مجلة رسالة الحقوق ISSN-2032-2075

الجريمة الإلكترونية في التشريع الجنائي العراقي
Cybercrime in Iraqi Criminal Legislation

بحث مقدم من قبل
م . د. خالد ريسان دخيل
الجامعة الاسلامية / فرع الديوانية

الخلاصة :
يُعدّ موضوع الجريمة الإلكترونية من الموضوعات القانونية المستحدثة التي فرضت نفسها بقوة على الواقع التشريعي العراقي في ظل التطور التقني والمعلوماتي المتسارع. فقد أصبحت الجرائم الإلكترونية تمثّل تهديداً مباشراً لأمن الأفراد والمجتمع والدولة، لما تتسم به من طبيعة معقدة وحدود افتراضية تتجاوز الإقليم والسيادة القانونية.
ويهدف هذا البحث إلى تحليل مفهوم الجريمة الإلكترونية وخصائصها وتمييزها عن الجرائم التقليدية واستعراض صورها الشائعة في البيئة العراقية، مع التركيز على مدى استجابة التشريع الجنائي العراقي لمواجهتها، كما يتناول البحث بالتحليل النصوص ذات الصلة في قانون العقوبات العراقي رقم (111) لسنة 1969، ومشروع قانون جرائم المعلوماتية، مبيّناً أوجه القصور في التنظيم القانوني القائم والجهود التشريعية الحديثة الرامية إلى تطويره.
وانتهى البحث إلى أن المنظومة القانونية العراقية ما تزال بحاجة إلى تحديثٍ تشريعي يتلاءم مع طبيعة الجريمة الإلكترونية، من خلال تشريع خاص ومتكامل يضمن تحقيق التوازن بين حماية الحقوق والحريات وبين مواجهة التهديدات الإلكترونية المتنامية.
الكلمات المفتاحية: الجريمة الإلكترونية، القانون الجنائي العراقي، التشريع، المجال الإلكتروني، نظام المعلومات

Abstract
Cybercrime has emerged as one of the most complex and challenging legal issues facing Iraq's criminal justice system in the digital era. With rapid technological development and the increasing reliance on information networks, cybercrimes now pose serious threats to individuals, society, and national security, often transcending geographical and jurisdictional boundaries.
This study analyzes the concept and characteristics of cybercrime, distinguishing it from traditional crimes, and examines its most common forms in the Iraqi context. It also evaluates the current Iraqi criminal legislation, particularly Law No. 111 of 1969 (the Penal Code), alongside the draft Cybercrime Law, highlighting their deficiencies and the need for legislative modernization.
The research concludes that Iraq's current legal framework remains inadequate to effectively address the dynamic nature of cybercrime. Therefore, it calls for the enactment of a comprehensive and specialized cybercrime law that balances personal freedoms with the necessity of protecting national cyber security.
Keywords: Terrorist crime, Iraqi killer, cyberspace law, information system

المقدمة

أولاً_ فكرة البحث:

شهد العالم خلال العقود الأخيرة تتحوّلاً جذرياً في أنماط التواصل والتعاملات الإنسانية، نتيجة الثورة التكنولوجية والمعلوماتية الهائلة التي فرضت حضورها في مختلف جوانب الحياة اليومية ومع هذا التطور المتسارع، برزت تحديات جديدة أمام التشريعات الوطنية، من أبرزها ظاهرة الجريمة الإلكترونية التي تعدّ من أخطر صور الجريمة المعاصرة، لما تتّسم به من طبيعةٍ خفيّة وسرعةٍ في التنفيذ وصعوبة في الإثبات والتتبع، إذ لم تعدّ الجريمة محصورة في النطاق المادي أو الجغرافي التقليدي، بل أصبحت ترتكب عبر الفضاء الرقمي الذي تجاوز الحدود السياسية والقانونية للدول.

وفي العراق، كما في سائر المجتمعات، لم يكن هذا التطور بمنأى عن ظهور أنماطٍ جديدةٍ من السلوك الإجرامي الذي يستهدف الأفراد والمؤسسات على حدٍّ سواء، من خلال اختراق الأنظمة المعلوماتية، أو التلاعب بالبيانات، أو نشر المحتوى المخلّ بالآداب، أو حتى استغلال المنصات الإلكترونية في الابتزاز والاحتيال. وقد أثارت هذه الجرائم تساؤلاتٍ قانونية جوهرية تتعلق بمدى قدرة التشريع الجنائي العراقي القائم على مواكبة هذا الواقع المستجد، وما إذا كانت نصوصه التقليدية كافيةً لمواجهة الجرائم التي تتخذ من التكنولوجيا وسيلةً وأداةً لارتكابها، فدراسة الجريمة الإلكترونية في إطار التشريع الجنائي العراقي تمثّل ضرورةً علميةً وتشريعية في آنٍ واحد، إذ تسهم في كشف أوجه القصور في النصوص الحالية، وتساعد على بناء تصور قانوني متكامل يوازن بين حماية الحقوق الفردية وضمان الأمن الرقمي للمجتمع، كما تتيح هذه الدراسة الوقوف على الاتجاهات التشريعية المقارنة والاستفادة من التجارب الدولية في صياغة قانونٍ وطني متطورٍ لمكافحة الجرائم الإلكترونية بما ينسجم مع المعايير الحديثة في الإثبات والعقاب.

وانطلاقًا من ذلك، يسعى هذا البحث إلى تحليل الإطار القانوني للجريمة الإلكترونية في العراق وبيان مدى انسجامه مع التطورات التقنية والالتزامات الدولية، وصولاً إلى اقتراح حلولٍ عمليةٍ وتشريعيةٍ تعزّز من فعالية الحماية الجنائية في مواجهة التهديدات المعاصرة.

ثانياً_ إشكالية البحث:

يتناول التشريع العراقي لأنماطٍ متعددةٍ من السلوك الإجرامي، ولكن ظهور الفضاء الإلكتروني جعل منه عاجزاً عن استيعاب العديد من صور الجريمة المستحدثة التي فرضها هذا الفضاء الإلكتروني، ومن هنا تنبع الإشكالية الرئيسة للبحث، والمتمثّلة في مدى قدرة التشريع الجنائي العراقي القائم على الإحاطة بالجريمة الإلكترونية بفاعليةٍ وكفاءة في ظلّ التطورات التقنية المتسارعة وتنامي الأساليب الإجرامية المعتمدة على الوسائل الرقمية.

ثالثاً_ أهمية البحث:

تنبع أهمية البحث من واقعٍ معاصرٍ أصبحت فيه التكنولوجيا جزءاً لا يتجزأ من حياة الإنسان اليومية، الأمر الذي جعل الفضاء الإلكتروني ساحةً جديدةً لارتكاب الجرائم بأشكالها المتعددة وتتجلى أهمية دراسة الجريمة الإلكترونية في التشريع الجنائي العراقي من كونها تمسّ أمن الأفراد والمجتمع والدولة على حدٍّ سواء، إذ إن ضعف المواجهة القانونية لهذا النوع من الجرائم يؤدي إلى آثارٍ خطيرةٍ على المستويات الاقتصادية والاجتماعية والأمنية. كما تكمن أهمية البحث في سعيه إلى تحليل الإطار القانوني العراقي من زاوية نقدية تطبيقية للكشف عن مدى كفايته في التعامل مع الجرائم الإلكترونية الحديثة، التي غالباً ما تتجاوز حدود الزمان والمكان، وتحتاج إلى أدوات قانونية متخصصة في مجالات الإثبات والتحقيق والعقاب ومن خلال هذا التحليل، يسعى البحث إلى تقديم اقتراحاتٍ تساهم في تطوير المنظومة القانونية بما يتناسب مع طبيعة الجريمة الإلكترونية ومتطلبات العدالة الجنائية الحديثة. إنّ أهمية هذا البحث لا تقتصر على الجانب القانوني البحت، بل تمتدّ إلى البعد الاجتماعي والأمني، إذ تسهم نتائجه في دعم صانعي القرار والمشرّعين في صياغة تشريعاتٍ قادرةٍ على حماية الأمن الرقمي العراقي وضمان حقوق المواطنين في بيئةٍ إلكترونيةٍ آمنةٍ ومنضبطة.

