الصعوبات الإجرائية في مواجهة جرائم الترهيب عبر مواقع التواصل الاجتماعي

حسن جابر جاسم
باحث دكتوراه / جامعة قم الحكومية
hh2020jj2020@gmail.com

استاذ مساعد دكتور محمد علي حاجي ده آبادي
جامعة قم الحكومية/ كلية القانون/ القانون الجنائي
dr_hajidehabadi@yahoo.com

الكلمات المفتاحية: جرائم الترهيب المجتمعي، الصعوبات الإجرائية، مواقع التواصل الاجتماعي، التحقيق، التعاون الدولي، الاختصاص القضائي.

كيفية اقتباس البحث

جاسم، حسن جابر ، محمد علي حاجي ده آبادي، الصعوبات الإجرائية في مواجهة جرائم الترهيب عبر مواقع التواصل الاجتماعي، مجلة مركز بابل للدراسات الانسانية، تشرين الثاني ٢٠٢٦، المجلد:١٦ ،العدد:١١ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Procedural difficulties in confronting intimidation crimes via social media

Researcher
Hassan Jaber Jassim
PhD Researcher / Qom State University

Assistant ProfessorDr
Mohammed Ali Haji Dehabadi
Faculty of Law / Criminal Law

Keywords : Social intimidation crimes, procedural challenges, social media, investigation, international cooperation, jurisdiction.

How To Cite This Article
Jassim, Hassan Jaber, Mohammed Ali Haji Dehabadi, Procedural difficulties in confronting intimidation crimes via social media,Journal Of Babylon Center For Humanities Studies, November 2026,Volume:16,Issue 11.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract:

Social media platforms have ushered in a technological revolution that connects the East and the West. However, procedural hurdles represent a major challenge for competent authorities addressing the crime of societal intimidation via social media—particularly during the inquiry and investigation stages—as the advanced technical nature of this criminal pattern has created a procedural reality that diverges from established traditional rules of criminal procedure. The significance of this study lies in the gravity of this emerging criminal phenomenon, which exploits advanced technical capabilities to carry out acts of intimidation that are difficult to detect or trace using conventional methods, thereby posing a direct threat to social security and the safety of individuals and institutions. Addressing this topic requires a descriptive-analytical approach to Iraqi law, organized into two sections. The study

yielded several findings, including that crimes of societal intimidation can involve tangible elements—such as fraud and extortion committed via social media—and that the crimes under study possess unique technical characteristics, most notably the reliance on smart systems and algorithms capable of self-analysis and autonomous decision-making, precise victim targeting, and the use of deepfake technology. Furthermore, the study concludes that, under current penal legislation, criminal liability for societal intimidation via social media remains confined to the natural person involved in designing, programming, directing, or exploiting the system to commit the criminal act, given that social media technologies lack legal personality. Moreover, the consequences that... Social media-based social intimidation crimes—particularly non-material offenses such as fraud and extortion—pose significant evidentiary challenges. The unique nature of these crimes, rooted in a rapidly changing, intangible digital environment, creates fundamental obstacles for investigative processes—specifically regarding the collection of digital evidence, the tracking of perpetrators, and the establishment of a link between the criminal act and the offender. This reality undermines the effectiveness of traditional procedural mechanisms, necessitating the development of criminal procedural rules and the fostering of greater integration between legal expertise and technical knowledge.

مستخلص:

مثلت مواقع التواصل الاجتماعي ثورة تقنية جعلت من العالم يتلاقى في غربه وشرقه، إذ تُعد الصعوبات الإجرائية من أبرز الإشكاليات التي تواجه السلطات المختصة في التصدي لجريمة الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي ولا سيما في مرحلتي التحري والتحقيق، إذ إن الطبيعة التقنية المتقدمة لهذا النمط الإجرامي قد أفرزت واقعاً إجرائياً مغايراً لما استقرت عليه القواعد التقليدية للإجراءات الجزائية، تتمثل أهمية دراسة البحث في خطورة هذا النمط الإجرامي المستحدث، لما ينطوي عليه من استغلال للقدرات التقنية المتقدمة في تنفيذ عمليات ترهيبية يصعب كشفها أو تتبع مرتكبيها بالوسائل التقليدية، الأمر الذي يشكل تهديداً مباشراً للأمن الاجتماعي ولحماية الأفراد والمؤسسات، إن الإلمام بموضوع البحث يفرض على الباحث إتباع منهج الدراسة الوصفي التحليلي للقانون العراقي ضمن مطلبين، وتوصلنا ضمن بحثنا لنتائج ومنها، أن جرائم الترهيب الاجتماعي قد تكون ذات طابع مادي ما هو الحال في جريمة الاحتيال والابتزاز باستخدام مواقع التواصل الاجتماعي، كما تبين أن الجرائم محل الدراسة تنفرد بخصائص تقنية متميزة، أبرزها اعتمادها على أنظمة ذكية وخوارزميات قادرة على التحليل الذاتي واتخاذ قرارات مستقلة، ودقة استهداف الضحايا، واستخدام تقنيات التزييف العميق، كما

نستنتج أن المسؤولية الجزائية عن جرائم الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي لا تزال في ظل التشريعات الجزائية النافذة، منحصرة في الشخص الطبيعي الذي يتدخل في تصميم النظام أو برمجته أو توجيهه أو استغلاله في ارتكاب الفعل الجرمي، وذلك لعدم تمتع تقنيات مواقع التواصل الاجتماعي بالشخصية، كما إن الأثار التي تخلفها جرائم الترهيب الاجتماعي عبر مواقع التواصل الاجتماعي لا سيما الجرائم الخاصة بالاحتيال والابتزاز ذات طبيعة غير مادية ، وهذا ما يمثل صعوبة أمام اثبات هذا النوع من الجرائم ، كما نستنتج أن خصوصية جريمة الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي، من حيث اعتمادها على بيئة رقمية غير مادية وسريعة التغير، أفرزت تحديات جوهرية أمام أعمال التحري والتحقيق، ولا سيما في ما يتعلق بجمع الأدلة الرقمية وتتبع مرتكبي الجريمة وإثبات الصلة بين السلوك الإجرامي والفاعل ويؤدي هذا الواقع إلى إضعاف كفاءة الوسائل الإجرائية التقليدية، الأمر الذي يفرض ضرورة تطوير القواعد الإجرائية الجزائية، وتعزيز التكامل بين الخبرة القانونية والمعرفة التقنية.

مقدمة:

أولاً: موضوع البحث

تُعد الصعوبات الإجرائية من أبرز الإشكاليات التي تواجه السلطات المختصة في التصدي لجريمة الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي ولا سيما في مرحلتي التحري والتحقيق، إذ إن الطبيعة التقنية المتقدمة لهذا النمط الإجرامي قد أفرزت واقعاً إجرائياً مغايراً لما استقرت عليه القواعد التقليدية للإجراءات الجزائية، فهذه الجريمة تُرتكب في بيئة رقمية افتراضية تعتمد على أنظمة ذكية وخوارزميات متطورة، الأمر الذي يؤدي إلى تراجع المظاهر المادية للجريمة ويُضعف من فعالية الوسائل الإجرائية التقليدية في الكشف عنها وجمع أدلتها، كما أن اعتماد الجناة على تقنيات الذكاء الاصطناعي ضمن مواقع التواصل الاجتماعي في تنفيذ الأفعال الاحتيالية، كالأتمتة، وتقنيات التزييف الرقمي، يخلق تحديات إجرائية متزايدة أمام جهات التحقيق، لاسيما في ظل محدودية المعرفة الفنية لدى القائمين على التحري ونقص الخبرة المتخصصة في التعامل مع الأدلة الرقمية الناتجة عن الأنظمة الذكية ، ويُضاف إلى ذلك أن طبيعة الجريمة ذاتها القائمة على العمل في فضاءات رقمية معقدة تُفضي إلى صعوبات ملموسة في تتبع السلوك الإجرامي واستخلاص الأدلة، الأمر الذي ينعكس سلباً على سلامة إجراءات التحقيق، كما يُلاحظ أن القواعد الإجرائية السائدة وُضعت أساساً للتعامل مع أنماط إجرامية تقليدية تقوم على الوجود المادي المباشر وهو ما يجعلها غير كافية في استيعاب الجرائم المعتمدة

على الأنظمة الذكية والتقنيات الرقمية المتقدمة، الأمر الذي يفرض الحاجة إلى تطوير آليات التحري والتحقيق بما ينسجم مع خصوصية البيئة الرقمية الحديثة وبجانب الصعوبات الإجرائية المحلية تبرز تحديات كبيرة على صعيد التعاون الدولي، إذ تصطدم الدول بعقبات في تنسيق جهود السلطات القضائية وتبادل الأدلة الرقمية وتعقب الجناة عبر الحدود فضلاً عن تنازع الاختصاص القضائي.

ثانياً: أهمية البحث

تتمثل أهمية دراسة البحث في خطورة هذا النمط الإجرامي المستحدث، لما ينطوي عليه من استغلال للقدرات التقنية المتقدمة في تنفيذ عمليات ترهيبية يصعب كشفها أو تتبع مرتكبيها بالوسائل التقليدية، الأمر الذي يشكل تهديداً مباشراً للأمن الاجتماعي ولحماية الأفراد والمؤسسات، فضلاً عن الكشف عن ضرورة وضع أطر قانونية فعالة قادرة على الحد من مخاطرها ومعالجة صورها المستحدثة وضمان تحقيق الحماية الجنائية اللازمة للأفراد.

ثالثاً: إشكالية البحث

إن إشكالية البحث تتجسد في التساؤلات الآتية:

١- ما الصعوبات الموضوعية التي تعترض التنظيم القانوني لجريمة الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي ولاسيما إشكالية إسناد المسؤولية الجزائية في ظل تدخل الأنظمة الذكية وتعدد أطرافها؟.

٢- ما أبرز الصعوبات الإجرائية التي تواجه جهات التحري والتحقيق في جمع الأدلة الرقمية وإثبات جريمة الترهيب المجتمعي عبر مواقع التواصل الاجتماعي؟

٣- إلى أي مدى يؤثر الطابع العابر للحدود لهذه الجريمة في مسألة الاختصاص القضائي وتنازع القوانين؟ .

٣- إلى أي مدى تسهم آليات التعاون الدولي القائمة في مواجهة الطابع العابر للحدود لجريمة الترهيب المجتمعي عبر مواقع التواصل الاجتماعي، وهل تستجيب لمتطلبات خصوصية هذا النمط من الجرائم؟.

رابعاً منهجية البحث

إن الإلمام بموضوع البحث يفرض على الباحث إتباع منهج الدراسة الوصفي التحليلي للقانون العراقي.

خامساً: خطة البحث

بناءً على تقدم ذكره بخصوص موضوع البحث سنقسم خطة البحث إلى مطلبين، يُخصص المطلب الأول لبيان المعوقات التي تواجه جهات التحقيق والتحري في التعامل مع جريمة الاحتيال باستخدام تقنيات الذكاء الاصطناعي، فيما يتناول المطلب الثاني صعوبات التعاون الدولي في مواجهة الجريمة .

المطلب الأول: المعوقات المتعلقة بجهات التحقيق والتحري

تُعد جهات التحقيق الركيزة الأساسية في تفعيل قواعد العدالة، إذ يقع على عاتقها عبء كشف الجريمة، وجمع أدلتها وتحديد مرتكبيها تمهيداً لمساءلتهم وفقاً لأحكام القانون، غير أن هذا الدور يواجه تحديات متزايدة ما هو الحال عند التعامل مع جريمة الاحتيال باستخدام تقنيات مواقع التواصل الاجتماعي لما تنطوي عليه من خصوصية تقنية وتعقيد إجرائي يخرج في كثير من الأحيان عن الإطار التقليدي للتحقيق الجزائي ، فطبيعة هذه الجريمة التي تُرتكب في بيئة رقمية تعتمد على أنظمة ذكية وخوارزميات متطورة تفرض على سلطات التحقيق متطلبات فنية ومعرفية خاصة قد لا تتوافر بالقدر الكافي في الواقع العملي.

