مجلة الميدان للدراسات الرياضية والاجتماعية والإنسانية
https://asjp.cerist.dz/en/PresentationRevue/444
المجلد: 09 العدد: 02 (2026) ص 21-31

الجرائم الإلكترونية وحدود التشريع: التحديات القانونية في ملاحقة الجرائم عبر الإنترنت

Cybercrime and the limits of legislation: legal challenges in prosecuting online crimes

سعيدي عبد القادر *
جامعة ابن خلدون – تيارت (الجزائر)
kadisaidi72@gmail.com

زروقي أمين زين العابدين
جامعة ابن خلدون – تيارت (الجزائر)
Hafid.titri@gmail.com

معلومات المقال

تاريخ الارسال:
2026/04/19
تاريخ القبول:
2026/04/26

الكلمات المفتاحية:
- ✓ الجرائم الإلكترونية
- ✓ القانون الجنائي
- ✓ الفضاء الرقمي

الملخص:

يتناول المقال موضوع الجرائم الإلكترونية باعتبارها أحد أبرز التحديات التي فرضها التطور السريع في تكنولوجيا المعلومات والاتصال. وتتميز هذه الجرائم بطابعها العابر للحدود وصعوبة تتبع مرتكبيها، مما جعلها تشكل إشكالًا حقيقيًا أمام التشريعات الجنائية التقليدية. كما يبرز المقال محدودية هذه التشريعات في مجالات الاختصاص القضائي، والإثبات الجنائي الرقمي، والتعاون الدولي. ويؤكد على ضرورة تطوير القوانين، وتعزيز الخبرات التقنية، وتحقيق التوازن بين الأمن الرقمي وحماية الحقوق والحريات، لمواجهة هذا النوع من الجرائم بشكل فعال.

Article info

Received
19/04/2026
Accepted
26/04/2026

Keywords:
- ✓ *Cybercrime,*
- ✓ *criminal law*
- ✓ *digital space*

Abstract :

The article addresses cybercrime as one of the most significant challenges arising from the rapid development of information and communication technologies. These crimes are transnational in nature and difficult to trace, posing a real challenge to traditional criminal legislation. The article highlights the limitations of existing laws in areas such as jurisdiction, digital criminal evidence, and international cooperation. It emphasizes the need to develop legal frameworks, enhance technical expertise, and balance digital security with the protection of rights and freedoms to effectively combat this type of crime.

* المؤلف المرسل

1. مقدمة:

شهد العالم في العقود الأخيرة تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصال، حيث أصبح الفضاء الرقمي جزءًا لا يتجزأ من الحياة اليومية للأفراد والمؤسسات على حد سواء. وقد أدى هذا التحول إلى بروز مجتمع معلوماتي جديد يعتمد بشكل أساسي على تبادل البيانات والمعرفة عبر الشبكات الإلكترونية، الأمر الذي ساهم في تسهيل العديد من الأنشطة الإنسانية، سواء كانت اقتصادية أو اجتماعية أو ثقافية. غير أن هذا التطور لم يخلُ من آثار سلبية، إذ أفرز نوعًا جديدًا من الجرائم يُعرف بالجرائم الإلكترونية، والتي باتت تشكل تهديدًا حقيقيًا للأمن الفردي والجماعي (الشمري، 2021).

وتُعد الجرائم الإلكترونية من الظواهر الإجرامية المعاصرة التي فرضت نفسها بقوة على ميدان القانون الجنائي، نظرًا لخصوصيتها وتميزها عن الجرائم التقليدية. فهي لا ترتبط بمكان محدد، ولا تتطلب وجودًا ماديًا للجاني في مسرح الجريمة، كما أنها تُرتكب باستخدام وسائل تقنية متطورة يصعب تتبعها أو التحكم فيها. وقد أشار (عرب، 2002) إلى أن هذه الجرائم تمثل تحولًا نوعيًا في الفكر الإجرامي، حيث انتقل الجناة من الأساليب التقليدية إلى استغلال الأنظمة المعلوماتية والشبكات الرقمية لتحقيق أهدافهم غير المشروعة.

ومن أبرز ما يميز الجرائم الإلكترونية طابعها العابر للحدود، حيث يمكن أن تُرتكب الجريمة في دولة، ويكون أثرها في دولة أخرى، بينما يوجد الجاني في دولة ثالثة، وهو ما يطرح إشكالات قانونية معقدة تتعلق بالاختصاص القضائي وتنازع القوانين. وفي هذا السياق، يؤكد (الجابري وآخرون، 2025) أن غياب التنسيق الفعال بين الأنظمة القانونية المختلفة يُعد من أبرز العوائق التي تحول دون ملاحقة مرتكبي هذه الجرائم بشكل فعال، خاصة في ظل اختلاف التشريعات الوطنية من حيث التعريف والتجريم والعقوبات.

كما أن التطور السريع في الوسائل التقنية يفوق في كثير من الأحيان قدرة التشريعات الجنائية على التكيف، مما يؤدي إلى ظهور فجوات قانونية تستغلها الشبكات الإجرامية. فالقوانين التقليدية وُضعت أساسًا لتنظيم الجرائم المادية التي تقع في نطاق جغرافي محدد، في حين أن الجرائم الإلكترونية تتجاوز هذه الحدود، مما يستدعي إعادة النظر في المفاهيم القانونية الكلاسيكية وتحديثها بما يتلاءم مع الواقع الرقمي الجديد (برادة، 2024).

إضافة إلى ذلك، تطرح الجرائم الإلكترونية تحديات كبيرة في مجال الإثبات الجنائي، حيث تعتمد هذه الجرائم على أدلة رقمية تتميز بخصائص فنية معقدة، مثل قابليتها للتعديل أو الإتلاف بسهولة، وصعوبة التحقق من مصدرها. وقد أشار (برادة، 2024) إلى أن حجية الدليل الرقمي لا تزال محل نقاش فقهي وقضائي، خاصة في ظل غياب معايير موحدة للتعامل معه، مما يؤثر سلبًا على فعالية العدالة الجنائية في هذا المجال.