رابعاً_ نطاق البحث:

ينحصر نطاق هذا البحث في دراسة الجريمة الإلكترونية ضمن إطار التشريع الجنائي العراقي، من حيث مفهومها القانوني وأركانها وصورها والعقوبات المقررة لها، وذلك من خلال تحليل النصوص النافذة وتفسيرها في ضوء القواعد العامة في قانون العقوبات. ويركّز البحث على الجرائم التي تُرتكب باستخدام الوسائل التقنية الحديثة أو عبر شبكة الإنترنت، أو التي تستهدف الأنظمة المعلوماتية والبيانات الرقمية، بوصفها محلاً للحماية الجنائية. ويقتصر البحث على بيان الأساس القانوني لتجريم الأفعال المرتبطة بالاعتداء على سرية المعلومات وسلامتها وتوافرها، وجرائم الدخول غير المشروع إلى الأنظمة، والاحتيال الإلكتروني والتزوير المعلوماتي، والابتزاز عبر الوسائط الرقمية، دون التوسع في الجرائم التقليدية التي قد تُرتكب بوسيلة إلكترونية ما لم يكن للوسيلة التقنية أثر جوهري في تكوين الركن المادي للجريمة وكما يركّز البحث على تحليل أركان الجريمة الإلكترونية (الركن الشرعي، والمادي، والمعنوي) وبيان إشكاليات التكييف القانوني، وموقف القضاء العراقي إن وجد، مع دراسة مدى كفاية النصوص الحالية لمواجهة التطور التقني المتسارع.

خامساً_ منهج البحث:

يعتمد هذا البحث على المنهج التحليلي بوصفه المنهج الرئيس، من خلال تحليل النصوص القانونية الواردة في التشريع الجنائي العراقي ذات الصلة بالجريمة الإلكترونية، وبيان مضمونها القانوني ومدى كفايتها في توفير الحماية الجنائية للأنظمة المعلوماتية والبيانات الرقمية، وذلك عبر تفسير هذه النصوص في ضوء القواعد العامة للقانون الجنائي ومبادئه

المستقرة.كما يستند البحث إلى المنهج الوصفي، من خلال عرض مفهوم الجريمة الإلكترونية وخصائصها وصورها المختلفة، وبيان طبيعتها القانونية وتمييزها عن الجرائم التقليدية بما يساعد على تكوين تصور واضح للإطار القانوني الذي تنظم من خلاله هذه الجرائم.ويستعين البحث أيضاً بالمنهج المقارن عند الضرورة، من خلال الإشارة إلى بعض التشريعات المقارنة والاتجاهات القانونية الحديثة، وذلك بهدف الاستفادة من التجارب التشريعية الأخرى في معالجة الجريمة الإلكترونية، وبيان أوجه القوة والقصور في التشريع العراقي.فضلاً عن ذلك، يعتمد البحث على المنهج الاستنباطي، من خلال استخلاص النتائج القانونية المتعلقة بمدى ملاءمة النصوص الجزائية القائمة لمواجهة الجرائم الإلكترونية، والوصول إلى مقترحات يمكن أن تسهم في تطوير الإطار التشريعي بما يتلاءم مع التطور التقني ومتطلبات الحماية الجنائية الحديثة.

سادساً_ الدراسات السابقة:

1. عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية، 2012.

تناولت هذه الدراسة الجريمة الإلكترونية من منظور قانوني مقارن، حيث ركزّت على تعريف الجريمة الإلكترونية، وبيان خصائصها وصورها المختلفة، مثل الاختراق الإلكتروني، والفيروسات والاحتيال المعلوماتي، فضلاً عن تحليل موقف التشريعات العربية والغربية من هذه الجرائم، وآليات مكافحتها والتعاون الدولي بشأنها، و كما بحثت الدراسة في طبيعة المجرم المعلوماتي، ودور القضاء في مواجهة الجرائم المرتكبة عبر الوسائل التقنية الحديثة، وقد أوضحت الدراسة أن الجريمة الإلكترونية أصبحت تمثّل نمطاً إجرامياً حديثاً يستوجب تطوير التشريعات الجنائية وتحديثها باستمرار لمواكبة التطور التكنولوجي المتسارع. خلصت الدراسة إلى أن النصوص الجنائية التقليدية لم تعد كافيةً وحدها لمواجهة الجريمة الإلكترونية، مما يفرض ضرورة وجود تشريعات خاصّةً تنظّم هذه الجرائم وتحدّد أركانها وعقوباتها بصورة واضحة.

2. محمد أمين الشوابكة، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية)، 2004.

بحثت هذه الدراسة ظاهرة جرائم الحاسوب والإنترنت باعتبارها نتيجةً طبيعية للتطور التكنولوجي، حيث تناولت مفهوم الجريمة المعلوماتية، وخصائصها، وصورها المختلفة إضافةً إلى بيان المخاطر الناتجة عن استخدام الإنترنت في ارتكاب الجرائم، و كما ركزّت الدراسة على تحليل الأبعاد القانونية لهذه الجرائم، وبيان الحاجة إلى توفير حمايةٍ قانونية للمعلومات والأنظمة الإلكترونية، وأوضحت الدراسة أن الإنترنت يمثّل إنجازاً حضارياً مهمّاً، لكنه في الوقت ذاته أوجد فرصاً جديدة لارتكاب الجرائم بوسائل حديثة ومتطورة، وتوصلت الدراسة إلى أن انتشار استخدام الإنترنت أدّى إلى ظهور أنماطٍ جديدة من الجرائم، الأمر الذي يتطلّب تطوير القواعد القانونية لتوفير حماية فعّالة للأنظمة المعلوماتية.

3. عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، عمّان، 2017.

تناولت هذه الدراسة جرائم تكنولوجيا المعلومات من خلال تحليل الأحكام القانونية المتعلّقة بها، وبيان أركانها وصورها المختلفة، مثل جرائم الدخول غير المشروع والاعتداء على البيانات، والتزوير الإلكتروني، وكما ركزّت الدراسة على بيان الطبيعة الخاصة لهذه الجرائم، ومدى اختلافها عن الجرائم التقليدية، وأثر ذلك على القواعد القانونية المتعلقة بالتجريم ، وخلصت الدراسة إلى أن الطبيعة التقنية للجريمة الإلكترونية تتطلب وجود تنظيم قانوني خاص يراعي خصوصيتها، ويضمن تحقيق الحماية الجنائية الفعّالة.

- **سابعاً_ خطة البحث:**

المقدمة

المبحث الأول: ماهية الجريمة الإلكترونية

المطلب الأول: مفهوم الجريمة الإلكترونية وخصائصها

الفرع الأول: التعريف الفقهي والتشريعي للجريمة الإلكترونية.

الفرع الثاني: الخصائص التي تميز الجريمة الإلكترونية عن الجرائم التقليدية.

المطلب الثاني: أنواع الجرائم الإلكترونية

الفرع الأول: الجرائم الموجهة ضد الأفراد والممتلكات

الفرع الثاني: الجرائم الموجهة ضد الدولة والنظام العام

المبحث الثاني: الجريمة الإلكترونية في التشريع الجنائي العراقي

المطلب الأول: الجريمة الإلكترونية في التشريع العراقي

الفرع الأول: قانون العقوبات العراقي رقم (111) لسنة 1969.

الفرع الثاني: مشروع قانون الجرائم المعلوماتية والجهود التشريعية الحديثة في العراق.

المطلب الثاني: تحديات مكافحة الجريمة الإلكترونية

الفرع الأول: صعوبة الإثبات والتحقيق في الجرائم الإلكترونية.

الفرع الثاني: سبل تطوير المنظومة القانونية العراقية في ضوء التجارب المقارنة.

الخاتمة

المبحث الأول/ الإطار العام للجريمة الإلكترونية

مع التوسّع السريع في استخدام التكنولوجيا والإنترنت، ظهرت الجريمة الإلكترونية التي تتّسم بالسرعة والخفاء وصعوبة التتبع، ولم تبقى الجرائم محصورةً في الفضاء الواقعي، بل أصبح الفضاء الرقمي ميداناً لممارسة أنماطٍ إجراميةٍ جديدةٍ تهدّد الأفراد والدولة على حدٍّ سواء، ومن خلال هذا المبحث سوف نتحدث عن مفهوم الجريمة الإلكترونية وخصائصها في المطلب الأول، وفي المطلب الثاني سوف نتحدث عن أنواعها.

المطلب الأول / مفهوم الجريمة الإلكترونية وخصائصها

تعدّ الجريمة الإلكترونية من الظواهر الجنائية الحديثة التي برزت مع التطور التكنولوجي وانتشار استخدام الإنترنت والأنظمة الرقمية في مختلف مجالات الحياة، فهذه الجرائم تختلف عن الجرائم التقليدية في طبيعتها ووسائل ارتكابها، مما استدعى دراسة دقيقة لمفهومها وحدودها القانونية وخصائصها المميزة [1] ، ويهدف هذا المطلب إلى تحديد مفهوم الجريمة الإلكترونية من منظور فقهي وتشريعي في الفرع الأول، وكذلك بيان الخصائص التي تميزها عن الجرائم التقليدية في الفرع الثاني.

الفرع الأول / التعريف الفقهي والتشريعي للجريمة الإلكترونية

تُعدّ الجريمة الإلكترونية نتيجةً لثورة المعلومات والاتصالات، ما جعلها محطّ اهتمام الفقهاء والمشرّعين على حدٍّ سواء، وقد اختلفت التعريفات الفقهية والتشريعية لهذه الجريمة نظراً لاختلاف الزوايا التي يتمّ من خلالها النظر إليها.