وتبرز المعوقات المتعلقة بجهات التحقيق بوصفها من أهم الإشكالات الإجرائية في هذا المجال، إذ تتجلى في محدودية الإلمام التقني بآليات عمل تقنيات مواقع التواصل الاجتماعي، وضعف الخبرة المتخصصة في التعامل مع الأدلة الرقمية المعقدة، فضلاً عن الاعتماد المستمر على أساليب تحري وتحقيق تقليدية لا تتلاءم مع طبيعة الجرائم الذكية ويترتب على ذلك قصور في القدرة على تتبع السلوك الإجرامي[١]، أو تحليل الأدلة الرقمية أو استيعاب الكيفية التي تُوظف بها الأنظمة الذكية في ارتكاب الفعل الاحتيالي، وبناءً على ما سبق سنقسم هذا المطلب إلى فرعين: نبين في الفرع الأول نقص المعرفة الفنية والخبرة التقنية لدى سلطات التحقيق، بينما يتناول الفرع الثاني التحديات المتعلقة بصعوبة التحري والتحقيق في البيئة الرقمية والتعامل مع الكم الهائل من البيانات الناتجة عن العمليات الاحتيالية الذكية.

الفرع الأول: نقص المعرفة الفنية والخبرة التقنية لدى سلطات التحقيق

يعد نقص الخبرة والمعرفة التقنية لدى الجهات المختصة بالتحقيق في الجرائم الرقمية، وخصوصاً جرائم الاحتيال باستخدام مواقع التواصل الاجتماعي من أبرز التحديات والإشكالات التي تواجه تطبيق العدالة فهذه الجرائم بطبيعتها معتمدة على أساليب رقمية متطورة وخوارزميات ذكية، ما يجعل جمع الأدلة وتحليلها واستنباطها عملية معقدة للغاية، تتطلب خبرة تقنية وقانونية متوازنة لا تتوفر دوماً في الأجهزة التحقيقية التقليدية [٢]علاوة على ذلك، فإن سرعة التطور التكنولوجي

المستمرة تشكل ضغطاً مستمراً على خبراء الأدلة الجنائية الرقمية والمحاكم على حد سواء، مما يصعب عليهما مواكبة أحدث الوسائل التقنية وأدوات الذكاء الاصطناعي المستخدمة في ارتكاب الجرائم ويؤثر على قبول الأدلة الرقمية في المسار القانوني نتيجة غياب المعايير واللوائح الدقيقة للتعامل معها ، وتتجلى آثار هذا النقص بشكل واضح في القدرة المحدودة لرجال القانون والمحاكم على فهم طبيعة الأدلة الرقمية والتي غالباً ما تشمل مفاهيم تقنية دقيقة مثل التشفير[٣]، وسجلات الدخول، والبصمات الرقمية، وتحليل البيانات الكبيرة، فغياب المعرفة المتخصصة بهذه العناصر يؤدي إلى عدم القدرة على تقييم مدى حجية الأدلة الرقمية، ويحد من إمكانية ربطها بالوقائع القانونية للجريمة، ما يؤدي إلى ضعف في تكوين القناعة القضائية حول المسؤولية الجزائية للمتهم كما أن الاعتماد على أساليب وتحقيق تقليدية يضاعف من صعوبة التعامل مع الجرائم الرقمية، نظراً لأن هذه الأساليب لا تتلاءم مع البيئة الافتراضية المعقدة التي تتم فيها جرائم الاحتيال عبر مواقع التواصل الاجتماعي، والتي غالباً ما تشمل أنظمة خوارزمية متطورة تعمل بشكل شبه مستقل، ما يجعل تحديد مرتكبي الجريمة أو تتبع أثرهم تحدياً كبيراً ويظهر هذا النقص أيضاً في عدم قدرة المحققين على التعامل مع الأدوات الرقمية الحديثة وعدم إلمامهم بـ"اللغة العلمية الرقمية" أو استيعاب طبيعة الجرائم التي تُرتكب باستخدام الذكاء الاصطناعي، حيث يمتلك الجناة غالباً معرفة تقنية متقدمة تمكنهم من إخفاء الأدلة الرقمية أو تزييفها، ما يزيد من صعوبة التحقيق ويعزز احتمالية إفلاتهم من العقاب [٤] وعليه نرى أن هذا الواقع يؤكد الحاجة الماسة إلى دمج خبرة قانونية وتقنية في فرق التحقيق بحيث تضم مختصين في علوم الحاسوب وتقنيات الذكاء الاصطناعي، إلى جانب محققين قانونيين ذوي خبرة جنائية، لضمان القدرة على تحليل الأدلة الرقمية بشكل صحيح بما يضمن سلامة الإجراءات القضائية، ومن جهة أخرى تُعد قلة الإلمام الفني والمعرفي بآليات التعامل مع الجرائم الإلكترونية، لا سيما جرائم الاحتيال وجرائم الابتزاز باستخدام مواقع التواصل الاجتماعي، من أبرز التحديات التي تواجه جهات التحقيق، إذ يفتقر العديد من المحققين والقضاة إلى التدريب المتخصص الذي يمكنهم من استيعاب طبيعة هذه الجرائم وأساليب ارتكابها، ما يضعف قدرتهم على جمع الأدلة الرقمية وتحليلها وتقييم حجيتها القانونية، خصوصاً أن هذه الأدلة تستند إلى معطيات تقنية دقيقة لا يغطيها الإعداد القانوني التقليدي [٥] ويبرز هذا النقص الحاجة إلى تبني استراتيجيات متكاملة تجمع بين التأهيل القانوني والتقني وتطوير وحدات متخصصة للتعامل مع الأدلة الرقمية المعقدة، إضافة إلى تعزيز الخبرة الرقمية المتخصصة لتمكين الجهات القضائية من التحقق من صحة الأدلة [٦].

وبناءً على ما سبق يتضح أن نقص الخبرة والمعرفة الفنية يمثل من أهم المعوقات التي تواجه الجهات المختصة بالتحقيق في جرائم مواقع التواصل الاجتماعي التي تخلق توتر ورهبة في المجتمع، ويترتب عليه قصور في القدرة على جمع الأدلة، وتحليلها، وربطها بالمسؤولية الجزائية، وهو ما يستدعي بذل جهود مستمرة لتطوير الكفاءات الفنية والقانونية، وتكوين فرق تحقيق متخصصة، بما يضمن فعالية التحقيق والعدالة في مواجهة هذه الجرائم المعقدة، أذ يعد إجراء الخبرة في الجرائم المعلوماتية بصورة عامة من أهم الإجراءات التي يجب على قاضي التحقيق والمحقق الجنائي القيام بها، إذ أن الاستعانة بالخبير تكون في غاية الأهمية في مثل هذه الجرائم التي ترتكب بدقة واحترافية عالية ولا يمكن اكتشافها إلا من قبل ذوي الخبرة والاختصاص[٧].

وتتميز الخبرة القضائية عن بقية إجراءات التحري والتحقيق الابتدائي من خلال الرأي الفني الذي يقدمه الخبير في كشف المحتوى المزيف عن الحقيقي، وتجري الخبرة [٨] بواسطة شخص يسمى الخبير، وتعد الجريمة محل الدراسة من الجرائم ذات الطبيعة الفنية والعلمية المعقدة، لأنها ترتكب باستخدام خوارزميات الذكاء الاصطناعي، وهذا ما يستدعي خبرة فنية للتأكد من الأدلة المعنوية مثل الصور أو التسجيلات الصوتية والفيديوهات التي تم ضبطها [٩] إذ تعد الخبرة تقييماً فنياً للأدلة المتحصلة حول الجريمة الواقعة، وتعتبر عنصراً أساسياً في التحقيق الابتدائي، حيث يوضح تقرير الخبير كيفية ارتكاب الجريمة وما هي البرامج المستخدمة فيها، وما إذا كان المحتوى مزيف فعلياً ، مما يجعل تقرير الخبير أحد الركائز التي يبني عليها القاضي قناعته القضائية [١٠] ولذا يشترط في الخبير مجموعة من الشروط الأساسية، أبرزها: ١- الإلمام بالبرمجيات وخوارزميات الذكاء الاصطناعي، بحيث يكون على دراية كاملة ببرامج الحاسوب والتطبيقات الرقمية المستخدمة في ارتكاب الجرائم الإلكترونية [١١]،٢- القدرة على فهم وتحليل خوارزميات الذكاء الاصطناعي المستخدمة في الاحتيال الرقمي، إضافة إلى الخبرة العملية والقدرة التقنية، بما يشمل المعرفة التفصيلية بأنظمة التشغيل وشبكات الإنترنت. ٣-القدرة على التعامل مع المعالجة الآلية للحواسيب، ونقل الأدلة الرقمية بطريقة تحفظ سلامتها وتمنع تلفها أو العبث بها. ٤- الالتزام بالقوانين واللوائح، بما في ذلك التقيد بأحكام قانون الإجراءات الجزائية وقوانين الإثبات وقانون مكافحة الجرائم المعلوماتية، واحترام جميع النصوص القانونية ذات الصلة أثناء جمع الأدلة وتقييمها، ومتابعة ظروف الجريمة بالكامل منذ لحظة ارتكابها وحتى اكتشافها، وفهم دوافع الجاني وأهدافه من ارتكاب الاحتيال باستخدام تقنيات الذكاء الاصطناعي، ٥- الاستمرار في الاطلاع على مستجدات التكنولوجيا والعلوم الحديثة، خصوصاً المتعلقة بالأمن السيبراني، والقدرة على تطبيق التقنيات الحديثة لمواجهة أساليب الاحتيال المتطورة[١٢].

ومن الأدوات التقنية الحديثة التي تساعد الخبراء في اكتشاف المحتوى المزيف، تأتي منصة سينتل (Sentinel) التي تعتمد على خوارزميات الذكاء الاصطناعي لتحليل الصور والفيديوهات الرقمية وإصدار تقارير دقيقة حول صحتها، ويستخدمها عدد من المنظمات الأوروبية الرائدة، إضافة إلى تطبيق فيك كاتجر (Fake Catcher) المطور من شركة إنتل بالتعاون مع جامعة ولاية نيويورك، والذي يعتمد على تقنية تدفق الدم في الوجه لتحليل الفيديوهات وكشف المزيف منها بدقة تصل إلى ٩٦% باستخدام التعلم العميق، وكذلك تقنية فونيم–فيسيمي (Phoneme–Viseme) المطورة من جامعات ستانفورد وكاليفورنيا، والتي تركز على كشف التناقض بين حركة الفم والكلمات المنطوقة لتحديد مدى مطابقة الفيديو للواقع وتعكس هذه المنصات والتقنيات التكامل بين الخبرة الفنية والأدوات الرقمية الحديثة لضمان كشف الحقيقة وتقديم أدلة دقيقة تدعم التحقيق القضائي [١٣].

الفرع الثاني: صعوبة التحري والتحقيق في البيئة الرقمية

يُعد التحري والتحقيق في الجرائم المرتكبة داخل البيئة الرقمية من أكثر المراحل الإجرائية تعقيداً وإثارة للإشكاليات القانونية والفنية، ولا سيما في ظل التطور المتسارع لتقنيات تكنولوجيا المعلومات وما أفرزته من أنماط إجرامية مستحدثة يأتي في مقدمتها الاحتيال باستخدام تقنيات مواقع التواصل الاجتماعي، فهذه الجرائم لا تنشأ في إطار مادي تقليدي يمكن معاينته بالحواس البشرية وإنما تقع ضمن بيئة رقمية كامنةُ[١٤] تتداخل فيه البيانات الرقمية، والخوارزميات الذكية، والأنظمة المؤتمتة[١٥] بما يجعل من مهمة سلطات التحري والتحقيق استخدام أدوات وأساليب تختلف جوهرياً عن تلك المعتمدة في الجرائم التقليدية [١٦]،الأمر الذي يستلزم تبني نهج تحقيقي تكاملي يقوم على دمج الممارسات التحقيقية التقليدية بالكفاءة الرقمية المتخصصة، بما يسمح بالربط بين العالمين المادي والافتراضي واستثمار الأدلة الرقمية والتقليدية معاً في إطار تحليلي شامل يعزز فعالية أعمال التحقيق[١٧]، إذ أن خصوصية البيئة الرقمية تفرض واقعاً إجرائياً مغايراً إذ لم يعد مسرح الجريمة مقصوراً على مكان جغرافي محدد، بل أصبح يمتد عبر شبكات إلكترونية مفتوحة، وخوادم سحابية، ومنصات التواصل الاجتماعي، وتطبيقات تعتمد على الذكاء الاصطناعي، تعمل في كثير من الأحيان ضمن بيئة تقنية عابرة للحدود وهو ما يجعل مسرح الجريمة الرقمية فضاء ديناميكياً ومعقداً يختلف جوهرياً عن مسرح الجريمة المادي، ويتطلب خبرات فنية متخصصة في مجال الأدلة الجنائية الرقمية لضمان دقة جمع الأدلة الرقمية وحفظها وتحليلها وفق معايير علمية واضحة ، مما يترتب على ذلك صعوبة تحديد نطاق الاختصاص المكاني، فضلاً عن الإشكالات المرتبطة بتحديد مكان ارتكاب الجريمة ، ويزداد تعقيد أعمال

التحري[١٨] والتحقيق بسبب الطبيعة غير الملموسة للدليل الرقمي، إذ يتكون هذا الدليل من بيانات ومعلومات إلكترونية لا تُدرك بالحواس الطبيعية، وإنما تظهر في صورة إشارات أو نبضات مغناطيسية أي رقمية [١٩] لا يمكن الوصول إليها أو تحليلها إلا بواسطة أدوات وبرمجيات تقنية متخصصة، أذ لا يترك الجاني في الغالب آثاراً مادية تقليدية كما هو الحال في الجرائم الواقعة على الأشخاص التي فيها للمحققين معاينةُ مسرح الجريمةُ وضبط الأدلة .