ومن جهة أخرى، فإن التحقيق في الجرائم الإلكترونية يتطلب توفر خبرات تقنية متخصصة، وهو ما قد لا يتوفر دائمًا لدى الجهات القضائية أو الأمنية، خاصة في الدول النامية. وفي هذا الإطار، يبرز دور التكوين المستمر والتدريب التقني في تعزيز قدرات المحققين والقضاة على التعامل مع هذا النوع من الجرائم. وقد بيّن (التومي وآخرون، 2024) أن ضعف الإمكانيات التقنية والبشرية يُعد من أبرز التحديات التي تواجه التحقيق الجنائي في الجرائم الإلكترونية، مما يؤدي في كثير من الأحيان إلى صعوبة الوصول إلى الجناة أو تقديمهم للعدالة.

كما تثير مكافحة الجرائم الإلكترونية إشكالية التوازن بين متطلبات الأمن وحماية الحقوق والحريات الأساسية، مثل الحق في الخصوصية وحرية التعبير. فالتوسع في استخدام وسائل المراقبة الرقمية قد يؤدي إلى انتهاك هذه الحقوق، مما يستدعي وضع ضوابط قانونية دقيقة تضمن عدم التعسف في استخدامها. وفي هذا السياق، أشار (بني عودة، 2024) إلى أن التشريعات الحديثة تسعى إلى تحقيق هذا التوازن من خلال وضع قواعد تنظم استخدام الوسائل التقنية في التحقيق، مع احترام الضمانات القانونية للأفراد.

وعليه، فإن دراسة الجرائم الإلكترونية وحدود التشريع في مواجهتها تكتسي أهمية بالغة، ليس فقط لفهم طبيعة هذه الظاهرة، بل أيضًا لتقييم مدى فعالية الأطر القانونية الحالية في التصدي لها. كما تبرز الحاجة إلى تطوير التشريعات الجنائية بما يتلاءم مع التحولات الرقمية المتسارعة، وتعزيز التعاون الدولي،

وتبادل الخبرات بين الدول، بما يسهم في بناء منظومة قانونية متكاملة قادرة على مواجهة التحديات التي تفرضها الجرائم الإلكترونية في العصر الحديث.

الإشكالية:

أفرزت الثورة الرقمية واقعًا جديدًا أعاد تشكيل مفاهيم الجريمة ووسائل ارتكابها، حيث لم تعد الجريمة مرتبطة بالحيز المادي التقليدي، بل انتقلت إلى فضاء افتراضي مفتوح يتسم بالسرعة والتعقيد وغياب الحدود الجغرافية. وقد أدى هذا التحول إلى بروز ما يُعرف بالجرائم الإلكترونية، التي أصبحت تمثل تحديًا حقيقيًا أمام أنظمة القانون الجنائي، سواء من حيث التأصيل النظري أو التطبيق العملي (الشمري، 2021).

وتكمن جوهر الإشكالية في عدم التناسب بين التطور المتسارع للتكنولوجيا والبطء النسبي في تطور التشريعات الجنائية، مما أدى إلى ظهور فجوة قانونية تستغلها الجماعات الإجرامية. فالتشريعات التقليدية صُممت لمواجهة أنماط إجرامية مادية ومحددة جغرافيًا، في حين أن الجرائم الإلكترونية تتسم باللامادية والعالمية، وهو ما يجعل تطبيق القواعد القانونية القائمة أمرًا معقدًا وغير كافٍ في كثير من الأحيان (برادة، 2024).

كما تطرح الجرائم الإلكترونية إشكالات متعددة تتعلق بتحديد الاختصاص القضائي، نظرًا لإمكانية ارتكاب الجريمة في أكثر من دولة في آن واحد. وهذا ما يثير تساؤلات حول الجهة المختصة بالملاحقة القضائية، والقانون الواجب التطبيق، خاصة في ظل غياب إطار دولي موحد وفعال للتعامل مع هذه الجرائم. وفي هذا السياق، يشير (الجابري وآخرون، 2025) إلى أن التباين بين التشريعات الوطنية يُضعف من فعالية الجهود الدولية في مكافحة الجرائم الإلكترونية، ويُسهم في إفلات العديد من الجناة من العقاب.

ومن ناحية أخرى، تبرز صعوبات كبيرة في مجال الإثبات الجنائي، حيث تعتمد الجرائم الإلكترونية على أدلة رقمية تتسم بخصائص تقنية معقدة، مثل سهولة التلاعب بها أو إخفائها، مما يثير إشكالات تتعلق بحجيتها ومدى قبولها أمام القضاء. وقد أكد (برادة، 2024) أن غياب معايير واضحة للتعامل مع الأدلة الرقمية يُعد من أبرز التحديات التي تواجه العدالة الجنائية في هذا المجال.

ولا يقتصر الأمر على الجوانب القانونية فحسب، بل يمتد ليشمل التحديات التقنية والبشرية، حيث يتطلب التحقيق في الجرائم الإلكترونية توفر خبرات متخصصة في مجال تكنولوجيا المعلومات، وهو ما قد لا يتوفر في جميع الأنظمة القضائية. وفي هذا الإطار، يوضح (التومي وآخرون، 2024) أن ضعف التكوين التقني لدى القائمين على إنفاذ القانون يُعد من العوامل التي تعيق فعالية ملاحقة الجرائم الإلكترونية.

إضافة إلى ذلك، تثير مكافحة الجرائم الإلكترونية إشكالية التوازن بين متطلبات الأمن وحماية الحقوق والحريات الأساسية، حيث قد تؤدي بعض الإجراءات، مثل المراقبة الرقمية أو جمع البيانات، إلى انتهاك الخصوصية أو تقييد حرية التعبير. وقد أشار (بني عودة، 2024) إلى أن تحقيق هذا التوازن يُعد من أبرز التحديات التي تواجه المشرّع في العصر الرقمي.