أولاً_ التعريف الفقهي للجريمة الإلكترونية

تعرّف الجريمة الإلكترونية بأنّها:" أيّ فعلٍ غير مشروعٍ يتمّ باستخدام الحاسوب أو الشبكات الإلكترونية، ويهدف إلى إلحاق الضرر بالأفراد أو المؤسسات أو الدولة [2]،

ويُلاحظ بأن هذا التعريف يركز على الوسيلة المستخدمة في ارتكاب الجريمة، وهي الأجهزة الإلكترونية والشبكات.

ثانياً_ التعريف التشريعي للجريمة الإلكترونية

أمّا على الصعيد التشريعي، فقد اختلفت الدول في تعريف الجريمة الإلكترونية، ففي العراق وعلى سبيل المثال، لا يوجد حتى الآن قانونٌ محددٌ يُعرّف الجريمة الإلكترونية بشكلٍ دقيق. لكن، في مسودة قانون الجرائم المعلوماتية، وُصِف "المحرر الإلكتروني" بأنه: "رسالة تتضمن معلومات تنشأ أو تُدمج أو تُخزن أو تُرسل كليًا أو جزئيًا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأي وسيلةٍ أخرى مشابهة [3]،هذا التعريف يُظهر محاولة المشرّع العراقي لمواكبة التطورات التكنولوجية، إلّا أن غياب قانون شامل يُعرّف الجريمة الإلكترونية ويُحدّد أركانها يُعدّ من أبرز التحديات القانونية في العراق. وبرأينا الشخصي فإنّ تعدّد التعريفات الفقهية والتشريعية للجريمة الإلكترونية يُبرز الحاجة الملحة إلى وضع تعريفٍ قانوني موحد ودقيق لهذه الجريمة، يتناسب مع التطورات التكنولوجية ويُسهم في تعزيز فعالية التشريعات في مكافحة الجرائم الإلكترونية.

الفرع الثاني / الخصائص التي تميز الجريمة الإلكترونية عن الجرائم التقليدية

تختلف الجريمة الإلكترونية عن الجرائم التقليدية بعدّة خصائص جوهرية تجعلها أكثر تعقيداً وصعوبةً في المكافحة، وهو ما دفع الفقهاء والمشرعين إلى إعادة النظر في المفاهيم التقليدية للجريمة والعقوبة. يمكن حصر أبرز هذه الخصائص فيما يلي:

أولاً_ طبيعة الجريمة الإلكترونية وغياب الحدود المكانية:

تتميز الجريمة الإلكترونية بأنّها لا ترتبط بمكانٍ ماديٍّ محدّد، بل يمكن ارتكابها عبر شبكة الإنترنت من أيّ مكانٍ في العالم، مما يجعل من الصعب تحديد موقع الجاني أو الضحية بدقة. كما أن الجريمة الإلكترونية غالباً ما تكون خفية، فلا يلاحظها الضحية إلّا بعد وقوع الضرر، بعكس الجرائم التقليدية التي يمكن كشفها سريعاً [4].

ثانياً_سرعة الانتشار وتأثير الأضرار:

يمكن للجريمة الإلكترونية أن تنتشر بسرعةٍ هائلة، خاصّةً عبر وسائل التواصل الاجتماعي والبريد الإلكتروني والبرمجيات الخبيثة، مما يؤدي إلى أضرارٍ واسعة النطاق خلال وقتٍ قصير، وهذا يختلف عن الجرائم التقليدية التي عادة ما تكون محدودة التأثير الزماني والمكاني [5].

ثالثاً_تعقيد الأدلة وصعوبة الإثبات:

تحتاج الجرائم الإلكترونية إلى أدواتٍ وتقنيات خاصة للتحقق من الأدلة الرقمية، مثل سجلات الخوادم وتحليل البيانات المشفرة، بينما تكون الأدلة في الجرائم التقليدية أكثر وضوحاً وقابليةٍ للعرض أمام المحاكم [6].

رابعاً_ استغلال الوسائل التكنولوجية كأداة ووسيلة:

في الجرائم الإلكترونية، تُستخدم التكنولوجيا ليس فقط كوسيلةٍ لارتكاب الجريمة، بل كعنصرٍ جوهري فيها مثل القرصنة، الاحتيال الرقمي، الابتزاز الإلكتروني، وهجمات الفدية. بينما الجرائم التقليدية غالباً ما تعتمد على الوسائل المادية التقليدية[7]، ونتيجةً لما تقدم، فإنّ هذه الخصائص تجعل الجريمة الإلكترونية أكثر خطورةً على المجتمع، لأنها تمتاز بالانتشار السريع والقدرة على التلاعب بالبيانات والمعلومات، كما أنها تتطلب من النظام القضائي العراقي تطوير أدوات التحقيق والتشريع لتواكب هذا الواقع الرقمي المتغير، كما أن غياب نصوصٍ واضحة وكاملة يزيد من الفجوة القانونية ويضعف قدرة القانون على حماية الأفراد والدولة [8].

المطلب الثاني / أنواع الجرائم الإلكترونية

تتميز الجريمة الإلكترونية بتنوع أشكالها وطرق ارتكابها، إذ لم تعد محصورةً في نمط واحد من الجرائم، بل شملت الأفراد والمؤسسات والدولة على حدّ سواء، فالتكنولوجيا الحديثة أتاحت للمجرمين وسائل سريعةٍ ومرنةٍ للنفاذ إلى المعلومات واختراق الخصوصيات، سواء لتحقيق مكاسب مالية أو لتحقيق أهدافٍ سياسية أو تخريبية، ويهدف هذا المطلب إلى استعراض أنواع الجرائم الإلكترونية وفقًا للأطراف المستهدفة، من حيث الجرائم الموجهة ضد الأفراد والممتلكات، والجرائم الموجهة ضد الدولة والنظام العام.

الفرع الأول / الجرائم الموجهة ضد الأفراد والممتلكات

تُعتبر الجرائم الإلكترونية الموجهة ضدّ الأفراد والممتلكات من أكثر أنواع الجرائم شيوعاً في العصر الرقمي، نظراً لاعتماد الأفراد بشكلٍ متزايدٍ على التكنولوجيا في حياتهم اليومية، و تشمل هذه الجرائم مجموعةً واسعة من الأفعال غير المشروعة التي تستهدف الأفراد مباشرة، سواء كان ذلك من خلال التسبب في ضررٍ مادي أو معنوي، وتمتاز هذه الجرائم بتنوع أساليبها ووسائل تنفيذها، إذ قد تتخذ شكل الابتزاز الإلكتروني أو الاحتيال المالي أو التشهير عبر الشبكات الاجتماعية، وكما تؤدي هذه الأفعال إلى زعزعة الثقة في التعاملات الرقمية، وتُلحق أضراراً نفسيةٍ واقتصادية جسيمة بالمجني عليهم، ويُعدّ التصدي لهذه الجرائم من التحديات الكبرى التي تواجه المشرّع العراقي، نظراً لصعوبة تتبع الجناة وغياب إطارٍ قانوني متكامل يواكب التطور التقني المستمر [9].

أولاً_ الابتزاز الإلكتروني:

يُعرّف الابتزاز الإلكتروني بأنه: "استخدام الوسائل الإلكترونية لتهديد الأفراد بنشر معلوماتٍ خاصةٍ أو صورٍ محرجة ما لم يتمّ دفع مبلغٍ مالي أو تلبية مطالب أخرى، و هذا النوع من الجرائم من أخطر الجرائم الإلكترونية، حيثُ يُلجأ فيه إلى استغلال المعلومات الشخصية للضحية لتحقيق مكاسب غير مشروعة [10].

ثانياً_ الاحتيال الإلكتروني:

يشمل الاحتيال الإلكتروني مجموعةً من الأفعال التي تهدف إلى خداع الأفراد للحصول على أموالهم أو معلوماتهم الشخصية بطرقٍ غير قانونية، و من أبرز أشكال الاحتيال الإلكتروني[11]:

1. التصيد الاحتيالي (Phishing): إرسال رسائل إلكترونية تبدو وكأنها من جهاتٍ موثوقة، بهدف خداع الضحية للكشف عن معلوماتٍ حساسة.
2. الاحتيال عبر الإنترنت (Online Fraud): إنشاء مواقع إلكترونية وهميةٍ لبيع منتجاتٍ أو خدماتٍ غير موجودة.

ثالثا_ التشهير الإلكتروني:

يُقصد بالتشهير الإلكتروني: "نشر معلوماتٍ كاذبة أو مضلّلة عن شخصٍ ما عبر الإنترنت بهدف الإضرار بسمعته، و يتمّ ذلك من خلال وسائل التواصل الاجتماعي، المنتديات، أو المدونات ويُعدّ من الجرائم التي تُسبّب أضراراً نفسيةٍ واجتماعية كبيرة للضحية [12].

