

جريمة الابتزاز والتهديد عبر وسائل التواصل الاجتماعي في ضوء نظام مكافحة جرائم المعلوماتية السعودي

شذى حامد عمر محمد *

كليات بريدة الأهلية-المملكة العربية السعودية

0009-0003-8380-9832 

محمد عبود حامد

جامعة الزعيم الازهري-السودان

0009-0008-1756-2161 

تاريخ النشر 2026-03-01

تاريخ القبول 2026-02-03

تاريخ الاستلام 2025-07-04

الملخص:

تناقش هذه الورقة البحثية جريمة الابتزاز والتهديد عبر وسائل التواصل الاجتماعي، باعتبارها ظاهرة إجرامية مركبة تجمع بين سلوك تقليدي وبيئة رقمية متطورة. يهدف البحث إلى تحليل أبعاد الجريمة من خلال ثلاثة محاور رئيسية: الإطار المفاهيمي، والتنظيم القانوني، والمواجهة الشاملة. اعتمد البحث على منهج وصفي تحليلي لفهم ماهية الجريمة وخصائصها، ومنهج قانوني تحليلي لتفكيك نصوص نظام مكافحة جرائم المعلوماتية السعودي، ومنهج مقارنة للاستفادة من التشريعات العربية والدولية. تُظهر النتائج أن الابتزاز الإلكتروني جريمة "متحورة" تضاعف وسائل التواصل الاجتماعي من خطورتها عبر خصائص مثل إخفاء الهوية وسرعة الانتشار. كما تبين أن الإطار التشريعي السعودي يوفر أساساً قوياً للملاحقة، لكن تبقى هناك تحديات عملية في الإثبات وتتبع الجناة عابري الحدود. وأكد البحث على عمق الآثار النفسية والاجتماعية على الضحايا، مما يجعل الوقاية والتوعية خط الدفاع الأول. ويوصي البحث بتحديث التشريعات لمواكبة التقنيات المستجدة كالتيهيف العميق، وتعزيز التعاون الدولي، وتكثيف التدريب المتخصص للجهات القضائية والأمنية، وإطلاق حملات توعوية شاملة، وتوفير برامج دعم متكاملة للضحايا.

الكلمات المفتاحية: الابتزاز الإلكتروني، وسائل التواصل الاجتماعي، نظام مكافحة جرائم المعلوماتية، الأمن السيبراني، ضحايا الجرائم الإلكترونية.

* المؤلف المراسل.

The Crime of Extortion and Threatening via Social Media in Light of the Saudi Anti-Cyber Crime Law

Abstract:

This research paper discusses the crime of extortion and threats via social media, treating it as a complex criminal phenomenon that combines traditional behavior with a sophisticated digital environment. The research aims to analyze the dimensions of this crime through three main axes: the conceptual framework, the legal regulation, and the comprehensive confrontation. The study employs a descriptive-analytical methodology to understand the nature and characteristics of the crime, a legal-analytical approach to deconstruct the provisions of the Saudi Anti-Cybercrime Law, and a comparative method to draw insights from Arab and international legislation. The findings indicate that electronic extortion is a "mutated" crime, with social media platforms amplifying its severity through features like anonymity and virality. The Saudi legislative framework provides a solid basis for prosecution, yet practical challenges remain in evidence and tracking transnational perpetrators. The research emphasizes the profound psychological and social impacts on victims, positioning prevention and awareness as the first line of defense. The paper recommends updating legislation to address emerging technologies like deep fakes, enhancing international cooperation, intensifying specialized training for judicial and security authorities, launching comprehensive awareness campaigns, and providing integrated support programs for victims.

