IRAQI Academic Scientific Journals

Sumer Journal of Legal Science
مجلة سومر للعلوم القانونية
P.ISSN: -3081-1082
https://sjls.edu.iq/index.php/su/ar/index

Vol. (1), No. (2) June 2026
Pages 81-104

المجلد (١) العدد (٢) حزيران ٢٠٢٦
الصفحة ٨١-١٠٤

Criminal liability for cyberattacks in Iraqi and comparative legislation

Dr. Basim Dhamad Diwan
College of Law - Sumer University

Abstract:
This study addresses the issue of criminal liability arising from cyberattacks, focusing on the inadequacy of traditional legal frameworks in accommodating the virtual nature of these crimes. The study aims to identify the legislative gap in Iraqi law resulting from the absence of a specialized law to combat cybercrime. This forces the judiciary to rely on provisions of the Penal Code No. 111 of 1969, which are primarily literal and may not adequately address attacks on digital values. Employing a descriptive, analytical, and comparative approach with Egyptian legislation (Law No. 175 of 2018), the research arrives at key findings, most notably the necessity of transitioning from purely physical punishments to a system that combines imprisonment, substantial financial penalties, and preventative technical measures. The study also addresses the challenge of digital evidence by proposing that electronic evidence be granted conclusive legal weight equivalent to physical evidence. The study recommends that the Iraqi legislature expedite the enactment of modern legislation that embraces the concept of digital sovereignty, while introducing rehabilitative measures such as digital community service for gifted youth, to ensure a delicate balance between criminal deterrence and technological advancement.

Keywords: Cyberattacks, criminal liability, Iraqi legislation, Egyptian law, digital evidence, digital sovereignty.

https://doi.org/10.66734/xtcgxa90

1: Email basem.dmad@uos.edu.iq
2 : Email:

Submitted: 22-4-2026
Accepted: 2-5-2026
Published:2-6-2026

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

المسؤولية الجنائية عن الهجمات السيبرانية في التشريع العراقي والمقارن

م.د. باسم ضمد ديوان

كلية القانون- جامعة سومر

المستخلص:

تتناول هذه الدراسة إشكالية المسؤولية الجنائية الناشئة عن الهجمات السيبرانية، بالتركيز على قصور القواعد التقليدية في استيعاب الطبيعة الافتراضية لهذه الجرائم. تهدف الدراسة إلى تشخيص الفجوة التشريعية في القانون العراقي نتيجة غياب قانون متخصص لمكافحة الجرائم المعلوماتية، مما يدفع القضاء للقياس على نصوص قانون العقوبات رقم ١١١ لسنة ١٩٦٩، وهي نصوص ذات قالب مادي قد لا تتلاءم مع الاعتداءات الواقعة على القيم الرقمية. وباعتماد المنهج الوصفي التحليلي المقارن مع التشريع المصري (قانون رقم ١٧٥ لسنة ٢٠١٨)، توصل البحث إلى نتائج جوهرية أبرزها: ضرورة الانتقال من العقوبات البدنية الصرفة إلى منظومة تجمع بين سلب الحرية والردع المالي الجسيم والتدابير التقنية الاحترازية. كما خلصت الدراسة إلى معالجة معضلة الإسناد الرقمي عبر اقتراح منح الدليل الإلكتروني حجية قطعية تماثل الأدلة المادية. وتوصي الدراسة المشرع العراقي بالإسراع في سن تشريع متطور يتبني مفهوم السيادة الرقمية، مع استحداث تدابير إصلاحية كالخدمة المجتمعية الرقمية للأحداث الموهوبين، لضمان موازنة دقيقة بين الردع الجنائي والتطور التقني.

الكلمات المفتاحية: الهجمات السيبرانية، المسؤولية الجنائية، التشريع العراقي، القانون المصري، الدليل الرقمي، السيادة الرقمية.

المقدمة

أولاً: التعريف بالموضوع:

أصبحت التقنيات الرقمية هي المحرك الأساس لمرافق الدولة الاستراتيجية ومنظوماتها الأمنية والاقتصادية، فقد واكب هذا التطور بزوغ ظاهرة إجرامية بالغة الخطورة تتمثل في الهجمات السيبرانية. هذه الهجمات لم تعد مجرد عبث إلكتروني عابر، بل استحالت سلاحاً فتاكاً قادراً على تقويض أركان الاستقرار عبر اختراق النظم المعلوماتية وتدمير البيانات أو تعطيل الخدمات العامة، وتبرز خطورة هذه الهجمات في طبيعتها العابرة للحدود، وسرعة تنفيذها، وصعوبة تقفي أثارها، ومن هنا تأتي هذه الدراسة لتسلط الضوء على المسؤولية الجنائية عن هذه الهجمات في التشريع العراقي الذي لا يزال يعتمد على القواعد العامة، مقارنة بالتشريع المصري الذي قطع شوطاً متقدماً بصدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، والذي قدم نموذجاً تشريعياً منضبطاً يستجيب لخصوصية الفضاء السيبراني.

ثانياً: مشكلة البحث:

تكمن المشكلة في أن الهجمات السيبرانية تتسم بطبيعة افتراضية تجعل من تحديد المسؤولية الجنائية أمراً في غاية التعقيد. حيث يثور التساؤل: إلى أي مدى نجحت القواعد العامة في العراق في توفير حماية جنائية موازية لما حققه المشرع المصري؟ وكيف يمكن للمشرع العراقي الاستفادة من التجربة المصرية في تكييف السلوك والنتيجة والعقوبة في الهجمات السيبرانية؟

ثالثاً: أهمية البحث:

تكمن أهمية البحث في السعي لرفد المكتبة القانونية العراقية بحلول تشريعية مستمدة من الواقع التطبيقي للقانون المصري، كونه من التشريعات العربية الرائدة التي وازنت بين مقتضيات الردع وحماية الحقوق الرقمية. وتبرز الأهمية العلمية في محاولة وضع خريطة طريق للمشرع العراقي لتبني سياسة جنائية حديثة للهجمات السيبرانية، مستلهمة من نجاح التجربة المصرية في معالجة إشكاليات الإثبات الرقمي وتفريد العقوبات التقنية.

رابعاً: منهجية البحث:

بدأت الدراسة بالمنهج الوصفي لتحديد الماهية القانونية والتقنية للهجمات السيبرانية، وتوصيف خصائصها التي تميزها عن الأنماط الإجرامية التقليدية، مع رصد واقع النصوص النافذة في العراق التي يتم طوعها لمعالجة هذه الظاهرة. ثم انتقل البحث إلى المنهج التحليلي لتفكيك الأركان المادية والمعنوية للجريمة، وتحليل مدى قدرة القواعد الكلاسيكية على استيعاب الاعتداءات الواقعة على القيم الرقمية. واختُتمت المنهجية بالمنهج المقارن عبر اتخاذ التشريع المصري (قانون رقم ١٧٥ لسنة ٢٠١٨) نموذجاً للموازنة، نظراً لحداثته وانضباط قواعده الموضوعية والإجرائية.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

خامساً: نطاق البحث:

يقتصر نطاق الدراسة في هذا البحث؛ وبالخصوص المبحث الثاني، على بيان موقف المشرع العراقي في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ ومشروع قانون الجرائم المعلوماتية في مسودته المطروحة على الانترنيت، وكذلك موقف المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

سادساً: هيكلية البحث:

تم تقسيم هذا البحث إلى مبحثين أساسيين، تناولنا في المبحث الأول؛ تعريف الهجمات السيبرانية وخصائصها وذاتيتها وأنواعها. بينما يركز المبحث الثاني؛ على التنظيم الجنائي لهذه الهجمات من حيث الأركان والمسؤولية والعقوبة لدى كل من المشرع العراقي والمصري.

المبحث الأول

مفهوم الهجمات السيبرانية

لأجل الإحاطة بهذا المفهوم من أهم الجوانب، سنقسم هذا المبحث إلى مطلبين؛ نخصص المطلب الأول منه لبيان تعريف وخصائص. أما المطلب الثاني، فسنكرسه لبحث ذاتية هذه الهجمات، مع تسليط الضوء على الأنواع المختلفة لها. على النحو الآتي:

المطلب الأول

تعريف وخصائص الهجمات السيبرانية

سنعمل في هذا المطلب على تفكيك المصطلح لغةً واصطلاحاً واستعراض الخصائص التي تميزه عن الجرائم التقليدية، وذلك من خلال تقسيم هذا المطلب إلى فرعين؛ نخصص الأول للتعريف، والثاني للخصائص الذاتية.