رابعاً_ سرقة الهوية الإلكترونية:

تتمثّل سرقة الهوية الإلكترونية في استخدام معلوماتٍ شخصيةٍ لشخصٍ آخر دون إذنه، بهدف ارتكاب أعمال غير قانونية.يشمل ذلك استخدام الأسماء، أرقام الهواتف، أو بيانات الحسابات البنكيّة للآخرين [13].

إن تزايد هذه الجرائم يُظهر الحاجة الملّحة لتطوير التشريعات والقوانين لمواكبة التطورات التكنولوجية، وبالتالي يتوجّب وضع قوانينٍ واضحةٍ تُحدّد أركان هذه الجرائم والعقوبات المناسبة لها. كما يجب على الأفراد توخي الحذر عند التعامل مع المعلومات الشخصية على الإنترنت، والابتعاد عن المواقع والروابط المشبوهة [14].

الفرع الثاني / الجرائم الموجهة ضدّ الدولة والنظام العام

تعتبر الجرائم الإلكترونية ضدّ الدول من أخطر أنواع الجرائم في البيئة الرقمية، لما لها من تأثيرٍ مباشرٍ على الأمن الوطني واستقرار المؤسسات العامة، فهي لا تستهدف الأفراد فحسب، بل تسعى إلى النيل من سيادة الدولة وشلّ قدراتها الأمنية أو الاقتصادية أو السياسية من خلال الوسائل التقنية الحديثة، وهذا ما سنتحدث عنه من خلال هذا الفرع وفق التالي:

أولاً_ اختراق الأنظمة المعلوماتية الحكومية:

يُقصد باختراق الأنظمة المعلوماتية تلك الأفعال التي يتمّ من خلالها التسلل غير المشروع إلى قواعد البيانات أو شبكات الحواسيب الخاصة بالجهات الرسمية أو الأمنية أو الاقتصادية، وغالباً ما تهدف هذه الأفعال إلى تعطيل الخدمات، أو سرقة البيانات الحساسة، أو العبث بالمعلومات لغرض الإضرار بالمصلحة العامة، والعراق، شأنه شأن بقية الدول، شهد اختراقاتٍ لمواقع مؤسسات رسمية، ما دعا الجهات الحكومية إلى إنشاء وحداتٍ متخصصة للأمن السيبراني ضمن وزارة الداخلية وجهاز الأمن الوطني [15].

ثانياً_ التجسس الإلكتروني:

التجسس الإلكتروني هو جمع المعلومات السرّية أو الحساسة عن أنظمة الدولة أو مؤسساتها الحيوية بوسائل تقنيةٍ دون إذنٍ قانوني، وغالباً ما يكون بدافعٍ سياسي أو عسكري أو اقتصادي وتزداد خطورة هذا النوع من الجرائم عندما يكون مدعوماً من جهاتٍ خارجيةٍ تسعى إلى تقويض الأمن الداخلي للدولة [16] . يُصنّف هذا النوع من الجرائم ضمن الجرائم الماسّة بأمن الدولة الخارجي لأنه يستهدف المعلومات ذات الطابع السيادي، كبيانات الأمن والدفاع، أو خطط البنية التحتية ويواجه

العراق تحديات في هذا المجال نظراً لاعتماده المتزايد على الأنظمة الرقمية في إدارة المرافق الحيوية دون وجود إطارٍ قانوني صارم يحدّد العقوبات الخاصة بالتجسس المعلوماتي [17].

ثالثاً_ الإرهاب السيبراني:

يُعتبر الإرهاب السيبراني من أخطر التحدّيات التي تواجه الدول في العصر الحديث، حيث يُستخدم الفضاء الإلكتروني كوسيلةٍلنشر الفكر المتطرف، أو لتنسيق الهجمات الإرهابية، أو لتعطيل البنى التحتية الحيوية كشبكات الكهرباء والاتصالات والمطارات، وقد أشارت العديد من التقارير الدولية إلى أنّ الجماعات الإرهابية باتت تعتمد على الإنترنت كوسيلةٍ للتجنيد وجمع التمويل ونشر الدعاية وهو ما يتطلّب من التشريعات الوطنية – ومنها التشريع العراقي – أن يضع نصوصاً واضحة تُجرّم هذا النمط من الجرائم، وتحدّد أركانها وعقوباتها بدقة [18]. ونحن نرى أنّ الجرائم الإلكترونية الموجهة ضدّ الدولة تمثّل تهديداً استراتيجياً للأمن القومي، لأنّها تُضعف الثقة في المؤسسات العامة وتفتح الباب أمام التدخلات الخارجية، ومن وجهة نظرنا، فإنّ معالجة هذه الظاهرة لا يمكن أن تكون تشريعيةً فقط، بل يجب أن تكون مؤسساتية وتقنية وتوعوية في الوقت نفسه، فالدولة بحاجةٍ إلى بناء منظومةٍ وطنية متكاملة للأمن السيبراني تشمل تطوير الكوادر الفنية وتحديث التشريعات، وتعزيز التعاون الدولي في مواجهة الجرائم العابرة للحدود الرقمية وكما ينبغي تفعيل الدور القضائي المتخصص في هذا المجال لضمان تطبيق القانون بعدالةٍ وفعاليةٍ.

المبحث الثاني/ الجريمة الإلكترونية في التشريع الجنائي العراقي

مع التطور الهائل في تكنولوجيا المعلومات والاتصالات، أصبح من الضروري أن تتواكب المنظومة القانونية مع هذا التحول الرقمي الكبير الذي أفرز أنماطاً جديدة من السلوك الإجرامي لم تكن معروفة من قبل، فقد تجاوزت الجرائم الإلكترونية الحدود الجغرافية التقليدية، وأصبحت تهدّد الأفراد والدولة على حد سواء، ممّا فرض على المشرّع العراقي تحدّياً مزدوجاً يتمثّل في حماية المجتمع من مخاطر هذه الجرائم، وضمان عدم المساس بالحقوق والحريات الرقمية للأفراد، وانطلاقاً من هذه التحدّيات يتناول هذا المبحث دراسة التنظيم القانوني للجريمة الإلكترونية في التشريع الجنائي العراقي، و ذلك من خلال بيان الإطار التشريعي المعتمد، وتحليل أوجه القصور و التحديات التي تعترض تطبيقه، مع محاولة استجلاء مدى توافقه مع المعايير الدولية الحديثة في مكافحة الجريمة الإلكترونية [19].

المطلب الأول / معالجة التشريع العراقي للجريمة الإلكترونية

أمام التطور المتسارع في تكنولوجيا المعلومات وانتشار استخدام الوسائط الرقمية في مختلف مجالات الحياة، وجد المشرّع العراقي نفسه أمام واقعٍ قانوني جديد فرض الحاجة إلى إعادة النظر في النصوص الجنائية التقليدية، فالقواعد القانونية التي صيغت لتنظيم الجرائم المادية لم تعد كافيةً للتعامل مع الجرائم ذات الطابع الإلكتروني، والتي تتسم بالتعقيد والتداخل العابر للحدود[20]، ولذلك حاول المشرّع العراقي خلال السنوات الأخيرة معالجة الجريمة الإلكترونية ضمن منظومة القانون الجنائي من خلال سنّ قوانين خاصةٍ ومشروعات تشريعية تهدف إلى مواكبة التطور الرقمي وحماية الأمن السيبراني، وقد تجلّى هذا الاهتمام في مشروع قانون الجرائم المعلوماتية الذي أعدّته الحكومة العراقية وناقشه مجلس النواب في أكثر من دورة تشريعية، ورغم هذه الجهود ما يزال الإطار القانوني العراقي يعاني من ثغراتٍ تنظيمية وتشريعيةٍ تحول دون الإحاطة الكاملة بظاهرة الجريمة الإلكترونية سواء من حيث تحديد المفاهيم أو من حيث الإجراءات القضائية الخاصّة بجمع الأدلّة الإلكترونية وإثباتها [21]، ومن هنا يهدف هذا المطلب إلى تحليل موقف التشريع العراقي من الجريمة الإلكترونية وبيان مدى فعاليته في التجريم والعقاب، مع مناقشة أوجه القصور التي تتطلب إصلاحاً تشريعياً يتناسب مع طبيعة هذه الجرائم المعاصرة، وذلك من خلال الفرعين التاليين:

الفرع الأول / النصوص ذات الصلة في قانون العقوبات العراقي رقم (111) لسنة 1969.

يشكّل قانون العقوبات العراقي رقم (111) لسنة 1969 الإطار التشريعي الأساسي لمعاقبة المجرمين والسلوك الإجرامي في العراق، ومع ظهور الجرائم الإلكترونية أصبح من الضروري دراسة مدى قدرة هذا القانون على مجابهة هذه الظاهرة الحديثة، نظراً لأنّ نصوصه صيغت قبل الثورة الإلكترونية ولم تأخذ في الاعتبار خصائص الجرائم القائمة على الوسائل المعلوماتية ممّا يجعله يواجه تحدياتٍ كبيرة تتعلّق بإثبات الوقائع الرقمية، وتحديد نطاق المسؤولية، وضمان حقوق الأطراف إضافةًإلى الإشكاليات المتعلقة بالولاية القضائية العابرة للحدود [22].