Keywords: *Electronic Extortion, social media, Anti-Cybercrime Law, Cyber security, Cybercrime Victims.*

مقدمة:

لقد أحدثت الثورة الرقمية، التي تتجسد أبرز ملامحها في انتشار وسائل التواصل الاجتماعي، تحولاً جذرياً في بنية المجتمعات الإنسانية وأساليب تفاعلها. فقد أزالته هذه المنصات الرقمية الحواجز الجغرافية، ومكنت الأفراد من إنشاء شبكات واسعة من العلاقات،

وتبادل الأفكار والمعلومات والتجارب بسهولة وسرعة لم يسبق لهما مثيل.¹ وعلى الرغم من الفوائد الجمة التي قدمتها هذه الوسائل في مجالات التعليم والتجارة والتواصل الإنساني، إلا أنها في الوقت ذاته فتحت الباب على مصراعيه لظهور أنماط جديدة من السلوكيات الإجرامية، التي وجدت في البيئة الرقمية مرتعاً خصباً للنمو والانتشار.²

تتمحور إشكالية هذا البحث حول الطبيعة المعقدة لواحدة من أخطر هذه الجرائم، وهي "جريمة الابتزاز والتهديد عبر وسائل التواصل الاجتماعي". تجمع هذه الجريمة بين فعل إجرامي تقليدي في جوهره، وهو الابتزاز القائم على التهديد والإكراه، ووسيلة تنفيذ حديثة ومتطورة، هي منصات التواصل الاجتماعي، مما يطرح تحديات مفاهيمية وقانونية وإجرائية فريدة. وعليه، يسعى هذا البحث إلى الإجابة عن تساؤلات جوهرية، أبرزها: ما هي ماهية جريمة الابتزاز الإلكتروني وخصائصها التي تميزها عن شكلها التقليدي؟ وكيف واجه المنظم السعودي هذه الظاهرة المستجدة في إطار "نظام مكافحة جرائم المعلوماتية"؟ وما هي أركانها القانونية وعقوباتها المقررة؟ وما هي التحديات التي تواجه إثباتها وملاحقة مرتكبيها؟ وأخيراً، ما هي الآثار المترتبة على الضحايا، وما هي سبل المواجهة الشاملة على المستويات الوقائية والعلاجية والدولية؟

للإجابة على هذه التساؤلات، سيتبع البحث منهجاً متكاملًا؛ حيث سيتم استخدام المنهج الوصفي التحليلي في استعراض المفاهيم والخصائص المتعلقة بالجريمة وبيئتها الرقمية. كما سيتم الاعتماد على المنهج القانوني التحليلي في تفكيك وتفسير النصوص النظامية ذات الصلة، وتحديدًا نظام مكافحة جرائم المعلوماتية السعودي. وأخيراً، سيوظف البحث المنهج المقارن من خلال عقد مقارنات مع بعض التشريعات العربية والدولية لإثراء التحليل وتقديم رؤية أوسع.

تنقسم خطة البحث إلى ثلاثة مباحث رئيسية، يليها خاتمة تتضمن أهم النتائج والتوصيات. يتناول المبحث الأول الإطار المفاهيمي للجريمة، من خلال تعريفها وتحديد خصائص البيئة الرقمية التي ترتكب فيها، وتصنيف صورها وأساليبها المتعددة. ويخصص

¹ - "تعريف وسائل التواصل الاجتماعي"، موسوعة الجزيرة، 7 مارس 2023؛ و"تعريف مواقع التواصل الاجتماعي"، شركة أفكار للبرمجيات وتقنية المعلومات، (تم الوصول إليه في 2 يوليو 2025).

² - أسباب الابتزاز الإلكتروني والآثار الاجتماعية والنفسية المرتبطة به: دراسة كيفية"، المجلة العربية للعلوم الإنسانية والاجتماعية، (2023).

المبحث الثاني لدراسة التنظيم القانوني للجريمة في النظام السعودي، حيث يتم تحليل أركانها المادية والمعنوية والشرعية، والعقوبات المقررة لها، وخصوصية إجراءات الإثبات والملاحقة. أما المبحث الثالث، فيتوسع في نطاق المواجهة ليتناول الآثار النفسية والاجتماعية على الضحايا، وآليات الوقاية ودعمهم، ويسلط الضوء على الجهود الدولية والمقارنة في هذا المجال.

