريم	صورة مشددة لاحقة
العقوبة	حبس وغرامة 100,000 – 300,000 درهم	تدخل في تكوين الاختراق، لا عقوبة مستقلة	حبس لا يقل عن ستة أشهر وغرامة 150,000 – 500,000 درهم

هذا التمييز الثلاثي يقدّم الإطار التحليلي الذي شدّد عليه المحكّم، ويُظهر أن التشريع الإماراتي اعتمد بناءً قانونيًا متدرجًا يربط بين الفعل والوصف والنتيجة، بما يتيح فهمًا أدق لطبيعة جريمة الاختراق السيبراني وحدودها (Official Gazette, 2021).

المطلب الرابع: مدى كفاية الجزاءات الإجرائية والجنائية في مواجهة تحديات الضبط والملاحقة عن بعد

يقتضي تقييم كفاية الجزاءات في مواجهة جرائم الاختراق السيبراني التمييز بين مستويين متكاملين: مستوى الجزاء الجنائي الموضوعي الذي أقره المرسوم بقانون اتحادي رقم (34) لسنة 2021، ومستوى الأدوات الإجرائية التي تتاح لسلطات الضبط القضائي في ملاحقة الجاني، ولا سيما في الحالات التي يُرتكب فيها الفعل من خارج حدود الدولة أو عبر وسائل تقنية تُعقّد عملية تحديد الهوية وإسناد الفعل إلى مرتكبه (Official Gazette, 2021; UAE Government Official Portal, 2024). ويؤدي هذا التمييز إلى إبراز أن فاعلية المواجهة التشريعية لا تتوقف عند مجرد تقرير العقوبة، بل تمتد إلى مدى قدرة المنظومة الإجرائية على الوصول إلى الفاعل، وضبط الأدلة الرقمية، وإحكام سلسلة الإثبات في بيئة تتسم بالسرعة والتبدل واللامادية.

وقد اعتمد المشرّع الإماراتي سلّمًا عقابيًا متدرجًا في مواجهة صور الاختراق المختلفة، يبدأ من العقوبة المقررة للاختراق البسيط، ثم يتدرج كلما اقترن الفعل بنتيجة أشد جسامة أو تعلق بأنظمة حكومية أو ببيانات بالغة الحساسية (Official Gazette, 2021). غير أن هذا التدرج، على أهميته، يظل في جانب منه ذا طبيعة ردعية نظرية ما لم يُدعَّم بوسائل إجرائية فعالة تتيح كشف الجريمة والتحقق من فاعلها وجمع أدلتها الرقمية في الوقت المناسب، وهو ما

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ينسجم مع الفلسفة العامة التي تقوم عليها الحماية السيبرانية في الدولة (Telecommunications and Digital Government Regulatory Authority, 2019; Cyber Security Council, 2023).

وتكشف الممارسة العملية أن الجرائم الإلكترونية تفرض تحديات خاصة على الأدوات الإجرائية التقليدية، إذ غالبًا ما يستخدم الجاني شبكات إخفاء الهوية أو خوادم خارج الدولة أو تطبيقات مشفرة تجعل تعقبه أكثر صعوبة، فضلًا عن كون الدليل الرقمي دليلًا سريع الزوال وقابلًا للتغيير أو المحو في أي لحظة. ومن ثم، فإن تشتت القواعد ذات الصلة بين قانون الإجراءات الجزائية، والمرسوم بقانون اتحادي رقم (34) لسنة 2021، والتشريعات الجزائية ذات الصلة، يحدّ من وجود إطار إجرائي متكامل يستجيب لطبيعة الجريمة السيبرانية الخاصة (Official Gazette, 2021). ويزداد هذا القصور وضوحًا عند النظر إلى عنصر الملاحقة عبر الحدود، حيث تظل آليات التعاون القضائي الدولي وتبادل الأدلة الرقمية بحاجة إلى مزيد من الضبط التشريعي والتنسيق المؤسسي.