أولاً_ أحكام النشر والقذف والتشهير:

تطبّق هذه الأحكام عندما يُستخدم الفضاء الإلكتروني لنشر محتوى مجرّم، سواء كان تشهيراً أو نشر مواد فاضحة أو مضلّلة، إلّا أن التطبيق العملي لهذه النصوص يتطلّب إثبات المنشور والمصدر الرقمي، وهو ما قد يشكّل تحدياً أمام المحاكم، خصوصاً عند استضافة المحتوى على خوادم خارج العراق [23].

ثانياً_ أحكام الإضرار بالممتلكات ووسائل الاتصال:

يتضمن القانون مواداً لمعاقبة التخريب أو الإتلاف لوسائل الاتصال العامة، والتي يمكن توسيع نطاقها لتشمل أعمال تعطيل الخدمات الرقمية أو استهداف البنى التحتية الإلكترونية، و هذا يسمح بملاحقة الأشخاص الذين يعرّضون الشبكات الوطنية للخطر أو يقومون بأعمال تشبه التخريب الرقمي [24].

ثالثاً_ أحكام الجرائم الاقتصادية والتزوير:

تشمل هذه الأحكام [25]:

1. الجرائم الاقتصادية: مثل الاحتيال والاختلاس وخيانة الأمانة، والتي يمكن تطبيقها على جرائم الاحتيال الإلكتروني (التصيد الاحتيالي، الاحتيال عبر الدفع الإلكتروني).
٢. الوثائق والتزوير: إنّ النصوص المتعلقة بتزوير المستندات الرسمية يمكن تفسيرها لتشمل المحررات الرقمية، إلّا أن غياب تعريفٍ صريح للمحرر الإلكتروني يحدّ من فعالية التطبيق.

رابعاً_ أحكام الأمانة والسرية وإساءة استخدام الواجب:

ترّكز هذه النصوص على حماية المعلومات السرية ومنع استغلال الوظائف العامة للوصول غير المشروع إلى قواعد البيانات أو تسريب معلوماتٍ حسّاسة، وهو أمرٌ ضروري في ظلّ الاعتماد المتزايد على الأنظمة الرقمية في المؤسسات الحكومية، و يمكن تطبيق هذه المواد على أيّ موظفٍ عام يستغل صلاحياته للوصول إلى معلومات رقمية بطريقة غير قانونية [26]. يمكننا القول إنّ قانون العقوبات العراقي يوفّر قاعدةً جنائية عامّة يمكن من خلالها ملاحقة العديد من صور الجرائم الإلكترونية، لكنّه يظلّ قاصراً عن معالجة خصوصية هذه الجرائم من حيث التعريف والعقوبة المناسبة وإجراءات التحقيق والإثبات الرقمي[27]، فمن وجهة نظرنا فإنّ معالجة الجريمة الإلكترونية تحتاج إلى مسارين متكاملين يتمثّل الأول في سنّ تشريعٍ خاص وواضح للجرائم الإلكترونية يعرّف المصطلحات ويحدّد الأركان والعقوبات وإجراءات التحقيق والإثبات الرقمية، والثاني تطوير قدراتٍ فنيّة وقضائية لضمان التطبيق العملي للنصوص وضمان فعالية إنفاذ القانون.

الفرع الثاني / مشروع قانون جرائم المعلوماتية والجهود التشريعية الحديثة في العراق

مع تصاعد ظاهرة الجرائم الإلكترونية وتعقّد أساليب ارتكابها، أدرك المشرّع العراقي أن النصوص التقليدية في قانون العقوبات رقم (111) لسنة 1969 المعدّل لم تعد كافيةً لمعالجة التحديات الرقمية الحديثة، ولذلك تمّ وضع مشروع قانون الجرائم المعلوماتية كخطوةٍ تشريعيةٍ رئيسية لمواجهة هذه الظاهرة، ومن خلال هذا الفرع سوف نتحدث عن أهدافه ومحاوره، ومن ثمّ تقييمه.

أولاً_ أهداف مشروع القانون:

يهدف هذا المشروع إلى العديد من الأهداف نذكر منها ما يلي:

1. تجريم الجرائم الإلكترونية بشكل واضح: يهدف المشروع إلى تحديد صور الجرائم الرقمية مثل الاختراق والتجسس والابتزاز الإلكتروني والتشهير الرقمي والاحتيال المالي عبر الإنترنت[28].
2. تحديد أركان الجريمة والعقوبات المناسبة، وحيث يوفّر المشروع نصوصاً دقيقة تحدّد أركان الجريمة الإلكترونية (الفعل، النية، الوسيلة)، مع مراعاة خصوصية الأدلّة الرقمية وطرق إثباتها[29].
3. تطوير الإجراءات القضائية للتحقيق في الجرائم الإلكترونية، حيث يتضمّن المشروع آلياتٍ محدّدة لجمع الأدلّة الإلكترونية وحفظها وتحليلها بما يضمن عدم فقدان أيّ بياناتٍ مهمة ويحقق العدالة مع احترام حقوق المتهم [30].

ثانياً_ أبرز محاور المشروع التشريعي

1. تعريف الجريمة الإلكترونية والمحرر الإلكتروني: يُقدّم المشروع تعريفاً رسميّاً للمحرر الإلكتروني والمعلومات الرقمية، مما يسهل تصنيف الأفعال المجرمة وتطبيق العقوبات [31].
2. تصنيف الجرائم حسب المستهدف [32] :
   - الجرائم ضد الأفراد: مثل الابتزاز، الاحتيال، التشهير الإلكتروني.
   - الجرائم ضد الدولة والنظام العام: مثل اختراق الأنظمة الحكومية، التجسس، الإرهاب السيبراني.
3. العقوبات المقررة: يتضمن المشروع عقوباتٍ مالية وجنائية تتناسب مع حجم الضرر الناتج عن الجريمة، مع تشديد العقوبات للجرائم التي تمسّ الأمن الوطني أو الممتلكات العامة[33].
4. التعاون الدولي ومكافحة الجرائم العابرة للحدود: يراعي المشروع ضرورة التعاون مع الجهات القضائية والأمنية الدولية لمكافحة الجرائم الإلكترونية العابرة للحدود، بما يتوافق مع الاتفاقيات الدولية في مجال الأمن السيبراني [34].

ثالثاً_ تقييم النصوص التشريعية وموقف المشروع من الجريمة الإلكترونية:

يمكن القول إنّ التشريع العراقي قد بدأ خطواتٍ مهمّة لمعالجة الجريمة الإلكترونية، لكنّه ما يزال في مرحلة التكيف مع العصر الرقمي، فقانون العقوبات رقم (111) لسنة 1969 المعدّل يوفّر قاعدةً عامة يمكن استغلالها لملاحقة بعض الجرائم الإلكترونية، مثل الاحتيال و التشهير والتزوير لكنّه يواجه تحدياتٍ أساسية نتيجة عدم وجود تعريفات واضحة للجرائم الإلكترونية وغياب نصوصٍ خاصة بالإثبات الرقمي والوسائل الحديثة [35]. و بالمقابل فإنّ مشروع قانون الجرائم الإلكترونية يمثّل تطوراً إيجابياً، فهو يقدّم تعريفاتٍ دقيقة للمفاهيم الرقمية، ويصنّف الجرائم حسب المستهدف، ويضع عقوباتٍ مناسبة ويستجيب لمتطلبات الإثبات الإلكتروني، كما يأخذ بعين الاعتبار التعاون الدولي لمواجهة الجرائم العابرة للحدود[36].ومن خلال ما سبق يمكننا تقييم التشريعين السابقين:

1. التشريع التقليدي محدود في تغطية الجرائم الحديثة، ويفتقد المرونة المطلوبة للتعامل مع الابتكارات التقنية المستمرة[37].
2. المشروع التشريعي الجديد يشكّل قاعدةً صلبة لكنه يحتاج إلى إجراءاتٍ تنفيذية ومؤسساتية مثل وحدات تحقيق متخصصة وخبراء في الأدلة الإلكترونية، لضمان فعالية التطبيق، ويتطلّب استمرار التطور الإلكتروني مراجعةً دورية للنصوص القانونية وتحديثها بما يتماشى مع التقنيات الحديثة لضمان حماية المجتمع والدولة دون المساس بحقوق الأفراد[38]. وفي النهاية فإنّ الموقف التشريعي العراقي يتحسن تدريجياً، لكنّه يحتاج إلى تكامل بين النصوص القانونية و

القدرات المؤسسية والوعي المجتمعي لمواجهة التحديات الرقمية بشكلٍ فعّال فالتشريع وحده لا يكفي، بل يجب دعمه بإجراءاتٍ عملية متطورة لضمان تطبيقه بفعاليةٍ وتحقيق الردع والعدالة[39]. من وجهة نظرنا الشخصية، وبالرغم أهمية المشروع، فإنّه يحتاج إلى إجراءات تنفيذية متكاملة تشمل تدريب القضاة والمحققين، وإنشاء وحداتٍ فنيّة متخصصة داخل أجهزة الأمن، وتوعية المواطنين بخطورة الجرائم الإلكترونية وطرق الحماية منها، وكما أن استمرار التطور التقني يفرض على المشرّع مراجعةً دورية للمشروع لتحديث تعريفات الجرائم والعقوبات بما يتناسب مع المستجدات.

