HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

الأحكام الإجرائية الخاصة بمكافحة جريمة التنمر الالكتروني ضد الأحداث

عمر حافظ جاسم[1]، محمد فرحات[1]

[1] الجامعة الإسلامية في بيروت، لبنان.

HNSJ, 2026, 7(6); https://doi.org/10.53796/hnsj76/69

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/76/69

تاريخ الاستقبال: 2026/05/20م تاريخ القبول: 2026/05/25م تاريخ النشر: 2026/06/01م

المستخلص

هدفت هذه الدراسة إلى بيان الأحكام الإجرائية الخاصة بمكافحة جريمة التنمر الإلكتروني ضد الأحداث، في ضوء ما تثيره هذه الجريمة من تحديات قانونية وتقنية تتصل بصعوبة الإثبات، وسرعة انتشار المحتوى الضار، وحساسية الفئة المستهدفة. وقد انطلقت الدراسة من إشكالية رئيسية تتمثل في مدى كفاية القواعد الإجرائية القائمة لمواجهة جرائم التنمر الإلكتروني الواقعة على الأحداث، ومدى قدرتها على تحقيق التوازن بين حماية الحدث، سواء كان مجنياً عليه أو طرفاً في الواقعة، وبين ضمانات الخصوصية والمحاكمة العادلة. واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية والآراء الفقهية ذات الصلة بمراقبة الاتصالات والأدلة الرقمية، مع الإفادة من المنهج المقارن في بيان بعض النماذج التشريعية، ولا سيما ما يتعلق بتنظيم التنصت والمراقبة الإلكترونية والتزامات مقدمي الخدمات المعلوماتية. وقد تناولت الدراسة محورين رئيسيين؛ أولهما أحكام مراقبة الاتصالات الإلكترونية في جرائم التنمر الإلكتروني ضد الأحداث، من حيث مشروعيتها وشروطها وقيمتها في الإثبات الجنائي، وثانيهما التزامات مقدمي الخدمات المعلوماتية ومسؤوليتهم في حفظ البيانات، والتعاون مع السلطات المختصة، ورصد المحتوى المسيء أو إزالته. وتوصلت الدراسة إلى أن معظم التشريعات لا تزال تفتقر إلى تنظيم إجرائي مستقل يراعي خصوصية جرائم التنمر الإلكتروني ضد الأحداث، كما أن إجراءات جمع الأدلة الرقمية ومراقبة الاتصالات تحتاج إلى ضوابط أكثر دقة، تضمن الإذن القضائي، وتحديد نطاق المراقبة ومدتها، وحماية سرية بيانات الحدث. كما كشفت الدراسة عن قصور في إلزام مقدمي الخدمات المعلوماتية بالتدخل السريع وحفظ الأدلة الرقمية ومنع تفاقم الضرر. وأوصت الدراسة بضرورة إصدار تشريع إجرائي خاص ينظم التحقيق والإثبات في جرائم التنمر الإلكتروني ضد الأحداث، مع إلزام مقدمي الخدمات والمنصات الرقمية بإنشاء آليات استجابة عاجلة للتبليغ عن المحتوى المسيء، وحفظ الأدلة، والتعاون مع الجهات القضائية، بما يحقق حماية فعالة للأحداث في البيئة الرقمية دون الإخلال بالحقوق والحريات الأساسية.

الكلمات المفتاحية: التنمر الإلكتروني، الأحداث، مراقبة الاتصالات، الأدلة الرقمية، مقدمو الخدمات المعلوماتية.

RESEARCH TITLE

Procedural Provisions for Combating the Crime of Cyberbullying Against Juveniles

Abstract

This study aims to examine the procedural provisions for combating the crime of cyberbullying against juveniles, in light of the legal and technical challenges posed by this crime, particularly the difficulty of proof, the rapid spread of harmful content, and the sensitivity of the targeted age group. The study is based on a central problem: the extent to which existing procedural rules are sufficient to address cyberbullying crimes committed against juveniles, and their ability to achieve a balance between protecting juveniles, whether as victims or as parties to the incident, and safeguarding privacy and fair trial guarantees. The study adopts the descriptive-analytical approach by analyzing relevant legal texts and jurisprudential opinions concerning communication surveillance and digital evidence, while also benefiting from the comparative approach in presenting selected legislative models, particularly those related to the regulation of interception, electronic surveillance, and the obligations of information service providers. The study addresses two main themes. The first concerns the provisions governing the surveillance of electronic communications in cyberbullying crimes against juveniles, in terms of their legality, conditions, and evidentiary value in criminal proof. The second concerns the obligations and liability of information service providers in preserving data, cooperating with competent authorities, monitoring harmful content, and removing it when necessary. The study concludes that most legislations still lack independent procedural rules that take into account the specific nature of cyberbullying crimes against juveniles. It also finds that procedures for collecting digital evidence and monitoring communications require more precise safeguards, including judicial authorization, defining the scope and duration of surveillance, and protecting the confidentiality of juveniles' data. The study further reveals shortcomings in obligating information service providers to intervene promptly, preserve digital evidence, and prevent the escalation of harm. The study recommends enacting special procedural legislation to regulate investigation and proof in cyberbullying crimes against juveniles. It also recommends obligating digital platforms and service providers to establish urgent response mechanisms for reporting harmful content, preserving evidence, and cooperating with judicial authorities, in a manner that ensures effective protection for juveniles in the digital environment without prejudice to fundamental rights and freedoms.

Key Words: Cyberbullying, Juveniles, Communication Surveillance, Digital Evidence, Information Service Providers.

المقدمة

تعد جرائم التنمر الالكتروني ضد الأحداث من أبرز التحديات التي أفرزها التطور التكنولوجي وانتشار وسائل التواصل الاجتماعي، إذ لم تعد هذه الجرائم مجرد سلوكيات فردية بسيطة، بل أصبحت ظاهرة معقدة تتطلب معالجة قانونية وإجرائية متخصصة، ونظراً للطبيعة الرقمية لهذه الجرائم فإنها تختلف عن الجرائم التقليدية من حيث وسائل ارتكابها، وصعوبة كشفها، وسرعة انتشار آثارها الأمر الذي يفرض ضرورة تبني قواعد إجرائية حديثة تتلاءم مع هذه الخصوصية.

وإن أساليب الوقاية من الإجرام المعلوماتي لا تكفي بحد ذاتها لمنع جرائم ونظراً للطابع الخاص لهذه الجريمة المتطلبة للذكاء البشري بالتقنية المعلوماتية التي تشكل فضاء واسع، يكثر فيه الثغرات التي من خلالها يرتكب المجرم المعلوماتي عملياته الجرمية، فلمواجهة جريمة تقنية المعلومات بكافة مراحلها لا بد من وجود قانون ينظم آليات الملاحقة والتحقيق والمحاكمة فيها، ويضع العقوبات المناسبة لها، من هذا المنطلق حرصت الدول المتقدمة على التحرك وبصورة مبكرة بغية عد العدة وإعداد نفسها لمواجهة هذه الجرائم من كافة النواحي التشريعية والفنية التقنية وكذلك إنشاء الأجهزة المتخصصة بمكافحة هذه الجرائم والتحري والتحقيق فيها بالإضافة إلى القضاء المختص بمحاكمة مرتكبيها، فيما بقيت دول أخرى من ضمنها أغلب الدول النامية ساكنة وولم تبرح مكانها في هذا الصدد.

أولاً_ أهمية البحث

تتجلى أهمية البحث في التصدي لتنامي جريمة التنمر الإلكتروني ضد الأحداث، التي تشكل تهديدًا خطيرًا للصحة النفسية والاجتماعية لهذه الفئة الهشة. كما تبرز الحاجة لوضع أحكام إجرائية رادعة تحقق التوازن بين حماية الأحداث وضمان محاكمة عادلة، وسد الفجوات القانونية في التشريعات الوطنية والدولية.

ثانياً_ إشكالية البحث

تنحصر الإشكالية في التساؤل حول مدى كفاية الأحكام الإجرائية الحالية لمكافحة التنمر الإلكتروني ضد الأحداث، وما إذا كانت تراعي خصوصية هذه الفئة من حيث التحقيق والمحاكمة والعقوبات البديلة. وتتفرع عنها إشكالات فرعية مثل: كيف يتم إثبات الجريمة مع صعوبة تتبع الأدلة الرقمية؟ وما آليات حماية الحدث من وصمة العار أثناء الإجراءات؟

ثالثاً_ منهج البحث

سيعتمد البحث على المنهج الوصفي التحليلي لدراسة النصوص القانونية والأحكام القضائية المتعلقة بالتنمر الإلكتروني ضد الأحداث. كما سيُستخدم المنهج المقارن للاستفادة من تجارب بعض الدول المتقدمة في هذا المجال، مع تطبيق منهج دراسة الحالة على نماذج واقعية لتقييم مدى فعالية الإجراءات المطبقة.

رابعاً_ هيكلية البحث

لمعالجة إشكالية هذا البحث سوف نقوم بتقسيم هذا البحث إلى مطلبين؛ الأول: أحكام مراقبة الاتصالات في جرائم التنمر الإلكتروني الواقعة على الأحداث، والثاني: التزامات مقدمي الخدمات المعلوماتية في سبيل مكافحة تلك الجرائم، على أن يسبق المطلبين تمهيد يوضح مفهوم التنمر الإلكتروني وخصائصه، ويعقبهما خاتمة بأهم النتائج والتوصيات الإجرائية.

المطلب الأول

أحكام مراقبة الاتصالات في جرائم التنمر الالكتروني الواقعة على الأحداث

تعد مراقبة الاتصالات الالكترونية من أهم الوسائل الحديثة التي تعتمدها الجهات المختصة في مواجهة الجرائم الرقمية، ولا سيما جرائم التنمر الالكتروني التي تستهدف فئة الأحداث. وقد فرضت طبيعة هذه الجرائم، التي ترتكب في بيئة افتراضية وتتسم بالخفاء وسرعة الانتشار، الحاجة إلى وضع أحكام قانونية خاصة تنظم إجراءات المراقبة وتحدد نطاقها، كما أن خصوصية هذه الفئة تستوجب توفير ضمانات إضافية لحمايتها أثناء مراحل التحقيق والإثبات، ومن هنا تبرز أهمية تنظيم مراقبة الاتصالات في إطار قانوني يحقق التوازن بين فعالية الكشف عن الجريمة وصون الحقوق والحريات وعليه سيتم تناول الأحكام الخاصة التي تحكم هذا المجال في ضوء خصوصية جرائم التنمر الالكتروني ضد الأحداث [1]، **لذلك سوف نقوم بتقسيم هذا المطلب إلى فرعين:**

الفرع الأول: مراقبة الاتصالات الالكترونية في جرائم التنمر الالكتروني الواقعة على الأحداث.