وفي سياق جرائم الاحتيال المعتمدة على مواقع التواصل الاجتماعي، تتفاقم هذه الإشكالية بشكل أوضح، إذ أن الجناة يوظفون تقنيات متقدمة، مثل التزييف العميق، والروبوتات الذكية، وخوارزميات التعلم الآلي، لإنتاج محتوى احتيالي عالي الدقة يصعب تمييزه عن المحتوى الحقيقي، كما تُستخدم هذه التقنيات في التلاعب بالصور أو الأصوات أو البيانات أو في محاكاة سلوكيات بشرية ،مما يؤدي هذا إلى تضليل الضحايا من جهة، وإرباك سلطات التحري والتحقيق من جهة أخرى، ومن أبرز الصعوبات التي تواجه جهات التحقيق في هذا المجال، سهولة إخفاء الأدلة الرقمية أو محوها أو التلاعب بها في وقت قصير[٢٠]، إذ يستطيع الجاني باستخدام وسائل تقنية متاحة نسبياً حذف سجلات النظام، أو تشفير البيانات، أو الاعتماد على برامج إخفاء الهوية والشبكات الافتراضية الخاصة، أو استغلال خصائص النسخ الاحتياطي وتكرار البيانات داخل البيئات السحابية ولا يقتصر الأمر على ذلك، بل قد يلجأ بعض الجناة إلى استخدام تقنيات مضادة للأدلة الجنائية الرقمية، تهدف إلى تضليل المحققين، أو عرقلة عملية التحليل الفني[٢١] أو إظهار الأفعال الإجرامية وكأنها ناتجة عن خلل تقني أو خطأ في النظام، لا عن سلوك إجرامي متعمد، ومن أبرز هذه التقنيات هي حذف أداوت التتبع [٢٢].

كما يواجه المحققون تحدي أخر يتمثل في الكم الهائل من البيانات الرقمية المطلوب فحصها وتحليلها، إذ يتطلب الوصول إلى دليل تمحيص آلاف الملفات والسجلات الرقمية المخزنة على الأجهزة، أو الخوادم، أو منصات التخزين السحابي، لاسيما في ظل النمو المتسارع لحجم البيانات الرقمية وتزايد تعقيد نظم تخزينها وتشفيرها[٢٣]، الأمر الذي يفرض على القائمين بالتحقيق تطوير مهاراتهم الفنية بصورة مستمرة لمواكبة التقنيات والأنماط الإجرامية المستحدثة وتتضاعف هذه الصعوبات عندما تكون الأدلة الرقمية محل التحقيق موجودة ضمن بيئات الحوسبة السحابية، حيث تبرز إشكالات قانونية معاصرة تتعلق بمسألة الإقليمية (فقدان الموقع)، وملكية البيانات، وحيازة الدليل (ملكية المحتوى الحسابيَ)، وإجراءات الضبط والمصادرة، فضلاً عن صعوبات التحقق من هوية المستخدم الحقيقي القائم بالفعل الإجرامي، ومن ناحية أخرى أن محدودية الكفاءات البشرية المؤهلة تقنياً تمثل عائقاً أمام فعالية التحري والتحقيق في الجرائم

الرقمية، إذ يتطلب التعامل مع الأدلة الرقمية مستوى عالياً من الخبرة الفنية والمعرفة المتخصصة في مجالات التحليل الرقمي ،وفي ظل النقص الذي تعاني منه بعض الأنظمة القضائية في هذا المجال، قد يؤدي ذلك إلى ضعف في جمع الأدلة أو تقييمها أو عرضها أمام القضاء مما ينعكس سلباً على الإجراءات[٢٤] .

وانطلاقاً من تعدد الصعوبات التي تعترض إجراءات التحري والتحقيق في الجرائم الرقمية، ولا سيما جرائم الاحتيال باستخدام تقنيات الذكاء الاصطناعي، تبرز الحاجة إلى اعتماد وسائل إجرائية حديثة تتلاءم مع طبيعة البيئة الرقمية وخصوصيتها المتغيرة، وفي هذا الاطار يُعد اللجوء إلى المراقبة الإلكترونية [٢٥] وسيلة فعالة لرصد الأنشطة المشبوهة في الفضاء الرقمي من خلال تتبع حركة البيانات وتحليل أنماط الاستخدام غير الاعتيادية، بما يسهم في كشف السلوك الإجرامي قبل اكتماله أو أثناء ارتكابه ، كما يشكل اعتراض المراسلات الرقمية أداة إجرائية مهمة في دعم التحقيق الجنائي، لما يوفره من معطيات تقنية تتعلق بمسارات الاتصال وتوقيتاته والأطراف المتداخلة فيه، الأمر الذي يساعد على تحديد الصلة بين الجاني والفعل الإجرامي، خاصة في الجرائم التي تُرتكب عن بُعد ويغيب فيها الاتصال المادي المباشر[٢٦]، وإلى جانب ذلك يبرز دور تقنيات الذكاء الاصطناعي في التحليل والكشف، إذ يمكن على الرغم من استخدامها في ارتكاب الجريمة ذاتها، توظيفها بصورة معاكسة لكشف المحتوى الاحتيالي وتحليل البيانات الضخمة واستخلاص الأنماط الإجرامية الخفية، بما يعزز من كفاءة أعمال التحري والتحقيق [٢٧]، إذ تسهم هذه الوسائل في تجاوز إشكالات فقدان الموقع، وضخامة البيانات، والطبيعة غير المرئية للأدلة الرقمية، بما يسمح بإعادة بناء الوقائع الإجرامية وتعزيز القدرة على الإثبات، شريطة أن تُمارس ضمن إطار قانوني منضبط يراعي الضمانات الدستورية ويحافظ على الحقوق والحريات الفردية.

وفي ضوء ما تقدم يتضح أن صعوبة التحري والتحقيق في البيئة الرقمية لا ترجع إلى عامل منفرد، بل هي نتيجة تفاعل معقد بين الطبيعة غير المادية للدليل الرقمي، والتطور المتسارع للتقنيات الذكية وضخامة البيانات والتحديات القانونية العابرة للحدود، فضلاً عن قصور المعرفة الفنية وضعف الخبرة التقنية لدى القائمين على أعمال التحري والتحقيق، وعليه نرى أن جرائم الاحتيال والابتزاز وبث الأخبار الكاذبة باستخدام مواقع التواصل الاجتماعي تفرض على المشرع وسلطات التحقيق إعادة النظر في الآليات الإجرائية التقليدية، واعتماد مقاربات أكثر تكاملاً تجمع بين الخبرة القانونية والكفاءة التقنية، بما يضمن فعالية التحري والتحقيق ويحقق التوازن بين مقتضيات مكافحة الجريمة الرقمية وحماية الحقوق والحريات الفردية.

المطلب الثاني: صعوبات التعاون الدولي في مواجهة الجريمة

أدى التوسع المتسارع في استخدام الفضاء الإلكتروني إلى نشوء علاقات قانونية جديدة تتجاوز الحدود الإقليمية التقليدية، ما أفرز تحديات جسيمة أمام النظم القضائية الوطنية، ويعد تنازع الاختصاص القضائي أبرز هذه التحديات، إذ ينشأ من تداخل القوانين الوطنية عند معالجة الأنشطة الرقمية العابرة للحدود، سواء تعلق الأمر بالجرائم السيبرانية أو الانتهاكات الرقمية أو المعاملات الإلكترونية، وتتمثل الإشكالية الرئيسة في صعوبة تحديد المحكمة المختصة مكانياً ونوعياً في بيئة لا تعترف بالحدود الإقليمية، ما يحول هذه المسألة إلى نقطة محورية لضمان حماية الحقوق القانونية وتطبيق القانون بفعالية، ويتطلب التوفيق بين مبادئ السيادة الوطنية ومتطلبات التعاون القضائي الدولي لضمان محاسبة الجناة [٢٨].

وفي الوقت ذاته أدى التسارع الهائل في التطور التكنولوجي واتساع استخدام الفضاء الإلكتروني إلى تصاعد معدلات الجرائم الإلكترونية ولاسيما تلك التي تتم عبر منصات التواصل الاجتماعي وتنوع صورها، بما يشكل تهديداً حقيقياً للأمن الاقتصادي والاجتماعي والسياسي للدول، وجعل التعاون الدولي ضرورة لا غنى عنها لمواجهتها والحد من آثارها ورغم جهود الدول التشريعية والأمنية وإبرام اتفاقيات دولية لتعزيز التعاون القضائي والأمني، يواجه هذا التعاون جملة من الصعوبات العملية، أبرزها ضعف آليات تبادل الأدلة الرقمية وتعقب الجناة، وبطء الإجراءات، واصطدامها بمبادئ السيادة الوطنية وحدود الولاية القضائية، مما يحد من فعالية مكافحة الجرائم الإلكترونية ويفتح المجال أمام إفلات مرتكبيها من المساءلة.

وبناءً على ذلك سنقسم هذا المطلب الى فرعين، يُخصص الفرع الأول لبيان إشكالية تنازع الاختصاص القضائي، فيما يتناول الفرع الثاني مظاهر ضعف آليات التعاون الدولي، ولاسيما في مجال تبادل الأدلة وتتبع الجناة، وآثار ذلك على فاعلية مكافحة هذا النوع من الجرائم.

الفرع الأول: إشكالية تنازع الاختصاص القضائي

إن التطورات التكنولوجية الحديثة أحدثت نقلة نوعية في طبيعة الفضاء الإلكتروني، إذ أصبح هذا الفضاء العالمي بيئة افتراضية لا تخضع للحدود الجغرافية التقليدية ويتيح التدفق غير المحدود للمعلومات والبيانات عبر شبكة الإنترنت، ما أضفى ديناميكية كبيرة على العلاقات بين الدول والمجتمعات، وسهل تبادل المعلومات في مختلف الميادين الاقتصادية والاجتماعية والثقافية، ومع ذلك فإن هذه الطبيعة العالمية للفضاء الرقمي أفرزت تحديات قانونية وقضائية غير مسبوقة أبرزها الإشكالية المرتبطة بتحديد المحكمة المختصة للنظر في النزاعات والجرائم العابرة للحدود، خاصة في ظل اختلاف التشريعات المحلية والدولية، وغياب إطار قانوني موحد ينظم التعامل مع

هذه القضايا [٢٩]، إذ أن النشاط البشري الذي انتشر في الفضاء الإلكتروني أنتج وقائع قانونية عابرة للحدود يصعب إخضاعها لقواعد الاختصاص القضائي التقليدية، التي استندت إلى معايير الإقليم، والشخص، ومكان وقوع الفعل أو الضرر، فبيئة الإنترنت بطابعها الافتراضي وغير المادي خلخلت المفاهيم التقليدية للاختصاص القضائي، وطرحت إشكالات متزايدة بشأن الجهة القضائية المختصة، ويُعزى تنازع الاختصاص في هذه البيئة إلى عوامل متشابكة، من أبرزها الطبيعة اللامركزية للفضاء الرقمي، وتعدد الروابط الممكنة بالنزاع، وتباين المعايير القانونية بين الدول، بالإضافة إلى عدم وجود آليات دولية فعالة لتنسيق هذه الاختصاصات[٣٠].

