ISSN: 1812-0512 (Print) 2790-346X (online)

Waist Journal for Human Sciences

Journal Homepage: https://wjfh.uowasit.edu.iq/index.php/wjfh/en

Research article

Electronic Extortion Crimes Against Women and Methods of Combating Them – A Comparative Analytical Study

Asst. Lect. Rusul Noori Gaeed

Al-Kut University College (Private University), Iraq

ARTICLE INFO

Keywords: Cyber-blackmail, cyber-harassment, cybersecurity, digital privacy

***Correspondence author*:**

rusul.gaeed@alkutcollege.edu.iq

Received: 21 **August** 2026
Revised: 24 **September** 2026
Accepted: 24 **September** 2026
Published: 25 **November** 2026

1812-0512 /© 2026 The Author(s). Published by Wasit Journal for Humanities Sciences, Wasit University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

***Cite*:**

Gaeed, R. N. (2026). Electronic Extortion Crimes Against Women and Methods of Combating Them – A Comparative Analytical Study. *Wasit Journal for Human Sciences*, *22*(4/Pt2). https://doi.org/10.31185/wjfh.Vol22.Iss4/Pt2.2244

ABSTRACT

This study examines the crime of electronic extortion against women and the challenges facing efforts to combat it. It defines the crime, outlines its features, and examines its effects on victims and the causes behind its spread. The research offers a theoretical framework that captures the phenomenon's social complexity, not just its legal dimension.

Using a descriptive-analytical method, the study is divided into two sections. The first covers the concept, elements, and characteristics of electronic extortion, while the second addresses ways of confronting it and the legal penalties involved through a comparative study of Iraqi, Egyptian, Jordanian, and Emirati legislation. Findings show that this crime against women continues to rise and that its particular features make investigation genuinely difficult.

The study underscores the importance of cooperation among individuals, communities, and governments in fighting this crime, along with support and empowerment for affected women, enabling them to access justice and ensuring that their rights and safety are protected online.

جريمة الابتزاز الإلكتروني المرتكبة ضد النساء وطرق مكافحتها – دراسة تحليلية مقارنة

م.م رسل نوري كعيد
جامعة الكوت الاهلية

المُستخلص

تناول هذه الدراسة جريمة الابتزاز الإلكتروني المرتكبة ضد النساء، وتقف عند التحديات التي تعترض مكافحتها. تبدأ بتعريف الجريمة واستعراض خصائصها، ثم تتوقف عند آثارها على الضحايا وصولاً إلى الأسباب الكامنة وراء تفشي هذه الظاهرة. وتطرح البحث إطاراً نظرياً يحاول أن يعكس قدر الإمكان الطبيعة الاجتماعية المعقدة لهذه الظاهرة لا الجانب القانوني وحده.

اعتمدت الدراسة على المنهج التحليلي المقارن، وقسم البحث على مبحثين: يعرض الأول ماهية جريمة الابتزاز الإلكتروني وأركانها وخصائصها وأسبابها، بينما يخصص الثاني لسبل التصدي لها والعقوبات المقررة في ضوء دراسة مقارنة بين التشريعات العراقية والمصرية والأردنية والإماراتية. وقد تبين من خلال هذا البحث أن جريمة الابتزاز ضد النساء في تصاعد مستمر يوماً بعد آخر، وأنها تحمل من الخصائص ما يجعل التحقيق فيها أمراً بالغ التعقيد.

وفي الخاتمة سوف نسلط الضوء على أهمية التعاون بين أفراد المجتمع والمنظمات والحكومات من أجل مخاربة هذه الجريمة. كما نشدد على أهمية الدعم والتمكين للنساء المتضررات من أجل الوصول إلى العدالة، وحماية حقوق النساء والحفاظ على سلامتهن في العالم الرقمي.

الكلمات المفتاحية: الابتزاز الإلكتروني، التحرش الإلكتروني، الأمان السيبراني، الخصوصية الرقمية

المقدمة

منذ ظهور وسائل التواصل الاجتماعي، استمرت جرائم الابتزاز الإلكتروني في الانتشار في العراق، وقد جذبت مثل هذه الجرائم الخطيرة انتباه كافة مناحي الحياة، وخاصة النساء والفتيات، وأسفرت عن سقوط العديد من الضحايا، ووصل الأمر إلى حد القتل والانتحار والاعتداء الجنسي. تنشأ مشكلة الابتزاز في المجتمع التي تفقد فيه الأسرة الاستقرار العاطفي، مما يؤدي إلى انحرافات سلوكية. كما أن لهذه الجريمة تأثيراً على قضايا الشرف والسمعة، حيث يعتبر المجتمع العربي، وخاصة العراق، من تلك المجتمعات التي تمثل فيها هذه الجريمة وصمة عار اجتماعية، وتجلب العار على الأسر والعائلات، وتجعلها نواة المشاريع الإجرامية وموضوعاً لها (إبراهيم، ٢٠١٩، ص. ٤).

الابتزاز الإلكتروني هو عملية التهديد بنشر صور أو مقاطع فيديو أو معلومات شخصية حساسة بقصد إيذاء شخص ما إذا لم تستجب لرغباته المالية أو الجنسية. كما يعتبر ذلك محاولة لإكراه الضحية وحرمانها من إرادته وحريته في إلحاق الأذى الجسدي أو النفسي

بالضحية، حيث يستخدم وسائل التواصل الاجتماعي أو غيرها من الوسائل لارتكاب جريمته، سواء كانت جسدية أو غير أخلاقية أو كلاهما (إبراهيم، ٢٠١٩، ص. ١٠).

وتكمن خطورة هذه الجريمة في السهولة والوسائل المتاحة للناس من جميع الأعمار، فضلاً عن سهولة محو الأدلة، وتعتبر الأسرة من أقوى المؤثرات الاجتماعية في تشكيل شخصية الإنسان.

