



الابتزاز الإلكتروني في الوسط الشبابي وسبل الوقاية منه عبر المؤسسات الشبابية والرياضية - دراسة

قانونية مجتمعية

الابتزاز الإلكتروني في الوسط الشبابي وسبل الوقاية منه عبر المؤسسات الشبابية والرياضية
- دراسة قانونية مجتمعية

م.د. علي عبدالهادي حميد

كلية القانون/ جامعة ذي قار

البريد الإلكتروني Email : ali.alhazah@utq.edu.iq

الكلمات المفتاحية: الابتزاز الإلكتروني، الشباب، الجرائم الإلكترونية، الوقاية، المؤسسات الشبابية والرياضية.

كيفية اقتباس البحث

حميد، علي عبدالهادي ، الابتزاز الإلكتروني في الوسط الشبابي وسبل الوقاية منه عبر المؤسسات الشبابية والرياضية - دراسة قانونية مجتمعية، مجلة مركز بابل للدراسات الانسانية، تشرين الأول ٢٠٢٦، المجلد: ١٦، العدد: ١٠ .

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 نسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

Registered في
ROAD

مفهرسة في
IASJ

Cyber Extortion Among Youth and Means of Prevention Through Youth and Sports Institutions: A Socio-Legal Study

Dr. Ali Abdulhadi Hamid
College of Law / University of Dhi Qar

Keywords : Electronic Blackmail, Youth, Cybercrime, Prevention, Youth and Sports Institutions.

How To Cite This Article

Hamid, Ali Abdulhadi , Cyber Extortion Among Youth and Means of Prevention Through Youth and Sports Institutions: A Socio-Legal Study ,Journal Of Babylon Center For Humanities Studies, October 2026,Volume:16, Issue 10.



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

This study examines electronic blackmail among young people as a crime associated with digital development and the widespread use of social media. It explains its concept, forms, causes, and legal treatment under Iraqi legislation, with particular emphasis on the preventive role of youth and sports institutions through legal and digital awareness and cooperation with relevant authorities. The study concludes that combining legal measures with community-based prevention is essential to reducing electronic blackmail and protecting young people. This study aims to clarify the legal and social nature of cyber extortion, analyze the criminal prosecution mechanisms provided by Iraqi legislation, and identify the most significant challenges to their implementation. Ultimately, it seeks to present a practical preventative framework for youth and sports institutions, based on legal awareness, digital security, guidance, and referral to the appropriate authorities.



The study employs an analytical approach, examining relevant legal texts and discussing relevant Iraqi judicial trends and applications. It also utilizes a descriptive approach to identify the manifestations, causes, and effects of cyber extortion among youth, while a practical approach is employed to formulate a set of mechanisms and proposals that youth and sports institutions can adopt in the field of prevention.

The study is divided into two sections: the first addresses the conceptual and social framework of cyber extortion among youth, and the second examines the criminal prosecution of cyber extortion within Iraqi legislation.

الملخص

يتناول البحث ظاهرة الابتزاز الإلكتروني في الوسط الشبابي بوصفها من الجرائم المرتبطة بالتطور الرقمي وانتشار وسائل التواصل الاجتماعي، وما تشكله من مخاطر قانونية واجتماعية على الشباب. ويهدف إلى بيان مفهوم الابتزاز الإلكتروني وصوره وأسبابه، وبيان موقف التشريع العراقي منه، مع التركيز على دور المؤسسات الشبابية والرياضية في الوقاية منه من خلال التوعية القانونية والرقمية وتعزيز التعاون مع الجهات المختصة. ويخلص البحث إلى أهمية الجمع بين المواجهة القانونية والوقاية المجتمعية للحد من هذه الظاهرة وحماية الشباب.

تهدف الدراسة إلى بيان الطبيعة القانونية والمجتمعية للابتزاز الإلكتروني، وتحليل وسائل المواجهة الجنائية التي يوفرها التشريع العراقي، والكشف عن أهم التحديات التي تعترض تطبيقها، وصولاً إلى تقديم تصور وقائي قابل للتطبيق داخل المؤسسات الشبابية والرياضية يقوم على الوعي القانوني والأمن الرقمي والإرشاد والإحالة إلى الجهات المختصة.

اعتمدت الدراسة المنهج التحليلي من خلال تحليل النصوص القانونية ذات الصلة ومناقشة بعض الاتجاهات والتطبيقات القضائية العراقية، إلى جانب المنهج الوصفي في تحديد مظاهر الابتزاز الإلكتروني وأسبابه وآثاره في الوسط الشبابي، مع توظيف المنهج التطبيقي في صياغة مجموعة من الآليات والمقترحات التي يمكن للمؤسسات الشبابية والرياضية اعتمادها في المجال الوقائي.

قسمت الدراسة إلى مطلبين ؛ خصص المطلب الأول للإطار المفاهيمي والمجتمعي للابتزاز الإلكتروني في الوسط الشبابي، وتناول المطلب الثاني المواجهة الجنائية للابتزاز الإلكتروني في التشريع العراقي .



مقدمة الدراسة

أولاً: التعريف بموضوع الدراسة:

أدى التطور المتسارع في تقنيات الاتصال وانتشار وسائل التواصل الاجتماعي إلى إحداث تحول جوهري في طبيعة العلاقات الإنسانية، ولا سيما في الوسط الشبابي الذي يمثل الفئة الأكثر تفاعلاً مع البيئة الرقمية. وعلى الرغم مما أتاحتها هذه التقنيات من فرص واسعة للتواصل وتبادل المعرفة، فإنها أوجدت في المقابل بيئة يمكن استغلالها في ارتكاب أنماط مستحدثة من السلوك الإجرامي، ومن أبرزها الابتزاز الإلكتروني الذي يقوم على توظيف الوسائل الرقمية في الضغط على إرادة المجني عليه وتهديده لتحقيق غايات غير مشروعة.

وتتضاعف خطورة الابتزاز الإلكتروني عندما يستهدف فئة الشباب؛ لما قد يترتب عليه من مساس بالخصوصية والاعتبار والحرية الشخصية، فضلاً عن آثاره الأسرية والاجتماعية والنفسية. كما تثير هذه الجريمة إشكالات قانونية تتصل بتكييف السلوك الإجرامي وإثباته وتحديد هوية مرتكبه، ولا سيما في ظل الطبيعة التقنية للجريمة وإمكان استخدام الحسابات الوهمية وسرعة تداول المحتوى الرقمي أو إخفائه.