الفرع الثاني: شروط المراقبة الالكترونية في جرائم التنمر الالكتروني الواقعة على الأحداث.

الفرع الأول

مراقبة الاتصالات الالكترونية في جرائم التنمر الالكتروني الواقعة على الأحداث

يثير التنصت على المكالمات الهاتفية إشكاليات عديدة بين الفقهاء فيما يتعلق بشرعيتها وقوتها القانونية كدليل في الإثبات الجنائي، والملاحظ أن المحققين يميلون إلى التنصت على المكالمات الهاتفية اعتقاداً بقدرتهم على اكتشاف بعض الجرائم الهامة التي تمس كيان المجتمع ككل، ومن المعلوم أن المصلحة العامة تفوق مصلحة الفرد في خصوصياته، وذلك لأن الأمن والسلامة العامة يفوقان قيمة ما يمكن للفرد التذرع به من حق في الخصوصية.

وتتجلى أهمية هذه الإشكالية بصورة أوضح في جرائم التنمر الالكتروني ضد الأحداث حيث تتم غالبية الأفعال الإجرامية عبر وسائل الاتصال الرقمية، كالمحادثات الخاصة أو الرسائل أو التعليقات عبر المنصات الالكترونية، ففي هذه الجرائم قد يشكل التنصت أو تسجيل المحادثات وسيلة حاسمة لكشف هوية الجاني وإثبات السلوك الإجرامي، خاصة في حالات الابتزاز أو التهديد أو الإساءة المتكررة غير أن خصوصية هذه الجرائم، لكونها تمس فئة الأحداث، تفرض ضرورة تشديد الضوابط القانونية عند اللجوء إلى هذه الوسائل بما يضمن حماية الضحية دون المساس غير المشروع بحقوق الأفراد[2].

وبالتالي، فإن استخدام وسائل مراقبة الاتصالات في جرائم التنمر الالكتروني ضد الأحداث يجب أن يقوم على توازن دقيق بين متطلبات الكشف عن الحقيقة وحماية الخصوصية، بحيث يسمح بها في إطار قانوني منظم يراعي خطورة الجريمة وحاجة الضحية إلى الحماية دون فتح المجال لانتهاكات غير مبررة للحقوق الأساسية[3].

ويضاف إلى ما تقدم أن الاعتماد على مراقبة الاتصالات في جرائم التنمر الالكتروني ضد الأحداث لا يقتصر على كونه وسيلة لكشف الجريمة، بل يمتد ليكون أداة وقائية تسهم في الحد من تفاقم الأضرار التي قد تلحق بالضحية، فغالباً ما تتسم

---

[1] أحمد رعد محمد الجيلاوي، التسجيل الصوتي وحجيته في الاثبات الجنائي، المركز العربي للنشر، القاهرة، 2017، ص 50.

[2] حميد عبد حمادي، مشروعية الدليل الالكتروني الناشئ عن التفتيش الجنائي، مجلة المدارات العملية للعلوم الإنسانية والاجتماعية، العدد 1، العراق، 2023، ص77.

[3] عبد المنعم أحمد، الجرائم الناشئة عن إساءة استعمال الهاتف المحمول ومدى المسؤولية عنها، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2013، ص 145.

هذه الجرائم بالاستمرارية والتكرار، الأمر الذي يجعل التدخل المبكر أمراً ضرورياً لحماية الحدث من الآثار النفسية والاجتماعية الخطيرة مثل القلق والاكتئاب والعزلة، ومن هنا فإن تمكين الجهات المختصة من تتبع الاتصالات المشبوهة يمكن أن يسهم في وقف الاعتداءات قبل تصاعدها[4].

ويمكن تعريف التسجيل الصوتي بأنه: "عبارة عن عملية ترجمة للتغيرات المؤقتة لموجات الصوت الخاصة بكلام أو موسيقى إلى نوع آخر من الموجات أو التغيرات الدائمة، ويكون التسجيل عادة بواسطة آلة تترجم موجات الصوت إلى اهتزازات خاصة، وتتفق هذه الاهتزازات مع الأصوات التي تحدثها بالضبط[5]، فالتسجيل لغة: سجل، يسجل، تسجيلاً: نقل الصوت إلى شريط آلة خاصة، مسجل: آلة للتسجيل[6].

أما اصطلاحاً: تعتبر المحادثات الشخصية والمكالمات التليفونية أسلوب من أساليب الحياة الخاصة للناس فهذه الأحاديث والمكالمات مجال لتبادل الأسرار وبسط الأفكار الشخصية الصحيحة دون حرج أو خوف من تنصت الغير، وتعني مراقبة المحادثات التليفونية من ناحية التنصت بمعني الأداة على المحادثات أو تسجيل المحدثات بأجهزة التسجيل، ولا يهم المستخدمة في تسجيل المحادثات التليفونية طالما أنها نقلت إلينا مضمون هذه المحادثة [7].

كما إن الطبيعة الرقمية لهذه الجرائم تفرض الاعتماد على الأدلة الالكترونية التي قد تكون عرضة للمحو أو التعديل في أي وقت مما يزيد من أهمية اللجوء إلى وسائل المراقبة والتسجيل في الوقت المناسب، فالتأخر في اتخاذ هذه الإجراءات قد يؤدي إلى ضياع الأدلة، وبالتالي إفلات الجناة من المساءلة، لذلك فإن مراقبة الاتصالات تمثل في كثير من الحالات الوسيلة الأكثر فاعلية للحفاظ على الدليل الرقمي وضمان سلامته، ومع ذلك لا بد من التأكيد على أن هذه الوسائل يجب أن تمارس ضمن إطار من الضمانات القانونية الصارمة خاصة عندما يتعلق الأمر بالأحداث سواء كانوا ضحايا أو حتى أطرافاً في الجريمة، إذ ينبغي أن تخضع المراقبة لرقابة قضائية دقيقة وأن تكون محددة في نطاقها الزمني والموضوعي مع الالتزام بعدم التوسع في جمع البيانات أو استخدامها خارج الغرض المحدد لها[8].

كما يبرز في هذا السياق دور الجهات القضائية في تقدير مشروعية الأدلة المستمدة من مراقبة الاتصالات حيث يتعين عليها التحقق من مدى احترام الإجراءات القانونية عند الحصول عليها ومدى ارتباطها المباشر بالجريمة محل التحقيق، فإذا ثبت أن هذه الأدلة تم الحصول عليها بطرق مشروعة، فإنها تعد ذات قيمة قانونية يمكن الاستناد إليها في الإثبات، أما إذا شابها خرق للضوابط القانونية، فقد يؤدي ذلك إلى استبعادها حمايةً للحقوق والحريات، وفي ضوء ذلك يمكن القول إن مواجهة جرائم التنمر الالكتروني ضد الأحداث تتطلب تبني مقاربة متوازنة تجمع بين الفعالية في الكشف عن الجريمة، واحترام الضمانات القانونية بحيث لا تتحول وسائل المراقبة إلى أداة لانتهاك الخصوصية بل تبقى وسيلة مشروعة تهدف إلى حماية المجتمع، ولا سيما الفئات الأكثر ضعفاً كالأحداث[9].

2-المراقبة الالكترونية

يقصد بالمراقبة الالكترونية إن مراقبة الهاتف تعني من ناحية التنصت على المحادثات، ومن ناحية أخرى تسجيلها بأجهزة

---

[4] حسنين المحمدي بوادي، الوسائل العلمية الحديثة في الاثبات الجنائي، منشأة المعارف، القاهرة، 2008، ص 67.

[5] أشرف قنديل، الوسائل الالكترونية ودورها في الاثبات الجنائي، دار الجامعة الجديدة، القاهرة، 2018، ص 169.

[6] عبد الغني أبو العزم، معجم الغني، دار الكتب العلمية، بيروت، 2013، ص 573.

[7] سمير الأمين، مراقبة التلفونات والتسجيلات الصوتية والمرئية، دار الكتب، القاهرة، 2000، ص 7.

[8] ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، القاهرة، 2009، ص 140.

[9] جواهر قوادري، صامت، رقابة سلطة التحقيق على اعمال الضبطية القضائية، دار الجامعة الجديدة، القاهرة، 2010، ص 35.

التسجيل، ويمكن الاكتفاء بمباشرة إحدى هاتين العمليتين التنصت أو التسجيل لقيام المراقبة، فالأخيرة قد تتم بمجرد التنصت، أو قد يكتفى بالتسجيل الصوتي الذي يسمع بعد ذلك، من ذلك يتبين أن مراقبة الإتصالات الهاتفية تعني أكثر من التنصت عليها، إذ يتم تتبع والتنصت عليها فضلاً عن تسجيلها [10].

وتتجلى أهمية هذه المراقبة في جرائم التنمر الالكتروني ضد الأحداث حيث تتم هذه الجرائم عبر وسائل الاتصال الرقمية مثل تطبيقات المراسلة ومنصات التواصل الاجتماعي، ففي هذه الحالة يمكن للضبط القضائي وفقاً للقانون مراقبة حسابات أو محادثات يشتبه في استخدامها للإساءة أو التهديد أو الابتزاز، بهدف كشف الجاني وحماية الحدث الضحية، كما يمكن تتبع الأنشطة الرقمية للمشتبه بهم مثل اختراق الحسابات أو نشر محتوى مسيء، مما يسهم في جمع الأدلة وإثبات الجريمة، غير أن خصوصية هذه الجرائم لكونها تمس فئة الأحداث، تفرض ضرورة الالتزام بضوابط أكثر دقة، بحيث تقتصر المراقبة على نطاق الجريمة فقط، دون التوسع في انتهاك الخصوصية مع مراعاة السرية وعدم إفشاء البيانات وبالتالي فإن المراقبة الالكترونية تعد وسيلة فعالة في مواجهة جرائم التنمر الالكتروني شريطة أن تمارس في إطار قانوني منظم يحقق العدالة ويحمي الحقوق في آنٍ واحد.

ورغم توكيد المشرع اللبناني على سرية التخابر عبر وسائل الإتصال، إلا أنه أجاز المراقبة الالكترونية ضمن شروط معينة، بهدف رصد الجرائم المستحدثة وضبطها، فالمادة الأولى من قانون التنصت رقم (140/99) تنص على أن «الحق في سرية التخابر الجاري داخلياً وخارجياً بأي وسيلة من وسائل الإتصال السلكية واللاسلكية بكل أنواعها مصون وفي القانون، ولا يخضع لأي نوع من أنواع التنصت أو المراقبة أو الإعتراض، أو الإفشاء إلا في الحالات التي ينص عليها هذا القانون، وبواسطة الوسائل التي يحددها ويحدد أصولها».