الفرع الأول

تعريف الهجمات السيبرانية

أولاً: التعريف اللغوي:

بالنظر في البناء اللفظي لمصطلح الهجمات السيبرانية، نجد أنه يتألف من تركيب وصفي يجمع بين مفردة عربية الأصل وأخرى معربة. فكلمة هجمات هي جمع هجمة، ومصدرها الفعل الثلاثي هجم،[١] وبمراجعة أمهات المعاجم العربية كلسان العرب لابن منظور[٢] والقاموس المحيط للفيروز آبادي،[٣] يتضح أن الهجوم يعني الانتهاء إلى الشيء بغتة، أو دخوله بغير إذن، ويشير في مضمونه إلى عنصر المفاجأة والاعتداء والقوة، وهو ما ينسجم مع طبيعة الفعل الجرمي الذي يقع قسراً على الإرادة والأنظمة.

أما وصف السيبرانية فهو تعريب للمصطلح الأجنبي سايبر (Cyber)، وبالبحث في الجذور اللغوية نجد أن هذا اللفظ لا أصل له في المادة اللغوية العربية القديمة، بل يرجع اشتقاقه إلى اللغة اليونانية من مفردة (Kybernetes) التي كانت تشير إلى الربان أو الموجه أو المسيطر. وبناءً على ذلك، يمكن استخلاص المعنى اللغوي المركب بأنه ذلك الاعتداء المباغت وغير المشروع الذي يتم عبر وسائط التحكم الرقمي والاتصال الشبكي. [٤]

ثانياً: التعريف الاصطلاحي:

تعددت المقاربات الفقهية في وضع تعريف جامع للهجمات السيبرانية، حيث تباينت هذه الاتجاهات بحسب الزاوية القانونية التي ينظر من خلالها الباحث. فقد ركز الاتجاه الأول على الوسيلة المستخدمة في الاعتداء، وممن تزعم هذا الاتجاه الفقيه الفرنسي جون براديل (Jean Pradel) الذي اعتبر الهجمة السيبرانية كل فعل اعتداء يتم تنفيذه من خلال معالجة المعطيات آلياً، بحيث تكون الأداة التقنية هي الوسيلة المحورية والوحيدة لإتمام الجريمة. [٥] بينما ذهب الاتجاه الثاني إلى التركيز على محل الاعتداء، وهو ما تبناه جانب من الفقه العربي، إذ عرفها بأنها سلوك غير مشروع يوجه للنيل من المعطيات المعلوماتية المخزنة أو المنقولة عبر الشبكات، سواء كان الغرض منها التجسس أو التخريب. أما الاتجاه الثالث فقد ركز على النتيجة الجرمية، وعرفها بأنها الوصول غير المصرح به لنظام معالجة بيانات يترتب عليه إتلاف أو تعطيل أو تغيير في تلك المعطيات بما يلحق ضرراً بصاحب الحق القانوني. [٦]

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

وعلى صعيد التشريعات والاتفاقات الدولية، نجد أن التوجه القانوني مال نحو التحديد الموضوعي للأفعال بدلاً من وضع تعريفات جامعة قد تتأثر بالتطور التقني. فبالنظر إلى اتفاقية بودابست للإجرام المعلوماتي لعام ٢٠٠١، نجدها لم تضع تعريفاً لغوياً لمصطلح الهجمة، بل حصرت الأفعال المكونة لها في صور الدخول غير القانوني والتدخل في البيانات والأنظمة. (٧)

وبناءً على ما تقدم من آراء وتوجهات، يمكننا تبني تعريف إجرائي يتسق مع متطلبات المسؤولية الجنائية، مفاده أن الهجمة السيبرانية "هي كل سلوك عمدي غير مشروع، يتحقق عبر البيئة الافتراضية باستخدام أدوات برمجية تقنية، يستهدف المساس بسلامة أو سرية أو استمرارية النظم المعلوماتية، وينتج عنه ضرر مادي أو معنوي تترتب عليه آثار عقابية".

الفرع الثاني

خصائص الهجمات السيبرانية

تتميز الهجمات السيبرانية بمجموعة من الخصائص الذاتية التي تنأى بها عن صور الجرائم التقليدية:

تتجلى الخصيصة الأولى في الطبيعة العابرة للحدود، حيث إن الهجمة السيبرانية لا تقيدها الحدود الجغرافية للدول ولا تخضع للموانع الفيزيائية التقليدية. فالجاني قد يباشر سلوكه الإجرامي من مكان يقع في قارة مختلفة تماماً عن المكان الذي يقع فيه النظام المعلوماتي المستهدف، وهذا التباعد المكاني بين الفعل والنتيجة يثير إشكالات قانونية معقدة تتعلق بالاختصاص القضائي والقانون الواجب التطبيق، فضلاً عن صعوبة ملاحقة الجناة دولياً. (٨)

أما الخصيصة الثانية فهي التخفي الرقمي وسهولة طمس الأدلة، إذ يعتمد مرتكبو الهجمات السيبرانية على تقنيات معقدة للتمويه وتشفير الهوية وتغيير مسارات التدفق المعلوماتي عبر خوادم وسيطة، مما يجعل من الصعب على جهات التحقيق الربط اليقيني بين الفعل والشخص الطبيعي المرتكب له. وتزداد هذه الصعوبة نظراً لكون الدليل الرقمي يتميز بالهشاشة وسهولة المحو أو التعديل في أجزاء من الثانية، مما يضعف من قيمة الأدلة المادية مقارنة بالجرائم الواقعية. (٩)

وتتمثل الخصيصة الثالثة في ضخامة الأضرار الناجمة عن الهجمة قياساً بالجهد المبذول والتكلفة المادية، فبينما تتطلب الجرائم التقليدية جسامة في الوسائل المادية وتخطيطاً ميدانياً، فإن الهجمة السيبرانية قد تنفذ بواسطة جهاز حاسوب بسيط وبرمجيات خبيثة، ومع ذلك فإن نتائجها قد تؤدي إلى شلل تام لمرافق حيوية في

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

الدولة كالطاقة أو المنظومات المصرفية، مما يترتب عليه خسائر اقتصادية واجتماعية تفوق بمراحل ما تخلفه الجرائم المادية الجسيمة. (١٠)

وتأتي الخصيصة الرابعة متمثلة في السرعة الفائقة في التنفيذ والتطور، حيث إن الهجمة السيبرانية تتم بسرعة الضوء عبر الشبكات، ولا تمنح المجني عليه أو أنظمة الحماية وقتاً كافياً للتصدي لها أو احتواء أثارها فور وقوعها. كما أن هذه الهجمات تتسم بالديناميكية، فما يعد اليوم ثغرة أمنية يتم معالجتها، يتطور غداً إلى نمط اختراق جديد، مما يفرز حالة من عدم الاستقرار التشريعي والحاجة المستمرة لتطوير النصوص القانونية لتواكب هذا التسارع التقني. (١١)

المطلب الثاني

ذاتية وأنواع الهجمات السيبرانية

بعد أن حددنا تعريف الهجمات السيبرانية وخصائصها، يبرز التساؤل حول الحدود الفاصلة بينها وبين المفاهيم الإجرامية الأخرى التي قد تتقاطع معها في البيئة الرقمية، كما يستلزم الأمر تصنيف هذه الهجمات بناءً على معايير علمية توضح تباين آثارها وأهدافها، وذلك وفقاً للفرعين الآتيين:

الفرع الأول

ذاتية الهجمات السيبرانية

إن الخلط بين المفاهيم قد يؤدي إلى انحراف في التكييف القانوني وبالتالي خلل في تقدير العقوبة. وتتجلى هذه الذاتية من خلال فك الاشتباك بين الهجمة السيبرانية وثلاثة مفاهيم محورية:

أولاً: التمييز بين الهجمة السيبرانية والاختراق المجرد:

يتمحور الفارق الجوهري هنا حول عنصر القصد الجنائي والغاية النهائية من الفعل. فالاختراق في صورته البسيطة قد لا يتعدى كونه ولوجاً غير مصرح به لنظام معلوماتي، وغالباً ما يحركه الفضول العلمي أو الرغبة في اختبار متانة الحواجز الأمنية دون انصراف إرادة الفاعل إلى إحداث تخريب أو تعطيل، وهو ما يُعرف في الأوساط التقنية بالاختراق الأخلاقي في بعض صوره. (١٢) أما الهجمة السيبرانية في المنظور الجنائي، فهي نشاط عدائي بطبيعته، لا يقف عند حدود تجاوز العقبات التقنية، بل يمتد ليشمل إرادة آثمة تتجه نحو النيل من استقرار المنظومة المعلوماتية. فبينما يكتفي المخترق المجرد بالاطلاع أو الوجود داخل النظام، تسعى الهجمة

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

إلى خلخلة المراكز القانونية المحمية عبر التغيير أو الحذف أو الإتلاف، ومما نلاحظه أن الهجمة السيبرانية تكون على مرتبة أعلى من الجسامة الجرمية مقارنة بالاختراق الساكن. (١٣)

ثانياً: التمييز بين الهجمة السيبرانية والجرائم المعلوماتية التقليدية:

يبرز وجه التمايز هنا في محل الاعتداء ودور التقنية في الجريمة. ففي الجرائم المعلوماتية التقليدية، كالاحتيال أو النصب الإلكتروني، تظل الجريمة في جوهرها جريمة اعتداء على الأموال، وتكون الوسيلة الرقمية مجرد أداة مستحدثة لتنفيذ السلوك التقليدي؛ أي أن الجريمة تقع بالحاسوب وليس على الحاسوب. أما في حالة الهجمة السيبرانية، فإن الاعتداء يقع أصالة على الكيان المعلوماتي ذاته بصفتة قيمة محمية لذاتها، حيث يكون الهدف هو تقويض سلامة البيانات أو منع الوصول إلى الأنظمة أو تعطيل البنية التحتية الرقمية. وبذلك، فإن الهجمة السيبرانية تخرج عن كونها مجرد وسيلة ارتكاب، لتصبح هي السلوك والنتيجة الموجهة ضد الحق في سلامة التعاملات الرقمية، مما يمنحها ذاتية تقنية صرفة تفتقر إليها الجرائم التقليدية التي تستخدم الفضاء الرقمي كقناة للتواصل الجرمي فقط. (١٤)

ثالثاً: التمييز بين الهجمة السيبرانية والإرهاب السيبراني:

على الرغم من وحدة الوسيلة التقنية، إلا أن التفرقة بينهما ترتكز على "الباعث والغاية"؛ فالهجمة السيبرانية مصطلح مرن قد يحركه الانتقام الشخصي أو المنافسة غير المشروعة دون اشتراط غاية عامة. في حين يمثل الإرهاب السيبراني صورة مشددة تستلزم قانوناً توفر باعث سياسي أو أيديولوجي يستهدف ترويع الآمنين أو إكراه السلطات العامة.(١٥) وبذلك تخرج الهجمة الإرهابية من دائرة الجرائم المعلوماتية العادية لتستقر في نطاق الجرائم الموجهة ضد أمن الدولة والمصالح العليا، مما يستتبع اختلافاً جذرياً في طبيعة المسؤولية وجسامة الجزاء المقابل.(١٦)

الفرع الثاني

أنواع الهجمات السيبرانية

تتعدد صور الهجمات السيبرانية وتتنوع باختلاف الغرض المتوخى منها أو الآلية التقنية المتبعة في تنفيذها، وهو ما يفرض علينا ضرورة تصنيفها للوقوف على جسامة كل نمط وآثاره القانونية.

تأتي في مقدمة هذه الأنواع هجمات حجب الخدمة، والتي تستهدف النيل من توافر النظام واستمراريته. وتعتمد هذه الهجمة على إغراق الخادم أو الشبكة المستهدفة بفيض هائل من البيانات والطلبات الوهمية التي

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

تفوق قدرتها الاستيعابية، مما يؤدي إلى شل حركتها وخروجها عن الخدمة بصورة مؤقتة أو دائمة، وتكمن الخطورة الجنائية هنا في منع المستخدمين الشرعيين من الوصول إلى حقوقهم الرقمية، وهو ما قد يتسبب في كوارث إذا ما وجهت هذه الهجمة نحو مرافق حيوية كالمستشفيات أو المصارف أو منصات الإدارة الحكومية. [١٧] ومثاله الواقعي ما شهدته المؤسسات الحيوية في بعض الدول من شلل تام نتيجة هجمات حجب الخدمة الموزعة، كالهجمات التي استهدفت القطاع المصرفي والخدمات الحكومية الإلكترونية في دول عدة عام ٢٠٢٣،[١٨] وهو ما يجسد مفهوم (التعطيل العمدي للمرافق) في الفكر الجنائي المستحدث.

أما النوع الثاني فيتمثل في هجمات البرمجيات الخبيثة، وهي برامج يتم دسها داخل النظام بطرق احتيالية لتقوم بمهام تخريبية، ويندرج تحت هذا النوع ما يعرف ببرامج الفدية التي تقوم بتشفير كافة بيانات المجني عليه، ومن ثم مساومته على دفع مبالغ مالية مقابل منح مفتاح فك التشفير ، ويمثل هذا النمط صورة مركبة من الجرائم؛ فهي هجمة تخريبية من جهة، وجريمة ابتزاز مالي من جهة أخرى، مما يثير إشكالات في تكييف العقوبة وتعدد الجرائم المترتبة على فعل واحد. [١٩] ويبرز في هذا السياق هجوم (Colonial Pipeline) عام ٢٠٢١ الذي استهدف أكبر خط أنابيب للوقود في الولايات المتحدة، حيث تم تشفير البيانات والمساومة على فدية مالية ضخمة، مما تسبب في أزمة طاقة حقيقية،[٢٠] وهو ما نكيفه قانونياً بأنه (جريمة مركبة) تجمع بين التخريب المعلوماتي والابتزاز.

ويبرز النوع الثالث في هجمات التجسس وسرقة المعطيات، وهي الهجمات التي لا تستهدف التخريب المادي للنظام بقدر ما تستهدف انتهاك سرية المعلومات، حيث يسعى الجاني من خلالها إلى الولوج غير المصرح به لقواعد البيانات لاستنساخ معلومات سرية، سواء كانت أسراراً عسكرية للدولة، أو بيانات مالية، أو خصوصيات فردية، وهذا النوع من الهجمات يتسم بهدوء التنفيذ وغياب الآثار المادية المباشرة، إلا أن خطورته تكمن في المساس بالحق في الخصوصية والأمن المعلوماتي القومي. [٢١] وتعد حادثة (SolarWinds) عام ٢٠٢٠ نموذجاً صارخاً لهذا النوع، حيث تم اختراق سلاسل التوريد البرمجية للوصول إلى بيانات حساسة في وكالات حكومية كبرى،[٢٢] مما كشف عن مفهوم (التجسس السيبراني الاستراتيجي) الذي لا يترك أثراً مادياً فورياً لكنه يقوض الأمن القومي للدول.

وأخيراً، نجد نوعاً بالغ الخطورة يسمى هجمات التخريب المادي المبرمج، وهي الهجمات التي تتجاوز آثارها الفضاء الافتراضي لتحدث دماراً ملموساً في الواقع المادي. ويتحقق ذلك عبر اختراق أنظمة التحكم

الصناعية المسؤولة عن إدارة المنشآت الحيوية مثل محطات توليد الطاقة أو أنظمة السدود أو شبكات المواصلات، ومن خلال التلاعب بالأوامر البرمجية لهذه الأنظمة، يمكن للجاني إحداث انفجارات أو حرائق أو تصادمات، مما يحول الهجمة السيبرانية إلى سلاح تدميري شامل تترتب عليه مسؤولية جنائية جسيمة قد تصل إلى حد الجنايات الكبرى، [٢٣] ويرى الباحث أن هذا النوع من الهجمات يمثل ذروة الخطورة الإجرامية، لأنه يخرج الجريمة من الافتراضي إلى المادي، مما قد يستوجب تكييفها كجريمة تخريب منشآت عامة وفق المادة ٣٥٣ من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، وذلك لربط الواقع التقني بالنصوص العقابية النافذة. ولعل أبرز وأخطر تجليات هذا النوع في العصر الراهن، هي العمليات التي تستهدف البنية التحتية من خلال التلاعب بالدوائر الإلكترونية والأوامر البرمجية للأجهزة المادية، كما حدث في واقعة (تفجير أجهزة النداء الآلي– Pagers) في لبنان عام ٢٠٢٤؛ حيث تم استغلال الثغرات التقنية في سلاسل التوريد أو التحكم عن بُعد لتحويل أجهزة اتصالات مدنية إلى أدوات تفجير مادية. [٢٤]

المبحث الثاني

التنظيم الجنائي للهجمات السيبرانية

سنقسم هذا المبحث إلى مطلبين؛ نبحث في الأول البنيان القانوني لهذه الجريمة (أركانها)، بينما نكرس الثاني لبيان الآثار العقابية وموانع المسؤولية وصعوبات الإثبات، وذلك في كلا التشريعين العراقي والمصري.