ويُعرف الاختصاص القضائي على أنه السلطة أو القدرة التي تتمتع بها المحكمة للبت في القضايا وفق معايير قانونية محددة، مثل مكان وقوع الجريمة أو إقامة الأطراف وفي النظم التقليدية يكون الاختصاص غالباً محلياً مرتبطاً بالحدود الجغرافية للدولة غير أن هذه المعايير تصبح غير كافية في الفضاء الرقمي إذ يمكن أن تتداخل القوانين والأنظمة القضائية وبالتالي، يصبح لكل محكمة نصيب من الولاية يخولها مباشرة الدعاوى المنظورة أمامها وبسط سلطانها القانوني على الوقائع المتصلة بها [٣١].

وتتجلى إشكالية تنازع الاختصاص القضائي بصورة أوضح عند تطبيقها على بعض صور الجرائم المعلوماتية المستحدثة وخاصة تلك الخاصة بمواقع التواصل الاجتماعي، ومنها جريمة الاحتيال والابتزاز ونشر الأخبار الكاذبة باستخدام مواقع التواصل الاجتماعي، التي تُعد من الجرائم الرقمية العابرة للحدود، فهذه الجريمة لا ترتبط بجنسية معينة أو فئة عمرية محددة، بل قد تطال ضحايا من مختلف الدول والمجتمعات، الأمر الذي يُضفي عليها بعداً دولياً واضحاً، ويجعل من الصعب حصرها ضمن نطاق اختصاص قضائي وطني واحد، ويؤدي هذا الطابع العابر للحدود إلى خضوع الجريمة لأكثر من أساس من أسس الاختصاص الجنائي في آن واحد ،فإذا ارتُكبت الجريمة داخل إقليم دولة معينة من قبل شخص أجنبي، انعقد الاختصاص لتلك الدولة استناداً إلى مبدأ الإقليمية، باعتباره المبدأ التقليدي الذي يمنح الدولة سلطة ملاحقة الجرائم الواقعة داخل حدودها ،وفي الوقت ذاته، قد تنعقد الولاية القضائية لدولة أخرى على أساس مبدأ الاختصاص الشخصي، متى كان الجاني أو المجنى عليه من رعاياها، كما قد يثور مبدأ الاختصاص العيني إذا ما ترتب على الجريمة تهديد لأمن دولة أو مساسٌ بمصالحها الجوهرية [٣٢]، غير أن اجتماع هذه المبادئ، بدلاً من أن يؤدي إلى تكاملها يفضي في كثير من الأحيان إلى تنازع إيجابي في الاختصاص، تتنافس فيه عدة دول على ملاحقة الجريمة أو إلى تنازع

سلبي قد تنأى فيه الدول عن تحمل عبء المتابعة، بما يفتح المجال أمام إفلات الجناة من العقاب [٣٣] .

وعليه من أجل حل هذه المشكلة يجب أن تتبنى الدول مبدأ الاختصاص القضائي الجنائي العالمي كأحد الحلول القانونية الممكنة لمعالجة هذا الخلل، ويقوم مبدأ الاختصاص القضائي العالمي على إقرار حق الدولة في ملاحقة ومعاقبة مرتكبي بعض الجرائم الخطيرة، بغض النظر عن مكان ارتكابها أو جنسية الجاني أو الضحية، تأسيساً على فكرة التضامن الدولي وحماية المصلحة العامة للمجتمع الدولي ،ويُنظر إلى هذا المبدأ بوصفه مكملاً لبقية مبادئ الاختصاص الجنائي، لا بديلاً عنها [٣٤]، ويستند مبدأ الاختصاص القضائي العالمي إلى فكرة التضامن الدولي بين الدول، اذ يهدف إلى منع إفلات مرتكبي الجرائم الخطرة من العقاب وتحقيق المصلحة العامة للمجتمع الدولي، وقد عرف هذا المبدأ بأنه: "صلاحية تقررت للقضاء الوطني في ملاحقة ومحاكمة مرتكبي انواع معينة من الجرائم التي يحددها التشريع الوطني دون النظر إلى لمكان ارتكابها ودون اشتراط توافر ارتباط معين يجمع بين الدولة وبين مرتكبيها أو ضحاياها، فيصبح تحديد نطاق اقليم الدولة أو تحديد مكان وقوع الجريمة أو النظر إلى جنسية مرتكبيها غير ذي جدوى" [٣٥]، إذ أن تبني مبدأ الاختصاص القضائي العالمي يأتي استجابة للإشكالات التي يثيرها مبدأ الاختصاص الإقليمي، إذ على الرغم من انسجام هذا الأخير مع متطلبات السيادة الإقليمية لكل دولة، إلا أنه أصبح في ظل التطور المتسارع للعالم الرقمي وتزايد انتشار الجرائم المعلوماتية، غير كافٍ لمواجهة المخاطر التي تهدد المجتمع الدولي، ومن ثم تبرز ضرورة إضفاء ولاية عامة لمبدأ الاختصاص القضائي العالمي على الجرائم الخطرة ذات الطابع العابر للحدود، بما يضمن ملاحقة مرتكبيها وعدم إفلاتهم من العقاب[٣٦]، وقد تبنى المشرع العراقي مبدأ الاختصاص الشامل من خلال إخضاع كل من يوجد داخل إقليم الدولة للمساءلة عن جريمة ارتكبها خارج البلاد بصفته فاعلاً أو شريكاً فيها [٣٧] كما تبنى المشرع الإماراتي، إذ نص على سريان أحكامه على كل من يرتكب فعلا خارج الدولة يجعله فاعلا أو شريكاً في جريمة وقعت كلها أو بعضها داخل إقليمها[٣٨]، وكذلك المشرع الإيطالي وفق المادة (٨) من قانون العقوبات رقم ١٣٩٨ لسنة ١٩٣٠ المعدل .

وفي ضوء ما تقدم نستخلص أن جريمة الاحتيال والابتزاز ونشر الأخبار الكاذبة باستخدام مواقع التواصل الاجتماعي من الجرائم الجسيمة والعابرة للحدود وأن مبدا الاختصاص القضائي العالمي يعد أحد الحلول القانونية الفعالة التي ينبغي للدول تبنيها لملاحقة مرتكبي هذه الجرائم بما يضمن منع افلاتهم من العقاب مع الحفاظ على سيادة الدولة.

الفرع الثاني: ضعف آليات التعاون الدولي في تبادل الأدلة وتتبع الجناة

أضحى التعاون الدولي ضرورة حتمية لمكافحة الجرائم العابرة للحدود، إذ أثبت الواقع العملي أن أي دولة مهما بلغت قدراتها التشريعية أو الأمنية أو القضائية لا تستطيع وحدها التصدي لهذه الجرائم المعقدة والمتطورة تكنولوجياً، ومع انتشار شبكات الاتصال والتواصل الرقمي التي تنقل البيانات والمعلومات عبر مسافات واسعة باستخدام تقنيات لا توفر ضمانات أمنية كاملة، تصدرت الجرائم الإلكترونية معدلات الجرائم العابرة للحدود، وبدأت تمثل تهديداً مباشراً للأمن الاقتصادي والاجتماعي والسياسي على المستوى الدولي[٣٩]، إذ أن التطور السريع لتكنولوجيا المعلومات والاتصالات، بما في ذلك استخدام الذكاء الاصطناعي وأدوات التزييف العميق (Deepfake)، أسهم في تعقيد أبعاد هذه الجرائم، وجعل من الصعب على التشريعات الوطنية مواكبتها بمفردها ،لذلك لم يعد امتلاك الدول للقوانين والإمكانات الأمنية والقضائية فقط كافياً، بل أصبح التنسيق والتجانس بين التشريعات والممارسات القضائية في مختلف الدول أمراً جوهرياً، لحماية مصالح دولية مشتركة وضمان فعالية الإجراءات القانونية في مواجهة هذه الجرائم ،وفي هذا الإطار، يمثل التعاون الدولي آلية أساسية لتبادل الأدلة، وتعقب مرتكبي الجرائم، ومواكبة التطورات التقنية، بما يتيح مواجهة المخاطر التي تهدد الثقة بين الدول وتعرقل الجهود الرامية إلى مكافحة الجرائم الإلكترونية بصورة عامة، ورغم أهمية التعاون الدولي في مكافحة الجرائم عبر مواقع التواصل الاجتماعي، إلا أنّ هذا التعاون يواجه مجموعة من المعوقات والتحديات التي تحد من فعاليته، وعليه سنتطرق الى هذه التحديات وفق النقاط التالية وذلك على النحو الآتي :-

١- عدم وجود نموذج موحد للنشاط الإجرامي

تُعد هذه الإشكالية من أبرز التحديات التي تواجه التعاون الدولي في مكافحة الجرائم الإلكترونية ولاسيما جرائم المواقع الخاصة بالتواصل الاجتماعي، إذ لا توجد حتى الآن اتفاقية عالمية أو إطار قانوني موحد لتجريم الأنماط المختلفة لهذه الجرائم ،فالأفعال التي تُعتبر مجرمة في دولة معينة قد تكون قانونية أو غير محددة في دولة أخرى، مما يخلق فجوات قانونية يستغلها المجرمون [٤٠]، وعليه نرى أن هذه المشكلة تزداد خطورة عند التعامل مع جرائم الاحتيال ونشر الأخبار الكاذبة باستخدام مواقع التواصل الاجتماعي، التي تقوم على أساليب مبتكرة ومتغيرة باستمرار، حيث يمكن للمجرمين استغلال هذا التباين التشريعي عبر ارتكاب عمليات احتيالية معقدة تتجاوز حدود الدولة ما يصعب ملاحقتهم قضائياً ويبرز الحاجة الملحة لتقارب النظم القانونية وتنسيق الجهود الدولية لمكافحة هذه الظاهرة.

٢- اختلاف النظم القانونية والاجرائية

يُعد اختلاف النظم القانونية والإجرائية بين الدول من أبرز التحديات التي تعيق فاعلية التعاون الدولي في مكافحة الجريمة، إذ إن تنوع القواعد الإجرائية المنظمة لمرحلتي التحري والتحقيق والمحاكمة قد يؤدي في كثير من الأحيان إلى إفلات الجناة من الملاحقة والعقاب ، إذ إن الأساليب والإجراءات التي تعتبر قانونية وفعالة في دولة ما قد تُرفض أو تُعتبر مخالفة في دولة أخرى، مثل المراقبة الإلكترونية أو الإجراءات المستترة[٤١]، ويزداد هذا التحدي وضوحاً مع الجرائم الحديثة كالاحتيال باستخدام تقنيات الذكاء الاصطناعي، التي تعتمد على أدوات رقمية متقدمة، مما يصعب جمع الأدلة وتعقب الجناة وضمان محاسبتهم وفق معايير موحدة.

٣- غياب المعاهدات أو الاتفاقيات الدولية الكافية

حتى في حال وجود بعض المعاهدات الثنائية أو الجماعية، فإنها غالباً لا توفر الحماية الكافية في مواجهة التقدم السريع للتقنيات الرقمية ونظم الذكاء الاصطناعي المستخدمة في الجرائم الإلكترونية، هذا النقص يجعل التعاون القضائي محدوداً ويؤخر الوصول إلى الأدلة، مما يقلل من فعالية مكافحة الجريمة العابرة للحدود[٤٢].

٤- تنازع الاختصاص القضائي الدولي

تنشأ هذه الإشكالية نتيجة اختلاف التشريعات والنظم القانونية بين الدول، حيث قد يرتكب الجاني فعلاً داخل دولة ويؤثر على دولة أخرى، ما يؤدي إلى وقوع الجريمة تحت اختصاص أكثر من جهة قضائية، فهذا التنازع يعقد الملاحقة ويؤخر العدالة، ويستلزم وضع معايير واضحة لتحديد الاختصاص وتنسيق جهود الدول [٤٣].