وتنص المادة (2) من ذات القانون على أنه «في حالات الضرورة القصوى، لقاضي التحقيق الأول في كل محافظة إما عفواً أو بناءً لطلب خطي من القاضي المكلف بالتحقيق أن يقرر اعتراض المخابرات التي تجري بواسطة أي من وسائل الاتصال المبينة في المادة الأولى، وذلك في كل ملاحقة بجرم يعاقب عليه بالحرمان من الحرية لمدة لا تقل عن سنة، يكون القرار خطياً ومعللاً ولا يقبل أي طريق من طرق الطعن، وتنص المادة الثالثة على ألا تتجاوز المدة شهرين وألا تمدد إلا وفقاً للأصول»، وتنص المادة (4) على أنه «يجري اعتراض المخابرات وتسجيلها ووضع محضر بمضمونها من قبل موظف الضابطة العدلية المكلف وفقاً للأصول، وذلك تحت سلطة القاضي الصادر عنه القرار ورقابته وإشرافه».

كما أن فعالية المراقبة الالكترونية في هذا المجال ترتبط بمدى قدرتها على مواكبة التطور التقني المستمر، إذ لم تعد جرائم التنمر الالكتروني تقتصر على الرسائل النصية أو المكالمات، بل امتدت إلى الصور والفيديوهات والبث المباشر والتطبيقات المشفرة، الأمر الذي يفرض على الجهات المختصة استخدام وسائل تقنية متقدمة قادرة على تحليل هذا النوع من البيانات، ويسهم ذلك في كشف أنماط السلوك الإجرامي وتحديد المسؤوليات بدقة خاصة في الحالات التي يكون فيها التنمر جماعياً أو يتم عبر حسابات وهمية.

ثانياً: حالات اللجوء إلى المراقبة الالكترونية

أثار موضوع التكييف القانوني للمراقبة جدالاً فقهياً وتمحور الخلاف حول اعتبار الدليل المستمد من مراقبة المحادثات الهاتفية دليلاً مستقلاً بذاته أم يندرج تحت نوع من معين الإجراءات المعروفة في القانون، من خلال ذلك نرى أن هنالك

[10] آدم عبد البديع، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، أطروحة مقدمة لنيل شهادة الدكتوراه الى جامعة المنصورة، القاهرة، 2010، ص 538.

أنواع للمراقبة نذكر منها:

1- التسجيل والمراقبة القضائية

وفي إطار جرائم التنمر الالكتروني ضد الأحداث، تبرز أهمية المراقبة القضائية بشكل واضح، حيث قد يصعب الكشف عن الجناة بوسائل تقليدية، خاصة عند استخدام حسابات وهمية أو تطبيقات مشفرة، وهنا يمكن للسلطة القضائية أن تأذن بمراقبة المحادثات أو الحسابات الرقمية التي يشتبه في استخدامها لارتكاب أفعال التنمر مثل التهديد أو الابتزاز أو التشهير[11]، كما تتيح هذه المراقبة إمكانية جمع أدلة رقمية موثوقة يمكن الاستناد إليها أمام القضاء بما يسهم في حماية الحدث الضحية وضمان عدم إفلات الجاني من العقاب غير أن ذلك يظل مشروطاً باحترام الضوابط القانونية من حيث تحديد مدة المراقبة ونطاقها وعدم التوسع فيها بما يمس خصوصية الأفراد دون مبرر[12].

2-التسجيل والمراقبة الادارية

يقصد به التنصت التي تجريه السلطة الإدارية أو السياسية بقصد جمع المعلومات المرتبطة بالأمن الوطني لمنع كل خطر يهدد كيان الدولة والمجتمع وهذا النوع قد قنن في بعض التشريعات منها اللبنانية التي تحول الدفاع الوطني ووزير الداخلية سلطة ممارسة تسجيل الأصوات بقرار خطي ومعلل يوافق عليه رئيس الوزراء وفق شروط معينة، فالتنصت الإداري ليس من إجراءات التحقيق ولا يقصد به الحصول على أدلة جريمة وإنما الغاية منه الحفاظ على كيان الدولة وبقائها ولكنهم لا يختلفان من حيث الأثر القانوني إذا تمخض عنه كشف جريمة أو العثور على أدلة جريمة وهي المتابعة والجزاء، لقد ذهب جانب من الفقه [13]، إلى اعتبار مراقبة المكالمات الهاتفية نوعاً من التفتيش وتخضع لضمانات وقيود ممارسته، ويستند أنصار هذا الاتجاه إلى اعتبارين: أحدهما موضوعي والآخر شكلي، فالاعتبار الموضوعي قد عبر عنه منتهييه بأن التفتيش هو التنقيب في وعاء السر بهدف ضبط ما يفيد في كشف الحقيقة، فالغاية منه هي كشف ستار السرية وإزاحة ستار الكتمان عنها للاستفادة بها في تقصي الحقيقة.

وهذا المعنى لا يتقيد بالكيان المادي لوعاء السر، فيستوي أن يكون مسكناً أو شخصاً أو متاعاً أو رسائل أو أسلاكاً هاتفية إذ لا عبرة بطبيعة كيان السر ذاته أو يكون شيئاً معنوياً يتعذر ضبطه إلا إذا اندمج في كيان مادي وذلك كالأسرار المدونة في الخطابات والمكالمات الهاتفية المسجلة على أشرطة التسجيل [14].

ويرى جانب من الفقه أن مراقبة المحادثات الهاتفية ليست نوعاً من التفتيش، إنما هي عبارة عن إجراء من إجراءات التحقيق، فهي من قبيل الملاحظة القضائية المباشرة [15]، إذ يشترط لممارستها أن تكون لذلك فائدة في ظهور الحقيقة في جريمة تتولى سلطات التحقيق أمر البحث فيها، ولكن ذلك الإجراء إجراء من نوع خاص يماثل في طبيعته التفتيش ولكنه ليس في حقيقته تفتيشاً، ومن حيث إن أقرب الإجراءات إليه هو إجراء التفتيش فقد عالجه المشرع في النطاق الذي عالج فيه التفتيش وأحاطه بالضمانات التي تحيط بتفتيش الرسالة.

يتضح أن مراقبة الاتصالات الالكترونية تمثل وسيلة أساسية في كشف جرائم التنمر الالكتروني ضد الأحداث، نظراً

---

[11] نادر عبد العزيز شافي، شروط التنصت واعتراض وسائل الاتصال، بحث منشور على الموقع الرسمي للجيش اللبناني، http://www.lebarmy.gov.pn/ar/mens/?1395#.vrv4604rtqo01 تاريخ الزيارة، 2026/1/8.

[12] أشرف عبد القادر قنديل، الوسائل الالكترونية ودورها في الاثبات الجنائي، مرجع سابق، ص 172.

[13] صالح عبد الزهرة حسون، أحكام التفتيش وآثاره في القانون العراقي، دار السنهوري، بغداد، 2003، ص 141.

[14] حسن صادق المرصفاوي، المرصفاوي في المحقق الجنائي، منشأة المعارف، القاهرة، 2007، ص 78.

[15] ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دار النهضة، القاهرة، 2010، ص 347.

لطبيعتها الرقمية وصعوبة إثباتها بالوسائل التقليدية غير أن اللجوء إلى هذه الوسيلة يثير إشكاليات قانونية تتعلق بحماية الخصوصية ومشروعية الدليل مما يستوجب إخضاعها لضوابط قانونية صارمة وعلى رأسها الإذن القضائي وتحديد نطاق المراقبة، كما أن خصوصية فئة الأحداث تفرض تعزيز هذه الضوابط لضمان عدم المساس بحقوقهم أثناء إجراءات التحقيق، وبالتالي فإن فعالية هذه الوسيلة ترتبط بتحقيق التوازن بين مقتضيات العدالة الجنائية وحماية الحقوق والحريات.

الفرع الثاني

شروط المراقبة الالكترونية في جرائم التنمر الالكتروني الواقعة على الأحداث

لما كانت المحادثات الالكترونية تعبيراً عن الحياة الخاصة وداخلة في نطاقها، فإنها تستمد حصانتها من حرمة هذه الحياة، وتزداد أهمية هذه الحماية عندما يتعلق الأمر بالأحداث بوصفهم فئة أكثر هشاشة تستوجب رعاية قانونية خاصة، ومن ثم فإن علة تجريم الاعتداء على هذه المحادثات، سواء باستراق السمع أو تسجيلها تتمثل في حماية حق الحدث في الخصوصية وصون سلامته النفسية من أي انتهاك لا سيما في إطار جرائم التنمر الالكتروني التي قد تستهدفه عبر هذه الوسائل[16].

أولاً_ مشروعية تسجيل ومراقبة الاتصالات

لا خلاف في أن تنظيم الإجراءات الجنائية يقوم على مفترضات ومرتكزات أساسية لا يمكن بدونها وصف النظام القانوني بالمشروعية ويأتي في مقدمتها مبدأ الشرعية الإجرائية، الذي يضاهي في أهميته مبدأ شرعية الجرائم والعقوبات، وتعد هذه الشرعية أداة أساسية لتنظيم استعمال السلطة في مواجهة الجريمة، بما يضمن حماية الحريات وحقوق الإنسان، وبالأخص حقوق الأحداث الذين يتمتعون بحماية مضاعفة في التشريعات الحديثة، وفي سياق جرائم التنمر الالكتروني ضد الأحداث، تبرز الحاجة إلى اللجوء إلى تسجيل ومراقبة الاتصالات كوسيلة فعالة للكشف عن الجريمة وإثباتها، نظراً لوقوعها في بيئة رقمية يصعب تتبعها بالوسائل التقليدية، غير أن مشروعية هذا الإجراء تظل رهناً بتوافر ضوابط قانونية دقيقة، تضمن عدم التعسف في استخدامه وتحقق التوازن بين مصلحة المجتمع في مكافحة الجريمة وحق الحدث في الخصوصية[17].

ولا جدال في أن السلطات المختصة تلاحق الواقعة الإجرامية منذ لحظة تجريمها مروراً بمراحل التحقيق والإجراءات الجزائية وصولاً إلى تنفيذ العقوبة، وفي جميع هذه المراحل تسعى السلطة التشريعية إلى وضع قواعد تكفل حماية حقوق الإنسان، ومنع المساس بها إلا في الحدود التي يجيزها القانون، ويزداد هذا الالتزام أهمية في الجرائم التي تمس الأحداث، حيث يتعين أن تتم إجراءات المراقبة والتسجيل في إطار من الضمانات المشددة، بما يحقق الحماية للضحية دون الإخلال بحقوق الأطراف الأخرى[18]، وعليه فإن الإدانة في جرائم التنمر الالكتروني الواقعة على الأحداث لا بد أن تقوم على أدلة مشروعة تم الحصول عليها وفقاً للقانون وبما يتفق مع قواعد الأخلاق والنزاهة، لاسيما أن هذه الجرائم تعتمد في إثباتها بشكل أساسي على مخرجات الوسائل الالكترونية التي تتطلب درجة عالية من الثقة والمصداقية، نظراً لاعتماد الأفراد عليها في تعاملاتهم اليومية.