يتعرض الكثير من النساء لهذا النوع من السلوك الإجرامي بسبب عدة عوامل متنوعة مثل التمييز الجنسي، والانتقام، والسيطرة، والترويع. ومن أمثلة جريمة الابتزاز الإلكتروني المرتكبة ضد النساء هي (التهديد بنشر المعلومات الخاصة، الابتزاز المادي، العنف النفسي والعاطفي، التحرش الرقمي). وخطورة هذا النوع من الجرائم لا تُقاس فقط بحجم الأضرار المادية، بل بعمق الأثر النفسي الذي يتركه في نفوس الضحايا: انتهاك للخصوصية، وللشرف، وللحرية الشخصية، يولّد قلقاً قد يمتد أثره لسنوات. ولذلك فإن مواجهته الفعلية تتطلب تضافر الجهود بين الجهات الحكومية والأجهزة الأمنية ومزودي الخدمة الإلكترونية ومؤسسات المجتمع المدني، كلٌّ من موقعه، لحماية النساء من هذا الشكل المستجد من الجرائم الجنسية عبر الإنترنت.

من المهم أن يتم تعزيز الوعي بجريمة الابتزاز الإلكتروني المرتكبة ضد النساء وتوفير الموارد والدعم اللازم للضحايا، ويجب على الضحايا أن يتصلوا بالسلطات المعنية والمنظمات غير الحكومية المتخصصة للحصول على المساعدة والدعم اللازمين، كما ينبغي على المؤسسات ومقدمي الخدمات الإلكترونية اتخاذ إجراءات لحماية المستخدمين وتعزيز الأمان الرقمي للنساء.

مشكلة البحث

تتمثل مشكلة هذا البحث في دراسة إحدى الجرائم الإلكترونية التي ظهرت بسبب الانتشار السريع لوسائل التواصل الاجتماعي واستخدامها من قبل العديد من الفئات، مما أدى إلى خلق مجتمع جديد على شبكة الإنترنت، مجتمع افتراضي له آثار سلبية وإيجابية. ويتضمن وصفاً وتحليلاً لجرائم الابتزاز التي تتعرض لها المرأة عبر وسائل التواصل الاجتماعي من خلال التعرف على أنواعها وتأثيراتها والظروف التي أدت إلى ظهورها، ومن خلال ذلك يتم وضع إطار نظري يعتبر هذا النوع من الجرائم حقيقة اجتماعية ناشئة عن ظاهرة اجتماعية ويعكس الطبيعة الاجتماعية للظاهرة المعاصرة بناءً على معطيات وسيكولوجية وجنائية ومنحرفة لكي نحاول فهم تطورها في ظاهرة العنف ضد المرأة، أو ما يسمى بالعنف الجنسي، لأنها تنطلق من الفرضيات الأساسية لهذه النظريات، ومن ثم يطرح سؤال البحث بالتركيز على مواقع الابتزاز الإجرامي ضد المرأة على شبكات التواصل الاجتماعي.

هدف البحث

يهدف البحث الحالي إلى تقديم فهم أعمق لطبيعة جريمة الابتزاز الإلكتروني المرتكبة ضد النساء والتحديات التي تواجهها النساء كضحايا، إذ يمكن تلخيص الأهداف إلى ما يأتي:

١. يسهم هذا البحث في رفع مستوى الوعي بجريمة الابتزاز الإلكتروني المرتكبة ضد النساء وبآثارها المدمرة على الضحية أولاً وعلى النسيج الاجتماعي عمومًا. كما يكشف البحث عن ثغرات قائمة في التشريعات الحالية لم تعد كافية لمواكبة هذا النمط المستحدث من الجرائم.

٢. المساهمة في تحسين ودعم الخدمات المتوفرة للنساء الضحايا وكذلك تطوير برامج أخرى للتوعية والتدريب والدعم النفسي والقانوني.

٣. يسلط البحث الحالي الضوء على هذه الجريمة لتكون نقطة انطلاقة للباحثين والأكاديميين والمؤسسات الأخرى من أجل الاستمرار في هذا المجال. يهدف البحث بشكل أساسي إلى إيجاد الحلول الجذرية والفعالة لمواجهة هذه الجريمة، وكذلك الحفاظ على حقوق النساء وشرفهن داخل البيئة الرقمية.

أهمية البحث

١. يوفر هذا البحث فهمًا أدق وأعمق لتجربة النساء كضحايا لهذه الجريمة. ومن خلال هذا الفهم يمكن أن نحسن من الدعم والمساعدة للضحايا وتوفير الحماية لهن وضمان أمنهن النفسي والجسدي.

٢. المساهمة في زيادة الوعي وتعزيزه بجريمة الابتزاز الإلكتروني المرتكبة ضد النساء وتوفير الموارد والدعم اللازم للضحايا.

٣. المساعدة في توجيه وتحسين التشريعات والسياسات المتعلقة بالابتزاز الإلكتروني للنساء من خلال ما يقدمه البحث من أدلة ومعرفة، وكذلك تطوير وتعزيز القوانين الحالية وإجراءات التحقيق لتكون أكثر صرامة.

٤. من الممكن أن يساهم البحث في تطوير التقنيات والأدوات للكشف عن هذه الجريمة والتصدي لها.

٥. يمكن للبحث أن يساهم في توجيه الجهود والاستراتيجيات العامة لمكافحة جريمة الابتزاز الإلكتروني ضد النساء.

منهج البحث

سيتبع هذا البحث منهجًا تحليليًا وصفيًا لفحص جريمة الابتزاز الإلكتروني المرتكبة ضد النساء وطرق مكافحتها، مع الاعتماد على المنهج المقارن لبيان مواقف التشريعات المختلفة.

هيكلية البحث

سيتم تقسيم الموضوع إلى مبحثين رئيسيين، حيث سيتناول الأول ماهية جريمة الابتزاز الإلكتروني، في حين سيختص المبحث الثاني بطرق مكافحة الابتزاز الإلكتروني والعقوبات المقررة.

