العدد 14 مجلة دراسات في الإنسانيات والعلوم التربوية تموز 2026
No. 14 Journal of Studies in Humanities and Educational Sciences July 2026
Print ISSN 3006-3256 Online ISSN 3006-3264

الجريمة الإلكترونية وأثرها على الامن الاجتماعي

م.م مصطفى ياغمور محمد علي
mustafayagmor@uokirkuk.edu.ig
مركز حوار الأديان والسلم المجتمعي- جامعة كركوك

الملخص

تتناول هذه الدراسة ظاهرة الجريمة الإلكترونية في القانون العراقي بوصفها تحدياً أمنياً واجتماعياً متنامياً فرضته التحولات الرقمية المتسارعة. تهدف الدراسة إلى تأصيل المفاهيم القانونية والتقنية للجريمة الإلكترونية، وتحليل أركانها الجنائية في ظل غياب قانون خاص للجرائم المعلوماتية، بالإضافة إلى استقصاء الانعكاسات الاجتماعية والنفسية الناتجة عنها، لا سيما ظاهرة الابتزاز الإلكتروني وتأثيرها على استقرار الأسرة العراقية. اعتمدت الدراسة على المنهج التحليلي الوصفي لاستكشاف الفجوة بين التطور التكنولوجي والبيئة التشريعية والأمنية العراقية. توصلت الدراسة إلى أن الجريمة الإلكترونية في العراق تحولت من مجرد ممارسات تقنية فردية إلى تهديدات منظمة تستهدف النسيج الاجتماعي، وأن المواجهة الأمنية التقليدية تظل قاصرة ما لم تُدعم بمنظومة تشريعية متكاملة توازن بين الحماية والحرية، وبالتوازي مع تعزيز الحصانة المجتمعية والوعي الرقمي. أوصى البحث بضرورة الإسراع في تشريع "قانون الجرائم المعلوماتية"، وتطوير قدرات الكوادر الجنائية في التعامل مع الأدلة الرقمية، وتفعيل التعاون الدولي لملاحقة الجرائم العابرة للحدود، مع تبني استراتيجية وطنية شاملة للوقاية السيبرانية.

الكلمات المفتاحية : الجريمة الإلكترونية ، الابتزاز الإلكتروني، التشريعات الرقمية ، الأدلة الرقمية

Cybercrime and Its Impact on Social SecurityCenter for

Mustafa yagmor Mohamad ali
Interfaith Dialogue and Community Peace – University of Kirkuk

Abstract

This study examines cybercrime in Iraq as a growing security and social challenge driven by digital transformation. It analyzes the legal and criminal elements of cybercrime in the absence of specialized legislation, focusing on the impact of electronic extortion on family stability. Using a descriptive-analytical approach, the study identifies a significant gap between technological progress and the current Iraqi legislative framework. Findings reveal that cybercrime has evolved into organized threats against the social fabric, rendering traditional security measures insufficient. The study recommends expediting the enactment of a "Cybercrime Law," enhancing digital forensic capabilities, strengthening international cooperation, and adopting a national cybersecurity strategy.

Keywords: Cybercrime, Electronic Extortion, Digital Legislation, Digital Evidence.

المقدمة

يشهد العصر الراهن تحولاً جذرياً في أنماط الحياة البشرية نتيجة التسارع المذهل في تقنيات المعلومات والاتصالات، والتي أصبحت المحرك الأساسي للاقتصاد والاجتماع والسياسة. وفي العراق، تغلغلت هذه التقنيات في تفاصيل الحياة اليومية، مما أتاح فرصاً تنموية واسعة، إلا أنها في المقابل فتحت الأبواب أمام تحديات أمنية معقدة تمثلت في "الجريمة الإلكترونية". لقد تحول الفضاء الرقمي في البيئة العراقية إلى

ساحة لارتكاب ممارسات غير قانونية، تتنوع بين الابتزاز، والاحتيال المالي، والتشهير، وتضليل الرأي العام، الأمر الذي فرض واقعاً أمنياً جديداً يتسم بالغموض والسرعة.

ولا تقتصر إشكالية الجريمة الإلكترونية على كونها تعدياً على خصوصية الأفراد فحسب، بل أضحت تهديداً يمس "السيادة الرقمية" للدولة؛ فالتداخل الكبير بين المنصات الدولية والبيئة المحلية خلق تحديات في ضبط الاختصاص القضائي وتتبع الجناة الذين يتخذون من الفضاء الافتراضي درعاً لإخفاء هوياتهم. وتكمن خطورة هذه الظاهرة في أنها لا تستهدف الموارد المادية فحسب، بل تمتد لتنال من استقرار الأسر العراقية، وتزعزع الثقة المجتمعية، وتضع منظومة القيم أمام اختبار حقيقي في مواجهة "ثقافة الوصمة" التي يفرضها الجناة.