ثانياً: أهمية الدراسة:

تتبع أهمية الدراسة من حيث إن مواجهة الابتزاز الإلكتروني لا ينبغي أن تقتصر على التدخل الجنائي اللاحق لوقوع الجريمة، وإنما تستلزم تبني سياسة وقائية تعمل على رفع مستوى الوعي القانوني والرقمي لدى الشباب. وفي هذا المجال يمكن للمؤسسات الشبابية والرياضية أن تؤدي دوراً مهماً بحكم اتصالها المباشر بفئة الشباب وقدرتها على توظيف برامجها وأنشطتها في التوعية والإرشاد والوقاية، بالتنسيق مع الجهات القضائية والأمنية والتقنية المختصة.

ثالثاً: مشكلة الدراسة:

تتمثل مشكلة الدراسة في التساؤل الرئيس الآتي: إلى أي مدى تكفل القواعد القانونية العراقية النافذة لمواجهة الابتزاز الإلكتروني في الوسط الشبابي؟ وكيف يمكن تفعيل دور المؤسسات الشبابية والرياضية في الوقاية منه؟ ويتفرع عنه البحث في مفهوم الابتزاز الإلكتروني وصوره وأسباب انتشاره، والأساس القانوني للمساءلة الجنائية عنه، وأبرز الإشكالات المرتبطة بالإثبات الرقمي، فضلاً عن تحديد الآليات المؤسسية التي يمكن اعتمادها للحد من تعرض الشباب لهذه الجريمة.

رابعاً: هدف الدراسة:

تهدف الدراسة إلى بيان الطبيعة القانونية والمجتمعية للابتزاز الإلكتروني، وتحليل وسائل المواجهة الجنائية التي يوفرها التشريع العراقي، والكشف عن أهم التحديات التي تعترض تطبيقها، وصولاً إلى تقديم تصور وقائي قابل للتطبيق داخل المؤسسات الشبابية والرياضية يقوم على الوعي القانوني والأمن الرقمي والإرشاد والإحالة إلى الجهات المختصة.

خامساً: منهج الدراسة:

اعتمدت الدراسة المنهج التحليلي من خلال تحليل النصوص القانونية ذات الصلة ومناقشة بعض الاتجاهات والتطبيقات القضائية العراقية، إلى جانب المنهج الوصفي في تحديد مظاهر الابتزاز الإلكتروني وأسبابه وآثاره في الوسط الشبابي، مع توظيف المنهج التطبيقي في صياغة مجموعة من الآليات والمقترحات التي يمكن للمؤسسات الشبابية والرياضية اعتمادها في المجال الوقائي.

سادساً: تقسيم الدراسة:

قسمت الدراسة إلى مطلبين ؛ خصص المطلب الأول للإطار المفاهيمي والمجتمعي للابتزاز الإلكتروني في الوسط الشبابي، وتناول المطلب الثاني المواجهة الجنائية للابتزاز الإلكتروني في التشريع العراقي .

المطلب الأول

الإطار المفاهيمي والمجتمعي للابتزاز الإلكتروني في الوسط الشبابي

أحدث التطور المتسارع في تقنيات الاتصال تحولاً واضحاً في طبيعة العلاقات الاجتماعية، ولا سيما بين فئة الشباب التي أصبحت البيئة الرقمية جزءاً أساسياً من نشاطها اليومي. وإلى جانب المنافع التي أتاحتها هذه البيئة، أفرزت أنماطاً مستحدثة من السلوك الإجرامي تستفيد من سهولة الاتصال وإخفاء الهوية وسرعة تداول المعلومات، ويأتي الابتزاز الإلكتروني في مقدمتها. ولا تكمن خطورته في استعمال وسيلة تقنية فحسب، وإنما في قدرة الجاني على تحويل المعلومات أو الصور أو المحادثات الخاصة إلى وسيلة ضغط تمس حرية المجني عليه في اتخاذ قراره وتضعه أمام خيار الاستجابة لمطالب الجاني أو تحمل النتائج التي يهدده بها. وقد أشارت الأحكام القضائية العراقية إلى ارتباط انتشار هذه الجريمة بتوسع استخدام التكنولوجيا ووسائل التواصل الاجتماعي، فضلاً عن خصوصيتها من حيث وسيلة ارتكابها وصعوبة إثباتها.

ومن هذا المنطلق، فإن دراسة الابتزاز الإلكتروني في الوسط الشبابي تقتضي أولاً تحديد مضمونه وتمييزه عن الظواهر الإلكترونية المشابهة، ثم الانتقال إلى دراسة العوامل التي تساعد على انتشاره وآثاره في الشباب والمجتمع.

الفرع الأول

مفهوم الابتزاز الإلكتروني وخصائصه وصوره

أولاً: مفهوم الابتزاز الإلكتروني:

لا ينبغي النظر إلى الابتزاز الإلكتروني باعتباره مجرد تهديد يقع بواسطة الهاتف أو شبكة الإنترنت؛ لأن جوهره يتمثل في استعمال التهديد وسيلة لإخضاع إرادة المجني عليه وحمله على تقديم منفعة أو القيام بتصرف أو الامتناع عنه تحقيقاً للغاية التي يستهدفها الجاني، بينما تمثل الوسيلة الإلكترونية البيئة التي يقع من خلالها هذا الضغط.

ومن الناحية القانونية فإن قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل لم يضع تعريفاً خاصاً لجريمة تحمل تسمية "الابتزاز الإلكتروني"، وهو ما جعل تحديد مفهومها وتكييفها يستندان إلى طبيعة السلوك المرتكب ومضمون التهديد والطلب الذي يقترن به. وهذا يعني أن التشريع العراقي لا يتضمن تنظيمًا خاصاً مستقلاً لهذه الجريمة، وأن التطبيقات القضائية تلجأ إلى النصوص العقابية القائمة بحسب عناصر الواقعة، وفي مقدمتها أحكام التهديد. وبناءً على ذلك يمكن، لأغراض هذه الدراسة، تعريف الابتزاز الإلكتروني بأنه:

سلوك عمدي يستخدم فيه الجاني وسيلة إلكترونية للضغط على إرادة شخص آخر، من خلال تهديده بإيقاع ضرر به أو بمصالحه أو بكشف أو نشر معلومات أو بيانات أو محتويات تمس خصوصيته أو اعتباره، بقصد حمله على تقديم منفعة أو القيام بفعل أو الامتناع عنه. وهذا التعريف المقترح يركز على أربعة عناصر مترابطة: السلوك العمدي، والوسيلة الإلكترونية، والتهديد أو الضغط، والغاية التي يسعى الجاني إلى تحقيقها. وبذلك لا تكون التقنية هي جوهر الابتزاز، وإنما وسيلة تمنح الفعل الإجرامي خصائص جديدة تتعلق بالسرعة والانتشار وإمكان التخفي وتجاوز الحدود الجغرافية.