بناءً على ما سبق، يمكن صياغة الإشكالية الرئيسية للبحث على النحو التالي:

إلى أي مدى تستطيع التشريعات الجنائية الوطنية مواكبة تطور الجرائم الإلكترونية، وما هي أبرز التحديات القانونية والتقنية التي تواجه ملاحقة مرتكبيها في ظل الطبيعة العابرة للحدود للفضاء الرقمي؟

كما تتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية:

ما مدى كفاية النصوص القانونية الحالية في تجريم الأفعال المرتبطة بالجرائم الإلكترونية؟

كيف يمكن معالجة إشكالية الاختصاص القضائي في الجرائم العابرة للحدود؟

ما هي التحديات المرتبطة بالإثبات الجنائي في البيئة الرقمية؟

كيف يمكن تحقيق التوازن بين مكافحة الجريمة وحماية الحقوق والحريات؟

ما دور التعاون الدولي في تعزيز فعالية ملاحقة الجرائم الإلكترونية؟

المصطلحات والمفاهيم

1. مفهوم الجريمة الإلكترونية

تُعرّف الجريمة الإلكترونية بأنها كل فعل غير مشروع يُرتكب باستخدام الحاسوب أو الشبكات المعلوماتية، أو يستهدف هذه الأنظمة بشكل مباشر أو غير مباشر. وتشمل هذه الجرائم

مجموعة واسعة من الأفعال مثل الاختراق، الاحتيال الإلكتروني، وانتحال الهوية. ويشير (الشمري، 2021) إلى أن غياب تعريف موحد للجريمة الإلكترونية في الفقه العربي يعكس تعقيد هذه الظاهرة وتعدد صورها.

2 .الفضاء السيبراني

يقصد به البيئة الافتراضية التي تتم فيها عمليات الاتصال والتفاعل عبر الإنترنت، والتي لا تخضع لحدود جغرافية واضحة. ويُعد هذا الفضاء الحاضنة الأساسية للجرائم الإلكترونية، حيث يتيح للجناة العمل في بيئة يصعب تتبعها أو السيطرة عليها (عرب، 2002).

3 .الدليل الرقمي

هو كل معلومة ذات قيمة إثباتية يتم تخزينها أو نقلها في شكل رقمي، ويمكن استخدامها أمام القضاء لإثبات وقوع الجريمة أو نسبتها إلى المتهم. ويؤكد (برادة، 2024) أن الدليل الرقمي يتميز بخصائص فريدة، مثل قابليته للنسخ والتعديل، مما يثير إشكالات تتعلق بحجيته وسلامته.

4 .الاختصاص القضائي

يعني سلطة الدولة في تطبيق قوانينها على الجرائم المرتكبة داخل إقليمها أو خارجه في بعض الحالات. وتزداد أهمية هذا المفهوم في الجرائم الإلكترونية نظرًا لطبيعتها العابرة للحدود، مما يؤدي إلى تنازع الاختصاص بين الدول (الجابري وآخرون، 2025).

5 .التحقيق الرقمي

هو مجموعة الإجراءات التقنية والقانونية التي تهدف إلى جمع وتحليل الأدلة الرقمية للكشف عن الجرائم الإلكترونية وتحديد مرتكبيها. ويشير (التومي وآخرون، 2024) إلى أن هذا النوع من التحقيق يتطلب مهارات متقدمة في تكنولوجيا المعلومات إلى جانب المعرفة القانونية.

الخلفية النظرية:

تُعد الجرائم الإلكترونية من الظواهر الإجرامية المعاصرة التي استدعت إعادة النظر في العديد من المسلّمات التقليدية في القانون الجنائي، وذلك نظرًا لخصوصية البيئة الرقمية التي تختلف جذريًا عن البيئة الواقعية من حيث طبيعة السلوك الإجرامي ووسائل ارتكابه وآليات مكافحته. ومن ثمّ، فإن فهم هذه الظاهرة يقتضي الاستناد إلى مجموعة من المقاربات النظرية التي تفسر نشأتها وتطورها وتُسهم في وضع آليات فعالة للتصدي لها.

1 .نظرية الفرصة الإجرامية في البيئة الرقمية

تُعد نظرية الفرصة الإجرامية من أبرز النظريات التي يمكن توظيفها في تفسير الجرائم الإلكترونية، حيث تفترض أن الجريمة لا تحدث فقط نتيجة لوجود دافع إجرامي، بل أيضًا بسبب توفر فرصة مناسبة في ظل غياب الرقابة. وفي الفضاء الرقمي، تتجلى هذه الفرص بشكل أوضح، نظرًا لسهولة الوصول إلى الأنظمة المعلوماتية، وضعف إجراءات الحماية في بعض الأحيان، فضلًا عن الطابع المفتوح للإنترنت.

وقد أشار (الشمري، 2021) إلى أن البيئة الرقمية تُعد بيئة خصبة لارتكاب الجرائم، حيث يمكن للجاني تنفيذ فعله الإجرامي دون الحاجة إلى التواجد المادي في مكان معين، مما يقلل من احتمالية اكتشافه. كما أن استخدام تقنيات مثل الشبكات الخاصة الافتراضية (VPN) والتشفير يزيد من صعوبة تتبع الجناة، وهو ما يعزز من فرص ارتكاب الجريمة دون خوف من العقاب.

2 .نظرية الردع وحدودها في الجرائم الإلكترونية

ترتكز نظرية الردع على فكرة أن العقوبة تُشكل وسيلة فعالة لمنع ارتكاب الجرائم، من خلال تخويف الأفراد من العواقب القانونية لأفعالهم. غير أن تطبيق هذه النظرية في مجال الجرائم الإلكترونية يواجه تحديات كبيرة، حيث إن فعالية الردع تعتمد على احتمال اكتشاف الجريمة ومعاقبة مرتكبها، وهو ما يكون ضعيفًا في البيئة الرقمية.

ويؤكد (برادة، 2024) أن انخفاض معدلات الكشف عن الجرائم الإلكترونية يُضعف من تأثير الردع، حتى في ظل وجود نصوص قانونية صارمة. كما أن الطابع العابر للحدود لهذه الجرائم يُعقّد من عملية تنفيذ العقوبات، خاصة في حال وجود الجاني خارج نطاق الولاية القضائية للدولة المتضررة.

3 .نظرية العولمة القانونية والتعاون الدولي

في ظل الطبيعة العابرة للحدود للجرائم الإلكترونية، برزت نظرية العولمة القانونية كإطار تحليلي يُبرز أهمية التعاون الدولي في مواجهة هذه الظاهرة. فالجريمة الإلكترونية قد تبدأ في دولة،

وتُنفذ في أخرى، وتُحدث آثارها في دولة ثالثة، مما يجعل من الصعب على دولة واحدة التعامل معها بشكل منفرد.