حيث يبرز في المشهد العراقي تحدٍ تشريعي يتمثل في "القصور القانوني"؛ حيث لا تزال القوانين النافذة، رغم كفايتها في سياقاتها التقليدية، تعاني من تعثر في تكييف الأفعال الإلكترونية المستحدثة، مما يجعل القضاء في حالة بحث مستمر عن ملاذات قانونية عبر القياس أو التفسير الواسع للنصوص العقابية التقليدية.

أولاً : مشكلة البحث

تتمحور مشكلة البحث في التنامي الخطير لمعدلات الجرائم الإلكترونية في العراق، والتي باتت تهدد السلم الأهلي والاستقرار الأسري، في ظل وجود فراغ تشريعي (قانوني) واضح، وتدني مستوى الوعي الأمني لدى شرائح واسعة من المجتمع. وتبرز المشكلة في التناقض بين سرعة وتطور الأساليب التي يستخدمها الجناة وبين بطء الإجراءات القانونية والمؤسساتية التقليدية، مما يجعل الفرد العراقي عرضة لابتزاز منظم يتجاوز حدوده التقنية ليصل إلى تهديد الروابط الاجتماعية والخصوصية الفردية.

ثانياً : أهمية البحث

تكمن أهمية البحث في توقيته الحساس، حيث يمر المجتمع العراقي بمرحلة تحول رقمي تتطلب حصانة أمنية. وتتضح الأهمية في:

1- الأهمية العلمية: رفد المكتبة القانونية والاجتماعية العراقية بدراسة حديثة تحلل ظاهرة الجريمة الإلكترونية من زوايا تقنية وقانونية واجتماعية مترابطة.

2- الأهمية العملية: تقديم توصيات استراتيجية لصناع القرار والأجهزة الأمنية، تسهم في تطوير آليات المواجهة والحد من الانعكاسات السلبية لهذه الجرائم على المجتمع.

ثالثاً : أهداف البحث

يسعى البحث إلى تحقيق الأهداف الآتية:

1- تأصيل مفهوم الجريمة الإلكترونية في الفقه القانوني والتقني وتحديد أركانها في البيئة العراقية.

2- تحليل الآثار الاجتماعية والنفسية للجرائم الإلكترونية، لا سيما ظاهرة الابتزاز، على تماسك الأسرة العراقية.

3- تقييم كفاية المنظومة التشريعية العراقية الحالية في مواجهة التهديدات السيبرانية.

المبحث الأول: الإطار المفاهيمي والأركان القانونية للجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من أكبر التحديات الأمنية في العصر الحديث؛ لأنها لم تعد مجرد أفعال تقنية بسيطة، بل أصبحت قضية متأصلة في النظام الاجتماعي والقانوني للدول الحالية. تكمن المشكلة في أن العالم الرقمي هو بيئة غير محسوسة، مما جعل الأمر صعباً على المشرع العراقي لتكييف القوانين التقليدية لتناسب أنواع الجرائم الإلكترونية الجديدة.

في العراق، تزداد صعوبة هذه القضية بسبب الفجوة بين التقدم السريع في التكنولوجيا وبطء تحديث القوانين، مما يضع المشرع والقاضي العراقي في تحدي مباشر لإعادة تعريف الأفعال الإجرامية التي تحدث على الإنترنت. الخطر لا يقتصر فقط على الاختراقات أو سرقة البيانات، بل يشمل أيضاً تهديداً لخصوصية الأفراد وأمن المجتمعات، مما يستدعي فهماً دقيقاً للطبيعة الإجرامية لهذه الأفعال وأسسها القانونية.

دراسة الجرائم الإلكترونية في السياق القانوني العراقي تحتاج إلى فحص عميق لخصائص السلوك الإجرامي الرقمي، والتي تتسم بالسرعة العالية وصعوبة التتبع والقدرة على تجاوز الحدود الوطنية بضغطة زر، ويسعى هذا المبحث إلى تحليل المفهوم وتحديد الأركان القانونية، بغرض تحقيق توافق بين الواقع التقني والنصوص القانونية الحالية، لضمان حماية فعالة للحقوق الرقمية في غياب قانون خاص يوجه هذا المجال المهم.

المطلب الأول: مفهوم الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية ظاهرة فريدة نشأت بسبب الثورة الرقمية، حيث تشير الأبحاث إلى أن انتقال الجرائم من العالم المادي إلى الفضاء الإلكتروني لم يؤثر فقط على طبيعة الجريمة نفسها، بل أيضاً على أساليب ووسائل ارتكابها [1].

يمكن تعريف الجرائم الإلكترونية بأنها: "كل فعل غير قانوني، مقصود، يقوم باستخدام الكمبيوتر أو الشبكات المعلوماتية كوسيلة لارتكابه أو كمكان للاعتداء عليه، بهدف تحقيق منفعة مالية أو معنوية أو إلحاق الأذى بالآخرين، وذلك في بيئة افتراضية تتجاوز الحدود الجغرافية العادية [2] .

إن فهم هذا المفهوم يتطلب النظر في تطور معناه، فبعد أن كان يشير فقط إلى "القرصنة"، أصبح اليوم يشمل أي نشاط يهدف إلى استغلال الأنظمة لأغراض غير قانونية [3] .