المبحث الأول: الإطار المفاهيمي لجريمة الابتزاز عبر وسائل التواصل الاجتماعي

يهدف هذا المبحث إلى تأسيس قاعدة معرفية متينة لفهم أبعاد جريمة الابتزاز الإلكتروني، وذلك من خلال تفكيك مصطلحاتها الأساسية، وتحليل خصائص البيئة الرقمية التي أفرزتها، وتصنيف صورها وأساليبها المتنوعة التي تتطور باستمرار مع تطور التكنولوجيا.

المطلب الأول: ماهية جريمة الابتزاز والتهديد الإلكتروني

لفهم جريمة الابتزاز الإلكتروني، لا بد من الرجوع أولاً إلى مفهومها التقليدي. فالابتزاز لغةً واصطلاحاً هو فعل يهدف إلى الحصول على مكاسب، سواء كانت مادية أو معنوية، من شخص آخر عن طريق الإكراه المعنوي والتهديد بإفشاء أسرار أو معلومات خاصة أو نسب أمور مخلة بالشرف إليه.¹ ومع انتقال هذا السلوك إلى الفضاء الرقمي، اكتسب المصطلح بعداً جديداً، ليُعرف الابتزاز الإلكتروني بأنه "استخدام الوسائل التقنية الحديثة مثل الإنترنت أو الأجهزة الإلكترونية للضغط على آخرين بهدف الحصول على منفعة غير مشروعة".²

من هنا، يمكن القول إن جريمة الابتزاز الإلكتروني ليست جريمة مستحدثة بالكامل، بل هي "جريمة متحورة" (Mutated Crime). فالجوهر الإجرامي واحد، وهو التهديد لحمل شخص على فعل شيء ضد إرادته، لكن ما تغير هو الوسيلة التي أصبحت تتم عبر فضاء رقمي يتمتع بخصائص فريدة تعمل "كمسرعات ومضاعفات" لخطورتها.³ ولزيادة دقة المفهوم، يجب تمييز الابتزاز الإلكتروني عن جرائم أخرى قد تتشابه معه كالتهشير الذي يهدف لمجرد الإساءة،

1- "التشريعات السعودية في مكافحة الابتزاز"، موقع المحامي، (تم الوصول إليه في 2 يوليو 2025)؛ و"تعريف الابتزاز"، موقع أمر أجواء للاستشارات، (2023).

2- "عقوبة الابتزاز الإلكتروني في السعودية"، مكتب إتيقان المتميز للمحاماة، (تم الوصول إليه في 2 يوليو 2025).

3- "الجوانب النفسية في الابتزاز الإلكتروني"، موقع ريسيرش جيت، (2019)؛ و"من تهديدات افتراضية إلى تبعات واقعية"، موقع مسار، (تم الوصول إليه في 2 يوليو 2025).

أو القرصنة التي قد تكون مرحلة تمهيدية له، أو الاحتيال القائم على الخداع لا التهديد الصريح.¹

المطلب الثاني: خصائص وسائل التواصل الاجتماعي كبيئة لارتكاب الجريمة

إن فهم سبب انتشار الابتزاز عبر منصات مثل فيسبوك، وإنستغرام، وتيك توك، وتويتر، يتطلب تحليل الخصائص البنيوية لهذه المنصات التي تجعلها مسرحاً مثالياً لمثل هذه الجرائم:

- التفاعلية والوصول العالمي: تتيح هذه المنصات للمستخدمين التواصل الفوري والمباشر مع أي شخص في أي مكان في العالم، مما يكسر الحواجز المادية ويوسع دائرة الضحايا المحتملين بشكل غير محدود.
- المحتوى الذي ينشئه المستخدم (UGC): صُممت هذه المنصات لتشجيع المستخدمين على مشاركة تفاصيل حياتهم اليومية، مما يوفر للجنة مادة وفيرة يمكن استخدامها لاحقاً في الابتزاز.
- إمكانية إخفاء الهوية (Anonymity): من السهل جداً إنشاء حسابات وهمية بأسماء وصور مزيفة، مما يمنح الجاني "لثاماً إلكترونياً" يخفي هويته الحقيقية، ويعقد بشكل كبير مهمة تتبعه.
- سرعة الانتشار (Virality): إن التهديد بنشر محتوى حساس يصبح أكثر رعباً وتأثيراً بسبب إمكانية انتشار هذا المحتوى كالنار في الهشيم في غضون دقائق معدودة.²
- تتجاوز المسألة مجرد الخصائص التقنية، لتصل إلى وجود علاقة سببية مباشرة بين تصميم هذه المنصات وزيادة معدلات الابتزاز. فهذه المنصات، بحكم نموذج عملها القائم على

1- "أحكام قضايا الابتزاز في القانون السعودي 2024"، مكتب أيوب القرني للمحاماة، 4 مايو 2024؛ و"أنواع الابتزاز الإلكتروني في دبي"، مكتب محامي دبي، (تم الوصول إليه في 2 يوليو 2025).

2- "ما هي خصائص السوشيال ميديا الرئيسية؟"، موقع غنائم، (تم الوصول إليه في 2 يوليو 2025)؛ و"خصائص مواقع التواصل الاجتماعي"، موقع نور بوك، (تم الوصول إليه في 2 يوليو 2025).

زيادة التفاعل، تشجع المستخدمين بشكل ممنهج على ما يمكن تسميته "بالمشاركة المفرطة" (Oversharing)، مما يقلل من إدراكهم للمخاطر ويجعلهم أكثر عرضة للاستغلال.¹

المطلب الثالث: صور وأساليب الابتزاز الإلكتروني

يتخذ الابتزاز الإلكتروني أشكالاً وأساليب متعددة، يمكن تصنيفها بناءً على دافع الجاني أو الطريقة التي يتبعها. فمن حيث الدافع، يوجد الابتزاز المادي وهو الأكثر شيوعاً، والابتزاز الجنسي وهو الأخطر تأثيراً، بالإضافة إلى الابتزاز العاطفي والاجتماعي والوظيفي.² وتظهر بعض الإحصائيات أن المطالب الجنسية تشكل نسبة كبيرة من دوافع المبتزين، حيث قدرت إحدى الدراسات أن 74% من مطالبيهم كانت ذات طبيعة جنسية.³

أما من حيث الأسلوب الإجرامي، فتتنوع الطرق بين الهندسة الاجتماعية وبناء علاقات ثقة وهمية، والتصدي الاحتمالي لسرقة بيانات الدخول، والبرمجيات الخبيثة للسيطرة على الأجهزة، واستغلال الحسابات المخترقة، وصولاً إلى الأسلوب الأكثر تطوراً وخطورة وهو التزييف العميق (Deep fakes)، الذي يستخدم الذكاء الاصطناعي لتركيب وجه الضحية على محتوى مسيء بشكل مقنع للغاية.⁴

المبحث الثاني: التنظيم القانوني لجريمة الابتزاز الإلكتروني في النظام السعودي

أدرك المنظم السعودي خطورة الجرائم الناشئة في الفضاء الرقمي، وسارع إلى وضع إطار تشريعي متخصص لمواجهتها. ويُعد "نظام مكافحة جرائم المعلوماتية"، الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ⁵، هو الركيزة الأساسية في التجريم والعقاب.

1- "الابتزاز الإلكتروني: دليل شامل"، برنامج غزة للصحة النفسية، (د.ت.)، ص.3.