ثانياً: تمييز الابتزاز الإلكتروني عن الجرائم والسلوكيات المشابهة:

يتقاطع الابتزاز الإلكتروني مع التهديد من حيث استعمال الجاني خوف وسيلة للتأثير في إرادة المجني عليه، إلا أن الابتزاز يتخذ صورة أكثر ارتباطاً بتحقيق غاية معينة؛ إذ لا يقف الجاني عند مجرد تخويف الضحية، وإنما يوظف هذا التخويف للوصول إلى مطلب محدد.



وتبرز أهمية هذه المسألة في التشريع العراقي؛ لأن المادة (١/٤٣٠) من قانون العقوبات تقوم، في إحدى صورها، على وجود تهديد مقترن بطلب أو تكليف بأمر أو الامتناع عن فعل^١. وقد أكدت محكمة التمييز الاتحادية أهمية تحديد واقعة التهديد وصورتها وماهية الطلب الصادر من المتهم؛ لأن ذلك يؤثر مباشرة في تحديد الوصف القانوني للجريمة وتقدير الأدلة^٢.

كما يختلف الابتزاز الإلكتروني عن التتمر الإلكتروني؛ فالتتمر قد يستهدف الإساءة إلى الضحية أو تحقيرها أو تخويفها أو عزلها اجتماعيًا، دون أن يكون مشروطاً بوجود مطلب يريد الجاني تحقيقه. أما الابتزاز، فيقوم في صورته المعتادة على استخدام ما يخشاه المجني عليه أداة لحمله على الاستجابة لإرادة الجاني. وقد أوضحت محكمة التمييز الاتحادية أن التكييف القانوني للسلوك الإلكتروني يختلف باختلاف الفعل؛ فقد يكون تهديداً أو قذفاً أو سباً أو غير ذلك، وهو ما يؤكد ضرورة عدم الخلط بين الظواهر الإلكترونية المختلفة.

ثالثاً: خصائص الابتزاز الإلكتروني

يتميز الابتزاز الإلكتروني بعدد من الخصائص التي تزيد من خطورته، ومن أبرزها الطابع التقني؛ إذ يستطيع الجاني استعمال الهاتف الذكي أو تطبيقات التواصل أو البريد الإلكتروني أو الحسابات الرقمية في الوصول إلى الضحية وممارسة الضغط عليها دون وجود مادي مباشر بين الطرفين. كما يتسم بإمكان إخفاء الهوية، سواء باستخدام حسابات وهمية أو أسماء مستعارة أو وسائل تقنية تصعب التعرف على الفاعل، وهو ما ينعكس على عمليات البحث والتحقيق والإثبات. ومن خصائصه أيضاً السرعة واتساع نطاق الضرر؛ فتهديد الضحية بنشر صورة أو تسجيل لم يعد مرتبطاً بنطاق مكاني محدود، وإنما يمكن أن يؤدي تنفيذ التهديد إلى تداول المحتوى خلال وقت قصير بين عدد كبير من الأشخاص^٣.

ويضاف إلى ذلك أن الابتزاز الإلكتروني قد يتخذ طابعاً عابراً للحدود، بحيث يوجد الجاني في دولة والضحية في دولة أخرى، وهو ما يثير إشكالات تتعلق بالاختصاص والتحقيق والوصول إلى الأدلة الرقمية. والطبيعة العابرة للحدود وإلى الصعوبات الإثباتية الناشئة عن الطبيعة التقنية للجريمة.

رابعاً: صور الابتزاز الإلكتروني في الوسط الشبابي

تتنوع صور الابتزاز بحسب الغاية التي يريد الجاني تحقيقها. فقد يكون ابتزازاً مالياً عندما يهدد الضحية بنشر صور أو بيانات أو معلومات مقابل دفع مبلغ مالي. وهذه الصورة ظهرت بالفعل في تطبيقات القضاء العراقي؛ فقد قضت المحكمة الجنائية المركزية في إحدى القضايا بإدانة متهم حصل على صور خاصة لفتاة بعد اختراق حسابها ثم ساومها على دفع المال مقابل عدم

نشرها، وطبقت المحكمة المادة (٤٣٠) من قانون العقوبات^٤. وقد يكون الابتزاز ذا غاية جنسية أو غير أخلاقية عندما يستغل الجاني الصور أو التسجيلات أو المحادثات الخاصة لإجبار الضحية على الاستمرار في علاقة أو القيام بسلوك لا تريده. كما يمكن أن يكون ابتزازاً نفعية لا تكون غايته مآلاً بصورة مباشرة، وإنما حمل الضحية على القيام بفعل يحقق مصلحة للجاني أو الامتناع عن عمل معين^٥. وقد يكون الدافع انتقامياً عندما يستغل الجاني محتوى خاصاً حصل عليه أثناء علاقة سابقة أو نزاع شخصي للإضرار بالمجني عليه والضغط عليه. وقد أبرزت الأحكام القضائية العراقية هذه الدوافع المختلفة، ومنها الدافع المالي والنفعي والانتقامي وغير الأخلاقي.

الفرع الثاني

أسباب انتشار الابتزاز الإلكتروني وآثاره في الوسط الشبابي

أولاً: العوامل المساعدة على انتشار الابتزاز الإلكتروني بين الشباب

لا يمكن تفسير انتشار الابتزاز الإلكتروني بعامل واحد؛ فهو نتيجة تفاعل عوامل تقنية واجتماعية وشخصية. ويأتي في مقدمتها الاستخدام المكثف لوسائل التواصل الاجتماعي وما يصاحبه أحياناً من ضعف الوعي بحدود الخصوصية الرقمية، الأمر الذي يؤدي إلى إتاحة قدر كبير من البيانات والصور والمعلومات الشخصية. كما يسهم التواصل مع الحسابات المجهولة أو الوهمية في توفير مدخل للمبتز؛ إذ قد تبدأ العلاقة بمحادثات عادية قبل أن تتطور إلى تبادل معلومات أو صور خاصة، ثم تتحول تلك المواد لاحقاً إلى وسيلة للضغط على الضحية.

ويبرز كذلك ضعف الثقافة القانونية والرقمية لدى بعض الشباب؛ فقد لا يدرك الشخص أهمية حماية الحسابات أو الاحتفاظ بالأدلة الرقمية عند تعرضه للتهديد، وقد يدفعه الخوف إلى حذف المحادثات أو الاستجابة للمبتز بدلاً من إبلاغ الجهات المختصة. ومن العوامل الاجتماعية المهمة الخوف من الوصمة ورد فعل الأسرة والمحيط الاجتماعي. وهذه المسألة ذات أهمية خاصة في البيئات المحافظة؛ إذ قد يعتمد المبتز على توقعه أن الضحية ستفضل الصمت على كشف الواقعة. وقد أشارت القرارات القضائية الى هذه المسألة صراحةً من حيث أن بعض الضحايا يحجمون عن الإخبار عن الابتزاز خوفاً من النتائج الاجتماعية، وهو ما يمنح الجاني فرصة للاستمرار في الضغط عليهم.