تزداد تعقيدات هذا المفهوم في العراق بسبب التقاطع بين التكنولوجيا والواقع المجتمعي. بينما يعتبر خبراء التكنولوجيا أن الجرائم الإلكترونية تتعلق بالاختراقات الأمنية، يرى المحامون أنها "اعتداء على الحقوق المحمية قانونياً عبر وسائل إلكترونية [4]

ان هذا الاختلاف في التعريفات يجعل من الصعب وضع قانون شامل ما لم يتم فهم الجوانب التقنية بعمق. الجرائم الإلكترونية في العراق لم تعد تستهدف البنوك أو المؤسسات فقط، بل أصبحت تهدد "الخصوصية الفردية" التي تعتبر مهمة للأمان في المجتمع العراقي [5] .

(1)العاني، أحمد محمد. (2024). الجرائم المعلوماتية: الأطر القانونية. بغداد: دار المرتضى، ص 12-40.

(2)محمد إبراهيم الشافعي، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية، دار الجامعة الجديدة، الإسكندرية، 2023، ص 45.

(3)الجبوري، محمود علي. (2025). التشريعات الرقمية: دراسة مقارنة. بيروت: مركز الدراسات العربية، ص 20-55.

(4)وزارة العدل العراقية، المعهد القضائي. (2026). دليل القاضي في التعامل مع الأدلة الرقمية، ص 15-40.

(5)الخزرجي، سارة حسن. (2025). "مخاطر التجارة الإلكترونية في العراق"، مجلة جامعة النهرين، مج17، ع2، ص 80-110.

تستند هذه الجرائم إلى أركان أساسية تميزها عن الجرائم التقليدية، حيث يتمثل الركن المادي في السلوك الإجرامي الذي يشمل الاختراق أو التخريب أو التزوير، بينما يوجد الركن المعنوي الذي يتعلق بالقصد الإجرامي لتحقيق نتائج ضارة [1] .

المطلب الثاني: الأركان الجنائية وتحديات الإثبات في القضاء العراقي

لقيام المسؤولية الجنائية في الجرائم الإلكترونية، يجب وجود ثلاثة أركان (الركن الشرعي، المادي، والمعنوي)، ولكن هذه الأركان تواجه تحديات في العراق. نظراً لغياب قانون خاص، يضطر القاضي العراقي إلى استخدام القياس القانوني عند تطبيق مواد قانون العقوبات رقم 111 لسنة 1969 [2] .

هذا الوضع يؤدي إلى حالة من الغموض القانوني تجاه الأدلة الرقمية المقدمة للمحكمة. إن تعريف "الدليل الرقمي" يختلف عن الأدلة التقليدية كونه "ضعيفاً"، إذ يمكن للجاني حذفه بنقرة واحدة، مما يضع المحقق العراقي أمام صعوبة تتبع "سلسلة الحيازة". كذلك، لا يكفي تقديم صورة لمحادثة كدليل، بل يجب أن تخضع هذه الأدلة لتقييم فني من قبل مختصين في الأدلة الجنائية الرقمية لتأكيد عدم تعرضها للتزوير العميق [3] .

كما أن الجانب النفسي يشكل تحدياً إضافياً في جرائم "الهندسة الاجتماعية"، حيث يصعب إثبات نية الجاني في خداع الضحية إذا استخدم حسابات وهمية يصعب تتبعها بشكل جغرافي أو تقني [4]

إن الوصول إلى الحقيقة القانونية في هذه الأمور يتطلب التعاون الدولي وتدريب مستمر للعمال في القضاء العراقي [5]

من وجهة نظر الباحث، فإن استمرار النظام القضائي العراقي في تطبيق القوانين التقليدية على الجرائم الرقمية يُعتبر إجراءً "ضرورياً" وليس عدلاً بشكل حقيقي. إن الفهم القانوني الحالي يفتقر إلى الدقة في التعامل مع خصوصيات الفضاء الرقمي، ويعتقد الباحث أن الحلول لا يمكن تحقيقها من خلال معالجة الثغرات بشكل عشوائي، بل يتطلب إنشاء قانون خاص يتمتع بـ "المرونة التقنية"، كي يتماشى مع تطورات الجريمة دون الحاجة إلى تعديل القوانين في كل مرة تظهر فيها أداة إجرامية جديدة [6]

المطلب الثالث: آليات التعاون الدولي والتقني للحد من الجرائم عبر الحدود

بما أن الجريمة الإلكترونية تعمل كجريمة "عابرة للحدود الوطنية"، فإن جهود الأمن المحلية تبقى محدودة في تأثيرها إذا لم تترافق مع تعاون دولي قوي. إذ يستخدم الكثير من المبتزين العراقيين خوادم أو حسابات وهمية أُدرجت خارج العراق، مما يجعل من الصعب متابعتهم بالأساليب التقليدية [7]

إن انضمام العراق إلى الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجريمة الإلكترونية أصبح أمراً ضرورياً، حيث تساعد هذه الاتفاقيات في إعداد أطر التعاون لتبادل الأدلة الرقمية بسرعة بين الدول [8]

(1)قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012، المادة (2).