المطلب الأول

البنيان القانوني للجريمة السيبرانية

تقوم الجريمة السيبرانية، كغيرها من الجرائم العمدية، على ركنين أساسيين: ركن مادي يتمثل في المظهر الخارجي للسلوك الإجرامي، وركن معنوي يمثل الجانب النفسي والنية الآثمة لدى الجاني. وسنفصل هذين الركنين من منظور التقنية الرقمية والتشريع المقارن في الفرعين الآتيين:

الفرع الأول

الركن المادي للهجمات السيبرانية

يُعد الركن المادي المظهر الخارجي الذي تخرج به الجريمة من حيز التفكير والتحريض إلى عالم الواقع، وهو في الهجمات السيبرانية يتخذ طبيعة خاصة نظراً لكونه يقع في بيئة افتراضية غير ملموسة. ولاكتمال هذا الركن، لابد من تضافر ثلاثة عناصر جوهرية تتمثل في السلوك الإجرامي، والنتيجة، ورابطة السببية:

أولاً: السلوك الإجرامي:

يقوم السلوك الإجرامي في الهجمات السيبرانية على نشاط إرادي يباشره الجاني، ويظهر في عالم الواقع عبر صورتين قانونيتين؛ تتمثل الأولى في الصورة الإيجابية التي تتبدى في حركة عضوية مادية باستخدام وسيلة تقنية تهدف إلى النفاذ غير المشروع للمنظومات المعلوماتية أو زرع برمجيات خبيثة تستهدف تغيير البيانات أو تعطيل عمل الخوادم، بينما تتمثل الصورة الثانية في السلوك السلبي أو الامتناع الذي يتحقق بترك فعل يوجبه القانون أو تفرضه الواجبات الوظيفية، ومثاله تعمد المسؤول عن أمن المعلومات الامتناع عن سد ثغرة برمجية معلومة لديه أو تعطيل جدران الحماية بقصد تسهيل وقوع هجمة خارجية حيث يعد الامتناع في هذه الحالة سلوكاً جرمياً كونه مكن من وقوع النتيجة الضارة.[٢٥]

ويواجه القضاء العراقي في هذا الصدد معضلة قانونية ناتجة عن عدم إقرار قانون مكافحة الجرائم المعلوماتية حتى تاريخه، مما أوجد فراغاً تشريعياً دفع القضاء الجنائي إلى محاولة سد هذه الثغرة عبر استعارة نصوص قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل وبالتحديد المادتين ٣٥٣ و٤٧٧ المتعلقتين بجرائم التخريب والإتلاف العمدي للأموال والممتلكات،[٢٦] غير أن هذا المسلك يواجه خللاً فقهياً جوهرياً كون هذه النصوص قد صُممت تاريخياً لحماية الأعيان المادية الملموسة كالعقارات والمنقولات بينما تقع الهجمة السيبرانية على بيانات ذات طبيعة معنوية ونبضات إلكترونية لا تندرج بدقة تحت المفهوم التقليدي للمال المادي ومن ثم فإن محاولة تكييف تدمير البيانات على أنه إتلاف مال مادي يوقع القاضي في محظور التفسير الواسع أو القياس في المسائل الجنائية وهو ما يتعارض بوضوح مع مبدأ شرعية الجرائم والعقوبات الذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص صريح يحدد السلوك بدقة وقت ارتكابه. [٢٧]

وعلى خلاف هذا الاضطراب في الواقع العراقي حسم المشرع المصري هذه الإشكالية بصدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ الذي قدم نموذجاً للانضباط القانوني عبر التحديد الدقيق

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

للأنماط التقنية المكونة للسلوك الإجرامي، حيث أفرد في المواد من ١٤ إلى ١٨ نصوصاً صريحة تجرم أفعالاً محددة كالدخول غير المشروع والاعتداء على سلامة البيانات والأنظمة،[٢٨] وبذلك تجاوز المشرع المصري عقبة المادية ولم يشترط وقوع الفعل على جسم ملموس بل جعل السلوك الجرمي قائماً بمجرد الاعتداء على المحتوى الرقمي أو المنظومة المعلوماتية مخرجاً القضاء من حرج التأويل، كما بسط المشرع المصري في المادة ٢٠ حماية خاصة للسلوك الذي يستهدف أمن الدولة أو البنية التحتية المعلوماتية السيادية بوصفها أفعالاً جسيمة تستوجب عقوبات مغلظة مما وفر حماية استباقية ومنضبطة للفضاء السيبراني. [٢٩]

ويرى الباحث أن استمرار المشرع العراقي في حالة الصمت التشريعي أمام تنامي التهديدات الرقمية يضع القضاء بين خيارين كلاهما ينطوي على خلل في منظومة العدالة فإما إطلاق سراح الجاني إعمالاً لمبدأ الشرعية أو التوسع في تفسير نصوص الإتلاف المادي إرضاءً لمنطق الضرورة الاجتماعية.

ثانياً: النتيجة الإجرامية:

تتمثل بصفة عامة في الأثر المترتب على السلوك الإجرامي والذي يحدث تغييراً في العالم الخارجي، وفي سياق الهجمات السيبرانية تتخذ هذه النتيجة طبيعة اعتبارية رقمية تتمحور حول المساس بسلامة البيانات أو إعاقة عمل المنظومات المعلوماتية، حيث تظهر في صور متعددة كحذف المعطيات أو تشفيرها أو تغيير محتواها بما يؤدي إلى فقدان الثقة في صدق المعلومات أو شل قدرة النظام على أداء وظائفه الحيوية وتكمن خصوصية هذه النتيجة في كونها غير ملموسة مادياً مما يثير إشكالاً في تكييف جسامة الضرر المتحقق مقارنة بالجرائم التقليدية. [٣٠]

وبالنظر إلى التوجه التشريعي العراقي، يلاحظ أن مسودة قانون الجرائم المعلوماتية[٣١] قد حاولت التوسع في نطاق النتيجة الإجرامية لتتجاوز الضرر الفردي البسيط وتصل إلى حد المساس بالأمن القومي والاقتصاد الوطني، وهو توجه يجد سنده القانوني في القواعد العامة الواردة في قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ وتحديداً المادة ١٦٤ التي تقرر عقوبات مغلظة تصل إلى الإعدام في حالات المساس بالوسائل الدفاعية للدولة،[٣٢] حيث يمكن تكييف المنظومات السيبرانية السيادية بوصفها جزءاً لا يتجزأ من الوسائل الدفاعية المستحدثة التي يتوجب بسط الحماية الجنائية عليها غير أن غياب النص الخاص يجعل من إثبات هذه النتيجة وتحديد رابطتها بالسلوك أمراً يخضع لتقدير المحكمة بناءً على تقارير الخبرة الفنية التي قد تتباين في توصيف حجم الضرر الرقمي. [٣٣]

وفي المقابل نجد أن المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ قد تبنى صياغة مرنة ومتطورة للنتيجة الإجرامية، حيث لم يقيد قيام الجريمة بحدوث ضرر مادي جسيم بل اعتبر مجرد انتهاك حرمة الحساب الخاص أو البريد الإلكتروني أو الدخول غير المشروع لموقع معلوماتي نتيجة كافية لانعقاد المسؤولية الجنائية وهو ما يسمى في الفقه الجنائي (بجرائم الخطر أو الجرائم ذات النتيجة الحكمية)، كما جعل المشرع المصري من تدمير البيانات أو تغييرها ظرفاً مشدداً للعقوبة خاصة إذا انصرفت النتيجة إلى الإضرار بالأنظمة المعلوماتية التابعة للدولة أو المرافق الحيوية، وبذلك يكون المشرع المصري قد وفر حماية مزدوجة تبدأ من لحظة المساس بالحق في الخصوصية الرقمية وتصل إلى حماية الكيان المعلوماتي للدولة من أخطار التخريب. (٣٤)

ونعتقد أن النموذج المصري في اعتبار مجرد "الولوج غير المصرح به" نتيجة جرمية هو المسلك الأنسب لضمان الردع الاستباقي ومنع تفاقم الفعل الإجرامي وصولاً إلى نتائج كارثية ومن ثم فإننا ندعو المشرع العراقي إلى ضرورة النص على نتائج إجرامية مستقلة تستوعب الخصوصية الرقمية وتفصل بين المساس بسرية البيانات وبين المساس بتكاملها وتوافرها لضمان تفريد عقابي يتناسب مع جسامة الأثر الناتج عن الهجمة.