ثانياً: الآثار المترتبة على الابتزاز الإلكتروني في الشباب

تتجاوز نتائج الابتزاز الاعتداء المباشر على إرادة الضحية؛ إذ يمكن أن تمس الخصوصية والاعتبار والحرية الشخصية والأمان الرقمي في الوقت نفسه. فالضحية تصبح تحت ضغط مستمر بين رفض مطلب الجاني والخوف من تنفيذ التهديد. وعلى المستوى الاجتماعي، قد يؤدي كشف المعلومات أو الصور الخاصة إلى مشكلات أسرية واجتماعية، فضلاً عن الإضرار بسمعة الضحية وعلاقاتها بمحيطها، فضلاً عن الآثار المرتبطة بهذه الجريمة ومنها الخوف والقلق والمشكلات الأسرية والاجتماعية التي قد تنتج عنها.

أما من الناحية القانونية، فتظهر الخطورة في أن الجريمة قد تتطور من تهديد رقمي إلى سلسلة من المطالب المتتابة؛ لأن استجابة الضحية لأول طلب لا تعني بالضرورة انتهاء الابتزاز. ومن هنا تتضح أهمية التدخل المبكر وحفظ الأدلة وعدم الانصياع للمبتز والتوجه إلى الجهات المختصة^٦.

ثالثاً: أثر الظاهرة في المجتمع والمؤسسات الشبابية:

لا ينبغي حصر الابتزاز الإلكتروني في العلاقة الفردية بين الجاني والمجني عليه؛ لأن اتساع الظاهرة ينعكس على شعور الشباب بالأمان في البيئة الرقمية وعلى الثقة في وسائل الاتصال الحديثة. كما يفرض على المؤسسات التي تتعامل مع الشباب مسؤولية أكبر في مجال التوعية والوقاية والإرشاد. وتزداد أهمية ذلك في المؤسسات الشبابية والرياضية لأنها تستطيع الوصول إلى الشباب خارج الإطار التقليدي للمدرسة أو الجامعة. ومن ثم يمكن أن تمثل هذه المؤسسات حلقة اتصال بين التوعية القانونية والتنقيف الرقمي والجهات المختصة بمكافحة الجريمة.

ويرى الباحث أن خصوصية الابتزاز الإلكتروني في الوسط الشبابي لا ترجع إلى حداثة الوسيلة التقنية وحدها، وإنما إلى اختلال ميزان السيطرة بين المبتز والضحية؛ فالمبتز يحاول تحويل خصوصية الشاب أو خوفه الاجتماعي إلى وسيلة للتحكم في إرادته. ولذلك فإن المواجهة الفاعلة لا تتحقق بالعقوبة وحدها، بل تتطلب الجمع بين التجريم والوعي القانوني والأمن الرقمي والتدخل المؤسسي المبكر، بما يقلل فرص وقوع الشباب ضحايا للابتزاز ويشجعهم على الإبلاغ عنه دون تردد.

المطلب الثاني

المواجهة الجنائية للابتزاز الإلكتروني في التشريع العراقي

أفرز التطور التقني صوراً إجرامية لم تكن حاضرة بالكيفية ذاتها عند وضع التشريعات العقابية التقليدية، ومن أبرزها الابتزاز الإلكتروني. وتثير هذه الجريمة إشكالية قانونية تتعلق بمدى قدرة النصوص العقابية النافذة على استيعاب سلوك يرتكب في بيئة رقمية، بينما صيغت غالبية تلك النصوص في ظل وسائل تقليدية لارتكاب الجريمة. وتزداد أهمية هذه الإشكالية في العراق في ظل عدم وجود قانون خاص ومستقل نافذ للجرائم المعلوماتية، الأمر الذي جعل القضاء يتعامل مع وقائع الابتزاز الإلكتروني من خلال النصوص العقابية القائمة، وفق طبيعة كل واقعة وعناصرها. وقد أكد القضاء العراقي في استمرار التعامل مع قضايا الابتزاز الإلكتروني استناداً إلى قانون العقوبات رقم (١١١) لسنة ١٩٦٩ المعدل، ولا سيما الأحكام المتعلقة بالتهديد.

ولا يعني غياب النص الخاص انعدام الحماية الجنائية، وإنما يقتضي البحث عن الوصف القانوني الذي تتوافر عناصره في الواقعة المعروضة. ومن ثم، فإن تحديد المسؤولية الجنائية في الابتزاز الإلكتروني يستوجب التمييز بين مجرد التهديد وبين التهديد الذي يقتضي بطلب أو تكليف بفعل أو امتناع عنه، فضلاً عن دراسة خصوصية الإثبات عندما يكون السلوك والأثر والدليل مرتبطاً ببيئة إلكترونية.

وانطلاقاً من ذلك، نقسم هذا المطلب إلى فرعين: نتناول في الأول التكييف القانوني للابتزاز الإلكتروني وأركان المسؤولية الجنائية، ثم نبحث في الثاني إشكاليات الحماية الجنائية والإثبات في جرائم الابتزاز الإلكتروني.

الفرع الأول

التكييف القانوني للابتزاز الإلكتروني وأركان المسؤولية الجنائية

أولاً: الأساس القانوني لتجريم الابتزاز الإلكتروني:

لم يفرد المشرع العراقي في قانون العقوبات رقم (١١١) لسنة ١٩٦٩ المعدل نصاً يحمل تسمية جريمة الابتزاز الإلكتروني، لذلك يقتضي تطبيق القواعد العامة البحث في مضمون السلوك ذاته بدلاً من الوقوف عند الوسيلة المستخدمة فيه. فإذا استخدم الجاني وسيلة إلكترونية لتهديد شخص بنشر صور أو معلومات خاصة، وكان التهديد مقترناً بطلب أو تكليف بفعل أو امتناع عنه، فإن الواقعة يمكن أن تدخل في نطاق المادة (٤٣٠) متى تحققت عناصرها القانونية.