وفي هذا السياق، يشير (الجابري وآخرون، 2025) إلى أن غياب التنسيق بين الأنظمة القانونية المختلفة يُعد من أبرز التحديات التي تواجه مكافحة الجرائم الإلكترونية، حيث تختلف الدول في تعريف هذه الجرائم، وفي تجريمها، وفي العقوبات المقررة لها. كما أن ضعف آليات التعاون القضائي الدولي، مثل تسليم المجرمين وتبادل المعلومات، يُسهم في إفلات الجناة من العقاب.

4 .نظرية التفاعل الاجتماعي في الفضاء الرقمي

تُفسر نظرية التفاعل الاجتماعي السلوك الإجرامي من خلال تأثير البيئة الاجتماعية والتفاعلات بين الأفراد. ومع ظهور وسائل التواصل الاجتماعي، أصبحت هذه التفاعلات تتم في بيئة رقمية، مما أدى إلى بروز أنماط جديدة من الجرائم، مثل التنمر الإلكتروني، والابتزاز، وانتحال الهوية.

وقد أوضح (بني عودة، 2024) أن هذه الجرائم ترتبط بشكل وثيق بطبيعة العلاقات الاجتماعية في الفضاء الرقمي، حيث يُمكن للجاني استغلال anonymity (إخفاء الهوية) لبناء علاقات وهمية مع الضحايا، ومن ثم استغلالهم بطرق غير مشروعة. كما أن غياب الرقابة الأسرية أو المجتمعية في هذا الفضاء يُسهم في تفاقم هذه الظواهر.

5 .المقاربة التقنية القانونية (التكامل بين القانون والتكنولوجيا)

تُعد المقاربة التقنية القانونية من أهم الاتجاهات الحديثة في دراسة الجرائم الإلكترونية، حيث تؤكد على ضرورة التكامل بين المعرفة القانونية والخبرة التقنية لفهم هذا النوع من الجرائم ومكافحته. فالقانون وحده لا يكفي إذا لم يكن مدعومًا بفهم عميق للتكنولوجيا التي تُستخدم في ارتكاب الجريمة.

ويشير (التومي وآخرون، 2024) إلى أن التحقيق في الجرائم الإلكترونية يتطلب مهارات متقدمة في تحليل البيانات، واسترجاع المعلومات، وفهم بنية الأنظمة المعلوماتية، وهو ما يستدعي تكوين فرق متعددة التخصصات تضم خبراء في القانون وتكنولوجيا المعلومات. كما أن تطوير أدوات تقنية حديثة يُعد أمرًا ضروريًا لتعزيز فعالية التحقيقات.

6 .نظرية المخاطر الرقمية

تُبرز هذه النظرية أن استخدام التكنولوجيا ينطوي على مجموعة من المخاطر التي قد تُستغل في ارتكاب الجرائم. فكلما زاد الاعتماد على الأنظمة الرقمية، زادت فرص استهدافها من قبل المجرمين. وتشمل هذه المخاطر الاختراقات الأمنية، وسرقة البيانات، والهجمات السيبرانية.

ويؤكد (الشمري، 2021) أن ضعف الوعي الأمني لدى المستخدمين يُعد من العوامل التي تُسهم في انتشار الجرائم الإلكترونية، حيث يُمكن استغلال هذا الضعف لتنفيذ هجمات احتيالية أو سرقة معلومات حساسة.

7 .المقاربة الحقوقية (التوازن بين الأمن والحرية)

تُركز هذه المقاربة على ضرورة تحقيق التوازن بين مكافحة الجرائم الإلكترونية وحماية الحقوق والحريات الأساسية، مثل الحق في الخصوصية وحرية التعبير. فالإفراط في استخدام وسائل المراقبة الرقمية قد يؤدي إلى انتهاك هذه الحقوق، مما يُثير إشكالات قانونية وأخلاقية.

وفي هذا الإطار، يشير (بني عودة، 2024) إلى أن التشريعات الحديثة تسعى إلى وضع ضوابط قانونية تضمن استخدام الوسائل التقنية في إطار احترام الحقوق الأساسية، من خلال اشتراط الحصول على إذن قضائي، وتحديد نطاق المراقبة، وضمان سرية البيانات.

من خلال استعراض هذه النظريات، يتضح أن الجرائم الإلكترونية تمثل ظاهرة معقدة ومتعددة الأبعاد، لا يمكن فهمها أو مكافحتها من خلال مقاربة واحدة فقط، بل تتطلب تكاملًا بين عدة نظريات تجمع بين الجوانب القانونية والتقنية والاجتماعية. كما تُبرز هذه الخلفية النظرية الحاجة إلى تطوير التشريعات، وتعزيز التعاون الدولي، وتكوين كفاءات متخصصة، بما يتلاءم مع طبيعة التحديات التي تفرضها البيئة الرقمية.

انطلاقًا من الإشكالية المطروحة حول مدى قدرة التشريعات الجنائية على مواكبة تطور الجرائم الإلكترونية، يتضح أن الإجابة لا يمكن أن تكون أحادية أو قطعية، بل تقتضي تحليلًا متعدد الأبعاد يجمع بين القانون والتكنولوجيا والتعاون الدولي، في إطار القانون الجنائي.

أولًا: محدودية التشريعات الجنائية التقليدية

تُظهر الدراسة أن التشريعات الجنائية التقليدية تعاني من قصور واضح في مواجهة الجرائم الإلكترونية، وذلك لعدة أسباب، من بينها:

-اعتمادها على مفاهيم مادية للجريمة (مكان، أداة، نتيجة).

-بطء عملية التحديث التشريعي مقارنة بسرعة التطور التكنولوجي.

-غياب نصوص صريحة تُجرّم بعض الأفعال الرقمية المستحدثة.