ثالثاً: علاقة السببية:

تمثل رابطة السببية الركن الجوهري الذي يربط السلوك الإجرامي بالنتيجة الضارة المتحققة وبدون ثبوت هذه الرابطة لا يمكن إسناد المسؤولية الجنائية إلى الفاعل، وفي بيئة الهجمات السيبرانية تكتسب هذه الرابطة تعقيداً خاصاً نظراً لطبيعة الوسط الرقمي الذي قد تتداخل فيه عدة عوامل تقنية تؤدي في مجملها إلى وقوع النتيجة الإجرامية، وتكمن الصعوبة العملية في الجزم بأن فعل الجاني المتمثل في حقن الأكواد الخبيثة أو توجيه تدفقات معلوماتية هو السبب الوحيد والمباشر في انهيار النظام أو تشفير البيانات خاصة في ظل احتمالية وجود ثغرات أمنية سابقة أو أخطاء تقنية من قبل المستخدمين أو حتى وقوع خلل مفاجئ في البنية التحتية للمنظومة المعلوماتية. (٣٥)

وبالرجوع إلى الواقع القضائي العراقي نجد أن إثبات رابطة السببية يظل رهيناً للقواعد العامة في قانون العقوبات التي تأخذ بنظر الاعتبار السبب الكافي لإحداث النتيجة، غير أن قصور هذه القواعد يتضح عند مواجهة السبب الأجنبي في الفضاء الرقمي حيث يصعب على القاضي الجنائي غير المتخصص تحديد اللحظة الدقيقة التي انقطعت فيها علاقة السببية بين فعل المهاجم والنتيجة الضارة ومن ثم فإن الاعتماد الكلي على

تقارير الخبرة الفنية في العراق يضع القضاء أمام تحدي المصداقية التقنية في ظل غياب معايير وطنية موحدة لاستخلاص الدليل الرقمي مما قد يؤدي في بعض الأحيان إلى إفلات الجناة من العقاب بدعوى وجود شك فني في انفراد سلوكهم بإحداث الضرر. (٣٦)

وعلى النقيض من ذلك نجد أن المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية قد وضع أسساً إجرائية متينة لضبط رابطة السببية من خلال تنظيم "سلسلة الحيازة الرقمية" وتوثيق الأثر التقني منذ لحظة انطلاق الهجمة وحتى وقوع النتيجة، وبموجب المادة ١١ من القانون المصري أصبحت الأدلة الرقمية المستخلصة وفق المعايير الفنية ذات حجية مطلقة في الإثبات الجنائي(٣٧) مما مكن القضاء المصري من استظهار رابطة السببية بيقين قضائي يستند إلى تتبع المسار التقني للسلوك والتحقق من مدى فاعلية هذا السلوك في إحداث النتيجة بصرف النظر عن وجود ثغرات فنية سابقة في النظام طالما أن فعل الجاني هو الذي استغل تلك الثغرات لتحقيق الغاية الإجرامية، مما يضمن عدم ضياع المسؤولية الجنائية في متاهات التعقيد البرمجي. (٣٨)

الفرع الثاني

الركن المعنوي للهجمات السيبرانية

لا تكتمل الجريمة السيبرانية بمجرد وقوع السلوك المادي وإحداث النتيجة، بل لابد من توافر رابطة نفسية تربط بين الجاني والفعل المرتكب، وهو ما يُعرف بالركن المعنوي. وباعتبار الهجمات السيبرانية من الجرائم العمدية بطبيعتها، فإن الركن المعنوي فيها يتخذ صورة القصد الجنائي بعنصرية (العلم والإرادة)، مع ضرورة البحث في مدى اشتراط القصد الخاص لتكييف الفعل كهجمة.

أولاً: القصد الجنائي العام:

يتحقق القصد العام في الهجمات السيبرانية حين تتجه إرادة الجاني إلى ارتكاب الفعل المكون للجريمة مع علمه بكافة عناصرها القانونية؛ ففي العلم: يجب أن يكون الجاني عالماً بأن النظام الذي يستهدفه هو نظام محمي وغير مصرح له بالدخول إليه أو العبث به. وفي سياق القضاء العراقي، واستناداً للقواعد العامة، فإن الجهل بالواقع (كأن يعتقد الشخص أنه يختبر نظاماً يمتلكه) قد ينفي القصد، لكن الجهل بالقانون (الادعاء بعدم معرفة تجريم الاختراق) لا يُعتد به. أما الإرادة: وهي انصراف نية الجاني إلى تحقيق السلوك الإجرامي (كحقن

الكود البرمجي الخبيث) والنتيجة المترتبة عليه (كتعطيل النظام او تشفير البيانات). [٣٩] وبناءً عليه، إذا تحققت النتيجة الضارة بسبب خلل فني عارض، أو نتيجة إهمال أو قلة احتراز غير مقصود، فإن المسؤولية الجنائية عن "هجمة سيبرانية" تنتفي تماماً؛ إذ إن وصف الهجمة يحمل في طياته بطبيعته معنى القصد والعمد، ولا يتصور قانوناً قيام هجمة سيبرانية عن طريق الخطأ غير العمدي، كونها جريمة مقصودة تستلزم إرادة آثمة تتجه نحو التخريب. [٤٠]

ثانياً: القصد الجنائي الخاص:

تتميز الهجمات السيبرانية في الفقه القانوني الحديث بضرورة توافر القصد الخاص، وهو انصراف نية الجاني إلى تحقيق غاية محددة تتجاوز مجرد الولوج غير المصرح به. ففي هجمات برامج الفدية، يجب توفر نية الابتزاز وتحصيل منفعة مالية، وفي هجمات التخريب، يجب توفر نية الإضرار بالبنية التحتية أو المساس بالأمن القومي. [٤١] وبالنظر إلى قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩، نجد أن مواد التخريب (مثل المادة ٣٥٣) تتطلب صراحة انصراف النية إلى إحداث التخريب،[٤٢] وبرأينا فإنه ما ينسجم مع طبيعة الهجمات السيبرانية التي لا تكتفي بخرق السرية، بل تستهدف النيل من تكامل وسلامة المعطيات.

ويتوافق المشرع المصري مع الاتجاه العام في اشتراط العمدية في جرائم الهجمات السيبرانية، بيد أنه وضع تمييزاً دقيقاً في المادة (١٤) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨؛[٤٣] حيث فرق بين "القصد العام" المتمثل في إرادة الدخول غير المشروع للنظام مع العلم بعدم الحق، وبين "القصد الخاص" الذي يتطلب انصراف نية الجاني إلى تحقيق غاية تخريبية محددة كإلغاء البيانات أو إتلافها أو تغييرها، كما أكد التشريع المصري ضمناً على خروج الأفعال غير العمدية الناجمة عن الإهمال أو التقصير التقني من نطاق التأثيم الجنائي بموجب هذا القانون، مما يؤصل لكون الهجمة السيبرانية فعلاً عدائياً مقصوداً في جوهره.[٤٤]

هذا ويمثل إثبات الركن المعنوي في الهجمات السيبرانية معضلة قضائية؛ نظراً لأن القاضي يتعامل مع نوايا مستترة خلف شاشات وخوارزميات. فكيف يمكن التفرقة بين "المخترق الهاوي" الذي قد يلج النظام بدافع التعلم، وبين "المهاجم" الذي يستهدف التدمير؟ هنا يتم الاستدلال على القصد من خلال القرائن المادية، مثل نوع الأدوات المستخدمة (برمجيات هدم)، وتوقيت الهجمة، وحجم الضرر الناتج، وهي قرائن يعتمدها القضاء

العراقي في تقدير جسامة الفعل وتكييفه. اما في المشرع المصري فإن التفريد المتقدم في الركن المعنوي يمنح القاضي مرونة في تقدير العقوبة بحسب جسامة الباعث النفسي للجاني. (٤٥)

ونعتقد أن النموذج المصري في تفريد القصد الجنائي يمثل الحل الأمثل لتجاوز قصور القواعد العامة ونطالب المشرع العراقي عند إقرار القانون المرتقب بتبني مفهوم القصد المتطور الذي يراعي الغايات السياسية والإرهابية للهجمات وعدم الاكتفاء بالقصد التقليدي لضمان عدم إفلات المحرضين والمخططين الذين لا يباشرون الفعل المادي بأنفسهم من العقاب الجنائي.

المطلب الثاني

الآثار المترتبة على المسؤولية الجنائية وموانعها

إذا ما تحقق البنيان القانوني للجريمة السيبرانية بركنيها المادي والمعنوي، انعقدت المسؤولية الجنائية في حق الجاني، مما يستتبع إيقاع الجزاء المقررة قانوناً. بيد أن خصوصية الفضاء السيبراني تفرض مراجعة لنوعية العقوبات، كما تثير إشكالات دقيقة حول موانع المسؤولية وصعوبات الإثبات التي قد تجعل العقاب متعذراً من الناحية العملية. وسنفصل ذلك في الفرعين الآتيين:

الفرع الأول

العقوبات والتدابير الاحترازية المقررة

تستوجب الطبيعة الفريدة للهجمات السيبرانية تبني سياسة جنائية مزدوجة، تجمع بين الجزاءات التقليدية التي تستهدف شخص الجاني، وبين التدابير التقنية التي تستهدف الوسائل والأدوات المستخدمة في الجريمة. ويهدف هذا التوجه إلى تحقيق الردع العام والخاص من خلال معالجة الخطورة الجرمية الكامنة في المهارة التقنية للجاني، وهو ما يمكن تفصيله وفق الآتي:

أولاً: العقوبات الأصلية:

يجد القضاء العراقي نفسه في ظل غياب قانون خاص لمكافحة الجرائم المعلوماتية مضطراً لإنزال العقوبات الواردة في قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل، حيث تتراوح العقوبات الأصلية بين الحبس والسجن تبعا لتكييف الهجمة السيبرانية بوصفها جريمة تخريب أو اعتداء على الأموال العامة أو مساساً بأمن الدولة وهي جنايات تستوجب عقوبات بدنية غليظة، بينما تكشف المسودة التشريعية العراقية المقترحة عن تحول

نحو تغليظ العقوبات المالية بشكل غير مسبوق إدراكاً بأن بواعث هذه الهجمات غالباً ما تستهدف تحقيق مكاسب اقتصادية غير مشروعة مما يجعل من الغرامة أداة ردع فاعلة لتجريد الجاني من عائده الجرمي. [٤٦] وفي المقابل نجد أن المشرع المصري قد جسد هذه الفلسفة واقعياً في قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، حيث قرر في المادة ٢٠ عقوبات أصلية تجمع بين الحبس والغرامات المالية الباهظة التي قد تصل إلى خمسة ملايين جنيه مصري خاصة في الهجمات التي تستهدف أصول الدولة المعلوماتية،[٤٧] وبذلك يكون المشرع المصري قد أوجد توازناً بين العقوبة السالبة للحرية والجزاء المالي لضمان الزجر الكافي الذي يتناسب مع جسامة الاعتداء على السيادة الرقمية.