وتنص المادة (١/٤٣٠) من قانون العقوبات، في جوهرها، على معاقبة من يهدد آخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره، أو بإسناد أمور مخدشة بالشرف أو إفشائها، متى كان التهديد مصحوبًا بطلب أو تكليف بأمر أو الامتناع عن فعل أو كان مقصودًا به ذلك. ويقرر النص عقوبة السجن مدة لا تزيد على سبع سنوات أو الحبس، وتظهر أهمية هذه المادة في أن اقتران التهديد بالطلب يجعل بنيانها قريبًا من الصورة القانونية التي يقع بها الابتزاز الإلكتروني عمليًا؛ فالمبتز لا يكتفي عادة بتهديد المجني عليه، وإنما يستعمل التهديد وسيلة لدفعه إلى تنفيذ غاية معينة.

وقد ذهب الاتجاه القضائي أن المادة (٤٣٠) تمثل أساسًا مهمًا لتكييف حالات الابتزاز التي يكون فيها التهديد مقترنًا بطلب، مع الإشارة إلى وجود اختلافات سابقة في بعض التطبيقات القضائية بشأن الوصف القانوني المناسب.

ثانيًا: التمييز بين المواد (٤٣٠ و ٤٣١ و ٤٣٢) من قانون العقوبات:

تقتضي الدقة عدم اعتبار كل تهديد إلكتروني ابتزازًا؛ لأن قانون العقوبات العراقي يميز بين صور متعددة للتهديد، فالمادة (٤٣٠) تعالج الصورة الأشد عندما تتوافر الأوصاف التي حددها النص ويكون التهديد مصحوبًا بطلب أو تكليف بأمر أو امتناع عن فعل أو مقصودًا به ذلك^٧، أما المادة (٤٣١) فتتناول التهديد بارتكاب جناية ضد النفس أو المال أو ضد نفس أو مال الغير، أو بإسناد أمور خادشة للشرف أو الاعتبار أو إفشائها، ولكن في غير الحالات المنصوص عليها في المادة (٤٣٠)^٨. بينما تتناول المادة (٤٣٢) صور التهديد الأخرى التي لا تدخل ضمن المادتين السابقتين^٩.

وعليه، فإن مجرد استخدام تطبيق إلكتروني لا يكفي لاختيار المادة العقابية، بل يجب تحديد مضمون التهديد، والغاية منه، وما إذا كان مقترنًا بطلب، وطبيعة ذلك الطلب. وهذا ما أكدته محكمة التمييز الاتحادية في قرارها رقم (١٨٥١/هيئة الأحداث/٢٠٢٤) المؤرخ في ٢٠/١٠/٢٠٢٤؛ إذ نقضت الحكم لعدم استكمال المحكمة تحديد واقعة التهديد وصورتها وماهية الطلب، مؤكدة أهمية ذلك في تحديد الوصف القانوني وتقدير الأدلة، وهذا القرار يقرر عمليًا أن وجود الطلب ليس تفصيلًا ثانويًا، بل عنصر مؤثر في التكييف القانوني عند تطبيق المادة (١/٤٣٠).

ثالثًا: الركن المادي للابتزاز الإلكتروني

يقوم الركن المادي، في الصورة محل الدراسة، على نشاط يصدر عن الجاني ويكون من شأنه التأثير في إرادة المجني عليه من خلال التهديد، مقرونًا بالغاية التي يستهدفها الفاعل متى كانت





داخلة في النموذج القانوني للنص المطبق، وفي البيئة الرقمية يمكن أن يقع التهديد بواسطة رسالة نصية، أو تطبيق للمحادثة، أو حساب على منصة اجتماعية، أو بريد إلكتروني أو غيرها من الوسائل التقنية. ولا تغير الوسيلة الإلكترونية بذاتها من جوهر التهديد، لكنها تمنحه خصائص مختلفة من حيث السرعة وإمكان إخفاء هوية الفاعل واتساع دائرة نشر المحتوى محل التهديد^{١٠}.

ويكتسب الطلب أهمية خاصة؛ فقد يتمثل في دفع المال، أو القيام بفعل معين، أو الامتناع عنه، أو تقديم منفعة للجاني. وبالتالي فإن تحديد الطلب يساعد على التمييز بين الابتزاز بالمعنى محل الدراسة وبين صور التهديد الأخرى، ومن ثم يمكن تحليل الركن المادي في صورته الإلكترونية من خلال عناصر مترابطة هي: فعل التهديد، ومضمونه، والوسيلة الإلكترونية المستخدمة، والطلب أو التكليف المقترن به متى اشترطه النص القانوني المنطبق.

رابعاً: الركن المعنوي

الابتزاز الإلكتروني من الجرائم العمدية؛ فلا يكفي تحقق النشاط المادي مجرداً عن الإرادة، وإنما يلزم أن تتجه إرادة الجاني إلى ممارسة التهديد مع علمه بطبيعته ومضمونه، ويتوافر القصد الجرمي متى كان الجاني مدركاً لما يتضمنه سلوكه من تهديد واتجهت إرادته إلى صدوره وتحقيق الغاية المرتبطة به. فإذا احتفظ الجاني مثلاً بصور خاصة للمجني عليه ثم استعملها عمداً للضغط عليه من أجل الحصول على مبلغ مالي أو حمله على تصرف معين، فإن تحديد القصد يستخلص من ظروف الواقعة ومضمون الرسائل والمحادثات وسائر الأدلة^{١١}.

ولا ينبغي الخلط هنا بين الدافع والقصد الجرمي؛ فقد يكون دافع الجاني مالياً أو انتقامياً أو غير ذلك، لكن اختلاف الباعث لا يغير بذاته من توافر القصد متى اكتملت عناصره القانونية. وقد رصدت التطبيقات والدراسات القضائية العراقية تعدد دوافع الابتزاز الإلكتروني بين المالية والنفعية والانتقامية وغيرها.

خامساً: خصوصية الوسيلة الإلكترونية وأثرها في التكيف

لا ينبغي أن يؤدي وصف الجريمة بأنها "إلكترونية" إلى إنشاء وصف قانوني غير منصوص عليه. فالوسيلة التقنية لا تستقل عن الفعل الذي يجرمه القانون؛ ولذلك يجب على القاضي البحث أولاً عن المضمون القانوني للسلوك ثم تحديد النص المنطبق عليه، وعليه، فقد يكون السلوك الإلكتروني تهديداً مقترناً بطلب فتتحقق المادة (٤٣٠) إذا استوفت الواقعة جميع عناصرها، وقد يكون تهديداً مجرداً يخضع لنص آخر، كما قد تتضمن الواقعة أفعالاً أخرى تستوجب أوصافاً قانونية إضافية بحسب ظروفها، وهذه المرونة تسمح للنصوص النافذة باستيعاب بعض الصور

المستحدثة، لكنها في المقابل تكشف عن إشكالية تتمثل في أن النصوص الحالية لم توضع أصلاً لمعالجة جميع الخصائص التقنية للجريمة الإلكترونية^{١٢}.