2- "أهم أنواع الابتزاز الإلكتروني"، شركة بصمة أمان، (تم الوصول إليه في 2 يوليو 2025)؛ و "أنواع الابتزاز الإلكتروني في السعودية"، مكتب الصفوة للمحاماة، (تم الوصول إليه في 2 يوليو 2025).

3- العتيبي، ماجد سعيد، "دور الأنظمة في الحد من جريمة الابتزاز الإلكتروني في النظام السعودي"، المجلة العربية للدراسات الأمنية، (2025)، نقلاً عن كتيب هيئة الأمر بالمعروف والنهي عن المنكر. (2019)

4- "كيف يتم الابتزاز الإلكتروني؟"، موقع اليوم السابع، (تم الوصول إليه في 2 يوليو 2025)؛ و "طرق الابتزاز الإلكتروني"، شركة بصمة أمان، (تم الوصول إليه في 2 يوليو 2025).

5- المملكة العربية السعودية، نظام مكافحة جرائم المعلوماتية، الصادر بقرار مجلس الوزراء رقم 79 بتاريخ 1428/3/7هـ.

المطلب الأول: الأركان المكونة لجريمة الابتزاز الإلكتروني

لا تقوم جريمة الابتزاز الإلكتروني في النظام السعودي إلا بتوافر ثلاثة أركان متكاملة:

- **الركن المادي:** وهو السلوك الخارجي الملموس، ويتكون من فعل التهديد الجدي، واستخدام وسيلة إلكترونية، ووجود طلب غير مشروع يهدف إلى حمل الضحية على القيام بفعل أو الامتناع عنه.¹
- **الركن المعنوي:** وهو النية الإجرامية، ويتطلب توافر القصد الجنائي العام (العلم والإرادة) والقصد الجنائي الخاص (نية إجبار المجني عليه على الاستجابة للطلب).²
- **الركن الشرعي (القانوني):** وهو النص النظامي الذي يجرم الفعل، ويتمثل بشكل أساسي في الفقرة الثانية من المادة الثالثة من نظام مكافحة جرائم المعلوماتية السعودي.³

المطلب الثاني: العقوبات المقررة في نظام مكافحة جرائم المعلوماتية

تنص المادة الثالثة من النظام على أن عقوبة الابتزاز الإلكتروني هي "السجن لمدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين".⁴ وتكمن الخطورة الحقيقية والتشديد العقابي عندما تكون المادة المستخدمة في الابتزاز تمس الآداب العامة أو القيم الدينية، حيث يقع الفعل تحت طائلة المادة السادسة من النظام، التي تفرض

1- "تعريف جريمة الابتزاز الإلكتروني"، مجلة كلية القانون، جامعة ذي قار، (2022)، ص. 5؛ و "أركان جريمة

الابتزاز الإلكتروني"، مكتب المحامي د. حسن الدراجي، (تم الوصول إليه في 2 يوليو 2025).

2- "أركان جريمة الابتزاز في النظام السعودي"، مكتب المحامي سند بن محمد الجعيد، (تم الوصول إليه في 2 يوليو 2025)؛ و "أركان جريمة الابتزاز الإلكتروني"، شركة بصمة أمان، (تم الوصول إليه في 2 يوليو 2025).

3- الفوزان، أحلام بنت عبد الله، "المسؤولية الجزائية عن جريمة الابتزاز الإلكتروني في النظام السعودي"، رسالة جامعية، جامعة الملك سعود، (2021).

4- "شرح المادة 3 من نظام الجرائم المعلوماتية في السعودية"، مكتب محاماة الدمام، (تم الوصول إليه في 2 يوليو 2025)؛ والعجيل، منصور عبد السلام، "جريمة الابتزاز الإلكتروني: دراسة مقارنة"، المجلة القانونية، (يوليو 2024).