المبحث الأول: ماهية جريمة الابتزاز الإلكتروني

المطلب الأول: تعريف جريمة الابتزاز الإلكتروني

المطلب الثاني: أركان جريمة الابتزاز الإلكتروني

المطلب الثالث: خصائص جريمة الابتزاز الإلكتروني

المطلب الرابع: أسباب جريمة الابتزاز الإلكتروني ودوافعها

المبحث الثاني: طرق مكافحة الابتزاز الإلكتروني والعقوبات المقررة – دراسة مقارنة

المطلب الأول: طرق مكافحة الابتزاز الإلكتروني

المطلب الثاني: العقوبات المقررة على جريمة الابتزاز الإلكتروني – دراسة مقارنة

المبحث الأول: ماهية جريمة الابتزاز الإلكتروني

يُعد الابتزاز الإلكتروني من الجرائم المستحدثة التي فرضتها التحولات التكنولوجية المتسارعة، وأصبح يشكل تهديدًا حقيقيًا للأمن الرقمي والاجتماعي، ولا سيما للنساء اللواتي يجدن أنفسهن في مواجهة أشكال متعددة من الاستغلال والتهديد. ونظرًا لتعدد صور هذه الجريمة وتشابك أبعادها القانونية والاجتماعية والنفسية، فإن دراستها تقتضي الوقوف عند ماهيتها من خلال تعريفها لغةً واصطلاحًا وقانونًا، ثم بيان أركانها التي لا تقوم إلا بها، وتحديد خصائصها التي تميزها عن الجرائم التقليدية، وأخيرًا تحليل الأسباب والدوافع التي تقف وراء انتشارها. وسيتناول هذا المبحث هذه المحاور في أربعة مطالب متكاملة.

المطلب الأول: تعريف جريمة الابتزاز الإلكتروني

الفرع الأول: التعريف اللغوي والاصطلاحي

الابتزاز في اللغة مأخوذ من "البَزّ" وهو السلب والنهب، يقال: بَزَّهُ يَبُزُّهُ بَزًّا، أي سَلَبَه. والابتزاز هو طلب الشيء بغير حق، أو أخذ الشيء قهرًا وقسرًا. ويُستعمل في لسان العرب بمعنى السلب والإلزام والإكراه على فعل شيء بغير رضا (ابن منظور، ١٩٩٣، ج٧، ص. ٣٥٣). والابتزاز هو الهيئة من لباس وسلاح (الفراهيدي، بدون سنة، ج٩١).

ويُعرف الابتزاز اصطلاحًا بأنه: "استخدام الضغط أو التهديد لإجبار شخص على القيام بفعل أو الامتناع عن فعل، بقصد الحصول على منفعة غير مشروعة" (أبو خطوة، بدون سنة، ص. ٥٥٩).

أما الابتزاز الإلكتروني (Electronic Blackmail)، فيقصد به: "استخدام وسائل الاتصال الإلكترونية والتقنيات الحديثة، كالبريد الإلكتروني ووسائل التواصل الاجتماعي والرسائل النصية، لتهديد شخص بنشر معلومات أو صور أو بيانات خاصة به، بهدف إجباره على دفع مبالغ مالية أو القيام بسلوك معين أو الامتناع عنه" (إسلامي، ٢٠٢١، ص. ٩٨).

الفرع الثاني: التعريف القانوني والفقهي

عرَّف الفقه القانوني الابتزاز الإلكتروني بأنه: "كل سلوك إجرامي يتم عبر وسائل إلكترونية، يتضمن تهديدًا للضحية بإفشاء أسراره أو نشر صوره أو معلوماته الخاصة، بغرض الحصول على منفعة مادية أو معنوية غير مشروعة" (عاشور، ٢٠٢٠، ص. ١١٧).

كما عُرِّف بأنه: "التهديد بإحداث ضرر للشخص أو لشيء متعلق به، سواء بشكل علني أو عبر الضغط على إرادة الشخص، باستخدام وسائل تقنية المعلومات" (العنزي، ٢٠١٧، ص. ١٩٤).

ومن الواضح أنه من بين الجرائم المعلوماتية التي تزايدت بشكل ملحوظ في الآونة الأخيرة، فإن جريمة الابتزاز هي الجريمة التي يتعرض فيها الشخص من قبل آخرين أو مجموعة محددة، وذلك لأن هناك أنواعًا وأشكالًا كثيرة من الابتزاز، ومن بينها ابتزاز الرجال للمرأة والعكس (اللوهية، ٢٠١٨).

أصبحت جرائم الابتزاز الإلكتروني من الجرائم المدرجة ضمن الجرائم الجنائية دوليًا، ووفقًا لآراء المشرعين في مختلف الدول فإن الحد الأقصى للعقوبة بموجب القانون الدولي قد يصل إلى ٢٠ عامًا، و١٥٠ مليون حالة ابتزاز ضد المرأة، وكما ذكرنا أعلاه فإن جريمة الابتزاز الإلكتروني هي أحد أشكال الجرائم المعلوماتية، وغالبًا ما تصبح النساء ضحايا لمثل هذه الجرائم (أحمد، ٢٠٢٠، ص٥٣٥).

المطلب الثاني: أركان جريمة الابتزاز الإلكتروني

لا تقوم الجريمة في أي نظام قانوني إلا إذا توافرت أركانها التي حددها القانون، وجريمة الابتزاز الإلكتروني كغيرها من الجرائم تتطلب لقيامها توافر ثلاثة أركان أساسية: الركن المادي، والركن المعنوي، والركن القانوني.

الفرع الأول: الركن المادي

وهو السلوك المادي الخارجي الذي يجرمه القانون، ويتمثل بالقيام بفعل أو الامتناع عن القيام بفعل أوجبه القانون، وبالتالي يعاقب القانون مرتكبه (العمومطي، ٢٠٢٣، ص. ١٣٣).

ويتكون الركن المادي لجريمة الابتزاز الإلكتروني من ثلاثة عناصر: الفعل الإجرامي، والنتيجة الجرمية، والعلاقة السببية بين النشاط الجرمي والنتيجة الإجرامية. ويختلف الركن المادي باختلاف الجرائم، ولكن بشكل عام لا بد أن يكون هناك مظهر خارجي، فالركن المادي هو المظهر الخارجي ويتضمن ماديات الجريمة أي له طبيعة مادية محسوسة (العمومطي، ٢٠٢٣، ص. ١٣٣).