ويؤكد (الشمري، 2021) أن العديد من التشريعات العربية لا تزال تعتمد على نصوص عامة يتم تأويلها لتشمل الجرائم الإلكترونية، وهو ما يؤدي إلى غموض قانوني قد يُستغل من قبل الجناة. كما يشير (برادة، 2024) إلى أن هذا القصور يُنتج فراغًا تشريعيًا يُضعف من فعالية الردع.

-مثال تطبيقي:

في حالات "الاختراق الأخلاقي" أو ما يُعرف بالـ Ethical Hacking، قد يصعب التمييز بين الفعل المشروع وغير المشروع في غياب نصوص واضحة، مما يُعقّد عملية التكييف القانوني.

ثانيًا: إشكالية الاختصاص القضائي وتنازع القوانين

تُعد مسألة الاختصاص القضائي من أبرز التحديات في ملاحقة الجرائم الإلكترونية، نظرًا لطبيعتها العابرة للحدود. فقد تتداخل عدة دول في الجريمة الواحدة:

-دولة وقوع الفعل

-دولة وجود الخادم(Server)

-دولة إقامة الضحية

-دولة إقامة الجاني

ويشير (الجابري وآخرون، 2025) إلى أن هذا التداخل يُنتج تنازعًا قانونيًا يُعيق الملاحقة القضائية، خاصة في ظل غياب اتفاقيات ملزمة أو اختلاف الأنظمة القانونية.

مثال تطبيقي:

جريمة احتيال إلكتروني تُرتكب من شخص في دولة "أ"، باستخدام خادم في دولة "ب"، ضد ضحية في دولة "ج". أي قانون يُطبق؟ وأي محكمة تختص؟ هذا التعقيد قد يؤدي إلى إفلات الجاني.

ثالثًا: تحديات الإثبات الجنائي الرقمي

يُعد الإثبات في الجرائم الإلكترونية من أكثر الجوانب تعقيدًا، حيث يعتمد على الأدلة الرقمية التي تتميز بـ:

-القابلية للتعديل أو الحذف بسهولة

-الحاجة إلى أدوات تقنية لاستخراجها

-صعوبة إثبات نسبتها إلى شخص معين

ويؤكد (برادة، 2024) أن غياب معايير موحدة للتعامل مع الأدلة الرقمية يُضعف من حجيتها أمام القضاء، كما أن نقص الخبرة التقنية لدى القضاة قد يؤثر على تقييم هذه الأدلة.

مثال تطبيقي:

في قضايا الابتزاز عبر وسائل التواصل، قد يُنكر المتهم مسؤوليته ويدّعي اختراق حسابه، مما يتطلب تحليلًا جنائيًا رقميًا لإثبات العكس.

رابعًا: التحديات التقنية والبشرية

تتطلب ملاحقة الجرائم الإلكترونية توفر بنية تقنية متطورة وكفاءات بشرية متخصصة، وهو ما لا يتوفر دائمًا، خاصة في الدول النامية. ويُبرز (التومي وآخرون، 2024) أن ضعف التكوين التقني لدى أجهزة إنفاذ القانون يُعد من أبرز معوقات التحقيق.

مثال تطبيقي:

عدم قدرة المحقق على تحليل جهاز حاسوب أو تتبع عنوان IP قد يؤدي إلى ضياع أدلة حاسمة.

خامسًا: إشكالية التوازن بين الأمن والحقوق

تُثير مكافحة الجرائم الإلكترونية إشكالية حساسة تتعلق بالتوازن بين:

-حماية الأمن الرقمي

-احترام الحقوق والحريات (الخصوصية، حرية التعبير)

ويؤكد (بني عودة، 2024) أن الإفراط في المراقبة الرقمية قد يؤدي إلى انتهاكات قانونية، مما يستدعي وضع ضوابط دقيقة.

الحلول المقترحة (مقاربة شاملة)

1. تحديث التشريعات الجنائية

-سن قوانين خاصة بالجرائم الإلكترونية

-إدراج تعريفات دقيقة للأفعال الإجرامية

-مواكبة التطورات التقنية بشكل دوري

(برادة، 2024) يؤكد ضرورة الانتقال من التشريع العام إلى التشريع المتخصص.

2. تعزيز التعاون الدولي

-الانضمام إلى الاتفاقيات الدولية

-إنشاء آليات لتبادل المعلومات

-تسهيل إجراءات تسليم المجرمين

(الجابري وآخرون، 2025) يشددون على أن التعاون الدولي هو الحل الأساسي.

3. تطوير منظومة الإثبات الرقمي

-اعتماد معايير دولية للأدلة الرقمية

-تدريب القضاة على التعامل مع الأدلة التقنية

-إنشاء مختبرات جنائية رقمية

4. بناء قدرات بشرية وتقنية

-تكوين متخصصين في التحقيق الرقمي

-إدماج التكنولوجيا في العمل القضائي

-التعاون مع خبراء الأمن السيبراني

(التومي وآخرون، 2024) يؤكدون أهمية التكوين المستمر.

5. تحقيق التوازن بين الأمن والحرية

-وضع ضوابط قانونية للمراقبة

-ضمان الرقابة القضائية

-حماية البيانات الشخصية

(بني عودة، 2024) يبرز أهمية الضمانات القانونية.

الاستنتاج العام:

في ضوء التحليل السابق لموضوع الجرائم الإلكترونية وحدود التشريع، يتبين أن هذه الظاهرة الإجرامية تمثل تحولًا نوعيًا في بنية الجريمة المعاصرة، إذ لم تعد مرتبطة بالمكان أو الزمان أو الوسائل التقليدية، بل أصبحت تعتمد على فضاء رقمي مفتوح تتداخل فيه الحدود الوطنية، وتتسارع فيه وتيرة التطور التقني بشكل يفوق في كثير من الأحيان قدرة المشرّع على الاستجابة. وقد أفرز هذا الواقع تحديات متعددة تمس جوهر النظام القانوني الجنائي، سواء من حيث التجريم أو الإثبات أو الاختصاص أو التعاون الدولي.