الفرع الثاني

إشكاليات الحماية الجنائية والإثبات في جرائم الابتزاز الإلكتروني

أولاً: إشكالية غياب التنظيم التشريعي الخاص:

تتمثل إحدى أبرز الإشكاليات في عدم وجود قانون عراقي خاص ومستقل نافذ للجرائم المعلوماتية يضع تنظيمًا متكاملًا للابتزاز الإلكتروني. وقد أكد مسؤولون قضائيون في ٢٠٢٦ أن المحاكم العراقية تواجه هذه الوقائع بالنصوص النافذة من قانون العقوبات، في ظل عدم وجود قانون مستقل للجرائم المعلوماتية.

ولا تتمثل المشكلة في غياب العقاب بصورة مطلقة؛ فالنصوص الحالية تستطيع استيعاب صور متعددة من السلوك. وإنما تكمن الإشكالية في أن الطبيعة الإلكترونية تثير مسائل لم تكن البيئة التقليدية للنصوص العقابية مصممة لمعالجتها تفصيلاً، ومنها إخفاء الهوية، والأدلة الرقمية، والحسابات الوهمية، وسرعة محو البيانات، والجرائم العابرة للحدود والتطور التقني المستمر. ومن ثم ينبغي التمييز بين وجود أساس قانوني للعقاب وبين اكتمال السياسة التشريعية الخاصة بمواجهة الجريمة الإلكترونية؛ فهما مسألتان مختلفتان.

ثانياً: صعوبة تحديد هوية الجاني

قد يستخدم المبتز حساباً وهمياً أو اسماً مستعاراً أو وسائل تقنية تخفي هويته الحقيقية، الأمر الذي يجعل الانتقال من الحساب المستخدم في الجريمة إلى تحديد الشخص المسؤول عنه من أهم مراحل التحقيق. وتزداد المشكلة عندما تستخدم حسابات متعددة أو وسائل اتصال خارج العراق؛ إذ تتداخل المسألة مع الحصول على البيانات من مقدمي الخدمات والتعاون الفني والقانوني بين الجهات المعنية.

ولهذا لم تعد مواجهة الابتزاز الإلكتروني مسألة قانونية محضة، وإنما تتطلب تكامل المعرفة القانونية مع الخبرة الفنية الرقمية.

ثالثاً: الدليل الرقمي وحجته في الإثبات

يمثل الدليل الرقمي محورياً أساسياً في إثبات الابتزاز الإلكتروني؛ لأن جانباً كبيراً من النشاط الإجرامي قد يترك أثره في الرسائل والمحادثات والصور والتسجيلات والبيانات المخزنة على الأجهزة أو منصات التواصل الاجتماعي. وتبرز هنا أهمية المحافظة على الدليل بطريقة تضمن سلامته وعدم العبث به؛ إذ إن سهولة تعديل الملفات الرقمية أو حذفها تفرض ضرورة مراعاة



الإجراءات الفنية والقانونية المتعلقة باستخراجها وتوثيقها وتحريزها، وهذا التطور يدل على أن سلامة الدليل الإلكتروني لا تتوقف على العثور على رسالة أو صورة، وإنما تمتد إلى كيفية الحصول عليها وحفظها ونسبتها إلى مصدرها والتأكد من سلامتها الفنية.^{١٣}

رابعاً: الذكاء الاصطناعي وإشكالية صحة المحتوى محل الابتزاز:

أصبحت تقنيات الذكاء الاصطناعي تثير تحدياً جديداً في جرائم الابتزاز؛ إذ يمكن إنشاء أو تعديل صور أو تسجيلات بطريقة تجعلها تبدو حقيقية، وهو ما يثير إشكالية تتعلق بتمييز المحتوى الأصلي عن المحتوى المصطنع أو المعدل، وقد اكتسبت هذه المسألة أهمية عملية حديثة جداً؛ ففي ١٦ سبتمبر ٢٠٢٦ استضاف مجلس القضاء الأعلى اجتماعاً بمشاركة جهات أمنية وتقنية لمناقشة إعداد دليل استرشادي متكامل لطبيعة الأدلة الرقمية في جرائم الابتزاز الإلكتروني، وتضمن النقاش آلية عمل خوارزميات الذكاء الاصطناعي القادرة على التزييف وأسس التعامل معها^{١٤}.

وبذلك أصبح التحقق الفني من أصالة المحتوى الرقمي جزءاً متزايد الأهمية في التحقيق، ولا سيما عندما ينكر أحد الأطراف صحة الصورة أو التسجيل أو يدعي أنه مولد أو معدل بواسطة تقنيات الذكاء الاصطناعي.

خامساً: الطبيعة العابرة للحدود

قد يوجد المجني عليه في العراق بينما يدير الجاني حسابه من خارج البلاد، أو تكون البيانات اللازمة للتحقيق محفوظة لدى شركة تقدم خدماتها من خارج الإقليم العراقي. وهنا تظهر مشكلات عملية تتصل بتحديد الفاعل والحصول على البيانات وسرعة المحافظة عليها.

سادساً: إحجام المجني عليه عن الإبلاغ

تتميز جريمة الابتزاز الإلكتروني بخصوصية أخرى تتمثل في احتمال تردد المجني عليه في الإبلاغ، خاصة عندما يتعلق التهديد بصور أو معلومات تمس حياته الخاصة أو سمعته، وقد أشارت الأحكام القضائية العراقية إلى أن الخوف من النتائج الاجتماعية قد يدفع بعض الضحايا إلى الإحجام عن الإخبار، ولا سيما في المجتمعات المحافظة.

وتكمن خطورة ذلك في أن الصمت قد يمنح المبتز مساحة للاستمرار في مطالبه. ومن هنا ترتبط الحماية الجنائية بالجانب المجتمعي للدراسة؛ لأن تشجيع الشباب على الإبلاغ وتوعيتهم بكيفية المحافظة على الأدلة والتعامل مع الواقعة يمثل جانباً وقائياً لا يقل أهمية عن العقوبة المقررة بعد وقوع الجريمة^{١٥}.

يرى الباحث أن الإشكالية الأساسية في مواجهة الابتزاز الإلكتروني في التشريع العراقي لا تتمثل في انعدام الحماية الجنائية، إذ تسمح النصوص النافذة بمعاينة عدد من صوره، وإنما تتمثل في الفجوة بين الطبيعة التقليدية لبعض النصوص العقابية والطبيعة التقنية المتغيرة للسلوك الإجرامي. ولذلك فإن فاعلية المواجهة تستلزم الجمع بين التطبيق الدقيق للنصوص القائمة وتطوير الإطار التشريعي والإجرائي الخاص بالأدلة الرقمية، فضلاً عن تعزيز التنسيق بين الجهات القضائية والأمنية والتقنية. كما أن حماية الشباب لا ينبغي أن تبدأ بعد وقوع الابتزاز، بل يجب أن تمتد إلى مرحلة سابقة تقوم على الوقاية والتوعية.