وقد أشار إليه المشرع العراقي في قانون العقوبات رقم (١١١) لسنة ١٩٦٩ في المادة ٢٨ منه بالقول: (سلوك اجرامي بارتكاب فعل جرمه القانون او الامتناع عن فعل امر به القانون).

وفي جريمة الابتزاز الإلكتروني يتمثل الركن المادي بالسلوك الإجرامي الصادر من المبتز تجاه الضحية كالتهديد أو الوعيد بنشر صور أو مقاطع فيديو أو أي بيانات أخرى تخص الضحية، أو عن طريق إرسال رسائل إلكترونية تتسم بالتهديد بالتشهير أو الفضيحة بأي وسيلة كانت عبر مواقع التواصل الاجتماعي، وهذا ما أشارت إليه المادة ٤٣٠ من قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل.

ويشترط لتحقق الركن المادي أن يكون المبتز جادًا في تهديده، وبعبارات صريحة، لا ضمنية، ولكن يفهم منه أن المبتز يهدده بأمر هو إفشاء أسرار الضحية إن لم يلبِّ رغبته، فالعقوبة تكمن في الضغط والإكراه الذي يقترن بالتهديد لإرغام الضحية على القيام بذلك (العمومطي، ٢٠٢٣، ص. ١٣٣).

الفرع الثاني: الركن المعنوي

يتمثل الركن المعنوي في القصد الجنائي، والذي يعني اتجاه إرادة الجاني إلى ارتكاب السلوك الإجرامي وإحداث النتيجة، مع علمه بذلك. ويمثل الركن المعنوي الأصول النفسية لماديات الجريمة (فايد، ١٩٨٧، ص.١٧).

وكون أن جريمة الابتزاز الإلكتروني من الجرائم العمدية فهي تقوم على توافر القصد العام ولا تحتاج إلى القصد الخاص، ويقوم القصد العام على عنصرين وهما العلم والإرادة. يُقصد بالعنصر الأول توافر العلم لدى الجاني وهو يعلم أنه يقوم بنشر صور فاضحة ومن ثم قيامه بالتهديد للحصول على منفعة شخصية في جريمة يعاقب عليها قانونًا، كما يتطلب أن يكون الجاني عالمًا بماهية الفعل أو الامتناع عن فعل يشكل جريمة قانونًا، ملحقًا ضررًا بالضحية (ثروت، ١٩٨٩، ص. ١١٨).

أما العنصر الثاني وهي الإرادة فيتطلب القانون أن تتجه رغبة الجاني في إلحاق الضرر بالضحية وتحقق النتيجة الجرمية المتمثلة بالابتزاز، ولا يتوقف على مدى علم الجاني بما لحقه من ضرر نفسي للضحية، لكن يمتد قصد الجاني إلى تهديده وتخويفه وإجباره على القيام بأفعال أو الامتناع عن أفعال. ويجب إثبات إرادة الفاعل في ارتكاب الجريمة دون أن تكون هناك موانع للمسؤولية، فإذا كان واقعًا عليه إكراه فلا يتحقق القصد الجنائي ولا تقع المسؤولية على الفاعل.

إن توجيه هذه الإرادة إلى ارتكاب السلوك الإجرامي لا يكفي لقيام الركن المعنوي، فمن اللازم أن توصف هذه الإرادة بأنها إرادة آثمة أو خاطئة، فهي توجد رابطة بين الفاعل والواقعة المجرمة بنص القانون (جواد، بدون سنة، ص٢٣٠؛ بهنام، ١٩٩٧، ص. ٨٦٥).

الفرع الثالث: الركن القانوني

ويقصد به وجود نص قانوني يجرم الفعل ويرتب عليه عقوبة. وفي القانون العراقي، لا يوجد نص خاص يجرم الابتزاز الإلكتروني، وإنما يتم تكييفه وفق نصوص عامة كالمادة ٤٣٠ من قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل.

وقد نصت المادة ٤٣٠ على: "يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من هدد آخر بارتكاب جناية ضد نفسه او ماله او ضد نفس او مال غيره او بأسناد امور مخدشة بالشرف او افشائها وكان ذلك مصحوبا بطلب او بتكليف بأمر او الامتناع عن فعل او مقصودا به ذلك" (قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل، المادة ٤٣٠).

كما نصت المادة ٤٣٢: "كل من هدد بالفعل او بالقول او الإشارة او الكتابة او شفاها او بواسطة شخص اخر يعاقب بالحبس مدة لا تزيد على سنة واحدة او بغرامة لا تزيد عن مائة دينار" (قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل، المادة ٤٣٢).

والمادة ٤٣٣: "القذف هو اسناد واقعة معينة الى الغير بإحدى طرق العلانية من شأنها لو صحت ان توجب عقاب من اسندت اليه او احتقاره عند اهل وطنه ويعاقب من قذف غيره بالحبس او بالغرامة او بإحدى هاتين العقوبتين. وإذا وقع القذف بطريقة النشر في الصحف او المطبوعات او بإحدى طرق الاعلام الأخرى عد طرفا مشددا للعقوبة" (قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل، المادة ٤٣٣).

والمادة ٤٣٨: "من نشر إحدى الطرق العلنية اخبارا او صورا او تعليقات تتصل بأسرار الحياة الخاصة او العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة إليهم" (قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل، المادة ٤٣٨).

وهناك إجراءات قانونية وقضائية للتعامل مع مجرمي الابتزاز الإلكتروني، وقد خصصت الجهات المعنية (وزارة الداخلية) و(جهاز الأمن الوطني) وحدات متخصصة (مكافحة الابتزاز الإلكتروني) لمكافحة هذا النوع من الجرائم.

المطلب الثالث: خصائص جريمة الابتزاز الإلكتروني

إن خصوصية جريمة الابتزاز الإلكتروني تجعلها تختلف عن الجرائم التقليدية في عدة جوانب، فبعض الخصائص ترتبط بالسلوك الإجرامي، والبعض الآخر يرتبط بشخصية الجاني.