٥- تمسك الدول بالسيادة الوطنية وغياب قنوات الاتصال الفعالة

لا يزال مبدأ السيادة الوطنية يشكل عائقاً أمام التعاون القضائي، إذ تحتفظ الدول بكافة السلطات على أراضيها وتقيّد وصول الجهات الأجنبية إلى بيانات أو أدلة مهمة (إضافة إلى ذلك، يفتقر التعاون الدولي إلى قنوات اتصال متخصصة تتيح للسلطات تبادل المعلومات بسرعة وفعالية، ما يجعل تتبع الجناة وتبادل الأدلة أمراً معقداً ويحد من قدرة الدول على مواجهة الجرائم العابرة للحدود، ومع إدراك هذه التحديات والمعوقات، برزت الحاجة إلى بيان الآليات العملية التي تُمكن الدول من التعاون فيما بينها لمكافحة الجرائم التي تتم من خلال مواقع التواصل الاجتماعي ذات الطابع العابر للحدود، ولاسيما جريمة الاحتيال ونشر الأخبار الكاذبة، وتتمثل هذه الآليات في صور التعاون القضائي المختلفة، التي تهدف إلى تجاوز العقبات الإجرائية وتسهيل تبادل الأدلة الرقمية وملاحقة الجناة، ومن أبرزها :-

أولاً :- السمساعدة القضائية المتبادلةُ

تعد المساعدة القضائية في المسائل الجنائية أحد أهم أنماط التعاون القضائي، أذ تعرف بأنها: "كل اجراء قضائي تقوم به دوله من شأنها تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"، وكذلك تُعرف بأنها: "طلب تتقدم به دوله ما الى دولة اخرى بقصد القيام بإجراء تحريات عن الجريمة أو إجراء تحقيق مشترك"، إذ تكتسب المساعدة القضائية أهمية خاصة في ملاحقة مرتكبي الجرائم الإلكترونية وإجراء التحقيقات الدولية بشأنها، نظراً لاعتماد هذه الجرائم على البنية الرقمية التي تتجاوز الحدود الإقليمية للدول إذ غالباً ما يتطلب كشف النشاط الإجرامي تتبع مسارات الاتصال الإلكتروني، سواء من خلال الحاسوب المستخدم في ارتكاب الجريمة أو الحاسوب الذي وقع عليه الاعتداء، وذلك بالاعتماد على السجلات التاريخية التي توضح بيانات الاتصال وتوقيته[٤٤]، غير أن هذا المسار يواجه صعوبات عملية وقانونية، خاصة عندما يكون مقدمو خدمات الإنترنت أو الخوادم الرقمية خارج الولاية القضائية للدولة التي تباشر التحقيق، الأمر الذي يستلزم اعتماد آليات فعالة للتعاون وتبادل المساعدة تتلاءم مع طبيعة الجرائم العابرة للحدود،[٤٥]وتتخذ المساعدة القضائية الدولية عدة صور، من أبرزها :-

١ -تبادل المعلومات

ويُقصد بتبادل المعلومات قيام الدولة المطلوب منها التعاون بتقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية أثناء نظرها في جريمة معينة، سواء ما يتعلق بالتهم الموجهة إلى رعاياها في الخارج، أو الإجراءات التي اتخذت بحقهم، وقد يشمل هذا التبادل كذلك السوابق القضائية للجناة، لما لها من دور في الكشف عن السجل الجنائي للجاني، وما يترتب على ذلك من آثار قانونية، كتشديد العقوبة في حالة العود أو عند تقرير وقف التنفيذ، ومع ذلك فإن هذا التبادل لا يزال يواجه صعوبات عملية، إذ يقتصر في الغالب على الدول التي تربطها اتفاقيات ثنائية أو إقليمية لتبادل المعلومات[٤٦].

وقد أكدت اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية (اتفاقية بودابست) هذا الاتجاه، حيث نصت على التزام الدول الأطراف بتقديم المساعدة المتبادلة فيما بينها وعلى أوسع نطاق ممكن لأغراض التحقيق في الجرائم الجنائية المتعلقة بنظم وبيانات الحاسوب أو جمع الأدلة الإلكترونية [٤٧]، كما أكدت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التزام الدول الأطراف بتبادل المساعدة فيما بينها في التحقيقات أو الإجراءات المرتبطة بجرائم تقنية المعلومات، بما في ذلك جمع الأدلة بشكل إلكتروني[٤٨].

٢-نقل الإجراءات

يقصد بنقل الإجراءات الجنائية قيام دولة ما استناداً إلى اتفاقية أو معاهدة دولية باتخاذ إجراءات جنائية بشأن جريمة ارتُكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توافرت مجموعة من الشروط القانونية، ومن أبرزها:-

أ:- تحقق مبدأ التجريم المزدوج، ويُقصد به أن يكون الفعل المنسوب إلى الشخص محل المتابعة مُجرماً في كل من الدولة الطالبة لنقل الإجراءات والدولة المطلوب إليها، بما يضمن احترام الأسس المشتركة للتجريم بين الدول المتعاونة.

ب:- شرعية الإجراءات المطلوب اتخاذها، وذلك بأن تكون الإجراءات الجنائية المراد مباشرتها مقررة ومشروعة في قانون الدولة المطلوب إليها نقل الإجراءات عن الجريمة ذاتها تطبيقاً لمبدأ الشرعية الإجرائية[٤٩] .

ج:- أهمية الإجراءات في كشف الحقيقة، بحيث تكون الإجراءات المطلوب اتخاذها ذات دور جوهري في الوصول إلى الحقيقة، كأن تكون أدلة الجريمة أو عناصرها المادية أو التقنية متوافرة داخل إقليم الدولة المطلوب إليها نقل الإجراءات.

د:- ألا تكون الجريمة المطلوب نقل الإجراءات بشأنها ذات طابع سياسي، إذ تحتفظ الدولة المطلوب إليها بحق رفض الطلب متى تعلق الأمر بجرائم تُصنف وفق تشريعاتها ضمن الجرائم السياسية.[٥٠]

ثانياً :- الإنابة القضائية

تعد الإنابة القضائية إحدى الصور الرئيسة للتعاون القضائي الدولي في المجال الجنائي، لما تؤديه من دور فاعل في تيسير سير الإجراءات الجنائية بين الدول، وبما يضمن استكمال التحقيقات اللازمة وتقديم المتهمين للمحاكمة، ويُقصد بالإنابة القضائية أنها طلب رسمي تتقدم به دولة إلى دولة أخرى للقيام بإجراء قضائي من إجراءات الدعوى الجنائية، يكون لازماً للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها مباشرته بنفسها خارج نطاق ولايتها الإقليمية ،وتبرز أهمية الإنابة القضائية بوصفها آلية قانونية للتغلب على القيود التي يفرضها مبدأ السيادة الإقليمية والذي يحول دون قيام سلطات دولة ما بمباشرة إجراءات قضائية داخل إقليم دولة أخرى، كإجراء سماع الشهود أو تنفيذ بعض أعمال التحقيق، الأمر الذي يستلزم اللجوء إلى السلطة القضائية في الدولة المطلوب إليها لتنفيذ هذه الإجراءات نيابةً عن الدولة الطالبة [٥١].

ثالثاً :- تسليم المجرمين

يُعد أحد أهم صور التعاون القضائي الدولي لمكافحة الجرائم العابرة للحدود، حيث تقوم الدولة التي يوجد على إقليمها المتهم وفق معاهدة أو على أساس المعاملة بالمثل بتسليمه للدولة الطالبة لملاحقته أو تنفيذ العقوبة شرط توفر مبدأ التجريم المزدوج وتكتسب هذه الآلية أهمية خاصة في الجرائم الإلكترونية، بما فيها الاحتيال باستخدام تقنيات الذكاء الاصطناعي، لضمان عدم إفلات المجرمين من العقاب ، وقد تناولت اتفاقية بودابست لمكافحة الجرائم الإلكترونية هذه المسألة في موادها (١٢، ٢٣، ٢٤، ٢٥)، إضافة إلى توصيات مجلس أوروبا، مما يعزز فعالية التعاون القضائي الدولي في مواجهة الجرائم العابرة للحدود[٥٢]، وإزاء ما يواجه التعاون القضائي الدولي من تحديات إجرائية وقانونية وما يفرضه الطابع العابر للحدود للجرائم الإلكترونية من صعوبات في تبادل الأدلة وتعقب الجناة، نرى الحاجة إلى إرساء أطر قانونية واتفاقية تُنظم هذا التعاون، وقد اتجه المجتمع الدولي في هذا السياق، إلى إبرام عدد من الاتفاقيات الدولية والإقليمية، فضلاً عن تفعيل دور المنظمات الشرطية الدولية بهدف تعزيز التنسيق بين الدول ومواجهة الجرائم المعلوماتية بما في ذلك الجرائم المستحدثة التي تستند إلى تقنيات الذكاء الاصطناعي، ورغم أن هذه الاتفاقيات وُضعت في مرحلة سابقة على الانتشار الواسع لتقنيات الذكاء الاصطناعي، إلا أنها تظل تشكل الإطار المرجعي الأساس للتعاون الدولي في مجال الجرائم الإلكترونية، إذ أرست مبادئ عامة للتجريم، والإجراءات، وتبادل المساعدة القضائية، يمكن البناء عليها وتطويرها لمواجهة الأنماط الإجرامية الحديثة، ولاسيما جرائم الاحتيال والتزييف المعتمدة على الذكاء الاصطناعي ومن أبرز هذه الاتفاقيات:-

١-الاتفاقية الاوربية لمكافحة الجرائم المعلوماتية (اتفاقية بودابست)[٥٣]

تُعد اتفاقية بودابست بشأن الجرائم المعلوماتية ، التي أعدها مجلس أوروبا واعتمدها عام ٢٠٠١، الركيزة الأبرز في مسار بناء نظام جنائي دولي عابر للحدود لمكافحة الجرائم الإلكترونية، فقد جاءت هذه الاتفاقية بوصفها أول إطار دولي متكامل يهدف إلى توحيد الجهود التشريعية والإجرائية للدول في مواجهة هذا النمط المستحدث من الإجرام، من خلال وضع حد أدنى من القواعد الموضوعية لتجريم الأفعال التي تمس أمن نظم وبيانات الحاسوب، إلى جانب إقرار آليات إجرائية تتلاءم مع خصوصية الأدلة الرقمية، كما أولت الاتفاقية أهمية خاصة لتعزيز التعاون الدولي السريع والفعال، مع الحرص على تحقيق التوازن بين متطلبات إنفاذ القانون وصون الحقوق والحريات الأساسية ، وبذلك رسخت اتفاقية بودابست إطاراً قانونياً مرجعياً للعمل

عبر الحدود في مجال الجريمة الإلكترونية، يصلح للاستناد إليه في التصدي لصور الاحتيال الإلكتروني المتطورة، بما في ذلك تلك القائمة على تقنيات مواقع التواصل [٥٤] .

٢- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات [٥٥]

وفي الإطار الإقليمي، جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ تتويجاً للجهود العربية الرامية إلى توحيد السياسة الجنائية في مواجهة الجرائم المعلوماتية ،وقد هدفت الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجالات التجريم، والتحقيق، وتبادل المعلومات، بما يحقق حماية المجتمع العربي وأمنه المعلوماتي مع التأكيد على احترام القيم الدينية والأخلاقية وحقوق الإنسان، وتمثل هذه الاتفاقية إطاراً مهماً لدعم الجهود المشتركة في مواجهة الجرائم الإلكترونية الحديثة رغم الحاجة إلى تطوير آلياتها لمواكبة الجرائم القائمة على مواقع التواصل الاجتماعي [٥٦] .

٣- دور منظمة الانتربول[٥٧]

إلى جانب الاتفاقيات الدولية، يضطلع دور المنظمات الشرطية الدولية، وفي مقدمتها المنظمة الدولية للشرطة الجنائية (الإنتربول)، بأهمية خاصة في دعم التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية العابرة للحدود ، إذ تهدف الإنتربول إلى تعزيز التنسيق وتبادل المعلومات بين أجهزة الشرطة في الدول الأعضاء، وتسهيل ملاحقة الجناة، دون المساس بسيادة الدول أو التدخل في الشؤون ذات الطابع السياسي أو الديني، وقد أكدت أهداف المنظمة على تشجيع التعاون الشرطي في إطار احترام القوانين الوطنية ومبادئ حقوق الإنسان[٥٨] بما يجعلها أداة مساندة فاعلة في مواجهة جرائم الاحتيال القائم على تقنيات الذكاء الاصطناعي .

وفي ضوء ما تقدم نستخلص أن ضعف آليات التعاون الدولي يُعد من أبرز العوائق التي تحول دون المكافحة الفعالة للجرائم الإلكترونية عبر مواقع التواصل الاجتماعي، ولاسيما جرائم الاحتيال ونشر الأخبار والشائعات الكاذبة المرعبة للمجتمع، لما تتسم به من طابع عابر للحدود وتعقيد تقني ،وقد تبين أن هذا الضعف يرتبط بتباين النظم القانونية والإجرائية بين الدول وبطء إجراءات تبادل الأدلة الرقمية، ومحدودية فاعلية صور التعاون القضائي التقليدية في الاستجابة السريعة لمتطلبات التحقيق الرقمي ،كما أن الاتفاقيات الدولية القائمة، رغم دورها في إرساء أطر عامة للتعاون، ما تزال غير كافية لمواكبة التطورات المتسارعة لتقنيات مواقع التواصل الاجتماعي، الأمر الذي يستدعي تطوير آليات تعاون أكثر مرونة وفعالية تحول دون إفلات الجناة من المساءلة الجزائية .