وعليه، يمكن استخلاص إجابات علمية دقيقة عن التساؤلات الجزئية التي بُنيت عليها الدراسة كما يلي:

أولًا: مدى كفاية النصوص القانونية في تجريم الأفعال الإلكترونية

يتضح أن التشريعات الجنائية الحالية، رغم محاولتها مواكبة التطور، لا تزال تعاني من قصور نسبي في الشمول والدقة. فبعض التشريعات تعتمد على نصوص عامة يتم من خلالها استيعاب الأفعال الإلكترونية بالتفسير، بدل النص الصريح والواضح، وهو ما يخلق نوعًا من الغموض القانوني.

وقد أكد ذلك (الشمري، 2021) الذي بيّن أن غياب تعريف موحد ودقيق للجرائم الإلكترونية في التشريعات العربية يؤدي إلى تفاوت في التجريم والعقاب، ويُضعف من مبدأ الشرعية الجنائية. وبالتالي، فإن الإجابة عن هذا التساؤل هي أن النصوص الحالية غير كافية بشكل كامل، وتحتاج إلى تحديث مستمر وتشريعات متخصصة.

ثانيًا: إشكالية الاختصاص القضائي في الجرائم العابرة للحدود

يتبين أن الجرائم الإلكترونية تُحدث تداخلًا معقدًا في الاختصاص القضائي، نظرًا لأن عناصر الجريمة قد تتوزع بين عدة دول. فقد يقع الفعل في دولة، بينما تقع النتيجة في دولة أخرى، وقد يوجد الخادم في دولة ثالثة، مما يخلق تنازعًا بين القوانين الوطنية. ويشير (الجابري وآخرون، 2025) إلى أن هذا التداخل يُضعف من فعالية الملاحقة القضائية، في ظل غياب إطار دولي موحد وملزم.

وعليه، فإن الإجابة هي أن إشكالية الاختصاص القضائي لا تزال غير محلولة بشكل كامل، وتحتاج إلى تعزيز التعاون القضائي الدولي ووضع قواعد موحدة لتحديد الاختصاص.

ثالثًا: التحديات المرتبطة بالإثبات الجنائي الرقمي

أثبتت الدراسة أن الإثبات في الجرائم الإلكترونية يُعد من أكثر الجوانب تعقيدًا، بسبب الطبيعة الخاصة للدليل الرقمي الذي يتميز بـ:

قابليته للتعديل والحذف

صعوبة إثبات مصدره

الحاجة إلى خبرة تقنية متخصصة

ويؤكد (برادة، 2024) أن حجية الدليل الرقمي لا تزال محل نقاش فقهي وقضائي، مما يؤدي إلى تفاوت في تقديرها أمام المحاكم.

وبناءً عليه، فإن الإجابة هي أن الإثبات الجنائي في البيئة الرقمية ما يزال غير مستقر قانونيًا ويحتاج إلى تقنين أوضح ومعايير تقنية موحدة.

رابعًا: فعالية آليات التعاون الدولي

تبيّن أن التعاون الدولي في مكافحة الجرائم الإلكترونية لا يزال محدود الفعالية، رغم وجود بعض الاتفاقيات الدولية. ويرجع ذلك إلى اختلاف الأنظمة القانونية، وتباين تعريف الجريمة الإلكترونية بين الدول، وصعوبة تبادل الأدلة والمعلومات بسرعة.

ويؤكد (التومي وآخرون، 2024) أن ضعف التنسيق الدولي يُعد من أبرز العوائق التي تواجه التحقيق في هذا النوع من الجرائم.

وعليه، فإن الإجابة هي أن التعاون الدولي موجود لكنه غير كافٍ وغير فعال بالشكل المطلوب.

خامسًا: التوازن بين مكافحة الجريمة وحماية الحقوق والحريات

أظهرت الدراسة أن هناك إشكالية حقيقية في تحقيق التوازن بين:

حماية الأمن الرقمي ومكافحة الجريمة

وضمان الحقوق والحريات الأساسية، خصوصًا الخصوصية وحرية التعبير

ويشير (بني عودة، 2024) إلى أن الإفراط في استخدام أدوات المراقبة الرقمية قد يؤدي إلى انتهاكات قانونية إذا لم يكن مضبوطًا بضوابط قضائية واضحة.

وبالتالي، فإن الإجابة هي أن هذا التوازن ممكن نظريًا لكنه صعب عمليًا ويحتاج إلى تشريعات دقيقة ورقابة قضائية فعالة.

بناءً على ما سبق، يمكن القول إن الجرائم الإلكترونية تمثل تحديًا بنيويًا للنظام القانوني الجنائي التقليدي، لأنها تكشف محدودية المفاهيم الكلاسيكية للجريمة، وتفرض إعادة صياغة العديد من المبادئ القانونية مثل الإقليمية، والإثبات، والاختصاص.

كما يتضح أن المواجهة الفعالة لهذه الجرائم لا يمكن أن تعتمد على التشريع الوطني وحده، بل تتطلب:

تحديثًا مستمرًا للقوانين

تعاونًا دوليًا فعالًا

تطويرًا تقنيًا في أساليب التحقيق

وتكوينًا متخصصًا للقضاة والمحققين

وفي النهاية، فإن الفجوة بين التطور التكنولوجي والتطور التشريعي لا تزال قائمة، لكن يمكن تقليصها تدريجيًا عبر مقاربة شاملة تجمع بين القانون والتكنولوجيا والتعاون الدولي.

الخاتمة:

في ختام هذه الدراسة حول الجرائم الإلكترونية وحدود التشريع، يتضح أن هذه الظاهرة لم تعد مجرد امتداد حديث للجريمة التقليدية، بل أصبحت نمطًا إجراميًا مستقلًا له خصائصه المميزة التي فرضت نفسها بقوة على المنظومة القانونية المعاصرة، وخاصة في إطار القانون الجنائي. فقد كشفت الدراسة أن البيئة الرقمية، بما توفره من سرعة، ولامحدودية، وإخفاء للهوية، قد أعادت تشكيل مفهوم الجريمة ذاته، وأفرزت تحديات غير مسبوقة على مستوى التجريم، والإثبات، والاختصاص القضائي، والتنفيذ.