أولاً: صعوبة إثبات السلوك الإجرامي

تتمثل إحدى أهم خصائص جريمة الابتزاز الإلكتروني في صعوبة إثبات سلوكها الإجرامي، لأنه غالبًا ما يكون من الصعب العثور على آثار مادية للجريمة. والسبب في ذلك هو أن الجناة غالبًا ما يستخدمون وسائل فنية وتقنية معقدة، كما أن الأفعال التي تشكل العنصر المادي تتميز بالسهولة والسرعة، فقد لا تستغرق أكثر من ثوانٍ معدودة، مثل المحو والعبث. ولذلك فإن هذه الجرائم بطبيعتها لا يبقى لها أي أثر بعد ارتكابها، وإذا وُجد فمن الصعب الحفاظ عليه بالوسائل الفنية (المقصودي، ٢٠١٥، ص. ٢٧).

ثانياً: الجريمة الناعمة

ومن خصائص جريمة الابتزاز الإلكتروني أنها جريمة ناعمة، لأنها لا تنطوي على عنف مثل الجرائم التقليدية كالجرائم الإرهابية والسرقات والسطو المسلح، ولكنها تنطوي على جرائم معلوماتية. ففي الأساس، نقل البيانات من كمبيوتر إلى آخر أو سرقة رصيد بنك معين إلكترونيًا لا يتطلب من الجاني استخدام العنف أو تبادل إطلاق النار مع أفراد الأمن. ومن هذا نجد أن جريمة الابتزاز الإلكتروني هي جريمة ناعمة وهادئة، ومن خصائصها غياب العنف (اليوسف، ٢٠١٥، ص٩٧).

ثالثاً: صعوبة تقديم الأدلة

ولعلنا نذكر الخاصة الثالثة لجريمة الابتزاز الإلكتروني وهي صعوبة تقديم الأدلة، لأن الفرق بينها وبين الجريمة التقليدية يكمن في صعوبة تقديم الأدلة. ويرجع ذلك إلى عدم وجود آثار تقليدية للجريمة، وعدم وجود أدلة مادية (بصمات الأصابع، والتخريب، والأدلة المادية) وسهولة محو الأدلة أو تدميرها في فترة زمنية قصيرة للغاية. وفي نفس السياق نضيف أن جهاز الشرطة والقضاء قليل الخبرة والقوانين الموجودة غير كافية (اليوسف، ٢٠١٥، ص٩٧).

رابعاً: البيئة الحاسوبية

ومن الجدير بالذكر أن من خصائص جريمة الابتزاز الإلكتروني أنها تحدث في البيئات الحاسوبية والشبكات العالمية، ومكان حدوثها هو المعلومات المخزنة على أجهزة الكمبيوتر وشبكاتها، وقد تحدث أيضًا على أجهزة الكمبيوتر وشبكاتها وسط المرحلة التشغيلية لنظام معالجة المعلومات الآلي، سواء المدخلات أو المعالجة أو المخرجات (عبد السميع، ٢٠١٨، ص٤١).

المطلب الرابع: أسباب جريمة الابتزاز الإلكتروني ودوافعها

تتعدد الأسباب التي تدفع مرتكبي جريمة الابتزاز الإلكتروني إلى ارتكاب أفعالهم الإجرامية، ويمكن تصنيف هذه الدوافع في ثلاثة فروع رئيسية:

الفرع الأول: الدوافع المالية

يُعد الدافع المالي من أهم دوافع الابتزاز الإلكتروني، حيث يسعى المبتز إلى الحصول على مبالغ مالية من الضحية مقابل عدم نشر معلوماتها أو صورها الخاصة. نظرًا لانتشار البطالة، يجد الشباب العاطلين عن العمل أن الابتزاز الإلكتروني من أسهل الطرق للحصول على المال، لذلك يطلب الشباب مبالغ مالية كبيرة من الفتيات. واستغل ضعفها بعرض أموال عليها مقابل عدم نشر صورة لها أو إفشاء سر (محمد، ٢٠١٧، ص١٧).

الفرع الثاني: الدوافع الجسدية

قد يهدف المبتز إلى إشباع رغباته الجنسية من خلال إجبار الضحية على إرسال صور أو مقاطع فيديو غير أخلاقية، أو ممارسة أفعال مخلة بالحياء. يبتز الشاب أي فتاة لإشباع غريزته، فيبدأ بتهديدها بالصور أو الفيديوهات، ويطرح عليها أسئلة جنسية مخالفة للشرع والقوانين (محمد، ٢٠١٧، ص١٧).

الفرع الثالث: الدوافع النفسية

تشمل الدوافع النفسية الرغبة في الانتقام، أو السيطرة على الضحية، أو الشعور بالتفوق والقوة، أو الكراهية، أو الحسد. يتمتع المبتز بشخصية سيكوباتية تميز بعدم النضج العاطفي وقد يشتهي السلوك المعادي للمجتمع بغض النظر عن القيم والأخلاق الاجتماعية أو قد يكون الدافع نتيجة لأي شكل من أشكال الانتقام من الفتاة (محمد، ٢٠١٧، ص. ١٧).

المبحث الثاني: طرق مكافحة الابتزاز الإلكتروني والعقوبات المقررة – دراسة مقارنة

تشكل التكنولوجيا الحديثة والاتصالات الإلكترونية تحدًا كبيرًا في عصرنا الحالي. ومع ذلك فإن الابتزاز الإلكتروني يعد مشكلة شائعة تواجهها الأفراد والمؤسسات على حد سواء. تهدف جرائم الابتزاز الإلكتروني إلى خلق شعور بالخوف والضغط والاستغلال لدى الضحايا،

وتستند إلى استخدام وسائل الاتصال الإلكترونية مثل البريد الإلكتروني والرسائل النصية ووسائل التواصل الاجتماعي. ومع زيادة استخدام الإنترنت والتقنيات الرقمية، أصبح الابتزاز الإلكتروني أكثر انتشارًا وتطورًا (حنش، ٢٠٢٠، ص. ٤٩).