وفي هذا الإطار يقتضي مبدأ مشروعية الدليل الجنائي في مجال الأدلة الرقمية أن تكون إجراءات الحصول على هذه المخرجات متوافقة مع القواعد القانونية والإجرائية المستقرة، وبما ينسجم مع القيم الأساسية للمجتمع خاصة عندما يتعلق الأمر بحماية الأحداث، فالتعامل مع البيانات الالكترونية، كالمحادثات أو التسجيلات أو الرسائل يجب أن يتم وفق ضوابط

---

[16] حسين إبراهيم، الوسائل العلمية الحديثة في الإثبات الجنائي، المؤسسة الحديثة للكتاب، القاهرة، 2014، ص 425.

[17] عمار عباس الحسيني، مبادئ علمي الاجرام والعقاب، التيمي للنشر، بغداد، 2012، ص 21.

[18] عمار عباس الحسيني، مبادئ علمي الاجرام والعقاب، مرجع سابق، 149.

محددة تضمن عدم انتهاك الخصوصية أو التعدي على الحقوق الأساسية، ويترتب على ذلك أنه إذا تم جمع الأدلة الالكترونية في جرائم التنمر ضد الأحداث بطريقة تخالف القواعد القانونية المنظمة، كأن تتم المراقبة أو التسجيل دون إذن قضائي أو خارج الحدود التي رسمها القانون، فإن هذه الأدلة تعد باطلة ولا يجوز الاستناد إليها في إصدار حكم بالإدانة، ويعد هذا البطلان ضمانة أساسية لحماية الحقوق والحريات، ويؤكد أن الغاية من مكافحة الجريمة لا تبرر استخدام وسائل غير مشروعة، حتى في مواجهة جرائم خطيرة تمس فئة الأحداث[19].

ثانياً_ أهمية مراقبة المكالمات وآلية المراقبة

القصد بالمكالمات الهاتفية الحديث الذي يتم بين شخصين أو أكثر غير متواجدين في مكان واحد بوساطة استخدام الهاتف أو باستخدام جهاز من أجهزة الإتصال الحديثة سلكية كانت أم غير سلكية، وهذا يعني إن مراقبة الهاتف تعني من ناحية التنصت على المحادثات، ومن ناحية أخرى تسجيلها بأجهزة التسجيل، ويمكن الاكتفاء بمباشرة إحدى هاتين العمليتين التنصت أو التسجيل لقيام المراقبة، وتبرز أهمية مراقبة المكالمات بشكل خاص في جرائم التنمر الالكتروني ضد الأحداث، نظراً لأن هذه الجرائم غالباً ما تتم عبر المحادثات الخاصة أو الاتصالات الرقمية، مثل الرسائل الصوتية أو المكالمات عبر التطبيقات، ففي حالات التهديد أو الابتزاز أو الإساءة المتكررة، يمكن لمراقبة هذه الاتصالات أن تكشف مضمون السلوك الإجرامي، وتحدد هوية الجاني، وتوفر دليلاً مباشراً يمكن الاستناد إليه في الإثبات الجنائي.

1-أهمية مراقبة المكالمات

يثير التنصت على المكالمات الهاتفية وكذلك مراقبة الاتصالات الرقمية، إشكاليات فقهية متعددة تتعلق بمدى مشروعيتها وقيمتها القانونية كدليل في الإثبات الجنائي، خاصة في الجرائم الحديثة كجرائم التنمر الالكتروني ضد الأحداث، ويلاحظ أن المحققين يميلون إلى اللجوء إلى هذه الوسيلة انطلاقاً من أهميتها في كشف الجرائم التي تمس أمن المجتمع وسلامته حيث تقدم المصلحة العامة على المصلحة الفردية المرتبطة بالخصوصية، لاسيما عندما يكون الهدف حماية فئة الأحداث من أفعال التهديد أو الابتزاز أو الإساءة المتكررة[20].

وبناءً على ذلك أصبح من الضروري التوفيق بين المصلحتين العامة والخاصة نظراً لكون مراقبة المكالمات تمثل إجراءً خطيراً يمس الحرية الشخصية، الأمر الذي يستوجب إخضاعه لضوابط قانونية صارمة كالحصول على إذن قضائي وتحديد نطاق المراقبة ومدتها بما يضمن تحقيق الغاية من الكشف عن الجريمة دون المساس غير المشروع بحقوق الأفراد، خاصة عندما يتعلق الأمر بالأحداث الذين يتمتعون بحماية قانونية خاصة[21].

ومن خلال الواقع العملي يتبين أن العديد من الأفعال التي ترتكب عبر الهاتف النقال أو التطبيقات الرقمية في إطار التنمر الالكتروني ضد الأحداث، هي في أصلها جرائم تقليدية كالقذف والسب والتهديد، غير أن الوسيلة التقنية قد منحتها نطاقاً أوسع وخطورة أكبر، إذ أصبح الهاتف أو التطبيق الرقمي أداة رئيسية في تنفيذ السلوك الإجرامي وتكراره، وفي هذا السياق تلعب وسائل المراقبة دوراً مهماً في تتبع هذه الأفعال وكشف مرتكبيها سواء من خلال تسجيل المكالمات أو تحديد الموقع أو تحليل البيانات الرقمية، بما يسهم في حماية الضحايا من الأحداث وتقديم الجناة إلى العدالة.

2-آلية مراقبة المكالمات

تتم مراقبة الاتصالات الالكترونية باستخدام أجهزة وتقنيات متطورة تصمم خصيصاً لتعقب الاتصالات والتقاطها وتحليلها دون أن يشعر أطراف الاتصال بخضوع محادثاتهم للمراقبة، وتكمن أهمية هذه الآلية في قدرتها على كشف الأفعال

---

[19] احمد ضياء الدين محمد، مشروعية الدليل في المواد الجنائية، دار النهضة، القاهرة، 2010، ص 402.

[20] علي وجيه حرقوص، قاضي التحقيق، ط2، منشورات الحلبي الحقوقية، بيروت، 2011، ص 138.

[21] سليم علي عبده، التفتيش في ضوء قانون أصول المحاكمات الجزائية الجديد، منشورات الحلبي الحقوقية، بيروت، 2006، ص 91.

الإجرامية التي تتم في الخفاء، وهو ما يتناسب مع طبيعة جرائم التنمر الالكتروني ضد الأحداث التي ترتكب غالباً عبر وسائل اتصال خاصة يصعب الوصول إليها بالطرق التقليدية[22].

حيث يتم وضع الخادم المعلوماتي لمزود الخدمات تحت المراقبة باستخدام تقنيات وبرامج متطورة تقوم بتعقب والتقاط وتخزين جميع المحادثات والرسائل الصادرة والواردة عبر الخادم المعلوماتي المراقب فيما إذا كان يشتبه باحتوائها على معلومات مجرمة أو متعلقة بجرائم خطيرة من مثل الجرائم الإرهابية أو جرائم الإتجار بالمخدرات وهذا هو ما يفهم أيضاً، من نص المادتين (20 و21) من الاتفاقية الأوروبية لمكافحة الجرائم الالكترونية التي استخدمت مصطلح الوسائل الفنية للدلالة على هذه الأجهزة والتقنيات[23].

ويمكن أن يتم التنصت عن طريق التجسس والذي يقصد به في هذا الصدد الإطلاع على معلومات خاصة بالغير مؤمنة في جهاز آخر، وليس مسموحاً لغير المخولين الإطلاع عليها، وذلك عن طريق تعقب الإتصالات التي يجريها المتهم مع غيره، أو عن طريق تعقب الجهاز الذي يستخدمه المتهم، وذلك بتحويله إلى أداة تجسس على المتهم ، ويكون ذلك عن طريق تشغيل الميكروفون الداخلي أو الكاميرا الخاصة بالجهاز عن طريق زرع برنامج في الجهاز دون علم المتهم به، إذ يمكن عن طريق هذا البرنامج تحديد أماكن المطلوبين بالتحديد حتى وإن كانت أجهزتهم في حالة إطفاء، ولا يمكن وقف عملية التجسس هذه إلا عن طريق نزع بطارية الهاتف النقال والشريحة نزعاً تاماً[24].

وفي سياق جرائم التنمر الالكتروني ضد الأحداث، تعد هذه الآليات ذات أهمية كبيرة، إذ تمكن الجهات المختصة من رصد الرسائل المسيئة أو التهديدات أو حالات الابتزاز التي يتعرض لها الحدث، وتحديد مرتكبيها حتى في حال استخدامهم لحسابات وهمية أو وسائل اتصال مخفية غير أن استخدام هذه الوسائل يجب أن يتم في إطار قانوني دقيق يراعي خصوصية الأفراد، ويمنح حماية خاصة للأحداث، بما يحقق التوازن بين فعالية الكشف عن الجريمة وصون الحقوق والحريات، والجدير بالذكر أن المراقبة لا تقتصر على تعقب أجهزة الهواتف النقالة فقط فكل جهاز من تلك الأجهزة الرقمية الحديثة يمكن أن يتم زراعة هذا البرنامج به ابتداء من الحاسوب ومشغلات الموسيقى والأجهزة الرقمية المثبتة في السيارات لنقل وتسجيل كل ما يدور من أحاديث سواء مباشرة أم تحفظ لكي يتم الاستماع اليها فيما بعد [25].

فضلاً عن ذلك فإن مراقبة المكالمات الهاتفية أضحت تتم بالاستعانة بالأقمار الصناعية [26]، وطائرات التجسس المسيرة بالطرق اللاسلكية، فضلاً عن البريد الالكتروني تعدد استخداماتها فمنها ما يلتقط الصوت ومنها ما يلتقط الفاكس والرسال[27].

المطلب الثاني

التزامات مقدمي الخدمات المعلوماتية في سبيل مكافحة جرائم التنمر الالكتروني الواقعة على الأحداث

أدى الانتشار الواسع لخدمات الإنترنت ومنصات التواصل الاجتماعي إلى تنامي دور مقدمي الخدمات المعلوماتية في البيئة الرقمية، باعتبارهم وسيطاً أساسياً في نقل وتخزين البيانات ومع تزايد جرائم التنمر الالكتروني ولا سيما تلك التي

---

[22] كوثر أحمد خالد، الاثبات الجنائي بالوسائل العلمية الحديثة، ط1، مكتب التفسير للنشر، أربيل، 2007، ص 219-220.