ومن الناحية العملية، وفّرت الدولة قنوات استجابة سريعة للإبلاغ عن الجرائم الرقمية، بما في ذلك المنصات الإلكترونية المخصصة لتلقي البلاغات وتحويلها إلى الجهات المختصة، الأمر الذي يعكس حرصًا مؤسسيًا على سرعة التدخل والاحتواء (UAE Government Official Portal, 2024; Cyber Security Council, 2023). غير أن هذه الآليات، على أهميتها في المرحلة الأولية، لا تكفي وحدها لمعالجة الإشكالات الأعمق المرتبطة بملاحقة الجناة عابرِي الحدود أو باستكمال متطلبات الإثبات الفني والقضائي، مما يكشف الحاجة إلى تطوير أوسع في البنية الإجرائية المواكبة للتجريم الموضوعي.

وبناءً على ذلك، يمكن القول إن تعزيز الكفاية الإجرائية في مواجهة جرائم الاختراق السيبراني يقتضي جملة من التوجهات التشريعية والتنظيمية، أهمها: استحداث فصل إجرائي خاص بضبط الجرائم الإلكترونية ضمن قانون الإجراءات الجزائية الاتحادي، يتضمن أحكامًا واضحة بشأن حجز الأدلة الرقمية وسلسلة حفظها، وتخصيص جهات تحقيق ونيابات متخصصة في الجرائم الإلكترونية، وتوسيع آليات التعاون القضائي الدولي لتبادل البيانات والأدلة الرقمية في الحالات العابرة للحدود، فضلًا عن النظر في تجريم حيازة أو تصنيع أدوات الاختراق والبرمجيات الخبيثة بوصفها أفعالًا تحضيرية مستقلة (Official Gazette, 2021; Cyber Security Council, 2023).

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ويؤكد هذا المنهج أن الردع الفعلي في المجال السيبراني لا يتحقق بعقوبة مشددة فحسب، بل بتكامل العقوبة مع منظومة إجرائية مرنة وسريعة وذات قدرة تقنية عالية.

المطلب الخامس: التحليل والمناقشة والنتائج

يكشف ما سبق عرضه في الإطار النظري والدراسات السابقة أن الأمن السيبراني لم يعد مفهومًا فنيًا محضًا، بل أصبح منظومة متكاملة تتداخل فيها الأبعاد التقنية والتشريعية والمؤسسية، بما يجعل مواجهة جرائم الاختراق رهينة بمدى تكامل هذه الأبعاد لا بوجود أحدها منفردًا (Al-Marri, 2023; UAE Government Official Portal, 2024). ويؤكد ذلك أن تطور وسائل الاعتداء على الأنظمة والبيانات يقابله دائمًا تطور موازٍ في وسائل الحماية، الأمر الذي يبرز الطبيعة المتغيرة والمستمرة للتهديدات السيبرانية، ويجعل فعالية الحماية القانونية مرتبطة بقدرة النصوص التشريعية على التكيف مع صور السلوك الإجرامي المستحدثة (Al-Azraq, 2021; Jaydul & 'Abbas, 2026).

كما تظهر التجربة الإماراتية أن بناء استراتيجية وطنية للأمن السيبراني، وإنشاء مجلس متخصص، والتقدم في المؤشرات الدولية، تمثل جميعها مؤشرات على وجود إرادة مؤسسية واضحة لمواجهة المخاطر السيبرانية (Telecommunications and Digital Government Regulatory Authority, 2019; Cabinet, 2020; Cyber Security Council, 2023). غير أن هذا التقدم المؤسسي، على أهميته، لا يكفي وحده لتحقيق الحماية الكاملة ما لم يواكبه ضبط تشريعي دقيق للمفاهيم المرتبطة بجريمة الاختراق، ولا سيما في ظل طبيعتها المتغيرة وسهولة تنفيذها عن بُعد وتعدد وسائل ارتكابها (Official Gazette, 2021; Al-Shamsi, 2022).

وتؤكد الدراسات السابقة أن أغلب الأدبيات اتجهت إما إلى المعالجة العامة للفضاء السيبراني، أو إلى المسؤولية المدنية، أو إلى حماية البيانات والخصوصية في إطار مقارن، في حين لم تُعالج بصورة كافية جريمة الاختراق السيبراني بوصفها جريمة مستقلة ذات طبيعة خاصة في التشريع الإماراتي (Al-'Awayshah, 2022; Al-Duwaykat, 2024; Al-Marri, 2023). ومن ثم، فإن الدراسة الحالية تتميز بتركيزها المباشر على جريمة الاختراق من حيث ماهيتها وصورها وأركانها ومسؤوليتها القانونية، في ضوء المرسوم بقانون اتحادي رقم (34) لسنة 2021 (Official Gazette, 2021; Al-Azraq, 2021).