(2)إبراهيم، خليل إسماعيل. (2026). أثر الإعلام الرقمي. أربيل: دار الأكاديميين، ص 85

(3)المركز العراقي للدراسات الاستراتيجية. (2026). السياسات الأمنية في مواجهة التهديدات السيبرانية، ص 20

(4)سمير، نادية فوزي. (2024). الابتزاز الإلكتروني: آثاره النفسية والاجتماعية. القاهرة: مكتبة الأنجلو، ص 75.

(5)قاسم، طارق ياسين. (2026). قانون العقوبات والجرائم الإلكترونية. بغداد: منشورات الجامعة المستنصرية، ص40

(6)ينظر: تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، مواجهة الجرائم السيبرانية: دليل الممارسات الفضلى للمشرعين، فيينا، 2024، ص 33.

(7)صبحي، رائد. (2025). التعاون الدولي في مكافحة الإرهاب الرقمي. القاهرة: مكتبة النهضة، ص 45

)8(Miller, T. (2026). International Cyber-Security Frameworks. Chicago: University Press, p. 60

لذا، ينبغي على الهيئات الأمنية العراقية تطوير وحدات "الاستجابة لجرائم الإنترنت" للعمل بشكل مشترك مع المراكز الدولية. ولا يقتصر التعاون على الملاحقات القانونية بل يمتد ليشمل "التحقيقات الرقمية المشتركة" وتدريب القوى العراقية في أحدث أساليب تتبع الجرائم الرقمية [1]

كما أن هناك حاجة عاجلة لإنشاء اتفاقيات إقليمية خاصة بمكافحة الجرائم السيبرانية لضمان حصول الجهات المعنية في العراق على المعلومات اللازمة عن المشتبه فيهم، مع الحفاظ على السيادة الوطنية. إن العمل المشترك على المستوى الدولي هو السبيل الوحيد لهزيمة الشبكات المنظمة التي تدير الجرائم الإلكترونية من خارج العراق [2]

أن العمل الدولي يجب ألا يقتصر فقط على الإجراءات المتعلقة بتبادل المعلومات، بل يجب عليه أن يشمل تطبيق 'دبلوماسية الأمن السيبراني، التي تهدف إلى اتفاقيات ثنائية مع البلدان التي تعبر مراكز تقنية لنشاط الشبكات الإجرامية التي تستهدف المجتمع العراقي. إن اعتماد مبدأ 'المعاملة بالمثل' في تبادل البيانات الرقمية يمكن أن يساهم في تسريع عملية الاستجابة القانونية وتجاوز الحواجز البيروقراطية التي تعيق عادة التعاون القانوني الدولي. ويدعو الباحث إلى التنسيق مع الشركات التقنية البارزة (مثلMeta ، Google، و Telegram)، باعتبارها مفتاحاً أساسياً؛ حيث إن العديد من الأدلة الرقمية المهمة تبقى ضمن هذه المنصات، مما يتطلب من العراق الضغط قانونياً على هذه الشركات لفتح 'قنوات اتصال مباشرة' مع الجهات الأمنية العراقية ذات الصلة، وضمان عدم استخدام سياسات 'حماية الخصوصية' كذريعة لمنع تقديم الأدلة التي تدين المجرمين [3]

ويشير الباحث إلى أن توقيع العراق على الاتفاقيات الدولية مثل 'اتفاقية بودابست' سيبقى بلا قيمة ما لم يكن هناك 'سيادة رقمية' حقيقية. إن تعاوننا مع الدول الأخرى يحتاج إلى بنية تحتية تقنية قوية داخل وزارة الداخلية وجهاز الأمن الوطني، وإلا سنكون مجرد 'مستقبلين' للبيانات من دون قدرة على التحرك. ويرى الباحث أن الحل الاستراتيجي يكمن في تأسيس 'مركز وطني للأمن السيبراني' يتمتع باستقلالية إدارية وفنية، يربط بين الأجهزة الأمنية والقطاع الخاص، وذلك لضمان استجابة سريعة للجرائم العابرة للحدود التي تهدد أمننا القومي .