[23] رشاد خالد عمر، المشاكل القانونية في الجرائم المعلوماتية، مرجع سابق، ص 175.

[24] عادل عزام الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، دار الثقافة، عمان، 2011، ص 164.

[25] مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت، ط1، دار الكتب القانونية، القاهرة، 2005، ص 22.

[26] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنلوجيا الاتصالات الحديثة، مرجع سابق، ص 513.

[27] فايق عوضين تحفة، الحماية القانونية والأمنية للاتصالات السلكية واللاسلكية، دار الكتب العلمية، القاهرة، 2014، ص 393.

تستهدف الأحداث، برزت الحاجة إلى تحديد التزامات هذه الجهات في مواجهة هذا النوع من الجرائم، إذ لم يعد دورها يقتصر على تقديم الخدمة، بل أصبح يمتد إلى المساهمة في الحد من المحتوى الضار وحماية المستخدمين كما تفرض طبيعة هذه الجرائم ضرورة التعاون بين مقدمي الخدمات والجهات المختصة لكشف الجناة ومنع تفاقم الأضرار، ومن هنا تبرز أهمية تنظيم التزامات مقدمي الخدمات المعلوماتية في إطار قانوني يوازن بين حرية الاستخدام وحماية الفئات الأكثر عرضة للخطر، كالأحداث[28].

استناداً لما سلف سوف نقوم بتقسيم هذا المطلب إلى فرعين، الفرع الأول: التزامات مقدمي الخدمات المعلوماتية، أما الفرع الثاني: مسؤولية مقدمي الخدمات المعلوماتية.

الفرع الأول

التزامات مقدمي الخدمات المعلوماتية

تتمثل أهمية القوانين الإجرائية الجزائية في تحقيق التوازن بين مصلحة المجتمع في ملاحقة الجناة وكشف الجرائم وبين حماية حقوق الأفراد، ولاسيما حقهم في الحرية والخصوصية وضمان حق الدفاع، وتبرز هذه الأهمية بشكل أكثر وضوحاً في جرائم التنمر الالكتروني الواقعة على الأحداث نظراً لحساسية هذه الفئة وضرورة توفير حماية قانونية خاصة لها، مع الحفاظ في الوقت ذاته على ضمانات المحاكمة العادلة وعدم المساس بحقوق الأفراد دون مبرر قانوني.

أولاً_ أهمية القوانين الإجرائية الجزائية في بيان التزامات مورد الخدمات

يلعب مقدمو خدمات الإنترنت دوراً محورياً في التغلب على الصعوبات التي تواجه الجهات التحقيقية في جرائم التنمر الالكتروني ضد الأحداث، إذ يسهمون في تسهيل عملية التعرف على مرتكب الجريمة أو على الأقل تحديد الوسيلة التي استخدمت في ارتكابها، مما يساعد في الوصول إلى الفاعل الحقيقي. كما يمكن الاستناد إلى البيانات التي يحتفظ بها مقدم الخدمة كدليل أو قرينة تعزز عملية الإثبات، خاصة في الجرائم التي تتم عبر وسائل رقمية يصعب تتبعها بالطرق التقليدية ويتحقق ذلك من خلال نظام بروتوكول الإنترنت(IP) الذي يعد من أهم الوسائل التقنية المستخدمة في تعيين الأجهزة المتصلة بالشبكة عبر عناوين رقمية فريدة، تتيح تحديد الموقع الجغرافي التقريبي للمستخدم ومن خلال هذه العناوين يمكن من حيث المبدأ تعقب النشاط الالكتروني المرتبط بأفعال التنمر حتى في حال استخدام الجناة لأسماء مستعارة أو بيانات غير صحيحة إذ يظل بالإمكان تحديد الخادم أو الملقم الذي تم من خلاله الاتصال.

وغالباً ما يكون هذا الخادم تابعاً لمقدم خدمة الإنترنت، الذي يحتفظ ببيانات المستخدمين نتيجة العلاقة التعاقدية التي تربطه بهم مما يتيح للجهات المختصة ووفقاً للقانون الوصول إلى الهوية الحقيقية للمستخدم وتكتسب هذه المسألة أهمية خاصة في جرائم التنمر الالكتروني ضد الأحداث حيث يلجأ الجناة في كثير من الأحيان إلى إخفاء هوياتهم أو استخدام حسابات وهمية بهدف الإفلات من المسؤولية الأمر الذي يجعل من دور مقدمي الخدمات عنصراً أساسياً في كشف الجريمة وتحقيق العدالة[29].

ثانياً_ دور مورد الخدمة

إن لمورد خدمة الإنترنت دوراً بالغ الأهمية في معالجة الإشكاليات التي تثيرها الإجراءات الجنائية في جرائم التنمر الالكتروني الواقعة على الأحداث، لما يقدمه من تسهيلات حيوية لعمل جهات الضبط القضائي أثناء التحقيق إذ يمكن هذه الجهات من تحديد وسيلة ارتكاب الجريمة، فضلاً عما يتوافر لدى مقدم الخدمة من بيانات مخزنة يمكن اعتبارها

[28] محمد عبد الكريم حسين الداوودي، المسؤولية الجنائية لمورد خدمة الإنترنت، مرجع سابق، ص114.

[29] طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، مرجع سابق، ص243.

بمثابة مسرح رقمي للجريمة بما تتضمنه من معطيات تقنية تكشف عن هوية الجاني وتحركاته ونشاطه الالكتروني الأمر الذي يسهم في دعم عملية التحقيق وتعزيز الأدلة، كما إن هذه البيانات قد تشكل قرائن قوية تساند الأدلة الأخرى وتساعد في بناء قناعة القاضي المختص عند تقديره لثبوت الجريمة، خاصة في الجرائم التي تتسم بطابع خفي مثل جرائم التنمر الالكتروني ضد الأحداث حيث يصعب الوصول إلى الجاني دون الاستعانة بالبيانات التقنية التي يحتفظ بها مقدم الخدمة، ونظراً لهذه الأهمية تبرز ضرورة قيام الدول بوضع أطر قانونية واضحة تنظم عمل موردي خدمات الإنترنت وتلزمهم بحفظ بيانات المستخدمين لفترات محددة، بما يتيح للجهات المختصة الاستفادة منها عند الحاجة مع ضرورة مراعاة عدم التعسف في ذلك أو انتهاك خصوصية الأفراد ويتطلب ذلك تحقيق توازن دقيق بين متطلبات مكافحة الجريمة وحماية الحقوق والحريات ولا سيما في ما يتعلق بفئة الأحداث التي تستوجب عناية قانونية خاصة.

وأيضاً توفير الأدلة من خلال حفظ المعطيات لدى خوادم مورد خدمة الإنترنت، والأدلة التي يستحصل عليها من خلال معاينة أداة الجريمة بعد ضبطها من خلال معرفة ال (IP) الخاص به عن طريق المورد[30]، والتي تساعد على إيجاد الجاني كما وتساعد أيضاً في إثبات الجريمة، وتوفير الأدلة التي من الممكن أن تكون من الركائز الأساسية التي تساهم في إثبات الجريمة وبالتالي مساعدة القاضي المختص في بناء أحكامه، ولكن هنالك إشكاليات أخرى تثيرها هذه الأدلة والتي تسمى أحياناً بالأدلة الرقمية، وتتمثل هذه الإشكاليات في مدى حجية الأدلة الرقمية في إثبات الجريمة، ومدى إمكانية بناء الحكم عليها من قبل القاضي المختص، وغيرها من الإشكاليات التي من الإمكان أن تكون كل واحدة منها موضوع أبحاث ودراسات، إلا أن هذه الإشكاليات من الممكن أن تقل حدتها من خلال سن التشريعات والقوانين بصددها هذا بخصوص أهمية مورد خدمة الإنترنت ودوره في الإجراءات الجنائية في مساعدة الحكومة وأعضاء الضبط القضائي في سبيل مكافحة جرائم تقنية المعلومات الواقعة على الحكومة ذاتها[31]، ولا يقتصر دور مقدمي الخدمات المعلوماتية على مجرد تمكين الجهات المختصة من تتبع العناوين الالكترونية وتحديد هوية المستخدمين، بل يمتد ليشمل التزامات قانونية وتقنية أوسع تفرضها طبيعة جرائم التنمر الالكتروني، وخاصة تلك التي تستهدف الأحداث، فهذه الجرائم غالباً ما ترتكب عبر منصات التواصل الاجتماعي أو تطبيقات المراسلة مما يجعل مقدمي هذه الخدمات في موقع مركزي يمكنهم من رصد المحتوى الضار أو التدخل للحد من انتشاره[32].

ومن أبرز هذه الالتزامات التزام مقدمي الخدمة بحفظ البيانات المتعلقة بالمستخدمين لفترة زمنية معينة، بما في ذلك بيانات الاتصال وسجلات الدخول وعناوين(IP) ، وذلك بهدف تمكين السلطات المختصة من الرجوع إليها عند الضرورة في سياق التحقيق، ويعد هذا الالتزام من أهم الوسائل التي تساعد في كشف مرتكبي جرائم التنمر الالكتروني ضد الأحداث، حيث قد يعتمد الجناة على إخفاء هوياتهم أو استخدام حسابات وهمية، إلا أن البيانات التقنية المخزنة لدى مقدم الخدمة تبقى قادرة على كشفهم[33]، كما يترتب على مقدمي الخدمات واجب التعاون مع السلطات القضائية والأمنية من خلال تزويدها بالمعلومات اللازمة للكشف عن الجريمة، وذلك بناءً على أوامر قضائية تضمن مشروعية هذا الإجراء، ويكتسب هذا التعاون أهمية خاصة في الحالات التي يكون فيها الحدث ضحية للتنمر الالكتروني، إذ يساهم في سرعة التدخل ووقف الاعتداءات قبل تفاقم آثارها النفسية والاجتماعية.

ومن جهة أخرى تبرز مسؤولية مقدمي الخدمات في مراقبة المحتوى المتداول عبر منصاتهم وذلك من خلال اعتماد

---

[30] محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، 2008، ص240.

[31] عبد الله القيسي، مدى مشروعية الوسائل العلمية في التحقيق، الطبعة الأولى، دار الثقافة للنشر، الأردن، 2017، ص81.

[32] فريد منعم جبور، حماية المستهلك عبر الأنترنت ومكافحة الجريمة الالكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2012، ص99.

[33] معتز محمد عفيفي، قواعد الاختصاص القضائي بالمسؤولية الالكترونية، دار الجامعة الجديدة، مصر، 2013، ص31.