الخاتمة

يتضح من خلال هذه الدراسة أن الابتزاز الإلكتروني يمثل أحد التحديات التي أفرزها التوسع في استخدام وسائل الاتصال الحديثة، وأن خطورته في الوسط الشبابي لا تقف عند حدود التهديد الإلكتروني، وإنما تمتد إلى المساس بحرية المجني عليه وخصوصيته واعتباره واستقراره الاجتماعي. كما أظهرت الدراسة أن المواجهة الفاعلة لهذه الظاهرة تقتضي الجمع بين الحماية الجنائية والوقاية المجتمعية؛ لأن التدخل العقابي، على أهميته، يبدأ في الغالب بعد وقوع الاعتداء، في حين تستهدف الوقاية تقليل فرص وقوعه والحد من آثاره في مرحلة مبكرة. وقد انتهت الدراسة إلى جملة من النتائج والتوصيات:

أولاً - النتائج:

١. إن الابتزاز الإلكتروني لا يختلف عن صور الابتزاز التقليدية في جوهر الضغط الواقع على إرادة المجني عليه، إلا أنه يتميز باستخدام البيئة الرقمية بما توفره من سرعة في الاتصال والنشر وإمكان إخفاء الهوية واتساع نطاق الضرر.
٢. لا يتضمن قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل تنظيمًا مستقلًا تحت مسمى جريمة الابتزاز الإلكتروني، الأمر الذي يجعل التكليف القانوني مرتبطًا بعناصر كل واقعة، مع إمكان تطبيق النصوص الخاصة بالتهديد، ولا سيما المادة (٤٣٠)، متى تحققت شروطها القانونية.
٣. كشفت الدراسة أن الطبيعة الرقمية للجريمة تثير تحديات خاصة في الإثبات، تتعلق بتحديد هوية الفاعل والمحافظة على الأدلة الرقمية والتحقق من سلامتها ونسبتها إلى مصدرها، فضلاً عن التحديات المستجدة الناشئة عن إمكان إنشاء أو تعديل المحتوى باستخدام تقنيات الذكاء الاصطناعي.

٤. يمثل إجماع بعض الضحايا عن الإبلاغ، نتيجة الخوف من الآثار الأسرية أو الاجتماعية أو المساس بالخصوصية، عاملاً يمكن أن يساعد المبتز على الاستمرار في ممارسة الضغط وتكرار مطالبه.

٥. تمتلك المؤسسات الشبابية والرياضية إمكانية مهمة للإسهام في الوقاية من الابتزاز الإلكتروني بحكم اتصالها المباشر بالشباب، إلا أن فاعلية هذا الدور تقتضي الانتقال من المبادرات التوعوية المنفرقة إلى برامج مؤسسية منظمة تجمع بين الثقافة القانونية والأمن الرقمي والإرشاد والتنسيق مع الجهات المختصة.

ثانياً - التوصيات:

١. ندعو المشرع العراقي إلى تطوير المعالجة التشريعية للجرائم المرتكبة في البيئة الرقمية بما يوفر تنظيمًا أكثر وضوحًا ودقة لصور الابتزاز الإلكتروني، مع مراعاة التطور المستمر في وسائل ارتكابه والأدلة الناشئة عنه.

٢. نوصي بتعزيز القدرات الفنية والقانونية للجهات المختصة بجمع الأدلة الرقمية وفحصها والمحافظة عليها، ووضع إجراءات واضحة تضمن سلامة الدليل الرقمي وإمكان التحقق من أصالته، ولا سيما في مواجهة المحتويات التي يمكن إنشاؤها أو تعديلها بواسطة تقنيات الذكاء الاصطناعي.

٣. نوصي مديريات الشباب والرياضة بتبني برنامج مؤسسي دوري للوقاية من الابتزاز الإلكتروني داخل المنتديات والمراكز والأندية الشبابية، يتضمن التوعية القانونية والتدريب على حماية الخصوصية والحسابات والبيانات الشخصية.

٤. نقترح تحديد نقاط اتصال أو موظفين مدربين في المؤسسات الشبابية الرئيسة لتقديم الإرشاد الأولي للشباب عند التعرض للابتزاز وتوجيههم إلى الجهات الرسمية المختصة، مع المحافظة على السرية واحترام الخصوصية وعدم التدخل في إجراءات التحقيق.

٥. نوصي بإقامة شراكة مستمرة بين المؤسسات الشبابية والرياضية والجهات القضائية والأمنية والتعليمية والتقنية المختصة، وتنظيم حملات وورش مشتركة، مع قياس أثر البرامج الوقائية بصورة دورية لضمان انتقال مواجهة الابتزاز الإلكتروني من التوعية المؤقتة إلى منظومة وقائية مؤسسية مستدامة.

الهوامش

^١ نصت المادة (١/٤٣٠) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل على " ١ - يعاقب بالسجن مدة لا تزيد على سبع سنوات او بالحبس كل من هدد اخر بارتكاب جناية ضد نفسه او ماله او ضد



نفس او مال غيره او باسناد امور مخدشة بالشرف او افشائها وكان ذلك مصحوبا بطلب او بتكليف بامر او الامتناع عن فعل او مقصودا به ذلك. ٢ - ويعاقب بالعقوبة ذاتها التهديد اذا كان التهديد في خطاب خال من اسم مرسله او كان منسوباً صدره الى جماعة سرية موجودة او مزعومة .

^٢ قرار محكمة التمييز الاتحادية المرقم ١٨٥١/هيئة الأحداث/٢٠٢٤ في ٢٠/١٠/٢٠٢٤ منشور على الموقع الإلكتروني لمجلس القضاء الأعلى <https://www.sjc.iq> .

^٣ حسام منصور محمد، جريمة الابتزاز الإلكتروني، مقال منشور على الموقع الإلكتروني لمجلس القضاء الأعلى <https://www.sjc.iq> .

^٤ قرار المحكمة الجنائية المركزية، رئاسة محكمة استئناف بغداد الرصافة الاتحادية، المرقم (٩/ج٢/٢٠٢٠) في ١٢/٣/٢٠٢٠ غير منشور .

^٥ قرار المحكمة الجنائية المركزية / الهيئة الثانية في محكمة استئناف الرصافة، بالعدد (٤٨٦ج٢/ ٢٠١٩ في ٣/٢٠١٩)، غير منشور .