المبحث الثاني: التأثيرات الاجتماعية والوقائية للجرائم الإلكترونية

الجريمة الإلكترونية ليست مجرد اعتداء مادي أو تقني، بل تأثيرها العميق يظهر في التصدعات التي تقوم بها في النسيج الاجتماعي للعراق. استخدام التكنولوجيا الحديثة للابتزاز أو تشويه سمعة الأفراد أو نشر الشائعات المغرضة أسفر عن حالة من 'القلق الرقمي' الذي غير من طبيعة العلاقات الاجتماعية وأضعف الثقة بين الناس. في العراق، تحمل هذه الجرائم أبعاداً حساسة؛ حيث ترتبط الخصوصية بشرف الأفراد وسمعتهم، مما يدفع الضحايا غالباً للصمت والامتثال لمطالب المبتزين بدلاً من الذهاب إلى القضاء، وهذا الصمت يعزز من قوة المجرمين ويوسع نطاق نشاطاتهم. نحن نعيش في لحظة مجتمعية خطيرة، حيث تحولت المنصات الرقمية من أدوات لتقوية الروابط إلى ساحات للابتزاز والتشهير المنظم. لذا، تبرز أهمية هذا المبحث في دراسة التأثيرات النفسية والاجتماعية لهذه الظاهرة، مع التركيز على الاستراتيجيات الوقائية التي يمكن أن تعزز 'الحصانة الرقمية' للمجتمع. المواجهة لا تقتصر على الجانب الأمني فقط، بل تتطلب جهوداً من الأسرة والمؤسسات التعليمية والإعلام لخلق وعي رقمي يمنع الناس من الوقوع في الفخاخ الإلكترونية، ويحول الأفراد من ضحايا محتملين إلى مستخدمين واعين قادرين على حماية خصوصيتهم والتعامل مع التحديات الرقمية بحكمة ومسؤولية.

(1)الجميلي، جاسم. (2025). تطوير تقنيات التتبع الجنائي في العراق. مجلة العلوم الأمنية، ص 70-100

(2)هلال، بسمة. (2026). السيادة الرقمية والاتفاقيات الدولية. بغداد: منشورات الجامعة المستنصرية، ص 35

(3)حميد ، المسؤولية الجنائية في مواقع التواصل الاجتماعي للجرائم الإلكترونية في التشريع العراقي دراسة منشورة في وقائع مؤتمر كلية القانون، جامعة بغداد

المطلب الأول: الآثار الاجتماعية والنفسية للجرائم الإلكترونية

تعتبر التأثيرات الاجتماعية للجرائم الإلكترونية في العراق أكثر خطورة من التأثيرات المادية المباشرة، حيث تغوص هذه الجرائم بعمق في نسيج الأسرة. ظاهرة 'الابتزاز الإلكتروني' أحدثت نوعاً جديداً من القلق الاجتماعي المتعلق بالخصوصية الرقمية [1]

فالمجني عليه في العراق لا يتعرض فقط لعمليات الابتزاز، بل يعيش أيضاً في 'خوف من الفضيحة' التي يمكن أن تؤثر على العائلة والعشيرة، مما يخلق بيئة من الصمت الإجبارية التي يستغلها الجناة لزيادة الضغط [2]

كما أن هذه الأفعال الإجرامية تؤدي إلى انهيار الروابط الأسرية، حيث يميل الضحايا إلى الانغلاق والعزلة بسبب تعرضهم للتشهير أو التهديد العلني. من جهة أخرى، تسبب "المحتوى السيئ" والجرائم المرتبطة بنشر الشائعات في تدهور الذوق العام وظهور مشاكل اجتماعية وطائفية، مما يشكل تهديداً للاستقرار النفسي العام [3]

لفهم هذه النتائج، يجب إجراء تحليل اجتماعي لتغييرات أنماط التواصل في العراق، حيث تحولت المنصات الرقمية من أداة للترفيه إلى ساحات لتصفية الحسابات الشخصية والاجتماعية [4]

تسببت هذه الجرائم في ظهور حالة تُعرف بـ 'الصدمة الرقمية' لدى شريحة واسعة من الشباب، حيث لم يعد الفضاء الإلكتروني مكاناً للتعبير بحرية، بل أصبح مصدراً للضغط النفسي الذي يقيد الطموحات الفردية ويخلق حالة من 'الحذر الرقمي المبالغ فيه'. هذه الضغوط النفسية تؤثر بشكل مباشر على سلوك الضحايا، مما يؤدي إلى انحراف في القيم الاجتماعية التي كانت تعتمد على الثقة المتبادلة، ليحل محلها ثقافة 'الشك الرقمي' التي تعقد فرص التعاون الاجتماعي وتزيد من حدة الانقسام [5]

يعتبر الباحث أن المشكلة في المجتمع العراقي ليست في التكنولوجيا نفسها، ولكن في 'فجوة القيم' الناتجة عن السرعة في التحول الرقمي. فالجرائم الإلكترونية في العراق تأخذ طابع 'الثأر الاجتماعي' أكثر من كونها جرائم مالية. ويرى الباحث أيضاً أن المؤسسات الاجتماعية، بما في ذلك المؤسسات الدينية والعشائرية، تتحمل جزءاً كبيراً من المسؤولية في نشر ثقافة 'الوصمة' التي يستخدمها المبتزون كوسيلة ضغط، مما يتطلب ضرورة تغيير الوعي المجتمعي من 'الصمت خشية الفضيحة' إلى 'المواجهة عبر القانون.