سياسات استخدام واضحة تحظر سلوكيات التنمر الالكتروني، ووضع آليات للإبلاغ عن المحتوى المسيء وإزالته عند ثبوت مخالفته، وقد أصبحت العديد من المنصات تعتمد على تقنيات الذكاء الاصطناعي لرصد المحتوى الضار بشكل تلقائي وهو ما يعزز من قدرتها على حماية الأحداث من التعرض لمثل هذه الأفعال[34]، كما تفرض طبيعة هذه الجرائم على مقدمي الخدمات اتخاذ تدابير وقائية، مثل توعية المستخدمين، وخاصة الأحداث، بمخاطر التنمر الالكتروني وسبل الحماية منه، وتوفير أدوات للرقابة الأبوية وتمكين الضحايا من حظر المعتدين أو الإبلاغ عنهم بسهولة، ويعد هذا الدور الوقائي مكملاً للدور الإجرائي إذ يسهم في الحد من انتشار هذه الظاهرة قبل وقوعها[35]، غير أن هذه الالتزامات تثير في المقابل إشكاليات قانونية تتعلق بحماية الخصوصية والبيانات الشخصية، حيث يجب على مقدمي الخدمات تحقيق توازن دقيق بين التزامهم بالتعاون مع السلطات، وبين احترام حقوق المستخدمين وعدم الإفصاح عن بياناتهم إلا في إطار قانوني مشروع. وتزداد أهمية هذا التوازن عندما يكون المستخدم حدثاً، لما يتمتع به من حماية خاصة في القوانين الوطنية والاتفاقيات الدولية.

وفي هذا السياق تبرز الحاجة إلى وضع تشريعات واضحة تنظم مسؤولية مقدمي الخدمات المعلوماتية، وتحدد نطاق التزاماتهم بدقة سواء فيما يتعلق بحفظ البيانات أو مراقبة المحتوى أو التعاون مع الجهات المختصة، كما ينبغي أن تتضمن هذه التشريعات ضمانات كافية لحماية حقوق الأحداث ومنع إساءة استخدام البيانات أو انتهاك الخصوصية تحت ذريعة مكافحة الجريمة.

وعليه فإن مقدمي الخدمات المعلوماتية يشكلون عنصراً أساسياً في منظومة مكافحة جرائم التنمر الالكتروني ضد الأحداث حيث يجمع دورهم بين الجانب التقني والإجرائي والوقائي بما يسهم في كشف الجريمة والحد من انتشارها وتحقيق الحماية القانونية لهذه الفئة في البيئة الرقمية.

الفرع الثاني

مسؤولية مقدمي الخدمات المعلوماتية

تباينت الآراء وتضاربت الأحكام حول مدى مسؤولية مورد خدمة الإنترنت جنائياً، وتتغير حدود هذه المسؤولية بإختلاف الوظائف التي يؤديها المورد، فبعض الاحيان يقوم بالوظيفة الأساسية فيقوم بالتوصيل فقط فيطلق عليه حينها متعهد الوصول وأحياناً يقوم بتسكين المواقع على الشبكة ويجعله متاحاً للمستخدمين ويسمى حينها متعهداً للإيواء، وأحياناً يقوم بأدوار ثانوية أخرى، كدور المنتج، وناقل المعلومات ومؤلف الرسالة.

وتزداد أهمية هذا الموضوع في جرائم التنمر الالكتروني الواقعة على الأحداث، حيث ترتكب هذه الجرائم عبر منصات وتطبيقات تديرها أو تستضيفها جهات مزودة للخدمات المعلوماتية، وفي هذه الحالة يثور التساؤل حول مدى مسؤولية هذه الجهات عن المحتوى المسيء أو الضار الذي يتم تداوله عبر منصاتها خاصة إذا كانت على علم به أو تم إخطارها به ولم تبادر إلى إزالته أو الحد من انتشاره، ومن هنا فإن تحديد المسؤولية الجنائية لمقدمي الخدمات يتطلب الأخذ بمعايير دقيقة، تقوم على التمييز بين الدور التقني المحض والدور الفعلي في إدارة المحتوى مع مراعاة عنصر العلم والإرادة، كما يستوجب الأمر وضع إطار قانوني واضح يحدد التزامات هذه الجهات خاصة في ما يتعلق بحماية الأحداث من مخاطر التنمر الالكتروني بما يحقق التوازن بين حرية تداول المعلومات ومكافحة الاستخدامات غير المشروعة للفضاء الرقمي.

---

[34] سعود جاسم المرزوقي، التعاون الدولي في مكافحة الجريمة الالكترونية، اتفاقية بودابست انموذجاً، المجلة الدولية للعلوم الإنسانية والاجتماعية، العدد 69، العراق، 2025، ص211.

[35] حميد عبد حمادي، مشروعية الدليل الالكتروني الناشئ عن التفتيش الجنائي، المرجع السابق، ص88.

أولاً_ المسؤولية الجنائية لمورد خدمة الإنترنت كمتعهد الوصول

إن مورد الخدمة هو شخص طبيعي أو معنوي يقوم ببث معلومات الرسائل المتعلقة بموضوع معين على الإنترنت بحيث يتمكن مستخدم هذه الشبكة من الحصول عليها مجاناً أو بمقابل مادي، ويعتبر بمثابة القلب النابض لبث الحياة في هذه الشبكة وتدفق المعلومات إليها [36]، وبالتالي فإن له دوراً رئيسياً في إطار المسئولية عنه وتوريد المعلومات هو نشرها، أي إطلاع الجمهور على مضمونها، بحيث تكون مقروءة لهم، أو مرئية، أو مسموعة [37]، وحيث إننا أمام صفحات ويب وشبكة إنترنت، فإن خدمة توريد المعلومات عبرها تأخذ وصف " وسيلة اتصال علنية " هدفها وضع مادة معلوماتية معينة نصوص، رسائل، صور، أصوات ... تحت تصرف مستخدمي الشبكة.

ويقصد بتوريد المعلومات عبر الشبكة قيام مزود المحتوى بتحميل البيانات والمعلومات إلى المساحات المخصصة على الخوادم أو أجهزة التخزين التابعة لمتعهد الإيواء، سواء كانت هذه المساحة مستأجرة أو مملوكة، وذلك بهدف إتاحتها للمستخدمين عبر شبكة الإنترنت، وقد يكون مورد المعلومات هو صاحب المادة المعلوماتية ومؤلفها أو يقتصر دوره على جمعها وتنظيمها ونشرها أي القيام بدور الوسيط بين مؤلف المحتوى والجمهور، ففي الحالة الأولى يجمع مورد المعلومات بين صفة المؤلف والناشر في آنٍ واحد، إذ يقوم بإنشاء المحتوى ونشره عبر الشبكة، أما في الحالة الثانية، فإنه يكتسب صفة الناشر فقط، حيث يقوم بنشر المحتوى استناداً إلى علاقة تعاقدية تربطه بصاحب المادة الأصلية، وفي كلتا الحالتين يكون له دور فعال في إتاحة المحتوى للجمهور مما يجعله طرفاً مؤثراً في تداول المعلومات في البيئة الرقمية، وتتجلى أهمية هذا الدور بشكل واضح في جرائم التنمر الالكتروني الواقعة على الأحداث، إذ إن مورد المعلومات قد يكون مسؤولاً عن نشر أو إتاحة محتوى يتضمن إساءة أو تشهيراً أو تهديداً موجهاً إلى الحدث، وبالنظر إلى سلطته في التحكم بالمحتوى سواء من حيث نشره أو حذفه أو تعديله فإنه يعد صاحب الدور الحقيقي في مراقبة المضمون المعلوماتي الالكتروني.

ومن هنا يمكن تشبيه مورد المعلومات في البيئة الرقمية بنظيره في وسائل الإعلام التقليدية، كمدير النشر أو رئيس التحرير، الذي يتحمل مسؤولية مراقبة المحتوى المنشور وضمان مشروعيته، وبالتالي فإن مسؤوليته في جرائم التنمر الالكتروني ضد الأحداث قد تقوم متى ثبت علمه بالمحتوى غير المشروع وعدم اتخاذه الإجراءات اللازمة لمنعه أو إزالته، الأمر الذي يستوجب إخضاعه لالتزامات قانونية واضحة تضمن حماية الفئات الضعيفة، وعلى رأسها الأحداث من مخاطر المحتوى الضار في الفضاء الرقمي، ومورد المعلومات أو صاحب المعلومات أو مورد المحتوي هو الشخص الذي يقوم بتحميل النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين[38]، وبالتالي تكون له سيطرة على المعلومات التي يعرضها على شبكة الإنترنت، ويتحمل نتيجة ذلك مورد المعلومات مسئولية احترام القانون بالنسبة للمعطيات التي يقدمها إلى المستخدمين الذين يتلقونها [39].

وعلى ذلك فإن مورد المعلومات هو الذي ينشئ الصفحات الشخصية، أما متعهد الإيواء فهو يساهم فقط في عملية النشر عن طريق الوسائل الفنية التي يضعها تحت تصرف منشئ الصفحات الشخصية فبذلك فإن مورد المعلومات يتميز عن متعهد الإيواء، من حيث إن هذا الأخير لا يقوم بتأليف أو جمع المضمون المعلوماتي الالكتروني، وإنما يعمل فقط على تخزينه على أجهزته بناء على اتفاقه مع مورد المعلومات ليتسنى للجمهور الاطلاع عليه على مدار الساعة، وتعتبر

---

[36] جميل عبد الباقي الصغير، القانون الجنائي والتكنلوجيا الحديثة، مرجع سابق، ص 157.

[37] أشرف جابر سيد، مسؤولية مقدمي خدمات الانترنت عن المضمون الالكتروني غير المشروع، دار النهضة العربية، القاهرة، 2010، ص 26.

[38] احمد السيد علي عفيفي، الاحكام العامة للعلانية في قانون العقوبات، دار النهضة، القاهرة، 2002، ص 552.

[39] عبد الرحمن هيكل، الضوابط الجنائية لحرية الرأي، دار الفكر الجامعي، القاهرة، 2017، ص 123.

خدمة التوريد هي خدمة نشر، والمورد هو الناشر، أما خدمة الإيواء فهي خدمة تأجير أو إعارة مكان على الشبكة، ومتعهد الإيواء هو المؤجر للمكان أو المعير له، فبالرغم من هذا الإختلاف إلا أنهما يلتقيان في المساهمة بتقديم الخدمة المعلوماتية عبر الإنترنت، فالبيانات والمعلومات لا يمكن أن تبث عبر الشبكة دون تدخلهما، ولا يمكن، في نفس الوقت أن تصل للجمهور دون وجود الوسائل الفنية اللازمة للربط المادي بين شبكات الاتصال عن بعد والحاسوبات الآلية للمستخدمين، ويعد صاحب المعلومات المخزنة المسؤول الأول عن تلك المعلومات التي يتم بثها بواسطة شبكة الإنترنت باعتبار أنه قد يكون مؤلفها أو أدخلها وخزنها في الموقع بعلمه ولحسابه الخاص، لذلك فإنه يسأل بوصفه فاعلاً أصلياً عن كل ما تتضمنه تلك المعلومات من أمور تخالف حكم القانون أو قد تسبب أضراراً للغير [40].