ثانياً: التدابير الاحترازية والعقوبات التبعية:

إدراكاً بأن المهاجم السيبراني يمتلك مهارة ذهنية تمثل مصدر خطورة دائمة فقد برزت الحاجة لتدابير تتجاوز مفهوم العقاب التقليدي لتستهدف شل قدرته على العودة للإجرام وتتمثل أبرز هذه التدابير في المصادرة الوجوبية للأجهزة والأنظمة المستخدمة في الهجمة وإغلاق المواقع أو الحسابات التي اتخذها الجاني منطلقاً لنشاطه وهو ما يمثل حكماً بالإعدام المعنوي لنشاطه في الفضاء الافتراضي كما تشمل هذه الحزمة عقوبة الحرمان من مزاولة المهنة أو حظر العمل في مراكز التقنية لفترة محددة كتدبير وقائي ضروري يمنع المتخصص من توظيف أدواته للنيل من أمن المجتمع. [٤٨]

وقد تفوق المشرع المصري في هذا الجانب بالنص صراحة في المادة ٤ على حجب المواقع كتدبير احترازي لدرء الخطر القائم، وفي المادة ١١ على المصادرة الوجوبية للأدوات والبرامج. [٤٩] بينما لا تزال المنظومة القانونية العراقية النافذة تفتقر للنصوص التي تمنح القاضي مرونة كافية لتطبيق هذه التدابير بصورة متخصصة على الجرائم الرقمية إذ تظل النصوص الحالية مادية القالب تنظر للنتيجة كأثر ملموس مما يولد خللاً في تقدير العقوبة حين تتم مساواة من يشل حركة مرفق حيوي بضغطة زر مع من يتلف جهازاً مادياً بسيطاً. [٥٠]

ونؤكد إقتفاء أثر المشرع المصري في تبني تدابير تقنية قادرة على سلب السلاح الرقمي من الجاني لضمان فاعلية الجزاء الجنائي وتطوير السياسة العقابية بما يتلاءم مع القيم الاعتبارية الرقمية المستهدفة بالهجمة.

الفرع الثاني

موانع المسؤولية وصعوبات الإثبات الجنائي

إن قيام الأركان المادية والمعنوية للجريمة السيبرانية لا يؤدي بالضرورة إلى توقيع العقاب، إذ قد تصطدم الدعوى الجزائية بموانع قانونية تعفي الجاني من المسؤولية، أو بعقبات إجرائية تجعل من إسناد الفعل إلى فاعله أمراً متعذراً بيقين.

أولاً: موانع المسؤولية الجنائية في الهجمات السيبرانية:

تتمثل أبرز موانع المسؤولية في الفضاء الافتراضي في حق الدفاع الشرعي الرقمي، حيث استقر الفقه والقضاء في مصر على إعمال القواعد العامة الواردة في قانون العقوبات (المواد ٢٤٥-٢٥١) بالقياس؛[٥١] فاعتبر أن صد الهجوم السيبراني الذي يهدد سلامة المنظومات المعلوماتية للدولة أو الأفراد يبيح للمسؤول التقني اتخاذ إجراءات مضادة لتعطيل مصدر الاعتداء، تأسيساً على أن حماية البيانات والأنظمة تماثل حماية المال المادي والنفس، شريطة الالتزام بضوابط الضرورة والتناسب. وفي المقابل، يجد القضاء العراقي نفسه مضطراً للقياس على حق الدفاع الشرعي التقليدي الوارد في قانون العقوبات رقم ١١١ لسنة ١٩٦٩، غير أن غياب النص الخاص في العراق يثير إشكالاً في تقدير التناسب بين فعل الدفاع والاعتداء الرقمي، مما يضع القائمين على أمن المعلومات تحت طائلة المسؤولية إذا تجاوز الرد التقني حدود الضرورة المادية المتعارف عليها قضائياً. [٥٢]

ثانياً: صعوبات الإثبات الجنائي:

تمثل عملية الإثبات التحدي الأكبر في الهجمات السيبرانية نظراً لسهولة طمس الأثر الرقمي وقدرة المهاجمين على التمويه الجغرافي، وهو ما يولد معضلة الإسناد التي تعاني منها المحاكم العراقية نتيجة عدم تحديث قانون أصول المحاكمات الجزائية بما يمنح الدليل المستخلص من الوسائط الرقمية حجية قطعية؛ إذ يظل الدليل الرقمي في العراق مجرد قرينة تخضع لتقدير القاضي الذي قد يتردد في بناء حكم بالإدانة استناداً إلى سجلات إلكترونية قابلة للتلاعب التقني. [٥٣] وخلافاً لهذا الوضع، حسم المشرع المصري هذه المعضلة في المادة (١١) من القانون رقم ١٧٥ لسنة ٢٠١٨،[٥٤] حيث منح للأدلة الرقمية ذات الحجية المقررة للأدلة المادية، وعزز ذلك بلائحة تنفيذية وضعت معايير فنية صارمة لحفظ الدليل وضمان سلامته عبر ما يعرف بسلسلة الحيازة، مما قلل من هامش الشك القضائي وحول الدليل الرقمي إلى ركيزة أساسية للإدانة. [٥٥]

ويرى الباحث أن حل معضلة الإثبات في العراق لا يتوقف عند غلظة العقوبة، بل يتطلب تقنيناً صريحاً لحجية الدليل الرقمي وتأهيل قضاء متخصص يجمع بين القانون والتقنية؛ فنحن ننتقد المنهج التشريعي العراقي الذي لا يزال يتعامل مع الخبير الفني كعنصر ثانوي، بينما يمثل في الجرائم السيبرانية "الشاهد الصامت" الذي يمتلك مفاتيح الحقيقة التقنية. لذا، فإننا نؤكد على ضرورة اقتفاء أثر المشرع المصري في وضع منظومة إجرائية متكاملة تضمن عدم ضياع المسؤولية الجنائية خلف ستار التعقيد البرمجي، وتوفر آليات للتعاون القضائي الدولي لضبط الهجمات العابرة للحدود، لضمان بسط السيادة القانونية على الفضاء الرقمي الوطني.

الخاتمة

في ختام هذه الدراسة الموسومة بالمسؤولية الجنائية عن الهجمات السيبرانية في التشريع العراقي والمقارن، والتي توخينا فيها تأصيل القواعد الموضوعية والإجرائية الحاكمة لهذا النمط الإجرامي المستحدث، نخلص إلى جملة من النتائج والتوصيات التي نراها ركيزة أساسية لتعزيز الحماية الجنائية للفضاء الرقمي الوطني:

أولاً: النتائج:

١- أثبتت الدراسة وجود فجوة قانونية ناتجة عن غياب قانون خاص بالجرائم المعلوماتية في العراق، مما يضطر القضاء للاستناد إلى نصوص قانون العقوبات التقليدي.

٢- تبين أن النصوص العقابية النافذة في العراق ذات طبيعة مادية، فهي صُممت لحماية الأعيان الملموسة والمنشآت المادية، ولا تستوعب بدقة الماهية المعنوية للبيانات والنبضات الإلكترونية.

٣- كشف التحليل المقارن عن حداثة السياسة الجنائية المصرية في القانون رقم ١٧٥ لسنة ٢٠١٨، والذي نجح في التوفيق بين العقوبات البدنية والردع المالي الجسيم، فضلاً عن تقنين التدابير الاحترازية التقنية.

٤- تظل رابطة السببية والإسناد الجنائي في العراق رهينة لتقارير الخبرة الفنية التي تفتقر لمعايير وطنية موحدة، على خلاف المشرع المصري الذي منح الأدلة الرقمية حجية قطعية تماثل الأدلة المادية.

٥- وجدنا إن الهجمة السيبرانية تتجاوز مفهوم الاختراق البسيط؛ فهي سلوك عدائي عمدي يستهدف تقويض سلامة النظام المعلوماتي، مما يستوجب تفريدها بعقوبات تتناسب مع بواعثها التخريبية.