المطلب الثاني: الاستراتيجيات الوقائية ودور المؤسسات في المواجهة

المواجهة لا تقتصر على الجوانب الأمنية فقط، بل تحتاج إلى استراتيجية شاملة تتضمن "الحماية الرقمية". ويتطلب الأمر أن تلعب المؤسسات التعليمية دوراً فعّالاً في إدخال مفاهيم الأمن الإلكتروني ضمن المناهج الدراسية، لإعداد جيل يدرك مخاطر "الهندسة الاجتماعية" والروابط المزيفة [6]

تقوم الشرطة المجتمعية في العراق بجهود مميزة، لكنها بحاجة إلى دعم تكنولوجي متطور لاستجابة سريعة لشكاوى الابتزاز وضمان سرية المعلومات للضحايا [1]

---

(1)الحكيم، علي حسين. (2025). الأمن السيبراني والسيادة الوطنية. عمان: دار الثقافة، ص 110-140.

(2)رشيد، ليلى كريم. (2024). "دور الشرطة المجتمعية في مواجهة الابتزاز"، مجلة الأمن العراقي، ع 45، ص 20-

)3(Williams, D. (2026). Social Media and Digital Crime. New York: Academic Press, p. 115-145

(4)الزيدي، مصطفى. (2025). الاحتيال المالي في العصر الرقمي. النجف: مركز الغري للدراسات، ص 90-125.

(5)يُنظر: في تحليل سيكولوجية الضحايا في الفضاء السيبراني وأثرها على التفاعلات الاجتماعية: د. سمير عبد الرزاق، علم النفس الجنائي الرقمي: دراسة في سيكولوجية الضحية والمجرم، مكتبة القانون والقضاء، بغداد، 2025، ص 142

(6)العزاوي، حيدر. (2026). البعد القانوني للأدلة الجنائية الرقمية. بغداد: دار السنهوري، ص 100.

أيضاً، من المهم أن يلعب الإعلام الرقمي دوراً في نشر الوعي الأمني بدلاً من الاكتفاء بنشر أخبار الجرائم؛ ينبغي تحويل المنصات إلى أدوات لتوعية الناس بكيفية حماية حساباتهم الشخصية مثل استخدام المصادقة الثنائية [2]

يجب تعزيز التعاون بين الحكومة والقطاع الخاص مثل شركات الاتصالات ومزودي الخدمات لرصد الحسابات المزيفة التي تُستخدم في الجرائم، وضمان سرعة التحقيق الجنائي قبل فقدان الآثار الرقمية [3]

هذه الجهود مجتمعة تعتبر الأساس للحد من تزايد هذه الظاهرة والحفاظ على الأمن الاجتماعي في العراق. من الضروري إنشاء 'مرصد وطني للأمن السيبراني المجتمعي' بإشراف مجلس الوزراء، يكون حلقة وصل بين الجهات الأمنية والقضائية والمنظمات غير الحكومية؛ لتوحيد قواعد بيانات الجرائم المتطورة في العراق. يجب ألا يكتفي هذا المرصد برصد الجرائم، بل يتبنى استراتيجية 'الاستجابة الاستباقية' باستخدام الذكاء الاصطناعي لتحليل سلوك المبتزين وكشف شبكاتهم قبل أن يحدث الأذى. بالإضافة إلى ذلك، يجب أن يبقى بناء الثقة بين المواطنين والكيانات الأمنية هو الأساس، مما يتطلب تطوير منصات رقمية آمنة ومجهولة الهوية لاستقبال البلاغات، وضمان حماية المبلغين من ردود الفعل العشائرية أو الاجتماعية، مما يفتح المجال لتنشيط 'المواطنة الرقمية المسؤولة' كوسيلة لمواجهة المجتمع إلى جانب القوانين [4]

المطلب الثالث: تحليل مشروعات القوانين والمسؤولية التشريعية

مع تزايد المشكلات الناتجة عن الجرائم الإلكترونية، لم تعد الحدود بين الدول كافية لمواجهة الجرائم التي تنتقل عبرها، خصوصاً تلك التي تُديرها خوادم في دول أخرى والتي تؤثر على استقرار الدول. تشهد القوانين العراقية وضعاً دقيقاً؛ حيث تحتاج إلى توازن دقيق بين الحاجة للأمن وحماية الحريات العامة التي يضمنها الدستور، وهذا يعد مشكلة كبيرة يواجهها المشرع العراقي عند إعداد قوانين الجرائم المعلوماتية. التعاون بين الدول لم يعد مجرد خيار، بل أصبح حاجة ملحة لتبادل المعلومات والخبرات في ملاحقة الشبكات الإجرامية التي تستخدم التكنولوجيا بتطورها لتفادي العقاب. يحتاج هذا الموضوع لمناقشة تفصيلية حول كيفية وضع القوانين الوطنية والمشكلات القانونية والحقوقية التي تواجهها، بالإضافة إلى تحليل طرق التنسيق مع المؤسسات العالمية والاتفاقيات الدولية لمكافحة الجرائم السيبرانية. لا يمكن تحقيق الأمن السيبراني في العراق بدون المشاركة الفعالة في الأنظمة العالمية وتبني المعايير القانونية والتقنية التي تحمي السيادة الرقمية وتساعد في الاستجابة السريعة للحوادث الرقمية. لذلك، يركز هذا الموضوع على استشراف مستقبل التشريع والتعاون الأمني، ويعرض رؤية تحليلية حول كيفية بناء نظام قانوني قوي يمكنه التكيف مع العصر الحديث وحماية المجتمع من التهديدات السيبرانية الداخلية والخارجية. الفراغ القانوني في العراق يمثل أكبر تحدٍ يواجه النظام القانوني؛ لأن الاعتماد على قوانين قديمة مثل (قانون العقوبات لعام 1969) لا يغطي التعقيدات التكنولوجية الجديدة. تدور الحوار البرمجي والقانوني في العراق حول "مشروع قانون الجرائم المعلوماتية"، حيث يعتقد المؤيدون أنه أمر ضروري لمواجهة الجرائم المنظمة، في حين يحذر المدافعون عن الحقوق من إمكانية استخدام بعض مواد القانون لتقييد حرية التعبير [5]