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

ويفهم من هذا التحليل أن الإشكال الحقيقي لا يكمن فقط في وجود نصوص قانونية تجرم أفعال الاختراق، وإنما في مدى كفاية هذه النصوص لاستيعاب التطور التقني المتسارع، وقدرتها على التمييز بين صور السلوك الإجرامي المختلفة، مثل الاختراق والدخول غير المشروع والإتلاف المعلوماتي (Official Gazette, 2021; Jaydul & Abbas, 2026). وعليه، فإن دور الأمن السيبراني في مواجهة جرائم الاختراق يتجاوز حدود الوقاية التقنية إلى الإسناد التشريعي والتحليل المؤسسي والتنسيق الإجرائي، بما يكفل حماية أكثر فاعلية للبيانات والأنظمة والمصالح الوطنية المرتبطة بها (UAE Government Official Portal, 2024; Cyber Security Council, 2023).

النتائج والتوصيات

أسفرت الدراسة عن عدد من النتائج، من أبرزها أن جريمة الاختراق من الجرائم المرتبطة ارتباطًا وثيقًا بالشبكات والأنظمة المتصلة رقميًا، وأن خطورتها ترجع إلى سهولة تنفيذها وإمكان ارتكابها عن بُعد وسرعة آثارها على البيانات والأنظمة المستهدفة. كما تبين أن التطور التقني، ولا سيما في مجال الذكاء الاصطناعي، يفتح المجال أمام صور جديدة من الاعتداء على البيانات والبرمجيات، بما يفرض على المشرّع مواكبة هذا التطور بصورة مستمرة. كذلك أظهرت الدراسة أن المشرّع الإماراتي خطا خطوات متقدمة في مجال مكافحة جرائم تقنية المعلومات، إلا أن الحاجة ما تزال قائمة إلى مزيد من الدقة في تحديد بعض المفاهيم والصور الإجرامية المرتبطة بالاختراق السيبراني.

وبناءً على ذلك، توصي الدراسة بضرورة تعريف الهجوم السيبراني والاختراق السيبراني تعريفًا تشريعيًا صريحًا، وتخصيص نصوص قانونية أكثر تحديدًا لتجريم استخدام أدوات وأنظمة الاختراق، مع استحداث حماية جزائية مشددة للأنظمة المعلوماتية الحكومية بالنظر إلى حساسيتها وخطورة الاعتداء عليها. كما توصي بضرورة التحديث المستمر للتشريعات ذات الصلة، بما يضمن استيعاب الأنماط المستحدثة من الجرائم الإلكترونية، وتعزيز التكامل بين الوسائل التقنية والآليات القانونية والمؤسسية، إلى جانب دعم الحلول الوقائية الذكية، مثل أنظمة الحماية المتقدمة وأدوات التنبؤ بالمخاطر السيبرانية قبل وقوعها.

الخاتمة

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الاجتماعية

E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

تأسيسًا على ما تقدم، يتضح أن الأمن السيبراني يمثل اليوم أحد المرتكزات الأساسية لحماية الدولة والمجتمع في البيئة الرقمية، وأن فاعلية دوره في مواجهة جرائم الاختراق لا تتحقق إلا من خلال رؤية شاملة تجمع بين الوقاية التقنية، والاستجابة المؤسسية، والتجريم التشريعي الدقيق. ومن ثم، فإن تطوير هذه المنظومة بصورة متكاملة يُعد ضرورة قانونية وعملية لضمان حماية البيانات والأنظمة المعلوماتية، وتعزيز أمن دولة الإمارات العربية المتحدة في مواجهة التهديدات السيبرانية المتجددة.

References

Al-'Awayshah, A. F. Sh. (2022). Al-mas'uliyyah al-madaniyyah li-muzawwidi al-khidmah fi al-amn al-sibrani [The civil liability of service providers in cybersecurity]. *Majallat Jami'at 'Amman al-'Arabiyyah li-al-Buhuth – Silsilat al-Buhuth al-Qanuniyyah*, *4*(2), 112–145.