على الرغم من أنه من المستحيل التصدي بشكل كامل للابتزاز الإلكتروني، إلا أن اتباع الإجراءات الوقائية يمكن أن يساعد في تقليل المخاطر وحماية الأفراد والمؤسسات من هذه الجريمة الإلكترونية الخطيرة. يجب أن يتعاون المجتمع بأكمله لمكافحة الابتزاز الإلكتروني وتوفير بيئة آمنة على الإنترنت للجميع.

المطلب الأول: طرق مكافحة الابتزاز الإلكتروني

الابتزاز الإلكتروني ضد المرأة هو تهديد خطير يعاني منه العديد من الأفراد. فيما يلي بعض الطرق المهمة لمكافحة الابتزاز الإلكتروني ضد المرأة:

١. التوعية والتعليم: يجب على المرأة أن تكون على دراية بأشكال الابتزاز الإلكتروني وأساليبه، وتعلم كيفية حماية خصوصيتها وتأمين حساباتها الشخصية عبر الإنترنت.

٢. تأمين الحسابات الشخصية: يتطلب من النساء اختيار كلمات مرور قوية ومميزة لكل حساب وتفعيل خاصية التحقق الثاني عند تسجيل الدخول، وتحديث البرامج دائمًا للتخلص من الثغرات الأمنية.

٣. الحذر عند استخدام الإنترنت: على النساء أخذ الحيطة والحذر عند استخدام مواقع التواصل الاجتماعي، وتجنب الموافقة على طلبات الصداقة أو الرسائل من أشخاص مجهولين الهوية، بالإضافة لذلك تجنب نشر صورها الشخصية ومعلوماتها الخاصة (الخالدي، ٢٠٢٠، ص٤٣).

٤. الإبلاغ عن الحالات: يجب على المرأة إبلاغ الجهات الخاصة كالشرطة أو الهيئات القضائية عن تعرضها لمثل هكذا حالات وتوثيق الأدلة المتعلقة بالحادثة لضمان حقها.

٥. الحصول على المساعدة القانونية: على الضحية التوجه لمحامي أو منظمة حقوقية في أقرب وقت ممكن للحصول على المشورة القانونية والدعم المعنوي (المولى، ٢٠١٩، ص. ١٠٢).

٦. التعاون والدعم: ينبغي على المرأة أن تبحث عن الدعم من الأصدقاء والعائلة والمجتمع المحلي، فقد تكون هناك منظمات ومراكز متخصصة تقدم الدعم النفسي والاجتماعي للمرأة المتضررة.

من المهم أن تتعامل المرأة بجدية مع حالات الابتزاز الإلكتروني وتبذل قصارى جهدها للحماية منه. ينبغي أن تعمل المجتمعات والحكومات أيضًا على تعزيز الوعي بمشكلة الابتزاز الإلكتروني واتخاذ إجراءات قوية لمكافحته ومعاقبة المعتدين.

المطلب الثاني: العقوبات المقررة على جريمة الابتزاز الإلكتروني – دراسة مقارنة

الفرع الأول: موقف المشرع العراقي

لا توجد كلمة (الابتزاز)بشكل صريح في قانون العقوبات العراقي النافذ رقم ١١١ لسنة ١٩٦٩ المعدل وأحكامه الجزائية، ولكن يمكن وصف بعض الأفعال التي تمثل في حد ذاتها ابتزازًا أو قد تشكل ابتزازًا بأنها جريمة جنائية. فالمشرع العراقي يحاول معالجة مشكلة الابتزاز الالكتروني من خلال تطبيق القوانين التقليدية الخاصة بالجرائم العادية دون وجود نص مستقل يأخذ بعين الاعتبار خصائص البيئة الرقمية. كذألك لا يوجد أي تنظيم قانوني للأدلة الرقمية فيما يتعلق بالتحفظ والفحص والتحليل وفي حالة كان الجاني من دولة والضحية من دولة آخري فهناك نقص في الولاية القضائية وهذا ما أكده المجلس القضائي الأعلى فيما يتعلق بطبيعة الجريمة العابرة للحدود وصعوبة إثباتها نظراً لاختفاء الأدلة الرقمية بسرعة واستخدام الحسابات المزيفة (ابراهيم ، ٢٠٢٢)

ومع ذلك يبقى النص التشريعي الحالي هو الأساس في محاكمة الجناة في جرائم الابتزاز الإلكتروني خاصة المادة ٤٣٠ في حالة كانت التهديدات تتعلق بالشرف أو الكشف عن أسرار مع وجود طلب فلا يزال هذا النص لا يقدم حلاً تشريعياً كاملاً لمشكلة الجرائم الرقمية من هذا النوع وأعتقد أنه يجب على المشرع العراقي التدخل إما من خلال إصدار قانون منفصل عن الجرائم او بتعديل قانون العقوبات العراقي النافذ ليتضمن نص يستوعب طبيعة هذه الجرائم ويعالج فجوتي الادلة الرقمية والاختصاص معا.

الفرع الثاني: موقف المشرع المصري

أصدر المشرع المصري القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، والذي خصص مواد قانونية لجرائم الابتزاز الإلكتروني، ومنها: "يعاقب بالحبس مدة لا تقل عن ستين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم شبكة معلوماتية أو وسيلة من وسائل تقنية المعلومات لتهديد شخص أو ابتزازه" (المادة ٢٥).

مزايا الموقف المصري: وجود نص خاص يجرم الابتزاز الإلكتروني، عقوبات رادعة، تعريف دقيق للجريمة.

الفرع الثالث: موقف المشرع الأردني

أصدر المشرع الأردني القانون رقم ٢٧ لسنة ٢٠١٥ المعدل لقانون العقوبات، والذي تضمن نصوصًا خاصة بجرائم الابتزاز الإلكتروني، ومنها: "يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسمائة دينار ولا تزيد على ثلاثة آلاف دينار كل من هدد آخر بواسطة شبكة معلوماتية أو وسيلة إلكترونية" (المادة ٤١٧ مكرر).