المطلب الثاني/ التحديات والاتجاهات المستقبلية لمكافحة الجريمة الإلكترونية

على الرغم من الجهود التشريعية الحديثة في العراق لمواجهة الجريمة الإلكترونية، إلّا أن هذه الظاهرة تظلّ تواجه تحدّياتٍ معقدة تتعلق بسرعة التطور التكنولوجي، وعبور الجرائم الإلكترونية للحدود وصعوبة جمع الأدلّة الإلكترونية وتحليلها بشكلٍ موثوق، وكما أن التداخل بين الحقوق الإلكترونية للأفراد ومتطلبات الأمن الوطني يزيد من تعقيد الإطار القانوني والتنفيذي لمكافحة هذه الجرائم [40]. من هنا، يهدف هذا المطلب إلى دراسة التحديات الراهنة التي تواجه مكافحة الجريمة الإلكترونية في العراق، مع تحليل الاتجاهات المستقبلية المحتملة لتعزيز الفاعلية القانونية والتقنية، بما يضمن حماية الأفراد والدولة على حدٍّ سواء، ويحقق التوازن بين الأمن وحقوق الإنسان في البيئة الإلكترونية الحديثة.

الفرع الأول / الصعوبات العملية في الإثبات والتحقيق في الجرائم الإلكترونية.

تُعدّ الجرائم الإلكترونية من التحدّيات المعقّدة التي تواجه النظام القضائي في العراق، خاصّةً في مجالات الإثبات والتحقيق، وتتجلى هذه الصعوبات في عدّة جوانب، نذكر منها:

أولاً_ غياب التشريع المتخصص:

رغم أنّ قانون العقوبات العراقي رقم (111) لسنة 1969 يتضمّن نصوصاً قد تُطبّق على بعض الجرائم الإلكترونية، إلّا أن غياب قانونٍ خاص بالجرائم الإلكترونية يجعل من الصعب تحديد الأفعال المجرّمة بوضوح، مما يؤدي إلى صعوبةٍ في التحقيق والإثبات [41].

ثانياً_ تحديات جمع الأدلة الرقمية:

يتطلّب جمع الأدلة الإلكترونية تقنياتٍ متخصصة وخبراتٍ فنيّة عالية، و في العراق لا توجد وحدات تحقيقٍ متخصصة في الجرائم الإلكترونية، مما يؤدي إلى صعوبة في جمع الأدلة وحفظها بشكلٍ قانوني، ممّا يؤثر على مصداقيتها في المحاكم[42].

ثالثاً_ صعوبة التتبع والتحقيق عبر الحدود:

تُرتكب العديد من الجرائم الإلكترونية عبر الإنترنت، مما يجعل من الصعب تحديد مكان ارتكاب الجريمة أو هوية الجاني. هذا التحدي يتطلب تعاونًا دوليًا وتنسيقًا بين الجهات المعنية لملاحقة الجناة[43].

رابعاً_ نقص الوعي والتدريب:

قلّةالوعي بين أفرادالشرطة والقضاء حول كيفية التعامل مع الجرائم الإلكترونية تؤدي إلى ضعفٍ في التحقيق والإثبات [44].

خامساً_ تعقيد الأدلة الرقمية والتحديات القانونية والأخلاقية:

تتميز الأدلّة الإلكترونية بتقلبّها وسهولة تعديلها أو مسحها، مما يجعل من الصعب الحفاظ على مصداقيتها، وكما يتطلّب التحقيق في الجرائم الإلكترونية التوازن بين حماية حقوق الأفراد وضمان الأمن العام، فمن الناحية العملية يمثّل نقص الخبرات الفنية والمعدات الحديثة أحد أبرز التحديات فالأدلّة الإلكترونية تحتاج إلى أدواتٍ متقدمة وتقنيات تحليلية دقيقة لضمان سلامة الإثبات وسلسلة الحيازة القانونية، كما أن عبور الجرائم الإلكترونية للحدود يجعل التعاون الدولي عنصراً أساسياً وفي الوقت الحالي توجد عراقيل إجرائية وتنظيمية تحدّ من سرعة وفعالية هذا التعاون [45] . ونرى، بأنّ معالجة هذه الصعوبات تتطلّب استراتيجية متعددة المستويات أولها تطوير تشريعٍ خاصٍّ بالجرائم الإلكترونية يشمل تعريفاتٍ دقيقة للجرائم أركانها والعقوبات المناسبة، مع التركيز على حماية الحقوق الرقمية للأفراد، وثانيها تأسيس وحداتٍ قضائية وتقنية متخصّصة تحقّق ما يتطلّبه التحقيق الفعّال في الجرائم الإلكترونية وجود وحدات مجهزة بخبراء تقنيين قادرين على جمع الأدلة الإلكترونية وتحليلها بطريقةٍ قانونية صحيحة، وثالثها التعاون الدولي والتنسيق مع المنظمات العالمية وذلك لضمان القدرة على تتبع الجناة عبر الحدود وتبادل الأدلة والخبرات القانونية والفنية. وأخيراً التدريب والتوعية للقضاة والشرطة والمواطنين، لتعزيز فهم خصائص الجرائم الإلكترونية وطرق الوقاية منها، وهذه الخطوات ليست اختيارية بل هي ضرورةٌ استراتيجية لحماية الدولة والمجتمع من المخاطر الإلكترونية المتزايدة، ولضمان أن يكون القضاء العراقي قادراً على مواجهة الجرائم الإلكترونية بكفاءةٍ وعدالة.

الفرع الثاني/ سبل تطوير المنظومة القانونية العراقية في ضوء التجارب المقارنة.

تُواجه المنظومة القانونية العراقية تحديات كبيرة في مجال مكافحة الجرائم الإلكترونية، نظراً للتطور السريع للتكنولوجيا وظهور أساليب إجرامية معقدة تتجاوز الحدود التقليدية، لذلك تُعدّ الاستفادة من التجارب القانونية المقارنة أمراً ضرورياً لتطوير التشريعات العراقية بما يتناسب مع المستجدات العالمية والمحلية [46].

أولاً_ تطوير التشريعات الخاصة بالجرائم الإلكترونية:

تفتقر التشريعات العراقية إلى قانون شامل ومُحدّد لمكافحة الجرائم الإلكترونية. على الرغم من أن قانون العقوبات رقم (111) لسنة 1969 المعدّل يتضمّن بعض النصوص التي يمكن تطبيقها على الجرائم الإلكترونية، إلّا أن غياب قانون

خاص يُعرّف الجرائم الإلكترونية ويحدّد العقوبات المناسبة يُشكّل فجوة قانونية، و في المقابل اعتمدت دول مثل فرنسا والإمارات العربية المتحدة قوانين متخصصة لمكافحة الجرائم الإلكترونية، مما ساعد في توضيح الأفعال المجرّمة وتحديد العقوبات المناسبة[47].

ثانياً_ تعزيز القدرات التقنية والتدريبية:

تُعاني الأجهزة الأمنية والقضائية العراقية من نقص في الخبرات والموارد اللازمة لمكافحة الجرائم الإلكترونية. لذلك، يُنصح بتأسيس وحدات متخصصة في مكافحة الجرائم الإلكترونية، وتوفير التدريب المستمر لأفراد الشرطة والقضاة على أحدث التقنيات وأساليب التحقيق، فتجربة دولة الإمارات العربية المتحدة في إنشاء "الهيئة الوطنية للأمن السيبراني" تُعدّ نموذجًا يُحتذى به في هذا المجال[48].

ثالثاً_ تعزيز التعاون الدولي والإقليمي:

نظراً للطابع العابر للحدود للجرائم الإلكترونية، و حيث يُعدّ التعاون الدولي والإقليمي أمراً حيوياً يستوجب على العراق الانضمام إلى الاتفاقيات الدولية المتعلقة بمكافحة الجرائم الإلكترونية، مثل اتفاقية بودابست لمجلس أوروبا، وتفعيل آليات التعاون مع الدول الأخرى لتبادل المعلومات والخبرات[49].