ثانياً: التوصيات:

١- نوصي المشرع العراقي بضرورة الإسراع في إقرار قانون مكافحة الجرائم المعلوماتية، شريطة الابتعاد عن صياغات العقوبات التقليدية وتبني مصطلحات تقنية دقيقة تستوعب القيم الرقمية المستهدفة.

٢- ندعو السلطة التشريعية إلى إدراج تدابير احترازية متخصصة كحجب المواقع، والمصادرة الوجوبية للأدوات والبرامج المستخدمة، والحظر المهني للمهاجمين المحترفين، لضمان سلب السلاح الرقمي من الجاني.

٣- نقترح على الحكومة العراقية استحداث نظام الخدمة المجتمعية الرقمية للأحداث المخترقين، لتوظيف مهاراتهم في تعزيز الأمن السيبراني بدلاً من إيداعهم المؤسسات الإصلاحية التقليدية التي قد تزيد من خطورتهم الإجرامية.

٤- نوصي مجلس النواب لتحديث قانون أصول المحاكمات، كما ونؤكد على محاكم الجزاء ضرورة منح الدليل الرقمي المستخلص وفق معايير فنية منضبطة حجية كاملة في الإثبات الجنائي، ووضع نظام سلسلة الحيازة الرقمية لضمان سلامة الأدلة من العبث.

٥- نوصي مجلس القضاء الأعلى بإنشاء دوائر قضائية متخصصة في الجرائم السيبرانية، وتأهيل القضاة وأعضاء النيابة تقنياً لتمكينهم من استخلاص القصد الجنائي والبت في معضلات الإسناد الفني المعقدة.

وبهذا، نضع هذه الدراسة وما تضمنته من رؤى تحليلية أمام صانع القرار التشريعي في العراق، أملاً في بناء سياج قانوني رصين يحمي السيادة الرقمية للدولة ويحقق العدالة في الفضاء الافتراضي.

الهوامش

(١) د. محمد حسن أحمد، دلالات الألفاظ الجنائية في المعاجم العربية: دراسة تأصيلية، مجلة الدراسات اللغوية والأدبية، جامعة الموصل، المجلد ٦، العدد ٢، ٢٠١٨، ص ١١٢.

(٢) ابن منظور، أبو الفضل جمال الدين محمد بن مكرم (ت ٧١١هـ)، لسان العرب، دار صادر، بيروت، الطبعة الثالثة، ١٤١٤هـ، مادة (هجم)، الجزء ١٢، ص ٥٩٦.

(٣) الفيروز آبادي، مجد الدين محمد بن يعقوب (ت ٨١٧هـ)، القاموس المحيط، تحقيق: مكتب تحقيق التراث في مؤسسة الرسالة، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت، الطبعة الثامنة، ٢٠٠٥، مادة (هجم)، ص ١١٦٢.

(٤) د. محمد بن عبد الله بن محمد المشيقح، المصطلحات التقنية في اللغة العربية: دراسة في الجذور والدلالات، مجلة جامعة القصيم (العلوم الإنسانية)، المجلد ١٢، العدد ٤، ٢٠١٩، ص ٣٤.

(٥) د. محمد السعيد رشدي، الجريمة المعلوماتية، دار النهضة العربية، القاهرة، دون طبعة، ٢٠١٨، ص ٣٢.

(٦) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، دون طبعة، ١٩٩٨، ص ١٤. وينظر أيضاً: د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، دون طبعة، ٢٠١٧، ص ١٩.

(٧) نقلاً عن: د. واثق هويدي المياحي، المواجهة القانونية لجرائم المعلوماتية في ضوء الاتفاقيات الدولية، المكتب الجامعي الحديث، الإسكندرية، ٢٠٢٠، ص ٥٥.

(٨) د. محمد فوزي إبراهيم، جرائم الفضاء السيبراني: دراسة في التحديات القانونية والقضائية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١، ص ٧٧.

(٩) د. عادل عبد العزيز السن، الأمن السيبراني: المفاهيم والأسس والتحديات، المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٢١، ص ٤٢.

(١٠) رشا علي مجيد، الآثار الاقتصادية والاجتماعية للهجمات السيبرانية، رسالة ماجستير، كلية الإدارة والاقتصاد، جامعة القادسية، ٢٠٢٢، ص ٥٨.

(١١) د. نوار دهام الزبيدي، السياسة الجنائية المعاصرة في مواجهة الجرائم المستحدثة، دار الكتب القانونية، مصر، ٢٠٢٠، ص ١٩٨.
(١٢) د. رامي متولي القاضي، المواجهة الجنائية لجرائم الاعتداء على الأنظمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٢٠، ص ١١٨.
(١٣) محمد سلمان فرج، الحماية الجنائية من الولوج غير المصرح به للمواقع الإلكترونية، رسالة ماجستير، كلية القانون، جامعة بابل، ٢٠١٧، ص ٥٤.
(١٤) د. عمار عباس الحسيني، الحماية الجنائية للمعلوماتية: دراسة في التشريع العراقي والمقارن، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ٤، العدد ١٢، ٢٠١٥، ص ٥٦.
(١٥) واثق هويدي المياحي، المصدر السابق، ص ١٤٢.
(١٦) د. علي كاظم الرفاعي، الإرهاب الإلكتروني وتحديات المواجهة القانونية، مكتبة زين الحقوقية، بيروت، ٢٠٢٣، ص ١٠٢.
(١٧) رامي متولي القاضي، المصدر السابق، ص ١٣٩.
(١٨) تقرير الحوادث السيبرانية السنوي، شركة كلاود فلير (Cloudflare)، تحليل هجمات حجب الخدمة الموزعة للقطاعات الحيوية لعام ٢٠٢٣، متاح على الرابط: (https://blog.cloudflare.com/ddos-threat-report-2023-q4/)، تاريخ الزيارة: ٢٠٢٦/٣/٢٢ الساعة ٢:٣٩ م.
(١٩) د. خالد ممدوح إبراهيم، جرائم تقنية المعلومات في ضوء القانون ١٧٥ لسنة ٢٠١٨، دار الفكر الجامعي، الإسكندرية، ٢٠١٩، ص ١٥٦.
(٢٠) وزارة العدل الأمريكية، بيان صحفي حول ضبط العوائد الجرمية لهجوم كولونيال بايبلاين، يونيو ٢٠٢١، متاح على موقع الوزارة (https://www.google.com/search?q=https://www.justice.gov/opa/pr/department-justice-seizes-632-bitcoin-allegedly-traceable-ransomware-attack-colonial-pipeline)، تاريخ الزيارة: ٢٠٢٦/٣/٢٢ الساعة ٢:٣٩ م.
(٢١) عمار عباس الحسيني، الحماية المصدر السابق، ص ٦٢.
(٢٢) تقرير شركة "مايكروسوفت" (Microsoft)"، تحليل هجوم سولار ويندز: تتبع الجهات الفاعلة في التهديدات السيبرانية الاستراتيجية"، ديسمبر ٢٠٢٠، متاح على الموقع الرسمي للشركة عبر الرابط:(https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack/)، تاريخ الزيارة: ٢٠٢٦/٣/٢٢ الساعة ٢:٣٩ م.
(٢٣) عادل عبد العزيز السن، المصدر السابق، ص ٦٤.
(٢٤) بيان خبراء الأمم المتحدة، المفوضية السامية لحقوق الإنسان، "تفجير أجهزة النداء في لبنان: انتهاكات مروعة للقانون الدولي"، سبتمبر ٢٠٢٤، متاح على الرابط:(https://www.google.com/search?q=https://www.ohchr.org/en/press-releases/٢٠٢٤/٠٩-exploding-pagers-and-radios-lebanon-are-terrifying-violations-international).
(٢٥) رامي متولي القاضي، مصدر سابق، ص ١٤٦.
(٢٦) تنظر: المادتين (٣٥٣) و (٤٧٧) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل النافذ.
(٢٧) د. عمار عباس الحسيني، مصدر سابق، ص ٧٢.
(٢٨) تنظر: المادتين (١٤ و١٨) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري النافذ.
(٢٩) تنظر: المادة (٢٠) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري.
(٣٠) ميسون محمود خلف، الكيان القانوني للجريمة المعلوماتية، مجلة الحقوق، جامعة النهرين، المجلد ١٥، العدد ٢، ٢٠١٣، ص ٨٤.
(٣١) تنظر: مسودة قانون الجرائم المعلوماتية العراقي، على الموقع الالكتروني(https://www.slideshare.net/slideshow/arabic-version-law/12177635)، تاريخ الزيارة ٢٠٢٦/٣/٢٢ الساعة ٢:٠٨ م.
(٣٢) تنظر: المادة (١٦٤) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.
(٣٣) ميسون محمود خلف، المصدر السابق، ص ٨٥.
(٣٤) خالد ممدوح إبراهيم، المصدر السابق، ص ٢١٢.
(٣٥) د. محمد أمين الرومي، الدليل الرقمي أمام القضاء الجنائي، دار المطبوعات الجامعية، الإسكندرية، ٢٠٢٠، ص ١٧٨.
(٣٦) د. علي كاظم الرفاعي، إثبات الجريمة المعلوماتية في قانون أصول المحاكمات الجزائية العراقي، مكتبة زين الحقوقية، بيروت، ٢٠٢١، ص ١٤٢.
(٣٧) تنظر: المادة (١١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري.
(٣٨) محمد أمين الرومي، المصدر السابق، ص ١٨٢.
(٣٩) د. مخلد خلف التركي، القصد الجنائي في الجرائم غير المادية، مجلة الرافدين للحقوق، جامعة الموصل، العدد ٥٥، ٢٠١٧، ص ٧٢.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