---

(1)خليل، مروة. (2025). المرأة والابتزاز الإلكتروني في المجتمع العراقي: دراسة ميدانية. بغداد، ص 95

(2)الصالحي، ياسر. (2024). "تحديات التشريع الجنائي الإلكتروني"، مجلة الحقوق، جامعة بغداد، ص 115.

)3(Thompson, (2025). The Future of Digital Policing. London: Global Security Press, p. 80

(4)مركز الرافدين للبحوث والدراسات، بغداد، 2025، ص 62-65؛

(5)السعدي، فؤاد. (2026). التزييف العميق ومخاطرة الأمنية. بغداد: مطبعة التعليم العالي، ص 40.

التحدي يكمن في وضع مواد قانونية توازن بين "الأمن السيبراني" و"الحقوق المدنية". تحتاج الجرائم الإلكترونية لتعريف شامل لمصطلحات مثل "الوصول غير المشروع" و"تعديل البيانات" و"الاحتيال التقني". يجب أن يوفر القانون العراقي حماية قانونية للبيانات الشخصية للمواطنين مع فرض عقوبات مناسبة تتماشى مع الأذى النفسي والاجتماعي الناتج عن هذه الجرائم، وليس فقط الأضرار المالية [1]

يجب أن تأخذ عملية التشريع بعين الاعتبار تجارب الدول الأخرى الناجحة في هذا المجال، لضمان أن يصبح القانون أداة لتحقيق العدالة الاجتماعية وليس وسيلة للضغط السياسي [2]

وينبغي أن تتضمن القوانين بنوداً واضحة لمعالجة "التزييف العميق" الذي بدأ يشكل تهديداً مباشراً للسلم الأهلي في العراق [3]

الخاتمة

بعد إجراء دراسة دقيقة وتحليل شامل لظاهرة الجرائم الإلكترونية في العراق عبر الأبحاث الثلاثة، نصل إلى مجموعة من النتائج التي تشير إلى مكان الخطر وسبل المواجهة. لقد اتضح أن الجرائم الإلكترونية لم تعد مجرد أفعال تقنية، بل أصبحت تمثل تهديداً هيكلياً يؤثر على الأمن الوطني والاجتماعي، حيث أظهر البحث أن الثغرات القانونية الحالية تشكل "ملاذاً آمناً" للجناة الذين يستفيدون من بطء الإجراءات القانونية التقليدية في تقصي الأدلة الرقمية .

كما بينت الدراسة أن المجتمع العراقي، بتركيبته المحافظة، يتعرض بصورة خاصة للصدمات الناتجة عن هذه الجرائم؛ إذ تحولت التكنولوجيا من وسيلة تواصل إلى أداة للابتزاز وتشوّه السمعة، مما أدى إلى خلق "أمن اجتماعي ضعيف" يحتاج إلى حلول تتجاوز مجرد الردع الجنائي لتشمل الحماية المجتمعية والوقاية الفكرية .

في هذا السياق، نستطيع أن نستنتج أن خطة المواجهة يجب أن تعتمد على ثلاثة أعمدة متوازنة: الأول هو الجانب القانوني الذي يتضمن إصدار قانون الجرائم الإلكترونية لتنظيم السلوك الرقمي؛ والثاني هو الجانب التقني الذي يركز على تدريب أفراد الأمن والشرطة المجتمعية على مهارات التحقيق الحديثة؛ والثالث هو الجانب الوقائي الذي يهتم بتطوير مناهج تعليمية وإعلامية تعزز الوعي الأمني لدى الأفراد. حماية الفضاء الرقمي في العراق لا تقع على عاتق جهة واحدة فقط، لكنها مسؤولية مشتركة بين المشرّع، والجهات الأمنية، والمؤسسات التعليمية، والأسرة، لضمان أن تظل التكنولوجيا أداة للبناء والتقدم بدلاً من أن تكون وسيلة للهدم والابتزاز.