وفرق بعض الفقه بين المسئولية الجنائية لموردي الخدمة تبعاً لقدرة مدير محطة الخدمة على الإشراف والرقابة والتحكم في المراسلات والكتابات التي تظهر على شبكة المعلومات الدولية غير محطة الخدمة التي يشرف عليها، وعليه فرق بين المعلومات والصور التي تظهر مباشرة بصفة آلية على الشاشات بعد إرسالها من المستخدم للموقع وهو ما يطلق عليه البث المباشر على الهواء والمعلومات التي يتم تخزينها بمعرفة مدير محطة الخدمة ثم يعاد بثها للمستخدمين في وقت لاحق وهو ما يطلق عليه البث غير المباشر.

ثانياً_ المسؤولية الجنائية لمورد خدمة الإنترنت كمتعهد إيواء

متعهد الإيواء أو مقدم خدمة الاستضافة هو أي شخص طبيعي أو معنوي يعرض إيواء صفحات الويب على حساباته الخادمة العملاقة وذلك مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة للزبون الذي ينشر ما يريد من نصوص أو صور أو تنظيم مؤتمرات أو ينشئ روابط معلوماتية مع المواقع الأخرى، فمتعهد الإيواء هو من يوطن أو يسكن الموقع على الشبكة حتي يكون متاحاً للمستخدمين وقد يكون متعهد الإيواء شركة تجارية أو أحد أشخاص القانون العام مثل الجامعات والمؤسسات العامة [41]، فعلى سبيل المثال يمكن أيضاً اعتبار الشخص الذي يوفر مساحة معينة داخل موقع ويب حتى إذا لم يتم تخزين الموقع بواسطة الخادم الخاص به، كمضيف.

ويقصد بمتعهدي إيواء المواقع كذلك، الشركات التي تقوم بإيواء المواقع المختلفة على الشبكة العنكبوتية، فهي الشركات التي تقوم باستضافة وإيواء المواقع المختلفة لتجعلها في متناول مستخدمي الإنترنت وذلك للسماح للغير بالاطلاع على محتوياتها في أي وقت، وعليه فلا تستطيع المواقع أن تتيح للمستخدمين بما فيها من معلومات وبيانات إلا من خلال متعهدي إيواء المواقع الذين يقومون بإيواء المواقع، وبالتالي إتاحة ما فيها من معلومات وبيانات للكافة وتقديم مساحة إعلانية عليه تخزن فيها كلمات أو صور أو رسوم من جانب الشركة مقدمة المحتوى.

فعمل المتعهد يتشابه إلي حد كبير بعمل مدير التحرير في الصحف المكتوبة التي تخصص مساحة إعلانية للإعلان فيها، وعليه فمتعهد الإيواء ليس هو مالك الموقع الذي يبث عليه المحتوى بل هو الذي يقوم بتثبيت وإيواء المواقع على الشبكة، كما أنه ليس كذلك المعلن الذي يقوم بالإعلان، ولكنه يؤمن خدمة ظهور هذه الإعلانات عبر الشبكة من خلال الموقع فلولاه ما تمكن صاحب الموقع من استخدامه ولا المعلن من تنفيذ إعلانه على الشبكة[42]، ويعتبر مورد الإيواء بمثابة القلب النابض لشبكة الإنترنت وتدفق المعلومات فيها[43].

---

[40] أحمد عبد الله المراغي، المسؤولية الجنائية لمقدمي خدمات الانترنت، المركز القومي للإصدارات القانونية، القاهرة، 2023، ص 116.

[41] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 155.

[42] محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة الجديدة، القاهرة، 2003، ص 202.

[43] عبد الرحمن هيكل، الضوابط الجنائية لحرية الرأي، مرجع سابق، ص 123.

وعليه يختلف عمل مورد الخدمة عن عمل متعهد الإيواء، فالأول يقتصر دوره على تمكين مستخدمي الإنترنت من الدخول أو الوصول إلي المواقع، أما الثاني فهو الذي يمكن المعلن من القيام بإعلانه عبر الشبكة وقد أولت بعض التشريعات متعهدي الإيواء بالتنظيم الخاص لمسئوليتهم الجنائية مثل التشريع الفرنسي في حين أغفلت بعض التشريعات تنظيم المسئولية الجنائية لهم، فالظاهر أن متعهد الإيواء يقتصر دوره على تقديم مساحة على الشبكة لمتعهد الخدمة الذي يقوم بتقديم المحتوى عليها، إلا أن هذا لا يعفيه من المسئولية الجنائية إذا ثبت علمه الفعلي بالمضمون غير المشروع للموقع الذي يؤويه.

فبالتالي أن مسئولية متعهد الإيواء تتقرر بحسب القواعد العامة للمسئولية فيمكن اعتباره شريكاً بالمساعدة لمتعهد الخدمة إذا قدم إليه الوسائل الفنية التي تمكنه من ارتكاب الجريمة وهو يعلم بالنشاط غير المشروع للفاعل الأصلي واتجه مع ذلك إلى تأجير المساحة على الشبكة لمتعهد الخدمة لمساعدته على ممارسة نشاطه غير المشروع [44].

ثالثاً: موقف التشريع العراقي من مسؤولية مقدم خدمة الانترنت

على الرغم من إنتشار إستخدام الحاسوبات الالكترونية في العراق ودخول شبكة الإنترنت وانتشارها وإعطاء الصلاحية للأفراد باستخدامها، إلا أن القانون العراقي لم يبحث أثر إساءة إستخدامها، إذ أن نصوص الدستور العراقي والتشريعات الجنائية الخاصة ليست كافية في توفير الحماية اللازمة في مواجهة إستخدام الحاسوبات الالكترونية، إذ ليس هناك قانون خاص بهذا الشأن [45].

إلا أن هنالك مشروع قانون للجرائم الالكترونية ولكنه لم يرتب أية مسؤولية على مورد خدمة الإنترنت بشكل مباشر وذلك بعد أن أسماه بالجهات التي تقوم بتزويد خدمة شبكة المعلومات، إلا أنه أشار في المادة (18) منه إلى أنه: "أولاً: يعاقب بالحبس أو بغرامة لا تقل عن 5000000 خمسة ملايين دينار ولا تزيد على 10000000 عشرة ملايين دينار كل من:

أ- قدم معلومات أو بيانات إلكترونية كاذبة إلى السلطات القضائية أو بعدم صحتها.

ب- امتنع عن تقديم معلومات أو بيانات إلى السلطات القضائية أو الإدارية."

ولكن لا نعرف ما إذا كان المشرع هنا يقصد بالنص مورد الخدمة أم لا: لأنه لم ينص عليه صراحة بالاسم ولم يحدد صفة هذا الشخص، وفي مناسبة أخرى جاء ذكر مورد الخدمة بصيغة الجهات التي تقوم بتزويد خدمة شبكة المعلومات أو الخدمات التقنية وذلك في المادة (26) أولاً فقرة ب [46]: إذ خول المشرع القاضي المختص بإصدار الأوامر لهذه الجهات بأنواعها لتقديم بيانات الإشتراك والمرور الجهة التحقيق إذا كان من شأنها أن تساهم في الكشف عن الجريمة.

الخاتمة

في ختام هذا البحث، نستعرض أبرز ما تم التوصل إليه من أحكام إجرائية تتعلق بمكافحة جريمة التنمر الإلكتروني ضد الأحداث، انطلاقاً من خطورة هذه الظاهرة وتأثيرها العميق على نفسية الضحية ونموه الاجتماعي. وقد تبين أن حماية الأحداث تستدعي تدخلاً تشريعياً استثنائياً يراعي هشاشة هذه الفئة، دون الإخلال بضمانات المحاكمة العادلة وحقوق الدفاع. كما أظهر التحليل وجود فجوات واضحة في تنظيم إجراءات مراقبة الاتصالات وجمع الأدلة الرقمية، وضعف آليات إلزام مقدمي الخدمات بالتعاون الفوري مع جهات العدالة. من هنا تأتي أهمية صياغة أحكام إجرائية خاصة بالحدث الجانح أو المجني عليه في هذا النوع المستحدث من الجرائم.

---

[44] جميل عبد الباقي الصغير، القانون الجنائي والتكنلوجيا الحديثة، مرجع سابق، ص 157.

[45] سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية، بيروت، 2011، ص380.

[46] ينظر مشروع قانون الجرائم المعلوماتية العراقي 2011.

أولاً: النتائج:

1_ تفتقر معظم التشريعات الحالية إلى قواعد إجرائية مستقلة للتعامل مع التنمر الإلكتروني ضد الأحداث، مما يؤدي للجوء إلى قواعد عامة لا تراعي خصوصية الحدث وحاجته للرعاية أثناء التحقيق والمحاكمة.

2_ أثبتت الدراسة أن مراقبة الاتصالات كإجراء استدلالي تفتقر لضوابط كافية تحمي الحدث من وصمة العار، كما أن التزامات مقدمي الخدمات المعلوماتية غالباً ما تكون فضفاضة وغير مقرونة بعقوبات رادعة.

ثانياً: المقترحات:

1_ نوصي بإصدار تشريع إجرائي خاص ينظم جمع الأدلة الرقمية في جرائم التنمر ضد الأحداث، يشترط وجود خبير نفسي أثناء التحقيق ويحظر نشر أي بيانات تعريفية بالحدث المجني عليه أو المتهم.

2_ نقترح إلزام منصات التواصل الاجتماعي بإنشاء وحدات استجابة سريعة متخصصة للتبليغ عن التنمر ضد الأحداث، وتغريمها مادياً في حال تأخرها في حذف المحتوى أو حفظ الأدلة لمدة لا تقل عن خمس سنوات.

قائمة المصادر والمراجع

أولاً: الكتب

1. عفيفي، أحمد السيد علي. (2002). *الأحكام العامة للعلانية في قانون العقوبات*. القاهرة: دار النهضة.

Afifi, Ahmed El-Sayed Ali. (2002). *General Provisions of Publicity in Penal Law*. Cairo: Dar Al-Nahda.

2. الجيلاوي، أحمد رعد محمد. (2017). *التسجيل الصوتي وحجيته في الإثبات الجنائي*. القاهرة: المركز العربي للنشر.

Al-Jilawi, Ahmed Raad Mohammed. (2017). *Audio Recording and Its Evidentiary Value in Criminal Proof*. Cairo: Arab Center for Publishing.