عقوبة أشد تصل إلى "السجن مدة لا تتجاوز خمس سنوات وبغرامة لا تتجاوز ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين".¹

إلى جانب العقوبات الأصلية، منح النظام القاضي سلطة جوازية لفرض عقوبات إضافية بموجب المادة الثالثة عشرة، تشمل مصادرة الأجهزة والأموال، وإغلاق المكان، ونشر ملخص الحكم.² كما يُشدد النظام العقوبة في حالاتٍ معيّنة، لاسيما إذا ارتكبت الجريمة في إطار عصابةٍ منظّمة، أو من قِبل موظفٍ عام، أو إذا كان المجني عليه قاصراً.³

المطلب الثالث: خصوصية الإثبات وإجراءات الملاحقة القضائية

يعتمد الإثبات في جريمة الابتزاز بشكل كلي على "الأدلة الرقمية"، التي تشمل الرسائل والمحادثات والتسجيلات ولقطات الشاشة وعناوين بروتوكول الإنترنت (IP Address).⁴ إلا أن إثبات الجريمة يواجه تحديات كبيرة، منها صعوبة تتبع الجناة الذين يستخدمون أدوات لإخفاء الهوية، وقابلية الدليل الرقمي للتلف أو التعديل، والأهم من ذلك، إحجام الكثير من الضحايا عن الإبلاغ خوفاً من الفضيحة.⁵

إدراكاً لهذا "الحاجز النفسي"، أنشأت السلطات السعودية منظومة متكاملة لتسهيل الإبلاغ بسرية تامة، تشمل الرقم الموحد (1909)، وتطبيق "كلنا أمن"، ومنصة "أبشر"، ومراكز الشرطة، بالإضافة إلى الدور المميز الذي تلعبه هيئة الأمر بالمعروف والنهي عن المنكر في استقبال البلاغات وتقديم الدعم والإرشاد.⁶

1- "نظام مكافحة جرائم المعلوماتية"، مكتب إتقان المتميز للمحاماة، (تم الوصول إليه في 2 يوليو 2025)؛

والمادة السادسة من نظام مكافحة جرائم المعلوماتية السعودي.

2- "أنواع الجرائم المعلوماتية"، مكتب المحامي محمد المنيع، (تم الوصول إليه في 2 يوليو 2025)، نقلاً عن المادة 13 من النظام.

3- العجيل، منصور عبد السلام، "جريمة الابتزاز الإلكتروني: دراسة مقارنة"، المجلة القانونية، يوليو. (2024).

4- انظر: "أركان جريمة الابتزاز الإلكتروني"، مكتب المحامي د. حسن الدراجي، (تم الوصول إليه في 2 يوليو 2025)؛ و "كيف تثبت قضية الابتزاز؟"، مكتب المحامي علي المهلكي، (تم الوصول إليه في 2 يوليو. 2024)

5- العجيل، منصور عبد السلام، "جريمة الابتزاز الإلكتروني: دراسة مقارنة"، المجلة القانونية، (يوليو 2024)؛ و "الحماية القانونية من جرائم الابتزاز الإلكتروني"، مجلة العلوم القانونية والاجتماعية، (2024)

6- "رقم مكافحة الابتزاز في السعودية"، مكتب غازي للمحاماة، (تم الوصول إليه في 2 يوليو 2025)؛ و "طريقة تبليغ عن الابتزاز"، شركة بصمة أمان، (تم الوصول إليه في 2 يوليو. 2025)

المبحث الثالث: المواجهة الشاملة للابتزاز الإلكتروني: الآثار والوقاية والتعاون الدولي

لا تقتصر مواجهة جريمة الابتزاز الإلكتروني على الجانب القانوني فحسب، بل تتطلب رؤية شاملة تتناول أبعادها الإنسانية والوقائية والدولية.