مزايا الموقف الأردني: تجريم صريح للابتزاز الإلكتروني، عقوبات رادعة، التركيز على الوسائل الإلكترونية.

الفرع الرابع: موقف المشرع الإماراتي

أصدر المشرع الإماراتي القانون الاتحادي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات، والذي تضمن نصوصًا خاصة بجرائم الابتزاز الإلكتروني، ومنها: "يعاقب بالحبس مدة لا تقل عن سنتين وبالغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من هدد شخصًا آخر بواسطة شبكة معلوماتية أو وسيلة إلكترونية" (المادة ٢٠).

مزايا الموقف الإماراتي: تجريم صريح وشامل، عقوبات رادعة جدًا، تغطية واسعة للجرائم الإلكترونية.

الفرع الخامس: أوجه القصور التشريعي ومقترحات التعديل

من خلال المقارنة بين الموقف العراقي والمواقف المقارنة، يتضح جليًا وجود قصور تشريعي في القانون العراقي، ونوصي بما يلي:

١. إضافة نص خاص يجرم الابتزاز الإلكتروني في قانون العقوبات العراقي، مع تعريف دقيق للجريمة.

٢. تشديد العقوبات لتكون رادعة، مع مراعاة الظروف المشددة.

٣. الاستفادة من التجارب المقارنة (المصرية، الأردنية، الإماراتية) في صياغة النصوص القانونية.

٤. تطوير آليات التحقيق في الجرائم الإلكترونية، وتدريب الجهات المختصة.

٥. تعزيز التعاون الدولي لمكافحة الجرائم العابرة للحدود.

الخاتمة

تشكل جريمة الابتزاز الإلكتروني المرتكبة بحق النساء تهديدًا حقيقيًا لا يمكن التهاون معه، فآثارها تمتد إلى ما هو أعمق من مجرد ضرر مادي، بل تتعدى إلى خصوصية المرأة وكرامتها وسمعتها التي يسعى المبتز إلى تشويهها واستغلالها بوصفها ورقة ضغط، والنتيجة أثر يمتد لبطال حياتها الاجتماعية والشخصية بل ويستقر أحيانًا في أعمق طبقات الحالة النفسية للضحية.

فمكافحة هذه الجريمة إذن ليست مهمة جهة واحدة بل هي مسؤولية تتوزع بين الحكومات والمنظمات المعنية وأفراد المجتمع على حد سواء. وعلى الحكومات تحديدًا أن تتحرك بجدية أكبر وتشدد التشريعات من جهة، وتطبيقها بصرامة فعلية لا شكلية من جهة أخرى. أما النساء المتضررات فيحتجن إلى جانب ذلك دعمًا قانونيًا ونفسيًا حقيقيًا يمكنهن من الوصول إلى العدالة.

في النهاية، يتطلب مكافحة جريمة الابتزاز الإلكتروني ضد النساء جهودًا مشتركة لتعزيز الوعي وتحقيق التغيير في المجتمع، والعمل معًا لضمان حقوق النساء والحفاظ على سلامتهن وكرامتهن في العالم الرقمي.

أولاً: النتائج

١. ابتزاز النساء هو أكثر أنواع الابتزاز الإلكتروني شيوعًا، مما يضاعف فرصة حصول المبتز على مكاسب من خلال الضغط على الضحية، بينما غالبًا ما تكون ردة فعل الضحايا بدافع الخوف.

٢. الخصائص المميزة للإنترنت تزيد من فرص المجرمين في الإفلات من العقاب، مثل مرونة الهوية، وصعوبة اكتشاف الجرائم الإلكترونية وإثباتها بسبب سهولة تدميرها.

٣. تتعدد وسائل تنفيذ جرائم الابتزاز الإلكتروني وانتهاك الخصوصية، وكلما كانت وسائل الاتصال وتكنولوجيا المعلومات أكثر تقدمًا، كلما كان من الأسهل على المبتز استخدام هذه الوسائل.

٤. وجود قصور تشريعي واضح في القانون العراقي، حيث لا يوجد نص خاص يجرم الابتزاز الإلكتروني، وإنما يتم تكييفه وفق نصوص عامة.

ثانياً: التوصيات

١. إضافة نص خاص يجرم الابتزاز الإلكتروني في قانون العقوبات العراقي، مع تعريف دقيق للجريمة، وتشديد العقوبات لتكون رادعة.

٢. تطوير آليات التحقيق في الجرائم الإلكترونية، وتدريب الجهات المختصة، ومواكبة التطورات التكنولوجية.

٣. الاستفادة من الخبرات والتجارب الدولية والإقليمية في صياغة القوانين المتعلقة بجرائم تقنية المعلومات.

٤. تعزيز دور وسائل الإعلام في نشر الوعي بمخاطر هذه الجريمة وتعريف أفراد المجتمع بأساليب المبتزين وطرق التعامل معهم.

٥. العمل على إضافة دورات متخصصة في التعليم الرقمي لجميع المراحل التعليمية لخلق جيل واعٍ ومتعلم يتقن التكنولوجيا الحديثة.

المراجع

أولاً: المصادر العربية

أولاً: الكتب

١. إبراهيم، خالد ممدوح (٢٠١٩). الجرائم المعلوماتية. دار الفكر الجامعي، الإسكندرية، مصر.

٢. أبو خطوة، أحمد شوقي. شرح الأحكام العامة لقانون العقوبات. دار النهضة العربية، القاهرة، بدون سنة طبع.

٣. ابن منظور، أبي الفضل جمال الدين بن مكرم (١٩٩٣). لسان العرب (ط٣). دار صادر، بيروت، المجلد الثاني عشر.

٤. بهنام، رمسيس (١٩٩٧). النظرية العامة للقانون الجنائي (ط٣). منشأة المعارف، الإسكندرية.

٥. ثروت، جلال (١٩٨٩). شرح قانون العقوبات – القسم العام. الدار الجامعية، بيروت.

٦. جبار، علي. جرائم الحاسوب والإنترنت. دار اليازوري العلمية، عمان، بدون طبعة.