3. محمد، أحمد ضياء الدين. (2010). *مشروعية الدليل في المواد الجنائية*. القاهرة: دار النهضة.

Mohammed, Ahmed Diaa El-Din. (2010). *The Legality of Evidence in Criminal Matters*. Cairo: Dar Al-Nahda.

4. المراغي، أحمد عبد الله. (2023). *المسؤولية الجنائية لمقدمي خدمات الإنترنت*. القاهرة: المركز القومي للإصدارات القانونية.

Al-Maraghi, Ahmed Abdullah. (2023). *Criminal Liability of Internet Service Providers*. Cairo: National Center for Legal Publications.

5. سيد، أشرف جابر. (2010). *مسؤولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع*. القاهرة: دار النهضة العربية.

Sayed, Ashraf Jaber. (2010). *Liability of Internet Service Providers for Unlawful Electronic Content*. Cairo: Dar Al-Nahda Al-Arabiya.

6. قنديل، أشرف .(2018) *الوسائل الإلكترونية ودورها في الإثبات الجنائي* .القاهرة: دار الجامعة الجديدة.

Qandil, Ashraf. (2018). *Electronic Means and Their Role in Criminal Proof*. Cairo: Dar Al-Jami'a Al-Jadida.

7. صامت، جواهر قوادري .(2010) *رقابة سلطة التحقيق على أعمال الضبطية القضائية* .القاهرة: دار الجامعة الجديدة.

Samet, Jawaher Qawadri. (2010). *The Supervisory Control of the Investigating Authority over Judicial Police Acts*. Cairo: Dar Al-Jami'a Al-Jadida.

8. المرصفاوي، حسن صادق .(2007) *المرصفاوي في المحقق الجنائي* .القاهرة: منشأة المعارف.

Al-Marsafawi, Hassan Sadeq. (2007). *Al-Marsafawi on the Criminal Investigator*. Cairo: Monshaat Al-Maaref.

9. بوادي، حسنين المحمدي .(2008) *الوسائل العلمية الحديثة في الإثبات الجنائي* .القاهرة: منشأة المعارف.

Bawadi, Hassanein Al-Mohammadi. (2008). *Modern Scientific Methods in Criminal Proof*. Cairo: Monshaat Al-Maaref.

10. إبراهيم، حسين .(2014) *الوسائل العلمية الحديثة في الإثبات الجنائي* .القاهرة: المؤسسة الحديثة للكتاب.

Ibrahim, Hussein. (2014). *Modern Scientific Methods in Criminal Proof*. Cairo: Modern Book Foundation.

11. الجبوري، سليم عبد الله .(2011) *الحماية القانونية لمعلومات شبكة الإنترنت* .بيروت: منشورات الحلبي الحقوقية.

Al-Jubouri, Salim Abdullah. (2011). *Legal Protection of Internet Information*. Beirut: Al-Halabi Legal Publications.

12. عبده، سليم علي .(2006) *التفتيش في ضوء قانون أصول المحاكمات الجزائية الجديد* .بيروت: منشورات الحلبي الحقوقية.

Abdo, Salim Ali. (2006). *Search Procedures in Light of the New Code of Criminal Procedure*. Beirut: Al-Halabi Legal Publications.

13. الأمين، سمير .(2000) *مراقبة التلفونات والتسجيلات الصوتية والمرئية* .القاهرة: دار الكتب.

Al-Amin, Samir. (2000). *Telephone Surveillance and Audio-Visual Recordings*. Cairo: Dar Al-Kutub.

14. حسون، صالح عبد الزهرة .(2003) *أحكام التفتيش وآثاره في القانون العراقي* .بغداد: دار السنهوري.

Hassoun, Saleh Abdul-Zahra. (2003). *Search Provisions and Their Effects in Iraqi Law*. Baghdad: Dar Al-Sanhouri.

15. الحيط، عادل عزام .(2011) *جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية* .عمّان: دار الثقافة.

Al-Hait, Adel Azzam. (2011). *Crimes of Defamation, Insult, and Contempt Committed through Electronic Media*. Amman: Dar Al-Thaqafa.

16.هيكل، عبد الرحمن .(2017) .*الضوابط الجنائية لحرية الرأي* .القاهرة: دار الفكر الجامعي.

Heikal, Abdulrahman. (2017). *Criminal Controls on Freedom of Opinion*. Cairo: Dar Al-Fikr Al-Jami'i.

17.أبو العزم، عبد الغني .(2013) .*معجم الغني* .بيروت: دار الكتب العلمية.

Abu Al-Azm, Abdul Ghani. (2013). *Al-Ghani Dictionary*. Beirut: Dar Al-Kutub Al-Ilmiyah.

18.القيسي، عبد الله .(2017) .*مدى مشروعية الوسائل العلمية في التحقيق*، الطبعة الأولى. الأردن: دار الثقافة للنشر.

Al-Qaisi, Abdullah. (2017). *The Legality of Scientific Methods in Investigation* (1st ed.). Jordan: Dar Al-Thaqafa for Publishing.

19.أحمد، عبد المنعم .(2013) .*الجرائم الناشئة عن إساءة استعمال الهاتف المحمول ومدى المسؤولية عنها*، الطبعة الأولى. القاهرة: دار النهضة العربية.

Ahmed, Abdel Moneim. (2013). *Crimes Arising from the Misuse of Mobile Phones and the Extent of Liability Therefor* (1st ed.). Cairo: Dar Al-Nahda Al-Arabiya.

20.حرقوص، علي وجيه .(2011) .*قاضي التحقيق*، الطبعة الثانية. بيروت: منشورات الحلبي الحقوقية.

Harqous, Ali Wajih. (2011). *The Investigating Judge* (2nd ed.). Beirut: Al-Halabi Legal Publications.

21.الحسيني، عمار عباس .(2012) .*مبادئ علمي الإجرام والعقاب* .بغداد: التيمي للنشر.

Al-Husseini, Ammar Abbas. (2012). *Principles of Criminology and Penology*. Baghdad: Al-Taymi Publishing.

22.تحفة، فايق عوضين .(2014) .*الحماية القانونية والأمنية للاتصالات السلكية واللاسلكية* .القاهرة: دار الكتب العلمية.

Tohfa, Fayek Awadain. (2014). *Legal and Security Protection of Wired and Wireless Communications*. Cairo: Dar Al-Kutub Al-Ilmiyah.

23.جبور، فريد منعم .(2012) .*حماية المستهلك عبر الإنترنت ومكافحة الجريمة الإلكترونية: دراسة مقارنة* .بيروت: منشورات الحلبي الحقوقية.

Jabbour, Farid Moneim. (2012). *Consumer Protection via the Internet and Combating Cybercrime: A Comparative Study*. Beirut: Al-Halabi Legal Publications.

24.خالد، كوثر أحمد .(2007) .*الإثبات الجنائي بالوسائل العلمية الحديثة*، الطبعة الأولى. أربيل: مكتب التفسير للنشر.

Khaled, Kawthar Ahmed. (2007). *Criminal Proof by Modern Scientific Methods* (1st ed.). Erbil: Al-Tafsir Publishing Office.

25.الشناوي، محمد .(2008). *جرائم النصب المستحدثة* .مصر: دار الكتب القانونية.

Al-Shennawi, Mohammed. (2008). *Modern Fraud Crimes*. Egypt: Dar Al-Kutub Al-Qanuniyah.

26.منصور، محمد حسين .(2003). *المسؤولية الإلكترونية* .القاهرة: دار الجامعة الجديدة.

Mansour, Mohammed Hussein. (2003). *Electronic Liability*. Cairo: Dar Al-Jami'a Al-Jadida.

27.موسى، مصطفى محمد .(2005). *المراقبة الإلكترونية عبر شبكة الإنترنت*، الطبعة الأولى. القاهرة: دار الكتب القانونية.

Mousa, Mostafa Mohammed. (2005). *Electronic Surveillance via the Internet* (1st ed.). Cairo: Dar Al-Kutub Al-Qanuniyah.

28.عفيفي، معتز محمد .(2013). *قواعد الاختصاص القضائي بالمسؤولية الإلكترونية* .مصر: دار الجامعة الجديدة.

Afifi, Moataz Mohammed. (2013). *Rules of Jurisdiction over Electronic Liability*. Egypt: Dar Al-Jami'a Al-Jadida.

29.بحر، ممدوح خليل .(2010). *حماية الحياة الخاصة في القانون الجنائي* .القاهرة: دار النهضة.

Bahr, Mamdouh Khalil. (2010). *Protection of Private Life in Criminal Law*. Cairo: Dar Al-Nahda.

30.فاروق، ياسر الأمير .(2009). *مراقبة الأحاديث الخاصة في الإجراءات الجنائية* .القاهرة: دار المطبوعات الجامعية.

Farouk, Yasser Al-Amir. (2009). *Surveillance of Private Conversations in Criminal Procedures*. Cairo: Dar Al-Matbouat Al-Jami'iyah.

ثانياً: المجلات والبحوث

1. حمادي، حميد عبد. (2023). مشروعية الدليل الإلكتروني الناشئ عن التفتيش الجنائي .*مجلة المدارات العلمية للعلوم الإنسانية والاجتماعية*، العدد 1، العراق.

Hammadi, Hamid Abdul. (2023). The legality of electronic evidence arising from criminal search. *Al-Madarat Scientific Journal for Humanities and Social Sciences*, Issue 1, Iraq.

2. المرزوقي، سعود جاسم. (2025). التعاون الدولي في مكافحة الجريمة الإلكترونية: اتفاقية بودابست أنموذجاً .*المجلة الدولية للعلوم الإنسانية والاجتماعية*، العدد 69، العراق.

Al-Marzouqi, Saud Jassim. (2025). International cooperation in combating cybercrime: The Budapest Convention as a model. *International Journal of Humanities and Social Sciences*, Issue 69, Iraq.

ثالثاً: الأطاريح

1. عبد البديع، آدم .(2010) .*الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي* .أطروحة دكتوراه، جامعة المنصورة، القاهرة.

Abdel Badi, Adam. (2010). *The Right to the Sanctity of Private Life and the Extent of Protection Guaranteed by Criminal Law*. Doctoral dissertation, Mansoura University, Cairo.

رابعاً: القوانين

1. *مشروع قانون الجرائم المعلوماتية العراقي*.(2011) .

The Iraqi Draft Cybercrimes Law. (2011).

خامساً: المواقع الإلكترونية

1. شافي، نادر عبد العزيز. شروط التنصت واعتراض وسائل الاتصال. بحث منشور على الموقع الرسمي للجيش اللبناني.

Shafi, Nader Abdel Aziz. Conditions for wiretapping and interception of communication means. A paper published on the official website of the Lebanese Army.