^٦ د. أحمد محمد البوشي: الابتزاز الإلكتروني مفهوم جديد في جرائم التهديد المعلوماتية، دار النهضة العربية، القاهرة ، الطبعة الأولى ، ٢٠٢٢ ، ص ٦٦ .

^٧ نصت المادة (٤٣٠) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ على " ١- يعاقب بالسجن مدة لا تزيد على سبع سنوات او بالحبس كل من هدد اخر بارتكاب جناية ضد نفسه او ماله او ضد نفس او مال غيره او باسناد امور مخدشة بالشرف او افشائها وكان ذلك مصحوبا بطلب او بتكليف بامر او الامتناع عن فعل او مقصودا به ذلك. ٢ - ويعاقب بالعقوبة ذاتها التهديد اذا كان التهديد في خطاب خال من اسم مرسله او كان منسوباً صدره الى جماعة سرية موجودة او مزعومة ."

^٨ نصت المادة (٤٣١) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ على " يعاقب بالحبس كل من هدد اخر بارتكاب جناية ضد نفسه او ماله او ضد نفس او مال غيره او باسناد امور خادشة للشرف او الاعتبار او افشائها بغير الحالات المبينة في المادة ٤٣٠ ."

^٩ نصت المادة (٤٣٢) من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ على " كل من هدد اخر بالقول او الفعل او الإشارة كتابة او شفاهاً او بواسطة شخص اخر في غير الحالات المبينة في المادتين ٤٣٠ و ٤٣١ يعاقب بالحبس مدة لا تزيد على سنة واحدة او بغرامة لا تزيد على مائة دينار ."

^{١٠} أسامة أحمد المناعسة ، جلال محمد الزعبي و حایل فاضل الهواوشة ، جرائم الحاسوب الآلي والانترنت ، دار وائل للنشر ، الأردن - عمان ، الطبعة الثالثة ، ٢٠٠١ ، ص ٢٣٠ .

^{١١} د. ثامر محمد صالح الابتزاز الإلكتروني دراسة تحليلية مقارنة، دار الفكر والقانون للنشر والتوزيع المنصورة، ٢٠٢٠ ، ص ٨٣ .

- ^{١٢} د. داليا عبد العزيز المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة، بحث منشور في مجلة جيل الأبحاث القانونية المعمقة، العدد ٢٥، ٢٠١٨، ص ٢٣٠.
- ^{١٣} د. خالد حسن أحمد لطفي جرائم الانترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠١٩، ص ١٤.
- ^{١٤} البيان المنشور على موقع مجلس القضاء الأعلى <https://www.sjc.iq> .
- ^{١٥} مارب سامي خضير، جريمة الابتزاز الإلكتروني عبر استخدام وسائل التواصل الاجتماعي دراسة مقارنة دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٢٣، ص ٧٨.

المصادر

أولاً: الكتب القانونية:

١. أحمد محمد البوشي: الابتزاز الإلكتروني مفهوم جديد في جرائم التهديد المعلوماتية، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٢٢.
٢. أسامة أحمد المناعسة، جلال محمد الزعبي و حائل فاضل الهواشة، جرائم الحاسوب الآلي والانترنت، دار وائل للنشر، الأردن - عمان، الطبعة الثالثة، ٢٠٠١.
٣. ثامر محمد صالح الابتزاز الإلكتروني دراسة تحليلية مقارنة، دار الفكر والقانون للنشر والتوزيع المنصورة، ٢٠٢٠.
٤. خالد حسن أحمد لطفي جرائم الانترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، ٢٠١٩.
٥. مارب سامي خضير، جريمة الابتزاز الإلكتروني عبر استخدام وسائل التواصل الاجتماعي دراسة مقارنة دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٢٣.

ثانياً: القرارات القضائية:

١. قرار محكمة التمييز الاتحادية المرقم ١٨٥١/هيئة الأحداث/٢٠٢٤ في ٢٠/١٠/٢٠٢٤ منشور على الموقع الإلكتروني لمجلس القضاء الأعلى <https://www.sjc.iq> .
٢. قرار المحكمة الجنائية المركزية / الهيئة الثانية في محكمة استئناف الرصافة، بالعدد (٤٨٦ ج٢ / ٢٠١٩ في ٣/ ٢٠١٩)، غير منشور.

ثالثاً: المقالات:



١. حسام منصور محمد، جريمة الابتزاز الإلكتروني، مقال منشور على الموقع الإلكتروني لمجلس القضاء الأعلى [./https://www.sjc.iq](https://www.sjc.iq)

رابعاً: الأبحاث:

١. د. داليا عبد العزيز المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة، بحث منشور في مجلة جيل الأبحاث القانونية المعمقة، العدد ٢٥، ٢٠١٨.

خامساً: القوانين:

١. قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل النافذ.

Sources

First: Legal Books:

١. Ahmed Mohamed Al-Boushi: Electronic Extortion: A New Concept in Cybercrime, Dar Al-Nahda Al-Arabiya, Cairo, First Edition, 2022.

٢. Osama Ahmed Al-Mana'seh, Jalal Mohamed Al-Zoubi, and Hail Fadel Al-Hawawsha: Computer and Internet Crimes, Dar Wael Publishing, Amman, Jordan, Third Edition, 2001.

٣. Thamer Mohamed Saleh: Electronic Extortion: A Comparative Analytical Study, Dar Al-Fikr Wal-Qanoun for Publishing and Distribution, Mansoura, 2020.

٤. Khaled Hassan Ahmed Lotfi: Internet Crimes: Between Cyber Piracy and Electronic Extortion, Dar Al-Fikr Al-Jami'i, Alexandria, First Edition, 2019.

٥. Marib Sami Khodair: The Crime of Electronic Extortion Through the Use of Social Media: A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, First Edition, 2023.

Second: Judicial Decisions:

١. Federal Court of Cassation Decision No. 1851/Juvenile Panel/2024 dated 10/20/2024, published on the Supreme Judicial Council website: <https://www.sjc.iq/>

٢. Decision of the Central Criminal Court/Second Panel of the Rusafa Court of Appeals, No. (486 J2/2019 dated 3/2019), unpublished.

Third: Articles:

.^١ Hussam Mansour Mohammed, "The Crime of Electronic Extortion," an article published on the Supreme Judicial Council website: <https://www.sjc.iq/>

Fourth: Research Papers:

.^١ Dr. Dalia Abdul Aziz, "Criminal Liability for the Crime of Electronic Extortion in the Saudi System: A Comparative Study," a research paper published in the Journal of In-Depth Legal Research, Issue 25, 2018.

Fifth: Laws:

.^١ Iraqi Penal Code No. 111 of 1969, as amended and in force.