الخاتمـــــــــــــــــــــة:

في خاتمة بحثنا لموضوع جزئية البحث سوف نحاول بيان بعض النتائج والمقترحات الخاصة بموضوع البحث ضمن الآتي:

أولاً: النتائج

١ـ أن جرائم الترهيب الاجتماعي قد تكون ذات طابع مادي ما هو الحال في جريمة الاحتيال والابتزاز باستخدام مواقع التواصل الاجتماعي، لما تنطوي عليه من اعتداء مباشر على الذمة المالية للمجنى عليه من خلال الاستيلاء على الأموال أو المنافع بوسائل احتيالية قائمة على الخداع والتضليل وبما ينسجم في جوهره مع المفهوم التقليدي لجريمة الاحتيال، مع اختلاف جوهري في الوسيلة الإجرامية المعتمدة.

٢ـ تبين أن الجرائم محل الدراسة تنفرد بخصائص تقنية متميزة، أبرزها اعتمادها على أنظمة ذكية وخوارزميات قادرة على التحليل الذاتي واتخاذ قرارات مستقلة، ودقة استهداف الضحايا، واستخدام تقنيات التزييف العميق، فضلاً عن غياب التفاعل المباشر بين الجاني والمجنى عليه، وطابعها العابر للحدود الجغرافية، الأمر الذي يزيد من خطورتها ويجعل اكتشافها وإثباتها أكثر تعقيداً مقارنة بصور الاحتيال التقليدي.

٣ـ نستنتج أن المسؤولية الجزائية عن جرائم الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي لا تزال في ظل التشريعات الجزائية النافذة، منحصرة في الشخص الطبيعي الذي يتدخل في تصميم النظام أو برمجته أو توجيهه أو استغلاله في ارتكاب الفعل الجرمي، وذلك لعدم تمتع تقنيات مواقع التواصل الاجتماعي بالشخصية القانونية وانتفاء الركن المعنوي اللازم لقيام المسؤولية الجزائية، كما يتبين أن ما بلغته هذه التقنيات من استقلالية، ولاسيما في جرائم الاحتيال العمدية، لا يرقى بعد إلى حد يبرر مساءلتها الجزائية بذاتها، الأمر الذي يجعل تحديد المسؤولية رهيناً بالخبرة الفنية، مع بقاء الحاجة قائمة لتطوير التشريعات مستقبلاً بما يواكب التطور التقني دون المساس بالمبادئ المستقرة للقانون الجنائي.

٤ـ إن الأثار التي تخلفها جرائم الترهيب الاجتماعي عبر مواقع التواصل الاجتماعي لا سيما الجرائم الخاصة بالاحتيال والابتزاز ذات طبيعة غير مادية ، وهذا ما يمثل صعوبة أمام اثبات هذا النوع من الجرائم . إلا إن ذلك لا يعني إن الجرائم المعلوماتية لا تتخلف عنها اثاراً مادية بشكل مطلق، فمن الممكن إن تتخلف عنها بعض الأثار المادية ومنها الأوراق التي حاول الجاني إن يجرب نتيجة التعديل الذي اجراه على البرنامج أو المعلومات التي قام على نسخها واستخراجها بواسطة الطابعة.

٥ ـ إن الجريمة الخاصة بترهيب أفراد المجتمع عبر مواقع التواصل الاجتماعي باعتبارها نمط مستحدث في نطاق الإجرام ذات طبيعة خاصة، والسبب في هذه الطبيعة هو إن الأداة التي يتم من خلالها ارتكاب الجريمة هي وسيلة جديدة ولم يتم استخدامها من قبل كوسيلة للاعتداء على نفس أو مال الغير.

٦ ـ نستنتج أن خصوصية جريمة الترهيب المجتمعي باستخدام مواقع التواصل الاجتماعي، من حيث اعتمادها على بيئة رقمية غير مادية وسريعة التغير، أفرزت تحديات جوهرية أمام أعمال التحري والتحقيق، ولا سيما في ما يتعلق بجمع الأدلة الرقمية وتتبع مرتكبي الجريمة وإثبات الصلة بين السلوك الإجرامي والفاعل ويؤدي هذا الواقع إلى إضعاف كفاءة الوسائل الإجرائية التقليدية، الأمر الذي يفرض ضرورة تطوير القواعد الإجرائية الجزائية، وتعزيز التكامل بين الخبرة القانونية والمعرفة التقنية.

ثانياً :- المقترحات

١- نقترح اعتماد إطار إجرائي خاص لمواجهة جرائم الاحتيال المرتكبة باستخدام مواقع التواصل الاجتماعي، يراعي الخصوصية التقنية لهذه الجرائم التي تُرتكب في فضاء رقمي معقد وتستند إلى أنظمة ذكية قادرة على التمويه والخداع وإخفاء الأثر الجرمي ،الأمر الذي يفرض ضرورة تطوير القواعد الإجرائية التقليدية عبر النص صراحة على إجراءات متقدمة للتحري والتحقيق وجمع الأدلة الرقمية .

٢- نقترح إدراج برامج تدريب إلزامية للقضاة في مجال الذكاء الاصطناعي وتطبيقاته الإجرامية، بما يعزز قدرة القضاء على استيعاب الأبعاد التقنية لجريمة الاحتيال الرقمي، وكذلك العمل على تأهيل وتطوير قدرات أعضاء الضبط القضائي والمحققين وقضاة التحقيق، من خلال تنظيم برامج تدريبية وورش عمل تخصصية تُعنى بطبيعة جرائم الاحتيال المرتكبة باستخدام تقنيات الذكاء الاصطناعي وذلك بهدف تمكينهم من فهم آليات عمل الأنظمة الذكية وأساليب توظيفها في الاحتيال ، وتعزيز مهاراتهم في كشف هذه الجرائم وتتبع مرتكبيها وجمع أدلتها الرقمية، لِما تتطلبه هذه الجريمة من كادر مهني متكامل يجمع بين الخبرة القانونية والمعرفة التقنية المتقدمة، ولاسيما في مجال الأمن السيبراني.

٣- ضرورة العمل على تعزيز الوعي المجتمعي بمخاطر وآثار إساءة استخدام مواقع التواصل الاجتماعي، من خلال تنظيم المؤتمرات والندوات العلمية والبرامج التوعوية في المؤسسات التربوية والإعلامية وسائر المؤسسات العامة والخاصة بهدف بيان الجوانب السلبية المحتملة لهذه التقنيات عند توظيفها بصورة غير مشروعة أو غير أخلاقية وبيان انعكاساتها القانونية

والاجتماعية، بما يسهم في ترسيخ ثقافة الاستخدام المسؤول للذكاء الاصطناعي والحد من الجرائم المرتكبة بواسطته.

٤- ولكون جريمة الترهيب المجتمعي من الجرائم العابرة للحدود الجغرافية للدول، نظراً لاعتمادها على الوسائل الإلكترونية والشبكات الرقمية التي تتجاوز الإقليم الوطني، نقترح ضرورة إبرام معاهدات واتفاقيات دولية بين الدول العربية والأجنبية، على غرار الاتفاقية العربية والاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، بهدف وضع تنظيم قانوني دولي موحد يحدد معالم هذه الجريمة، بما يُسهم في تعزيز التعاون القضائي والأمني الدولي لمواجهتها وملاحقة مرتكبيها بفاعلية.

٥- نقترح تعزيز وتطوير مستوى التعاون الدولي لمواجهة جرائم الترهيب عبر مواقع التواصل الاجتماعي، من خلال تفعيل آليات التعاون الأمني الدولي، ولاسيما في مجال تبادل المعلومات والخبرات بين الجهات المختصة، وتأهيل الكوادر المعنية بمكافحة هذا النوع من الجرائم ،ويشمل ذلك تعزيز دور أجهزة الشرطة الدولية وفي مقدمتها منظمة الشرطة الجنائية الدولية (الإنتربول)، في دعم الأجهزة الأمنية الوطنية بالحصول على البيانات والمعلومات المتعلقة بالجناة والوقائع الإجرامية العابرة للحدود.

الهوامش

(١) حيمي سيدي محمد معوقات التحقيق الجنائي في الجرائم الالكترونية ، بحث منشور في المجلة الأكاديمية للبحوث القانونية والسياسية ، المجلد ٦ ، العدد ١ ، ٢٠٢٢، ص ١٧٤٥.

(٢) دوارة فاطمة الزهرة، د.عبدلي حمزة ، الخبرة في التحقيقات الرقمية كآلية للبحث والتحري عن الجرائم الخاصة، بحث منشور في مجلة الاستاذ الباحث للدراسات القانونية والسياسية ، المجلد ١٠ ، العدد ٢، ٢٠٢٥، ص ٤٥٠ و ٤٥٢.

(٣) يقصد بالتشفير" هو عملية تشويش المعلومات بحيث لا يمكن فك تشفيرها وقراءتها إلا من قبل شخص لديه مفتاح فك التشفير الصحيح يستخدم لإخفاء الأدلة أو جعلها غير قابلة للقراءة على النظام المخترق، إذ يستخدم مرتكبو الجرائم المعلوماتية العديد من طرق التشفير المختلفة ولجعل البيانات قابلة للاستخدام لا يمكن أحيانا فك تشفير البيانات المشفرة مما يؤثر سلباً على عملية التحقيق.

(٤) دوارة فاطمة الزهرة ، عبدلي حمزة ، مصدر سابق ، ص ٤٥٣.

(٥) دوارة فاطمة الزهرة ، عبدلي حمزة ، المصدر نفسه ، ص ٤٥٩ .

(٦) بن مالك احمد، الخال أبراهيم ، دور الادلة الرقمية في الاثبات الجنائي ، بحث منشور في مجلة العلوم الإنسانية ، المجلد ٥، العدد ١، ٢٠٢١، ص ١١٥.

(٧) صابرين جاسم مكطوف، المسؤولية الجزائية عن جرائم التزييف العميق " دراسة مقارنة "، رسالة ماجستير، جامعة ميسان ، كلية القانون ، ٢٠٢٥، ص ١٤٦ .

[٨] تعرف الخبرة بشكل عام بأنها: " تقدير مادي أو ذهني يبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أو بجسم الجريمة أو المواد المستعملة في ارتكابها أو آثارها" أنظر: عبد الأمير العكيلي ـ سليم إبراهيم حربة، شرح قانون أصول المحاكمات الجزائية، الجزء الأول ، لبنان ، ٢٠١٥، ص ١٢٦ . وكذلك تعرف بانها: " إبداء رأي فني من شخص مختص فنيا بشأن واقعة ذات أهمية في الدعوى الجنائية " أنظر: محمود نجيب حسني، الاختصاص والإثبات في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١٢٢ وكذلك عرفها البعض بأنها: "المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الاثنين معا أي العمل والدراسة، ومن هنا يطلق على ذوي هذه المهارات بالخبراء". انظر: مختار تابري، الخبرة في الجريمة المعلوماتية، بحث منشور في مجلة الحوار المتوسطي، المجلد ١١، العدد٣، ٢٠٢٠، ص ٣٨٢.

[٩] خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الاسكندرية ، ٢٠٢٠، ص ٥٣.

[١٠] سالي اياد عبد العزيز الخالدي، مدى قدرة القانون في مواجهة الجريمة الالكترونية، ط ١، دار هاتريك للنشر، أربيل ، ٢٠٢٣، ص٨١.

[١١] حيمي سيدي محمد ، مصدر سابق، ص ١٧٤٥.

[١٢] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط ١، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٢٨٩.

[١٣] صابرين جاسم مكطوف، مصدر سابق، ص ١٤٧ وما بعدها .

[١٤] عماد بلغيث. جغلولي يوسف، صعوبات التحقيق في الجرائم الالكترونية، بحث منشور في مجلة الرسالة للدراسات والبحوث الإنسانية ، المجلد ٦ ، العدد ٣ ، ٢٠٢١، ص ٧٨ .