وقد تبين من خلال التحليل أن التشريعات الجنائية الحالية، رغم تطورها النسبي في بعض الدول، لا تزال تعاني من فجوة واضحة بين النص القانوني والواقع العملي للجرائم الإلكترونية. فهذه التشريعات غالبًا ما تعتمد على قواعد تقليدية وُضعت لمعالجة جرائم مادية محلية، في حين أن الجرائم الإلكترونية تتسم بطابع عابر للحدود، وبتقنيات متغيرة باستمرار، مما يجعل النصوص القانونية في حالة تأخر دائم عن التطور التقني. وهو ما يؤدي إلى صعوبة في التكييف القانوني لبعض الأفعال، وإلى تفاوت في تطبيق القانون من دولة إلى أخرى (الشمري، 2021).

كما أظهرت الدراسة أن إشكالية الاختصاص القضائي تُعد من أبرز التحديات التي تواجه العدالة الجنائية في هذا المجال، حيث إن تداخل عناصر الجريمة بين عدة دول يُعقّد تحديد الجهة المختصة بالملاحقة والتحقيق. وهذا الوضع يُنتج في بعض الحالات فراغًا قضائيًا أو تنازعًا بين الأنظمة القانونية، مما قد يؤدي إلى إفلات بعض الجناة من العقاب. وفي هذا السياق، يتأكد أن غياب إطار دولي موحد وفعال لا يزال يشكل عائقًا رئيسيًا أمام مكافحة الجرائم الإلكترونية (الجابري وآخرون، 2025).

ومن جهة أخرى، فإن مسألة الإثبات الجنائي الرقمي تظل من أكثر المسائل حساسية وتعقيدًا، نظرًا للطبيعة غير المادية للأدلة الإلكترونية، وإمكانية تعديلها أو حذفها بسهولة، فضلًا عن الحاجة إلى خبرات تقنية دقيقة لتحليلها. وقد بينت الدراسة أن

هذا النوع من الأدلة لا يزال يفتقر في كثير من الأنظمة القانونية إلى تنظيم دقيق يحدد شروط قبوله وحجيته أمام القضاء، مما ينعكس سلبًا على فعالية العدالة الجنائية (برادة، 2024).

كما أن التحقيق في الجرائم الإلكترونية يكشف عن حاجة ملحة إلى تطوير القدرات البشرية والتقنية للأجهزة المختصة، حيث لم يعد كافيًا الاعتماد على الوسائل التقليدية في البحث والتحقيق، بل أصبح من الضروري إدماج التكنولوجيا الحديثة في العمل القضائي والأمني. وفي هذا الإطار، يتضح أن ضعف التكوين التقني يشكل أحد أبرز نقاط الضعف في مواجهة هذا النوع من الجرائم (التومي وآخرون، 2024).

إضافة إلى ذلك، خلصت الدراسة إلى أن مكافحة الجرائم الإلكترونية لا يمكن أن تتم بمعزل عن احترام الحقوق والحريات الأساسية، وعلى رأسها الحق في الخصوصية وحرية التعبير. فالتوسع غير المنضبط في أدوات المراقبة الرقمية قد يؤدي إلى انتهاكات خطيرة، مما يستوجب وضع توازن دقيق بين متطلبات الأمن وحماية الحقوق، عبر ضمان رقابة قضائية فعالة وواضحة (بني عودة، 2024).

وبناءً على ما سبق، يمكن القول إن مواجهة الجرائم الإلكترونية تتطلب رؤية شاملة ومتكاملة، لا تقتصر على الجانب القانوني فقط، بل تشمل أيضًا الأبعاد التقنية والمؤسساتية والدولية. فالتشريع وحده لا يكفي، كما أن التكنولوجيا وحدها لا تحسم الإشكال، وإنما المطلوب هو تكامل بين هذه العناصر في إطار استراتيجية شاملة لمكافحة الجريمة في الفضاء الرقمي.

وفي ضوء هذه النتائج، يمكن التأكيد على أن مستقبل مكافحة الجرائم الإلكترونية مرهون بمدى قدرة الأنظمة القانونية على التكيف المستمر مع التطور التكنولوجي، وعلى قدرتها في بناء شراكات دولية فعالة، وتطوير أدوات التحقيق والإثبات، مع الحفاظ في الوقت ذاته على المبادئ الأساسية للعدالة الجنائية وضمان حقوق الأفراد.

وبذلك، فإن هذه الدراسة لا تدعي تقديم حلول نهائية، بقدر ما تسعى إلى إبراز تعقيد الظاهرة وتشابك أبعادها، وفتح المجال أمام المزيد من البحث والتطوير التشريعي والقضائي لمواكبة التحولات المتسارعة في العالم الرقمي.

التوصيات والاقتراحات:

بناءً على ما توصلت إليه الدراسة من نتائج تتعلق بظاهرة الجرائم الإلكترونية وحدود التشريع، وما كشفته من تحديات قانونية وتقنية ومؤسساتية في إطار القانون الجنائي، فإن معالجة هذه الظاهرة لا يمكن أن تتحقق من خلال حل واحد أو إجراء منفرد، بل تتطلب حزمة متكاملة من التوصيات التشريعية والتنظيمية والتقنية والتكوينية، على النحو الآتي:

أولًا: تحديث وتطوير التشريعات الجنائية

تُعد التشريعات الجنائية حجر الأساس في مواجهة الجرائم الإلكترونية، غير أن فعاليتها تبقى مرهونة بمدى قدرتها على مواكبة التطور التكنولوجي المستمر. وعليه، يُوصى بـ:

سن قوانين خاصة ومستقلة تُعنى حصريًا بالجرائم الإلكترونية بدل الاكتفاء بالنصوص العامة.

تحديث التعاريف القانونية المتعلقة بالجريمة الرقمية بشكل دوري بما يتماشى مع المستجدات التقنية.

إدراج صور جديدة من الجرائم المستحدثة مثل الجرائم المرتبطة بالذكاء الاصطناعي، والهجمات السيبرانية المتقدمة، واستغلال البيانات الضخمة.

توحيد المفاهيم القانونية قدر الإمكان داخل التشريعات الوطنية لتفادي الغموض والتأويل الواسع.

ويؤكد (الشمري، 2021) أن غياب النصوص الدقيقة يؤدي إلى صعوبة في التكييف القانوني وإضعاف مبدأ الشرعية الجنائية.