Al-Azraq, N. N. (2021). Muhaddidat al-mas'uliyyah al-jina'iyyah li-jara'im al-ikhtiraq wa al-i'tirad wa al-intihal wa aliyyat al-dabt wa al-rad' fi al-tashri'at al-'Arabiyyah fi al-'asr al-raqmi: Dirasah tahliliyyah muqaranah [Determinants of criminal liability for hacking, interception, and impersonation crimes and mechanisms of control and deterrence in Arab legislation in the digital age: A comparative analytical study]. *Majallat al-Buhuth al-I'lamiyyah*, *56*(3), 1041–1080. https://doi.org/10.21608/jsb.2021.150183

Al-Duwaykat, F. M. D. (2024). *Nitaq al-himayah al-jaza'iyyah li-al-bayanat al-shakhsiyyah al-iliktruniyyah fi al-qanun al-Urduni* [The scope of criminal protection for electronic personal data in Jordanian law] [Unpublished master's thesis]. Al-Isra University.

Al-Marri, R. M. (2023). Al-amn al-sibrani wa himayat al-anzimah al-iliktruniyyah: Dirasah tahliliyyah ta'siliyyah [Cybersecurity and the protection of electronic systems: An analytical foundational study]. *Majallat al-Dirasat al-Qanuniyyah wa al-Iqtisadiyyah*, *9*(1), 959–1008.

Al-Nasir, M. (2023). Ashkal intihak al-fada' al-sibrani wa wasa'iluha wa atharuha [Forms of cyberspace violation, its means, and its effects]. *Majallat al-Nadwah li-al-Dirasat al-Qanuniyyah*, *40*, 86-120.

E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

Al-Qatatshah, B. F. H. (2024). *Al-himayah al-jina'iyyah li-khususiyyat al-bayanat al-shakhsiyyah al-raqmiyyah: Dirasah muqaranah* [Criminal protection of the privacy of digital personal data: A comparative study] [Unpublished doctoral dissertation].

Al-Sayyid, Kh. S. (2022). *Al-amn al-qawmi al-iliktruni wa jara'im al-ma'lumat* [Electronic national security and information crimes]. Dar al-Nahdah al-'Arabiyyah.

Al-Shamsi, R. Gh. (2022). *Himayat al-khususiyyah al-raqmiyyah fi zill tatbiqat al-dhaka' al-istina'i: Dirasah tahliliyyah muqaranah* [Protecting digital privacy in light of artificial intelligence applications: A comparative analytical study] [Unpublished master's thesis]. United Arab Emirates University.

Cabinet. (2020). *Decision No. (55) of 2020 on the Establishment of the Cyber Security Council*. Official Gazette, Issue 678.

Cyber Security Council. (2023). *Cyber Security Council*. United Arab Emirates.

Department of Defense, U.S. (1985). *Trusted Computer System Evaluation Criteria (TCSEC)*. DoD 5200.28-STD.

International Telecommunication Union. (2020). *Global cybersecurity index 2020*. ITU.

Jaydul, M., & 'Abbas, H. (2026). Himayat al-khususiyyah wa al-amn al-raqmi fi al-qanun al-jina'i [Protecting privacy and digital security in criminal law]. *Al-Majallah al-'Arabiyyah li-al-'Ulum al-Qanuniyyah*, *7*(1), 27–33.

Khalifah, A. F. (2015). *Al-jara'im al-massah bi-amn al-dawlah* [Crimes affecting state security]. Dar al-Wafa'.

Lynn, A. (2011). The earliest computer security policies. *IEEE Security & Privacy*, *9*(6), 72–75.

McAfee Associates. (1988). *VirusScan user manual*. McAfee Associates, Inc.

Mitnick, K., & Simon, W. (2011). *In the realm of fear: The man who tricked the world's most wanted hacker*. Wiley.

Official Gazette. (2021). *Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes*. Government of the United Arab Emirates.

Sladek, S. (1989). The 414s and the MILNET hack. *2600: The Hacker Quarterly*, *6*(2), 40-42.

Telecommunications and Digital Government Regulatory Authority. (2019). *National cybersecurity strategy*. Government of the United Arab Emirates.

Tomlinson, R. (1984). *The first network email*. http://openmap.usc.edu/silk/1stEmail.html

Law, Policy, and Social Science
مجلة القانون والسياسة والعلوم الإجتماعية
E-ISSN: 2948-3964, Vol. 5, No. 1, 2026, pp. 40-60

UAE Government Official Portal. (2024). *Cyber safety and digital security*. Government of the United Arab Emirates.