[١٥] Automation: " وتعني التشغيل الآلي أو الذاتي، ويطلق على العمليات التي تعمل ذاتيا بدون تدخل بشري باستخدام أجهزة الحاسب الآلي المبنية على المعالجات والبرمجيات، فهي فن جعل الإجراءات تنفذ بشكل تلقائي" أنظر: بخيت مبارك رشدي، أثر الأتمتة على تحسين قيادة المؤسسات ، بحث منشور في مجلة المعرفة، العدد ٣٠ ، ٢٠٢٥، ص ١٨٤.

[١٦] دوارة فاطمة الزهرة ، عبدلي حمزة ، مصدر سابق ، ص ٤٥٤.

[17] İlker Ali, Aybeyan Selim, (The Role of Digital Forensic Analysis in Modern Investigations), Journal of Emerging Computer Technologies, Volume4, Issue 1, 2024, p 4.

[١٨] تعرف عملية التحري الرقمي: "بأنها عمل قانوني وأمني يقوم به المتحري مستخدماً حواسه الممكنة عبر شبكات المعلومات بواسطة التكنولوجيا الرقمية، لتحقيق غرض معين وهو الحصول على بيانات ومعلومات توضيحية عن الأشخاص والأماكن والاشياء بهدف ضبط الجريمة وتخزين النتيجة في ملف رقمي"، أنظر: مصطفى محمد موسى، دليل التحري عبر شبكات الانترنت ، دار الكتب القانونية ، مصر، ٢٠٠٥، ص ٢٢.

(١٩) عماد بلغيث، جغلولي يوسف، مصدر سابق ، ص ٧٩.

(٢٠) حيمي سيدي محمد، مصدر سابق، ص ١٧٤٦

(21) Sonu Surakanti, Sam Goundar, Joshua Dwight, Countering anti-forensic tactics in cybercrime investigations, International Journal of Information Security, 2025, p1.

(٢٢) حذف أداوت التتبع تعني: "عملية إزالة أي آثار للنشاط الإجرامي بهدف تجنب الاكتشاف بعد اختراق النظام المستهدف مثل تعطيل برامج مكافحة الفيروسات، أو حذف سجلات النظام، وما إلى ذلك" .

(٢٣) حيمي سيدي محمد، مصدر سابق، ص ١٧٤٧.

(٢٤) يقصد بالتحقيق" مجموعة الإجراءات التي تباشرها الجهة المكلفة بالتحقيق لدى وقوع الجريمة، بغاية البحث والتنقيب عن الأدلة التي تفيد في الكشف عن الحقيقة باعتبارها جريمة ذات خصائص وطبيعة خاصة، هذا ما يجعل التحقيق الجنائي فيها مختلف عن التحقيق الجنائي في الجرائم العادية، إذ يكون التحقيق في الجريمة المعلوماتية تحقيقاً جنائياً معلوماتياً، باعتبار أن مسرح ومحيط هذه الجريمة هو القضاء الإلكتروني والبيانات التقنية" أنظر، حمزة محمد الهادي التومي، علي سعد امحمد ، رمضان محمد الزنيقري، التحقيق الجنائي في الجرائم الإلكترونية، المؤتمر العلمي الثاني لطلاب المرحلة الجامعية والدراسات العليا، الجامعة الاسمرية الإسلامية ، ليبيا، ٢٠٢٤، ص ٣٥١.

(٢٥) تعرف المراقبة الالكترونية: "بأنها وسيلة يقوم بها عضو من أعضاء الضابطة القضائية ذو كفاءة تقنية عالية، وباستخدام تقنيات وبرامج إلكترونية، بهدف جمع المعلومات والبيانات عن المشتبه به سواء أكان شخصاً أم مكاناً أم شيئاً، وذلك لتحقيق غرض أمني. ومن ذلك مثلاً أن يقوم عضو الضابطة القضائية بمراقبة أحد الهكر أثناء اختراقه لحاسوب المجني عليه، أو الدخول إلى أحد المواقع ومراقبة مستخدميه الذين اتخذوه وسيلة للاحتيال على الأشخاص " أنظر: أحمد محمد العمر، الدليل الرقمي وحجيته في الاثبات الجزائي، بحث منشور في مجلة الدراسات الفقهية والقانونية، العدد ٣ ، ٢٠٢٠، ص ١٤٦.

(٢٦) صابرين جاسم مكطوف ، مصدر سابق ، ص ١٦٥ و ص ١٦٧.

(٢٧) محمد مصطفى عدنان الشافعي، جريمة الاحتيال الإلكتروني في عصر الذكاء الاصطناعي، بحث منشور في مجلة القرار للبحوث العلمية المحكمة، المجلد ٧، العدد ٢٠، ٢٠٢٥ ، ص ٣٠٣.

(٢٨) عبد الرحمن جعيد، مراد قريبيز، المسائل القانونية المثارة بشأن تنازع الاختصاص القضائي في الفضاء الالكتروني، بحث منشور في المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد ٩ ، العدد ٢ ، ٢٠٢٥، ص ٨٤٥.

(٢٩) عبد الرحمن جعيد ــ مراد قريبيز، المصدر السابق، ص ٨٤٤.

(٣٠) عبد الرحمن جعيد، مراد قريبيز، المصدر السابق، ص ٨٤٦.

(٣١) عبد الرحمن جعيد ــ مراد قريبيز ، المصدر السابق ، ص ٨٤٦.

(٣٢) صابرين جاسم مكطوف، مصدر سابق، ص ١٧٦ .

(٣٣) هدية أحمد محمد زعتر، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها، بحث منشور في مجلة البحث القانونية والاقتصادية، العدد ٨٤ ، ٢٠٢٣ ، ص ١١١.

[٣٤] صابرين جاسم مكطوف، مصدر سابق ، ١٧٦.

[٣٥] هشام بوحش، مبدأ الاختصاص القضائي العالمي ودورة في تحقيق العدالة الجنائية ، بحث منشور في مجلة جامعة الأمير عبد القادر للعلوم الاسلامية، مجلد ٣٦ ، عدد ٣ ، ٢٠٢٢، ص ٢٧٨

[٣٦] وردي طيب، الاختصاص القضائي في جرائم الانترنت، رسالة ماجستير، جامعة الدكتور مولاي الطاهر سعيدة ، كلية الحقوق والعلوم السياسية ، ٢٠١٥، ص ٤٤ وما بعدها .

[٣٧] المادة (١٣) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

[٣٨] المادة (٢٢) من قانون الجرائم والعقوبات الاماراتي رقم (٣١) لسنة ٢٠٢١.

[٣٩] سامي جاد واصل، التعاون الدولي في مكافحة الجرائم الالكترونية، بحث منشور في مجلة القانون والتكنولوجيا، المجلد ٣، العدد ١، ٢٠٢٣، ص ٥٩.

[٤٠] سامي جاد واصل ، مصدر سابق، ص ٨٤.

[٤١] سامي جاد واصل، المصدر نفسه ، ص ٨٥ وما بعدها .

[٤٢] الطيبي البركة، حاج سودي محمد إشكالية الإثبات في الجرائم الالكترونية، بحث منشور في مجلة آفاق علمية، المجلد ١١ ، العدد ١، ٢٠١٩، ص ٢٧٩.

[٤٣] جاسم خربيط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، بحث منشور في مجلة القانون للدراسات والبحوث القانونية، العدد ١٢ ، ٢٠١٦، ص ٣٦.

[٤٤] سامي جاد واصل ، مصدر سابق ، ص ٨٦.

[٤٥] عدنان قحطان عزيز، زينة محمد كاظم، التعاون الدولي للحماية من الجرائم الماسة ببيانات ونظم الكمبيوتر، بحث منشور في مجلة المعهد، مجلة علمية محكمة مفتوحة المصدر، ٢٠٢٣، ص ٢٣٨.

[٤٦] عدنان قحطان عزيز، زينة محمد كاظم، المصدر السابق، ص ٢٣٩.

[٤٧] المادة (٢٥) من اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١.

[٤٨] المادة (٣٢) من الاتفاقية العربية لمكافحة الجرائم المعلوماتية لعام ٢٠١٠.

[٤٩] سامي جاد واصل، مصدر سابق، ص ٧٥.

[٥٠] عدنان قحطان عزيز ــ زينة محمد كاظم ، مصدر سابق، ص ٢٤٠ .

[٥١] سامي جاد واصل، مصدر سابق، ص ٧٦.

[٥٢] فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، بحث منشور في مجلة البحوث في الحقوق والعلوم السياسية، المجلد ٨، العدد ١، ٢٠٢٢، ص٤٤٢.

[٥٣] أبرمت اتفاقية بودابست لمكافحة الجرائم الإلكترونية في العاصمة المجرية بتاريخ ٢٣/١١/٢٠٠١، وتعد من أهم وأبرز الاتفاقيات الدولية التي أقرت لمواجهة الجرائم الإلكترونية، وذلك استجابة للتطور المتسارع في تقنيات المعلومات والاتصال، وما رافقه من توسع في استخدام شبكات المعلومات وتسارع تدفق البيانات، بما أفرز مخاطر جدية تهدد أمن الدول واستقرارها، وقد جاءت هذه الاتفاقية نتيجة رغبة دول مجلس أوروبا والدول الأعضاء في إرساء إطار قانوني مشترك يعتمد على تدابير تشريعية وإجرائية فعالة لمكافحة هذا النمط

المستحدث من الجرائم والحد من آثاره المدمرة ، وتتكون الاتفاقية من ديباجة وأربعة أبواب رئيسة، وقد عالج الباب الثالث مسألة التعاون الدولي . للمزيد حول الاتفاقية انظر الرابط التالي :-

https://share.google/B8og58nW37Q5DwlB9

(٥٤) زينب عبد الواحد عبد الوهاب، دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود: التحديات والآفاق، بحث منشور في مجلة سر من رأى للدراسات الإنسانية، المجلد ٢١، العدد ٨٤، ٢٠٢٥، ص ٣٤٠.

(٥٥) أبرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ٢١/١٢/٢٠١٠ في مقر الأمانة العامة لجامعة الدول العربية بالقاهرة، وقد وقعت عليها ثلاث وعشرون دولة عربية، من بينها دولة الإمارات العربية المتحدة ، وجمهورية العراق. وقد جاءت هذه الاتفاقية في خمسة فصول، تضمن الفصل الأول الأحكام العامة، بينما خصص الفصل الثاني لأحكام التجريم والعقاب، وتناول الفصل الثالث الأحكام الإجرائية، في حين عالج الفصل الرابع الأحكام الخاصة بالتعاون القضائي ومبادئ الاختصاص، واختتمت الاتفاقية بالفصل الخامس الذي تضمن الأحكام الختامية ، وقد نصت المادة الأولى من الاتفاقية على هدفها، والمتمثل في تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم، حفاظاً على أمن الدول العربية ومصالحها، وسلامة مجتمعاتها وأفرادها. للمزيد حول الاتفاقية أنظر الرابط التالي :-

https://share.google/BONeV0JK3vYJ6sTNA.

(٥٦) صابرين جاسم مكطوف، مصدر سابق ، ص ١٧٢.

(٥٧) تعد منظمة الشرطة الجنائية الدولية (الإنتربول) أكبر منظمة شرطية دولية ، وقد أنشئت سنة ١٩٢٣، ويقع مقرها الرئيسي في مدينة ليون بالجمهورية الفرنسية ، وتضم المنظمة في عضويتها ١٩٦ دولة، مما يجعلها إحدى أهم آليات التعاون الشرطي على المستوى الدولي ، وتتألف المنظمة من أجهزة رئيسية تتمثل في الجمعية العامة، واللجنة التنفيذية، والأمانة العامة، والمكاتب المركزية الوطنية، إضافة إلى المستشارين ولجنة ضبط ملفات الإنتربول، وتهدف هذه المنظمة إلى تأمين وتنمية التعاون المتبادل على أوسع نطاق بين سلطات الشرطة الجنائية في الدول الأعضاء، وذلك في إطار احترام القوانين الوطنية لكل دولة، فضلا عن إنشاء وتطوير المؤسسات والآليات الكفيلة بالمساهمة الفعالة في الوقاية من الجرائم ومكافحتها. للمزيد حول المنظمة أنظر الرابط التالي :-

https://share.google/RV5XZVuobtgQzoGOQ

(٥٨) سامي واصل جاد ، مصدر سابق، ص ٦٤.

قائمة المصادر

أولاً: الكتب

١.خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الاسكندرية ، ٢٠٢٠.

٢.خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، ط ١، دار النهضة العربية، القاهرة، ٢٠٠٩.