ثانيًا: تعزيز التعاون الدولي في مكافحة الجرائم الإلكترونية

نظرًا للطبيعة العابرة للحدود لهذه الجرائم، فإن المواجهة الفعالة تستلزم تعاونًا دوليًا واسعًا، ويتمثل ذلك في:

-الانضمام إلى الاتفاقيات الدولية الخاصة بالجرائم السيبرانية وتفعيلها بشكل عملي.

-إنشاء آليات سريعة لتبادل المعلومات بين الأجهزة القضائية والأمنية في مختلف الدول.

-تسهيل إجراءات تسليم المجرمين في الجرائم الإلكترونية دون تعقيدات بيروقراطية.

-توحيد الحد الأدنى من التجريم والعقوبات بين الدول لتفادي "الملاذات الآمنة" للمجرمين.

ويشير (الجابري وآخرون، 2025) إلى أن ضعف التنسيق الدولي يُعد من أبرز أسباب إفلات الجناة من العقاب.

ثالثًا: تطوير منظومة الإثبات الجنائي الرقمي

يُعد الإثبات الرقمي من أكثر الجوانب حساسية في الجرائم الإلكترونية، ولذلك يُوصى بـ:

-وضع معايير قانونية وتقنية موحدة لقبول الأدلة الرقمية أمام القضاء.

-إنشاء مختبرات وطنية متخصصة في الأدلة الرقمية الجنائية.

-اعتماد بروتوكولات صارمة لحفظ وتحليل البيانات الرقمية لضمان سلامتها من التلاعب.

-تكوين قضاة ووكلاء جمهورية في مجال تحليل الأدلة الإلكترونية.

وقد أكد (برادة، 2024) أن حجية الدليل الرقمي لا تزال تحتاج إلى تأطير قانوني دقيق يضمن موثوقيته أمام القضاء.

رابعًا: تعزيز القدرات البشرية والتقنية

إن مواجهة الجرائم الإلكترونية تتطلب موارد بشرية مؤهلة وتقنيات متطورة، ولذلك يُوصى بـ:

-إنشاء فرق متخصصة في التحقيق الرقمي داخل أجهزة الشرطة والقضاء.

-إدماج تخصصات الأمن السيبراني في تكوين رجال القانون.

-تنظيم دورات تدريبية مستمرة حول أحدث أساليب الجريمة الإلكترونية.

-توفير تجهيزات تقنية متطورة لرصد وتتبع الأنشطة الإجرامية عبر الإنترنت.

ويؤكد (التومي وآخرون، 2024) أن ضعف التكوين التقني يُعد من أهم العوائق أمام فعالية التحقيق الجنائي.

خامسًا: تحقيق التوازن بين الأمن الرقمي وحماية الحقوق

من الضروري عند مكافحة الجرائم الإلكترونية الحفاظ على التوازن بين متطلبات الأمن وضمان الحقوق الأساسية، ويتم ذلك عبر:

-إخضاع عمليات المراقبة الإلكترونية لإذن قضائي مسبق.

-تحديد نطاق جمع البيانات بشكل دقيق ومحدود.

-تعزيز حماية البيانات الشخصية للمستخدمين.

-منع أي استخدام تعسفي للتقنيات الرقابية.

ويشير (بني عودة، 2024) إلى أن حماية الخصوصية يجب أن تبقى مبدأً أساسيًا حتى في ظل مكافحة الجريمة الرقمية.

سادسًا: نشر الوعي الرقمي والمجتمعي

تُعد الوقاية من الجرائم الإلكترونية لا تقل أهمية عن مكافحتها، ولذلك يُوصى بـ:

-إطلاق حملات توعية حول مخاطر الاستخدام غير الآمن للإنترنت.

-إدراج الثقافة الرقمية في المناهج التعليمية.

-توعية المستخدمين بطرق الحماية من الاحتيال والاختراق.

-تشجيع الاستخدام الآمن والمسؤول للتكنولوجيا.

سابعًا: إدماج التكنولوجيا في العمل القضائي

لمواكبة التطور الرقمي، يجب تحديث منظومة العدالة عبر:

-رقمنة الإجراءات القضائية.

-استخدام الذكاء الاصطناعي في تحليل البيانات الجنائية.

-إنشاء قواعد بيانات وطنية للجرائم الإلكترونية.

-تسريع إجراءات التحقيق عبر الأنظمة الرقمية.

ثامنًا: اقتراحات بحثية مستقبلية

نظرًا لتطور هذا المجال باستمرار، يُقترح ما يلي:

-دراسة تأثير الذكاء الاصطناعي على الجريمة الإلكترونية.

-تحليل دور العملات الرقمية في الجرائم المالية.

-مقارنة فعالية التشريعات العربية في مكافحة الجرائم الإلكترونية.

-دراسة العلاقة بين الجرائم الإلكترونية والأمن القومي.

يتضح أن مكافحة الجرائم الإلكترونية تتطلب مقاربة شاملة ومتكاملة تقوم على:

-تحديث التشريع

-تعزيز التعاون الدولي

-تطوير الأدلة الرقمية

-رفع الكفاءة البشرية

-حماية الحقوق والحريات

-ونشر الوعي الرقمي

وهو ما يعكس أن المواجهة الفعالة لهذه الظاهرة لا يمكن أن تكون قانونية فقط، بل هي منظومة متكاملة تجمع بين القانون والتكنولوجيا والسياسة والتوعية المجتمعية.

قائمة المراجع :

-برادة، عبد الرزاق. (2024). الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي.

-الجابري، زايد علي ناصر، يوسف، عارف فهمي، وأحمد، نصار محمد. (2025). آليات الاستدلال والتحقيق في جرائم الإنترنت.

-بني عودة، ثائر خضر أحمد. (2024). جريمة انتحال الشخصية الإلكترونية.

-الشمري، مصطفى إبراهيم سلمان. (2021). الجرائم الإلكترونية وتأثيرها في العراق.

-التومي، حمزة محمد، امحمد، علي سعد، والزنقري، رمضان محمد. (2024). التحقيق الجنائي في الجرائم الإلكترونية.

–عرب، يونس. (2002). جرائم الكمبيوتر والإنترنت.