(٤٠) قاسم عبد الحميد السعدي، الخطأ الجنائي في الجرائم التقنية: دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة بابل، ٢٠١٨، ص ٨٨.
(٤١) محمد سامي الشوا، مصدر سابق، ص ٤٨.
(٤٢) تنظر: المادة (٣٥٣) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩.
(٤٣) تنظر: المادة (١٤) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري.
(٤٤) محمد سامي الشوا، مصدر سابق، ص ٤٩.
(٤٥) محمد أمين الرومي، مصدر سابق، ص ١٩٢.
(٤٦) نوار دهام الزبيدي، المصدر السابق، ص ٢٤٢.
(٤٧) تنظر: المادة (٢٠) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري.
(٤٨) د. إياد مطشر الحياوي، التدابير الاحترازية في الجرائم المستحدثة، مجلة القضاء المقارن، العراق، العدد ٨، ٢٠١٨، ص ٦٢. ونود الاشارة بهذا الصدد، الى أن المشرع العراقي في المادة ١٠١ من قانون العقوبات جعل المصادرة جوازية للمحكمة في الغالب، بينما تقتضي طبيعة الهجمات السيبرانية أن تكون المصادرة وجوبية للأدوات البرمجية لمنع تكرار الجريمة.
(٤٩) تنظر: المواد (٤) و (١١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري.
(٥٠) نوار دهام الزبيدي، مصدر سابق، ص ٢٤٥.

(٥١) تنظر: (المواد ٢٤٥-٢٥١) من قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧ المعدل النافذ.
(٥٢) زياد خالد الجبوري، الدفاع الشرعي في الفضاء السيبراني بين الإباحة وتجاوز الحدود، مجلة تكريت للحقوق، جامعة تكريت، المجلد ٦، العدد ٢، ٢٠٢١، ص ٢٢٥.
(٥٣) علي كاظم الرفاعي، المصدر السابق، ص ١٦٨.
(٥٤) تنظر: المادة (١١) من القانون رقم ١٧٥ لسنة ٢٠١٨ المصري.
(٥٥) محمد أمين الرومي، مصدر سابق، ص ٢٠٥.

المصادر

أولا: المعاجم اللغوية:

١) ابن منظور، أبو الفضل جمال الدين محمد بن مكرم (ت ٧١١هـ)، لسان العرب، دار صادر، بيروت، الطبعة الثالثة، ١٤١٤هـ، مادة (هجم)، الجزء ١٢.

٢) الفيروز آبادي، مجد الدين محمد بن يعقوب (ت ٨١٧هـ)، القاموس المحيط، تحقيق: مكتب تحقيق التراث في مؤسسة الرسالة، مؤسسة الرسالة للطباعة والنشر والتوزيع، بيروت، الطبعة الثامنة، ٢٠٠٥، مادة (هجم).

ثانياً: الكتب والمؤلفات:

١) د. محمد السعيد رشدي، الجريمة المعلوماتية، دار النهضة العربية، القاهرة، دون طبعة، ٢٠١٨.

٢) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، دون طبعة، ١٩٩٨.

٣) د. علي كاظم الرفاعي، الإرهاب الإلكتروني وتحديات المواجهة القانونية، مكتبة زين الحقوقية، بيروت، ٢٠٢١.

٤) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، دون طبعة، ٢٠١٧.

٥) د. واثق هويدي المياحي، المواجهة القانونية لجرائم المعلوماتية في ضوء الاتفاقيات الدولية، المكتب الجامعي الحديث، الإسكندرية، ٢٠٢٠.

٦) د. محمد فوزي إبراهيم، جرائم الفضاء السيبراني: دراسة في التحديات القانونية والقضائية، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١.

٧) د. عادل عبد العزيز السن، الأمن السيبراني: المفاهيم والأسس والتحديات، المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٢١.

٨) د. نوار دهام الزبيدي، السياسة الجنائية المعاصرة في مواجهة الجرائم المستحدثة، دار الكتب القانونية، مصر، ٢٠٢٠.

٩) د. رامي متولي القاضي، المواجهة الجنائية لجرائم الاعتداء على الأنظمة المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٢٠.

١٠) د. خالد ممدوح إبراهيم، جرائم تقنية المعلومات في ضوء القانون ١٧٥ لسنة ٢٠١٨، دار الفكر الجامعي، الإسكندرية، ٢٠١٩.

١١) د. محمد أمين الرومي، الدليل الرقمي أمام القضاء الجنائي، دار المطبوعات الجامعية، الإسكندرية، ٢٠٢٠، ص ١٧٨.

١٢) د. علي كاظم الرفاعي، إثبات الجريمة المعلوماتية في قانون أصول المحاكمات الجزائية العراقي، مكتبة زين الحقوقية، بيروت، ٢٠٢١، ص ١٤٢.

ثالثاً: الرسائل الجامعية والأطاريح:

١) رشا علي مجيد، الآثار الاقتصادية والاجتماعية للهجمات السيبرانية، رسالة ماجستير، كلية الإدارة والاقتصاد، جامعة القادسية، ٢٠٢٢.

٢) محمد سلمان فرج، الحماية الجنائية من الولوج غير المصرح به للمواقع الإلكترونية، رسالة ماجستير، كلية القانون، جامعة بابل، ٢٠١٧.

٣) قاسم عبد الحميد السعدي، الخطأ الجنائي في الجرائم التقنية: دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة بابل، ٢٠١٨.

رابعاً: البحوث القانونية والمقالات:

١) د. محمد حسن، دلالات الألفاظ الجنائية في المعاجم العربية: دراسة تأصيلية، مجلة الدراسات اللغوية والأدبية، جامعة الموصل، المجلد ٦، العدد ٢، ٢٠١٨.

رقم الإيداع في دار الكتب والوثائق :2895 لسنة 2025م

٢) د. محمد بن عبد الله بن محمد المشيقح، المصطلحات التقنية في اللغة العربية: دراسة في الجذور والدلالات، مجلة جامعة القصيم (العلوم الإنسانية)، المجلد ١٢، العدد ٤، ٢٠١٩.

٣) د. عمار عباس الحسيني، الحماية الجنائية للمعلوماتية: دراسة في التشريع العراقي والمقارن، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ٤، العدد ١٢، ٢٠١٥.

٤) ميسون محمود خلف، الكيان القانوني للجريمة المعلوماتية، مجلة الحقوق، جامعة النهرين، المجلد ١٥، العدد ٢، ٢٠١٣.

٥) د. مخلد خلف التركي، القصد الجنائي في الجرائم غير المادية، مجلة الرافدين للحقوق، جامعة الموصل، العدد ٥٥، ٢٠١٧.

٦) د. إياد مطشر الحياوي، التدابير الاحترازية في الجرائم المستحدثة، مجلة القضاء المقارن، العراق، العدد ٨، ٢٠١٨.

٧) زياد خالد الجبوري، الدفاع الشرعي في الفضاء السيبراني بين الإباحة وتجاوز الحدود، مجلة تكريت للحقوق، جامعة تكريت، المجلد ٦، العدد ٢، ٢٠٢١.

خامساً: الدساتير والقوانين:-

١) قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل النافذ.

٢) قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ المصري النافذ.

٣) قانون العقوبات المصري رقم ٥٨ لسنة ١٩٣٧ المعدل النافذ.

سادساً: الروابط الألكترونية:

1) https://www.google.com/search?q=https://www.cloudflare.com/the-net-observed/ddos-report-٢٠٢٣-q .(/٤

2) https://www.google.com/search?q=https://www.justice.gov/opa/pr/department-justice-seizes-٦٣٢-bitcoin-allegedly-traceable-ransomware-attack-colonial-pipeline .(

3) https://www.google.com/search?q=https://www.microsoft.com/en-us/security/blog/١٨/١٢/٢٠٢٠/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack .(/

4) https://www.google.com/search?q=https://www.ohchr.org/en/press-releases/٠٩/٢٠٢٤/exploding-pagers-and-radios-lebanon-are-terrifying-violations-international .

5) https://www.slideshare.net/slideshow/arabic-version-law/ .(١٢١٧٧٦٣٥