٣.سالي اياد عبد العزيز الخالدي، مدى قدرة القانون في مواجهة الجريمة الالكترونية، ط ا، دار هاتريك للنشر، أربيل ، ٢٠٢٣.

٤.عبد الأمير العكيلي ـ سليم إبراهيم حربة، شرح قانون أصول المحاكمات الجزائية، الجزء الأول ، لبنان ، ٢٠١٥.

٥.محمود نجيب حسني، الاختصاص والإثبات في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٩٢.

٦.مصطفى محمد موسى، دليل التحري عبر شبكات الانترنت ، دار الكتب القانونية ، مصر، ٢٠٠٥.

ثانياً: الرسائل والأطاريح الجامعية

١ـ صابرين جاسم مكطوف، المسؤولية الجزائية عن جرائم التزييف العميق " دراسة مقارنة "، رسالة ماجستير، جامعة ميسان ، كلية القانون ، ٢٠٢٥.

ثالثاً: البحوث

١.أحمد محمد العمر، الدليل الرقمي وحجيته في الاثبات الجزائي، بحث منشور في مجلة الدراسات الفقهية والقانونية، العدد ٣ ، ٢٠٢٠.

٢.بخيت مبارك رشدي، أثر الأتمتة على تحسين قيادة المؤسسات ، بحث منشور في مجلة المعرفة، العدد ٣٠ ، ٢٠٢٥.

٣.بن مالك احمد، الخال أبراهيم ، دور الادلة الرقمية في الاثبات الجنائي ، بحث منشور في مجلة العلوم الإنسانية ، المجلد ٥، العدد ١، ٢٠٢١.

٤.جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، بحث منشور في مجلة القانون للدراسات والبحوث القانونية، العدد ١٢ ، ٢٠١٦.

٥.حمزة محمد الهادي التومي، علي سعد امحمد ، رمضان محمد الزنيقري، التحقيق الجنائي في الجرائم الإلكترونية، المؤتمر العلمي الثاني لطلاب المرحلة الجامعية والدراسات العليا، الجامعة الاسمرية الإسلامية ، ليبيا، ٢٠٢٤.

٦.حيمي سيدي محمد معوقات التحقيق الجنائي في الجرائم الالكترونية ، بحث منشور في المجلة الأكاديمية للبحوث القانونية والسياسية ، المجلد ٦ ، العدد ١ ، ٢٠٢٢.

٧.دوارة فاطمة الزهرة، د.عبدلي حمزة ، الخبرة في التحقيقات الرقمية كآلية للبحث والتحري عن الجرائم الخاصة، بحث منشور في مجلة الاستاذ الباحث للدراسات القانونية والسياسية ، المجلد ١٠ ، العدد ٢، ٢٠٢٥.

٨.زينب عبد الواحد عبد الوهاب، دور القانون الجنائي الدولي في مكافحة الجرائم السيبرانية عبر الحدود: التحديات والآفاق، بحث منشور في مجلة سر من رأى للدراسات الإنسانية، المجلد ٢١، العدد ٨٤، ٢٠٢٥.

٩.سامي جاد واصل، التعاون الدولي في مكافحة الجرائم الالكترونية، بحث منشور في مجلة القانون والتكنولوجيا، المجلد ٣، العدد ١، ٢٠٢٣.

١٠.الطيبي البركة، حاج سودي محمد إشكالية الإثبات في الجرائم الالكترونية، بحث منشور في مجلة آفاق علمية، المجلد ١١ ، العدد ١، ٢٠١٩.

١١.عبد الرحمن جعيد، مراد قريبيز، المسائل القانونية المثارة بشأن تنازع الاختصاص القضائي في الفضاء الالكتروني، بحث منشور في المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد ٩، العدد ٢ ، ٢٠٢٥.
١٢.عدنان قحطان عزيز، زينة محمد كاظم، التعاون الدولي للحماية من الجرائم الماسة ببيانات ونظم الكمبيوتر، بحث منشور في مجلة المعهد، مجلة علمية محكمة مفتوحة المصدر، ٢٠٢٣.
١٣.عماد بلغيث. جغلولي يوسف، صعوبات التحقيق في الجرائم الالكترونية، بحث منشور في مجلة الرسالة للدراسات والبحوث الإنسانية ، المجلد ٦ ، العدد ٣ ، ٢٠٢١.
١٤.فريد ناشف، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، بحث منشور في مجلة البحوث في الحقوق والعلوم السياسية، المجلد ٨، العدد ١، ٢٠٢٢.
١٥.محمد مصطفى عدنان الشافعي، جريمة الاحتيال الإلكتروني في عصر الذكاء الاصطناعي، بحث منشور في مجلة القرار للبحوث العلمية المحكمة، المجلد ٧، العدد ٢٠، ٢٠٢٥ .
١٦.مختار تابري، الخبرة في الجريمة المعلوماتية، بحث منشور في مجلة الحوار المتوسطي، المجلد ١١، العدد٣، ٢٠٢٠.
١٧.هدية أحمد محمد زعتر، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها، بحث منشور في مجلة البحث القانونية والاقتصادية، العدد ٨٤ ، ٢٠٢٣.
١٨.هشام بوحش، مبدأ الاختصاص القضائي العالمي ودورة في تحقيق العدالة الجنائية ، بحث منشور في مجلة جامعة الأمير عبد القادر للعلوم الاسلامية، مجلد ٣٦ ، عدد ٣ ، ٢٠٢٢.
١٩.وردي طيب، الاختصاص القضائي في جرائم الانترنت، رسالة ماجستير، جامعة الدكتور مولاي الطاهر سعيدة ، كلية الحقوق والعلوم السياسية ، ٢٠١٥.

رابعاً: المصادر الأجنبية

1-İlker Ali, Aybeyan Selim, (The Role of Digital Forensic Analysis in Modern Investigations), Journal of Emerging Computer Technologies, Volume4, Issue 1, 2024
2-Sonu Surakanti, Sam Goundar, Joshua Dwight, Countering anti-forensic tactics in cybercrime investigations, International Journal of Information Security, 2025.

رابعاً: القوانين

١.قانون العقوبات الايطالي رقم ١٣٩٨ لسنة ١٩٣٠ المعدل .
٢.قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.
٣.قانون الجرائم والعقوبات الاماراتي رقم (٣١) لسنة ٢٠٢١.

خامساً: الروابط الالكترونية

1-https://share.google/B8og58nW37Q5DwlB9
2-https://share.google/BONeV0JK3vYJ6sTNA
3-https://share.google/RV5XZVuobtgQzoGOQ

List of Sources

First: Books

.١Khaled Hassan Ahmed Lotfi, Mechanisms of Criminal Investigation in Information Technology Crimes, Dar Al-Fikr Al-Jami'i, Alexandria, 2020.

.٢Khaled Mamdouh Ibrahim, The Art of Criminal Investigation in Cybercrimes, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2009.

.٣Sally Ayad Abdul Aziz Al-Khalidi, The Extent of the Law's Ability to Confront Cybercrime, 1st ed., Hatrik Publishing House, Erbil, 2023.

.٤Abdul Amir Al-Akeeli - Salim Ibrahim Harba, Explanation of the Code of Criminal Procedure, Part One, Lebanon, 2015.

.٥Mahmoud Najib Hosni, Jurisdiction and Evidence in the Code of Criminal Procedure, Dar Al-Nahda Al-Arabiya, Cairo, 1992.

.٦Mustafa Muhammad Musa, A Guide to Investigating via Internet Networks, Dar Al-Kutub Al-Qanuniyya, Egypt, 2005. Second: University Theses and Dissertations

.١Sabreen Jassim Maktoof, Criminal Liability for Deepfakes: A Comparative Study, Master's Thesis, University of Maysan, College of Law, 2025.

Third: Research Papers

.١Ahmed Mohammed Al-Omar, Digital Evidence and its Admissibility in Criminal Proceedings, Research published in the Journal of Jurisprudential and Legal Studies, Issue 3, 2020.

.٢Bakheet Mubarak Rashdi, The Impact of Automation on Improving Institutional Leadership, Research published in Al-Ma'rifah Journal, Issue 30, 2025.

.٣Bin Malik Ahmed, Al-Khal Ibrahim, The Role of Digital Evidence in Criminal Proceedings, Research published in the Journal of Human Sciences, Volume 5, Issue 1, 2021.

.٤Jassim Kharbit Khalaf, Difficulties in Criminal Evidence in Cybercrimes, Research published in the Law Journal for Legal Studies and Research, Issue 12, 2016. 5. Hamza Mohamed Al-Hadi Al-Toumi, Ali Saad Mhammed, Ramadan Mohamed Al-Zaniqri, "Criminal Investigation in Cybercrimes," Second Scientific Conference for Undergraduate and Postgraduate Students, Al-Asmariya Islamic University, Libya, 2024.

.٦Himi Sidi Mohamed, "Obstacles to Criminal Investigation in Cybercrimes," research published in the Academic Journal of Legal and Political Research, Volume 6, Issue 1, 2022.

.٧Douara Fatima Al-Zahra, Dr. Abdelli Hamza, "Expertise in Digital Investigations as a Mechanism for Searching for and Investigating Special Crimes," research published in the Al-Ustadh Al-Bahith Journal for Legal and Political Studies, Volume 10, Issue 2, 2025.

.٨Zainab Abdel-Wahid Abdel-Wahab, "The Role of International Criminal Law in Combating Cross-Border Cybercrimes: Challenges and Prospects," research published in the Sar Man Ra'a Journal for Human Studies, Volume 21, Issue 84, 2025. 9. Sami Jad Wasel, International Cooperation in Combating Cybercrime, research published in the Journal of Law and Technology, Volume 3, Issue 1, 2023.

.١٠Al-Tayyibi Al-Baraka and Haj Soudi Muhammad, The Problem of Evidence in Cybercrime, research published in the Journal of Scientific Horizons, Volume 11, Issue 1, 2019.

.١١Abdul Rahman Jaid and Murad Quraibiz, Legal Issues Raised Regarding Jurisdiction Conflicts in Cyberspace, research published in the Academic Journal of Legal and Political Research, Volume 9, Issue 2, 2025.

.١٢Adnan Qahtan Aziz and Zeina Muhammad Kazem, International Cooperation for Protection Against Crimes Affecting Computer Data and Systems, research published in the Institute Journal, an open-source peer-reviewed scientific journal, 2023.

.١٣Imad Balghith and Jaghlouli Yousef, Difficulties in Investigating Cybercrime, research published in the Al-Risala Journal for Human Studies and Research, Volume 6, Issue 3, 2021. 14. Farid Nashef, "Mechanisms of International Cooperation in Combating Cybercrime," published in the Journal of Research in Law and Political Science, Volume 8, Issue 1, 2022.

.١٥Muhammad Mustafa Adnan Al-Shafi'i, "Electronic Fraud in the Age of Artificial Intelligence," published in the Al-Qarar Journal for Scientific Research, Volume 7, Issue 20, 2025.

.١٦Mukhtar Tabri, "Expertise in Cybercrime," published in the Mediterranean Dialogue Journal, Volume 11, Issue 3, 2020.

.١٧Hadiya Ahmed Muhammad Za'tar, "The Legal Problems of Transnational Cybercrime and Ways to Confront Them," published in the Journal of Legal and Economic Research, Issue 84, 2023.

.١٨Hisham Bouhch, "The Principle of Universal Jurisdiction and Its Role in Achieving Criminal Justice," published in the Journal of Prince Abdul Qadir University for Islamic Sciences, Volume 36, Issue 3, 2022. 19. Wardi Tayeb,

Jurisdiction in Cybercrimes, Master's Thesis, Dr. Moulay Tahar Saida University, Faculty of Law and Political Science, 2015.

Fourth: Foreign Sources

-١İlker Ali, Aybeyan Selim, (The Role of Digital Forensic Analysis in Modern Investigations), Journal of Emerging Computer Technologies, Volume 4, Issue 1, 2024

-٢Sonu Surakanti, Sam Goundar, Joshua Dwight, Countering anti-forensic tactics in cybercrime investigations, International Journal of Information Security, 2025.

Fourth: Laws

.١Italian Penal Code No. 1398 of 1930, as amended.

.٢Iraqi Penal Code No. (111) of 1969, as amended.

.٣UAE Penal Code No. (31) of 2021. Fifth: Electronic Links

-١https://share.google/B8og58nW37Q5DwlB9

-٢https://share.google/BONeV0JK3vYJ6sTNA

-٣https://share.google/RV5XZVuobtgQzoGOQ