رابعاً_ التوازن بين الأمن وحماية الحقوق الرقمية:

من الضروري أن تراعي التشريعات العراقية التوازن بين تعزيز الأمن السيبراني وحماية حقوق الأفراد في الفضاء الرقمي، فيجب أن تتضمن القوانين ضماناتٍ لحماية الخصوصية وحقوق الإنسان، مع وضع آلياتٍ فعّالة لمكافحة الجرائم الإلكترونية، و تأتي تجربة الاتحاد الأوروبي في تطبيق "اللائحة العامة لحماية البيانات" (GDPR) تُعدّ مثالًا على كيفية تحقيق هذا التوازن[50]. يتضح لنا أن المنظومة القانونية العراقية لم تواكب التطورات الرقمية بشكلٍ كامل، فجرائم الفضاء الإلكتروني تتسم بسرعة التغير وتعقيد الأساليب وعبور الحدود، وهو ما يجعل التشريعات التقليدية غير كافية لمواجهتها، فغياب نصوص متخصصة يحدّ من قدرة القضاء على التحقيق الفعّال والإثبات القانوني، ويزيد من احتمال التفاوت في الأحكام القضائية ويضعف الردع القانوني. إن الاستفادة من التجارب المقارنة لدول مثل فرنسا والإمارات والاتحاد الأوروبي توضح أهمية وجود قانون شامل للجرائم الإلكترونية، مع تحديد واضح للجرائم وأركانها والعقوبات المناسبة ووسائل الإثبات، مع مراعاة الحقوق الرقمية للأفراد، كما تظهر التجارب الدولية فاعلية إنشاء وحدات قضائية وتقنية متخصصة وربط التشريع بالتعاون الدولي لمواجهة الجرائم العابرة للحدود، مما يعزّز من قدرة الدولة على الردع وتحقيق العدالة. من وجهة نظرنا، فإنّ تطوير المنظومة القانونية العراقية يتطلّب استراتيجيةً شاملة تشمل سنّ تشريعٍ متخصص يوضّح تعريف الجرائم وأركانها وعقوباتها وآليات الإثبات الرقمي إلى جانب تأسيس وحداتٍ فنيّة وقضائيةٍ متخصصة لضمان جمع الأدلة الرقمية وتحليلها بطريقةٍ قانونية سليمة، مع تدريب القضاة والشرطة على أحدث أساليب التحقيق الرقمي، و كما يجب تعزيز التعاون الدولي والإقليمي لضمان القدرة على تتبع الجناة عبر الحدود وتبادل الخبرات القانونية والفنية، مع مراعاة حماية الحقوق الرقمية للأفراد ووضع آليات توازن بين الأمن السيبراني وخصوصية الأفراد و بالتأكيد فإنّ اعتماد هذه الاستراتيجية سيحوّل التحديات الحالية إلى فرص لتعزيز فاعلية القانون العراقي في مواجهة الجرائم الإلكترونية، ويضمن حماية المجتمع والدولة معاً مع الحفاظ على العدالة وحقوق الأفراد الإلكترونية.

الخاتمة

وفي ختام هذا البحث، يتضح لنا بأنّ الجريمة الإلكترونية تمثّل تحدياً متزايداً أمام التشريع الجنائي العراقي في ظلّ التطور السريع للتكنولوجيا واتساع نطاق استخدام الوسائل الرقمية، وقد أظهر التحليل أن النصوص الجزائية القائمة توفّر قدراً من الحماية، إلّا أنها لا تزال بحاجةٍ إلى تطوير لتواكب الطبيعة الخاصة لهذه الجرائم، و كما أن خصوصية البيئة الإلكترونية تفرض إعادة النظر في بعض المفاهيم التقليدية للقانون الجنائي بما ينسجم مع الواقع التقني الحديث، ومن ثم فإن تعزيز الإطار التشريعي وتحديثه يعتبر أمراً ضرورياً لضمان حماية فعالة للأنظمة المعلوماتية وتحقيق الأمن القانوني في المجال الإلكتروني.

الاستنتاجات:

توصل الباحث إلى عدّة نتائج هامة تتعلق بالتشريع العراقي لمكافحة الجريمة الإلكترونية:

1. يتبيّن من خلال الدراسة أن التشريع الجنائي العراقي لم يضع تنظيماً متكاملاً ومستقلّاً للجريمة الإلكترونية، وإنّما يعتمد في معظمه على تطبيق النصوص العامة في قانون العقوبات، الأمر الذي يثير إشكالياتٍ في التكييف القانوني لبعض الأفعال ذات الطبيعة التقنية الخاصة.
2. كشفت الدراسة أن الطبيعة غير المادية للجريمة الإلكترونية، واعتمادها على الوسائط الإلكترونية، تُحدث صعوباتٍ عملية في الإثبات والتحقيق، مما يستلزم تطوير آليات إجرائية وتقنية متخصصة لمواكبة هذا النوع من الجرائم وضمان فاعلية الملاحقة الجزائية.
3. أظهرت النتائج أن التطور التقني المتسارع يفوق في كثيرٍ من الأحيان سرعة التطور التشريعي، مما يفرض على المشرّع العراقي اعتماد سياسة جنائية مرنة وديناميكية قادرة على استيعاب المستجدات التقنية، وتوفير حمايةٍ قانونية أكثر وضوحاً وشمولاً للفضاء الإلكتروني.

المقترحات:

بناءً على النتائج السابقة، يُوصى بما يلي:

1. يرى الباحث ضرورة قيام المشرّع العراقي بإصدار قانونٍ خاص ومستقل ينظّم الجرائم الإلكترونية، و يتضمّن تعريفاً واضحاً لهذه الجرائم وصورها المختلفة، ويحدّد أركانها والعقوبات المقررة لها بما يتلاءم مع طبيعتها التقنية، بدلاً من الاعتماد على النصوص العامة التي قد لا تستوعب خصوصيتها بشكل كافٍ.
2. يقترح الباحث تطوير القواعد الإجرائية المتعلقة بجمع الأدلّة الإلكترونية، من خلال وضع نصوصٍ قانونية تنظّم آليات ضبط وتحليل الدليل الإلكتروني، بما يضمن سلامته وقابليته للاعتماد القضائي، ويعزّز من فعاليّة إجراءات التحقيق والملاحقة الجزائية.
3. يوصي الباحث بضرورة إنشاء وحداتٍ متخصصة ضمن الأجهزة الأمنية والقضائية تُعنى بمكافحة الجرائم الإلكترونية، وتزويدها بالكوادر المؤهلة والتدريب الفني والقانوني اللازم بما يسهم في رفع كفاءة التعامل مع هذا النوع من الجرائم.
4. يؤكّد الباحث أهمية تعزيز الوعي القانوني لدى مستخدمي الوسائل الإلكترونية بشأن مخاطر الجريمة الإلكترونية وآثارها القانونية، من خلال برامج توعوية وتثقيفية، بما يسهم في الحد من انتشار هذه الجرائم والوقاية منها.
5. يقترح الباحث الاستفادة من التجارب التشريعية المقارنة في مجال مكافحة الجرائم الإلكترونية، والعمل على تبني أفضل الممارسات القانونية التي أثبتت فعاليتها، بما يسهم في تطوير التشريع العراقي وتحقيق حماية جنائية أكثر شمولاً وفاعليّة.

الهوامش

(1)عبد العال، الديربي ومحمد، صادق، إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات في مجال مكافحة جرائم المعلوماتية والإنترنت، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 26.

(2)إبراهيم، مصطفى، سلمان، الجرائم الإلكترونية وتأثيرها في العراق، بحث مقدّم إلى مؤتمر مركز الدراسات الاستراتيجية – جامعة الموصل 2021، ص٨.

(3)أسامة، سعدون، العبيدي، الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، كلية الكنوز الجامعة، البصرة، العراق، العدد ٣، المجلد ١، ٢٠٢٤، ص223.

(4)أسامة، سعدون، العبيدي، الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، مرجع سابق، ص225

(5) روئ، محمد، يعقوب، التحديات الإجرائية المتصلة بالجرائم المعلوماتية في التشريع العراقي، مجلة دجلة للعلوم الإنسانية، جامعة النهرين، 2025، ص153.

(6)عبود، زهير كاظم، وكالة الأنباء العراقية، مقالة بعنوان الجرائم الإلكترونية في القانون العراقي متاحة على الرابط، تاريخ الزيارة 2025\11\5. https://ina.iq/ar/articles/192472--.html

(7)إبراهيم، مصطفى، سلمان، الجرائم الإلكترونية وتأثيرها في العراق، مرجع سابق، ص٩.

(8)عبد الإله، محمد، النوايسة، جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، عمان، 2017، ص 58.

(9)ناظم، طلال، الزهيري، إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الأخلاقيات الرقمية في العراق. مجلة آفاق للأبحاث السياسية والقانونية، المجلد 7، العدد 1، ٢٠٢٤، ص 223.

(10)عبد الإله، محمد، النوايسة، مرجع سابق، ص 65

(11)أسامة، سعدون، العبيدي، الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، مرجع سابق، ص228.