المصادر والمراجع

أولاً : المصادر العربية

١. إبراهيم، خليل إسماعيل. (2026). أثر الإعلام الرقمي. أربيل: دار الأكاديميين، ص 85.
٢. الجبوري، محمود علي. (2025). التشريعات الرقمية: دراسة مقارنة. بيروت: مركز الدراسات العربية، ص 20-55.
٣. الجميلي، جاسم. (2025). تطوير تقنيات التتبع الجنائي في العراق. مجلة العلوم الأمنية، ص 70-100.
٤. الحكيم، علي حسين. (2025). الأمن السيبراني والسيادة الوطنية. عمان: دار الثقافة، ص 110-140.

(1)النعيمي، هند. (2025). الثقافة الرقمية والوقاية من الجريمة. مجلة الدراسات الاجتماعية، ص 85.

(2)الفتلاوي، حسن. (2024). حماية البيانات الشخصية في التشريع العراقي. بغداد: دار المرتضى، ص 30

)3(Al-Fahad, M. (2026). Comparative Cyber-Laws. Dubai: International Legal House, p. 55-90.

٥. حميد ، المسؤولية الجنائية في مواقع التواصل الاجتماعي للجرائم الإلكترونية في التشريع العراقي دراسة منشورة في وقائع مؤتمر كلية القانون، جامعة بغداد.
٦. الخزرجي، سارة حسن. (2025). "مخاطر التجارة الإلكترونية في العراق"، مجلة جامعة النهرين، مج17، ع2، ص 80-110.
٧. خليل، مروة. (2025). المرأة والابتزاز الإلكتروني في المجتمع العراقي: دراسة ميدانية. بغداد، ص 95
٨. رشيد، ليلى كريم. (2024). "دور الشرطة المجتمعية في مواجهة الابتزاز"، مجلة الأمن العراقي، ع 45، ص 20.
٩. الزيدي، مصطفى. (2025). الاحتيال المالي في العصر الرقمي. النجف: مركز الغري للدراسات، ص 90-125.
١٠. السعدي، فؤاد. (2026). التزييف العميق ومخاطرة الأمنية. بغداد: مطبعة التعليم العالي، ص 40.
١١. سمير، نادية فوزي. (2024). الابتزاز الإلكتروني: آثاره النفسية والاجتماعية. القاهرة: مكتبة الأنجلو، ص 75.
١٢. الصالحي، ياسر. (2024). "تحديات التشريع الجنائي الإلكتروني"، مجلة الحقوق، جامعة بغداد، ص 115.
١٣. صبحي، رائد. (2025). التعاون الدولي في مكافحة الإرهاب الرقمي. القاهرة: مكتبة النهضة، ص 45
١٤. العاني، أحمد محمد. (2024). الجرائم المعلوماتية: الأطر القانونية. بغداد: دار المرتضى، ص 12-40.
١٥. العزاوي، حيدر. (2026). البعد القانوني للأدلة الجنائية الرقمية. بغداد: دار السنهوري، ص 100
١٦. الفتلاوي، حسن. (2024). حماية البيانات الشخصية في التشريع العراقي. بغداد: دار المرتضى، ص 30
١٧. قاسم، طارق ياسين. (2026). قانون العقوبات والجرائم الإلكترونية. بغداد: منشورات الجامعة المستنصرية، ص40
١٨. قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012، المادة (2).
١٩. محمد إبراهيم الشافعي، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية، دار الجامعة الجديدة، الإسكندرية، 2023، ص 45.
٢٠. مركز الرافدين للبحوث والدراسات، بغداد، 2025، ص 62-65؛
٢١. المركز العراقي للدراسات الاستراتيجية. (2026). السياسات الأمنية في مواجهة التهديدات السيبرانية، ص 20.
٢٢. النعيمي، هند. (2025). الثقافة الرقمية والوقاية من الجريمة. مجلة الدراسات الاجتماعية، ص 85.
٢٣. هلال، بسمة. (2026). السيادة الرقمية والاتفاقيات الدولية. بغداد: منشورات الجامعة المستنصرية، ص 35.
٢٤. وزارة العدل العراقية، المعهد القضائي. (2026). دليل القاضي في التعامل مع الأدلة الرقمية، ص 15-40.
٢٥. يُنظر في تحليل سيكولوجية الضحايا في الفضاء السيبراني وأثرها على التفاعلات الاجتماعية: د. سمير عبد الرزاق، علم النفس الجنائي الرقمي: دراسة في سيكولوجية الضحية والمجرم، مكتبة القانون والقضاء، بغداد، 2025، ص 142
٢٦. ينظر: تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC) ، مواجهة الجرائم السيبرانية: دليل الممارسات الفضلى للمشرعين، فيينا، 2024، ص 33.

ثانياً : المصادر الأجنبية

1. Al-Fahad, M. (2026). Comparative Cyber-Laws. Dubai: International Legal House, p. 55-90.
2. Miller, T. (2026). International Cyber-Security Frameworks. Chicago: University Press, p. 60
3. Thompson, (2025). The Future of Digital Policing. London: Global Security Press, p. 80
4. Williams, D. (2026). Social Media and Digital Crime. New York: Academic Press, p. 115-145