٧. حمادي، خالد عبد الله (٢٠١٩). الاحتيال الإلكتروني – فن اختراق العقول الهندسة الاجتماعية. وزارة الداخلية العراقية، مديرية العلاقات والإعلام.

٨. فايد، محمد (١٩٨٧). المسؤولية الجنائية للطبيب عن إفشاء سر المهنة. دار النهضة العربية، القاهرة.

٩. المولى، عبد الغني جاد (٢٠١٩). دور الدليل الإلكتروني في الإثبات الجنائي. دار الفكر الجامعي، الإسكندرية.

١٠. الفراهيدي، أبو عبد الرحمن الخليل العين. تحقيق مهدي المخزومي وإبراهيم السامرائي. بدون طبعة، دار ومكتبة الهلال، الجزء ٧.

ثانياً: الرسائل والأطاريح

١. حنش، سارة محمد (٢٠٢٠). المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية. رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن.

٢. اللوهية، افراح بنت خميس (٢٠١٨). مشكلة الابتزاز الإلكتروني لدى طلبة مرحلة التعليم ما بعد الأساسي ودور الخدمة الاجتماعية في المجال المدرسي في التعامل معها. رسالة ماجستير، جامعة السلطان قابوس، عمان.

ثالثاً: الدوريات والبحوث

١. إسلامي، رضا (٢٠٢١). الابتزاز الإلكتروني في أنواعه وأسبابه ووسائله وآثاره وعقوبته في الفقه الإمامي والقانون العراقي. مجلة أبحاث ميسان، العدد ٣٤.

٢. زمزمي، إبراهيم بن أحمد (٢٠١٩). الجرائم المعلوماتية – دراسة وفق نظام مكافحة جرائم المعلوماتية السعودي. مجلة جامعة الأندلس للعلوم والتقنية، المجلد ١٠، العدد ٧٥، اليمن.

٣. سعدات، محمود (٢٠١٥). خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية. المملكة العربية السعودية.

٤. عاشور، أميل جبار (٢٠٢٠). المسؤولية القانونية عن جريمة الابتزاز الإلكتروني في مواقع التواصل الاجتماعي – دراسة مقارنة. مجلة أبحاث ميسان، المجلد ١٦، العدد ٣١.

٥. عبد السميع، كمال (٢٠١٨). الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي. دار الجامعة الجديدة، مصر.

٦. العمومطي، ربي أحمد (٢٠٢٣). الشروع في جريمة الابتزاز الإلكتروني. مجلة جامعة تكريت للحقوق، السنة ٧، المجلد ٧، العدد ٣، الجزء ٢.

٧. الغالبي، رامي. جريمة الابتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق. مجلة ثقافتنا الأمنية، الإصدار الثاني، وزارة الداخلية العراقية.

٨. محمد، شريف حسين (٢٠١٧). الجريمة الإلكترونية – معرفة وتقويض الجوانب الخطرة من التكنولوجيا. الاقتصاد والتجارة، مصر.

٩. المقصودي، محمد علي (٢٠١٥). الجرائم المعلوماتية – خصائصها وكيفية مواجهتها قانونيًا. جامعة الإمام محمد بن سعود الإسلامية، السعودية.

١٠. الهادلي، عبد الرضا ناصر (٢٠٢١). آثار الابتزاز الإلكتروني بين الفقه الإمامي والقانون العراقي. مجلة ميسان للدراسات الأكاديمية، العدد ٤١.

١١. اليوسف، عبد الله محمد (٢٠١٥). الجرائم المعلوماتية والدليل الجنائي – مسميات وخصائص وأبعاد اجتماعية وأمنية وصحية. مجلة فكر، العدد ٥، جامعة نايف العربية للعلوم الأمنية، السعودية.

١٢. العنزي، ممدوح رشيد (٢٠١٧). الحماية الجنائية للمجني عليه من الابتزاز. المجلة العربية للدراسات الأمنية، المجلد ٣٣، العدد ٧٠، السعودية.

١٣. أحمد، هديل سعد (٢٠٢٠). جريمة الابتزاز الإلكتروني للنساء، العدد ٢، مجلة جامعة الأنبار للعلوم القانونية والسياسية، العراق.

١٤. الخالدي، عبير نجم (٢٠٢٠). دور الوعي الاجتماعي في مواجهة الابتزاز الإلكتروني للمرأة، المؤتمر العلمي الدولي الثاني، المجلد ٤، العدد ٣٨، نقابة الأكاديميين العراقيين، مجلة جامعة واسط، العراق.

رابعاً: القوانين

١. دستور جمهورية العراق لسنة ٢٠٠٥.

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

٣. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

٤. قانون العقوبات الأردني رقم ٢٧ لسنة ٢٠١٥ المعدل.

٥. القانون الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات.

٦. قانون منع إساءة استخدام الاتصالات الكردستاني رقم ٦ لسنة ٢٠٠٨.

خامساً: المواقع الإلكترونية على الإنترنت

١.موقع مجلس القضاء الأعلى العراقي: https://www.sjc.iq/qanoun/disciplinary

٢. قرار محكمة التمييز الاتحادية، رقم ٩٨٩–٢٠١٤، منشور على الموقع الرسمي لمجلس القضاء الأعلى.

٣. قرار محكمة الجنايات المركزية الثانية، رقم ٢٠١٨/٩/٤/٢/٣٨٥٣ غير منشور.

٤. إبراهيم، حمادة حبيب (٢٠٢٢). التكييف القانوني لجريمة الابتزاز الإلكتروني في التشريع العراقي، مجلس القضاء الأعلى العراقي. https://www.sjc.iq/view.69769/

ثانياً: المصادر الأجنبية

United Nations, Office on Drugs and Crime Prevention (2007). Compendium of United Nations Standards and Norms in Crime Prevention and Criminal Justice. New York.

Al-Ghalibi, Rami. The Crime of Electronic Blackmail and the Mechanism for Combating it in the Republic of Iraq. Our Security Culture Magazine, Second Edition, Iraqi Ministry of Interior.