(12)أحمد، عبد الله، المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها: دراسة تحليلية تأصيلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص 156

(13)) أحمد، عبد الله، المراغي، مرجع سابق، ص 159

(14)سلمان، مصطفى، إبراهيم، الجرائم الإلكترونية وتأثيرها في العراق، مرجع سابق، ص13

(15)عبد الرحمن، الرميح، مدى إمكانية تطبيق نصوص القانون الجنائي على الجرائم المعلوماتية، مجلة النهرين للعلوم القانونية والسياسية، جامعة النهرين، المجلد 10، العدد 1، 2022، ص 285

(16) لينا، متعب محمد، الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012، ص ٤٢.

(17)علي، عبد الله، محمد، الحماية الجزائية للمنصات الإلكترونية – دراسة مقارنة، رسالة ماجستير،كلية الحقوق، جامعة كربلاء، 2022، ص٥٩.

(18)عبد العال، الديربي و محمد، صادق، إسماعيل، مرجع سابق، ص134

(19)محمد، أمين، الشوابكة، جرائم الحاسوب و الإنترنت(الجرائم الإلكترونية)، دار الثقافة للنشر و التوزيع، عمان، 2011، ص 123.

(20)فخري، عبد الرزاق، الحديثي، شرح قانون العقوبات – القسم العام، القاهرة: دار العاتك، 2007، ص٦٧.

(21)محمد، أمين، الشوابكة، مرجع سابق، ص ١٤٥.

(22)ضحى، حسن، فليح، دور التكنولوجيا في أزمة نصوص التجريم والعقاب." مجلة المعهد العدد 20، 2025، ص 233.

(23)صلبي، عبد الرزاق، فخري، الحديثي، مرجع سابق، ص٧٠.

(24)قانون العقوبات رقم (111) لسنة 1969 المعدل، مرجع سابق

(25)فخري، عبد الرزاق، الحديثي، مرجع سابق، ص٧٧.

(26)ضحى، حسن، فليح، مرجع سابق، 235.

(27)فخري، عبد الرزاق، الحديثي، مرجع سابق، ص١٣٤.

(28)المادة الخامسة من مشروع قانون جرائم المعلوماتية لسنة ٢٠١١ العراقي والمعدل عام ٢٠١٩.

(29)عبد الرحمن، الرميح، مرجع سابق، ص287.

(30)على عبد الله، علوان، محمد، مرجع سابق، ص ٧٠.

(31)ناظم، طلال، الزهيري، مرجع سابق، ص268.
(32)أسامة، سعدون، العبيدي، سعدون، الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، مرجع سابق، ص240.
(33)عبد الرحمن، الرميح، مرجع سابق، ص295.
(34)المادة ١٩ من مشروع قانون جرائم المعلوماتية لسنة ٢٠١١ العراقي والمعدل عام ٢٠١٩.
(35)عبد الله، علوان، محمد، مرجع سابق، ص٨٩.
(36)أسامة، سعدون، العبيدي، الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، مرجع سابق، ص242.
(37)محمد، أمين، الشوابكة، مرجع سابق، ص١٤٧.
(38)أسامة، سعدون، العبيدي، الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، مرجع سابق، ص٢٤٤.
(39)سالم، روضان، الموسوي، شرح قانون العقوبات_ القسم الخاص، بغداد، دار السهنهوري، ٢٠١٠، ص ١٤٦.
(40)عبد الكريم، فاضل، عبد الستار، شرح قانون أصول المحاكمات الجزائية، العراقي، بغداد، دار الثقافة القانونية ، ٢٠٠٥، ص١٦٧.
(41)عبد الله، علوان، محمد، مرجع سابق، ص ٨٩.
(42)أسامة، سعدون، العبيدي، مرجع سابق، ص244.
(43)منظمة ARTICLE 19، تحليل قانون الجرائم الإلكترونية ومسوداته في العراق (حقوق التعبير والحماية الرقمية).
(44)منظمة ARTICLE 19، تحليل قانون الجرائم الإلكترونية ومسوداته في العراق (حقوق التعبير والحماية الرقمية)
(45)عبد الجليل، أحمد، السعدي، الابتزاز الإلكتروني في العراق: دراسة قانونية اجتماعية، مجلة جامعة بابل للعلوم القانونية والسياسية، المجلد 11، العدد 2، ٢٠٢٣، ص 56
(46)عبد الجليل، أحمد، السعدي، مرجع سابق٦٠.
(47)جبار، حسين، حميد، آليات الحد من جرائم الاحتيال الإلكتروني في التشريع العراقي، مجلة كلية القانون، جامعة القادسية، المجلد 7، العدد 1 ،2024، ص 42.
(48)زينب، عبد الكريم، الموسوي، الإثبات في الجرائم الإلكترونية بين الواقع القانوني والتقني، مجلة كلية الحقوق – جامعة بغداد، المجلد 45، العدد ،202ص، ص 145
(49)جبار، حسين حميد، مرجع سابق، ص 50
(50)زينب، عبد الكريم، الموسوي، مرجع سابق، ص 149

قائمة المراجع

- **الكتب:**

1. أحمد، عبدالله، المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها : دراسة تحليلية تأصيلية مقارنة، المركز القومي للإصدارات القانونية، تطالقاهرة، ٢٠١٧.
2. فخري، عبد الرزاق، الحديثي، شرح قانون العقوبات _القسم العام، القاهرة، دار العاتك، ٢٠٠٧.
3. سالم، روضان، الموسوي، شرح قانون العقوبات_ القسم الخاص، بغداد، دار السنهوري، ٢٠١٠.
4. عبد العال، الديربي و محمد، صادق، اسماعيل، الجرائم الالكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات في مجال مكافحة جرائم المعلوماتية و الانترنت، ط١، المركز القومي للإصدارات القانونية، ٢٠١٢.
5. عبد الإله، محمد، النوايسة، جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية ، دار وائل للنشر و التوزيع، عمان، ٢٠١٧.
6. عبد الكريم، فاضل، عبد الستار، شرح قانون أصول المحاكمات الجزائية العراقي، بغداد، دار الثقافة القانونية، ٢٠٠٥.
7. محمد، أمين الشوابكة، جرائم الحاسوب و الانترنت(الجرائم الإلكترونية)، دار الثقافة للنشر و التوزيع، عمان، ٢٠١١.

- **المجلات العلمية**

1. جبارحسين حميد، آليات الحد من جرائم الاحتيال الإلكتروني في التشريع العراقي، مجلة كلية القانون، جامعة القادسية، المجلد7العدد1 ،2024
2. عبد الرحمن، الرميح، مدى إمكانية تطبيق نصوص القانون الجنائي على الجرائم المعلوماتية. مجلة النهرين للعلوم القانونية والسياسية، جامعة النهرين، المجلد 10، العدد 1، 2022.
3. ناظم، طلال،الزهيري، إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الأخلاقيات الرقمية في العراق. مجلة آفاق للأبحاث السياسية والقانونية، المجلد 7، العدد 1، ٢٠٢٤.
4. عبد الجليل، أحمد، السعدي، الابتزاز الإلكتروني في العراق: دراسة قانونية اجتماعية، مجلة جامعة بابل للعلوم القانونية والسياسية، المجلد 11، العدد 2، ٢٠٢٣.
5. مصطفى ،إبراهيم ،سلمان، الجرائم الإلكترونية وتأثيرها في العراق، بحث مقدّم إلى مؤتمر مركز الدراسات الاستراتيجية – جامعة الموصل ،الموصل، 2021.
6. أسامة، سعدون، العبيدي،الجريمة الإلكترونية في الواقع العراقي دراسة وتحليل، كلية الكنوز الجامعة، البصرة، العراق، العدد٣المجلد١، ٢٠٢٤
7. ضحى، حسن، فليح، دور التكنولوجيا في أزمة نصوص التجريم والعقاب، مجلة المعهد رقم 20 ، 2025.
8. رؤى محمد يعقوب، التحديات الإجرائية المتصلة بالجرائم المعلوماتية في التشريع العراقي،مجلة دجلة للعلوم الإنسانية، جامعة النهرين، 2025.

- **الرسائل الجامعية**

1. علي ، عبد الله، محمد، الحماية الجزائية للمنصات الإلكترونية – دراسة مقارنة، جامعة كربلاء، 2022، رسالة ماجستير .
2. لينا، متعب،الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة النهرين، 2012.

- **القوانين**

1. مشروع قانون جرائم المعلوماتية لسنة ٢٠١١ العراقي و المعدل عام ٢٠١٩ ، مجلس النواب العراقي، الدائرة القانونية، بغداد، 2019.
2. قانون العقوبات رقم (111) لسنة 1969 المعدل. الوقائع العراقية، العدد 1778 (15 آب 1969).
3. منظمة ARTICLE 19، تحليل قانون الجرائم الإلكترونية ومسوداته في العراق (حقوق التعبير والحماية الرقمية).

- **المواقع الإلكترونية**

١. https://ina.iq/ar/articles/192472--.html