المطلب الأول: الآثار النفسية والاجتماعية المترتبة على الضحايا

إن الضرر الحقيقي لجريمة الابتزاز الإلكتروني يتجاوز أي خسارة مادية، حيث يستهدف كرامة الضحية وأمنها النفسي. وتشمل الآثار النفسية اضطرابات القلق والاكتئاب، وفقدان الثقة بالنفس وبالأخرين، والشعور بالذنب والخجل، وقد تصل في الحالات القصوى إلى التفكير في الانتحار. أما الآثار الاجتماعية فتتمثل في العزلة الاجتماعية، والتفكك الأسري، والإضرار بالسمعة المهنية والدراسية.¹ وتكون فئات النساء والمراهقين أكثر عرضة لهذه الآثار المدمرة نظراً للضغوط الاجتماعية وقلة الخبرة.²

المطلب الثاني: آليات الوقاية وسبل دعم الضحايا

تظل أبسط الإجراءات الوقائية، المتمثلة في السلوك الفردي الحذر أو ما يعرف بـ "النظافة الرقمية"، هي خط الدفاع الأول. وتشمل تأمين الحسابات بكلمات مرور قوية وتفعيل المصادقة الثنائية، وإدارة إعدادات الخصوصية، والحذر في التفاعل والمشاركة، واستخدام برامج الحماية.³ وعلى المستوى المؤسسي والمجتمعي، يبرز دور الجهات الحكومية في التوعية،

1- "الآثار النفسية للابتزاز الإلكتروني"، موقع ريسيرش جيت، (2024): و "الآثار النفسية للابتزاز الإلكتروني على الضحايا"، موقع الإمارات اليوم، 9 نوفمبر 2024.

2- "الابتزاز الإلكتروني: دليل شامل"، برنامج غزة للصحة النفسية، (د.ت.): والعتيبي، ماجد سعيد، "دور الأنظمة في الحد من جريمة الابتزاز الإلكتروني في النظام السعودي"، المجلة العربية للدراسات الأمنية، (2025).

3- "طرق الوقاية من الابتزاز الإلكتروني"، موقع سببك أب، 1 يونيو 2024؛ و "الابتزاز الإلكتروني في 2025: المخاطر، الأسباب، وطرق الحماية"، موقع تقنين، (تم الوصول إليه في 2 يوليو 2025).

ودور هيئة الأمر بالمعروف والنهي عن المنكر في الدعم، ومسؤولية منصات التواصل الاجتماعي في تطوير سياسات أكثر صرامة.¹

أما عند وقوع الجريمة، فالنصيحة الأساسية هي عدم الاستجابة لمطالب المبتز إطلاقاً، وقطع التواصل معه، وحفظ جميع الأدلة، مع ضرورة توفير دعم نفسي وقانوني متخصص للضحية.²

المطلب الثالث: الجهود الدولية والمقارنة في مكافحة الجريمة

إن الطبيعة العالمية للإنترنت تجعل من جريمة الابتزاز "جريمة عابرة للحدود"، مما يؤكد أن المواجهة الوطنية تظل "محدودة الأثر" دون تعاون دولي فعال.³ وتُعد "اتفاقية بودابست للجرائم الإلكترونية (2001)" أو لمعاهدة دولية شاملة في هذا المجال، كما يلعب الإنترنت دوراً حيوياً في تسهيل التعاون الشرطي الدولي.⁴ ومؤخراً، في ديسمبر 2024، اعتمدت الجمعية العامة للأمم المتحدة اتفاقية جديدة لمكافحة الجريمة السيبرانية، مما يمثل خطوة تاريخية لتعزيز التعاون الدولي.⁵

وبمقارنة التشريعات العربية، نجد أن القانون الإماراتي والمصري والأردني يتفقون مع النظام السعودي في تجريم الفعل، مع وجود تباينات في شدة العقوبات وتفاصيل التجريم، مما يعكس الاهتمام الإقليمي المتزايد بمواجهة هذه الظاهرة.

1- "جرائم الابتزاز الإلكتروني عبر وسائل التواصل الاجتماعي"، مكتب مصالحة للمحاماة، (تم الوصول إليه في 2 يوليو 2025).

2 يوليو 2025)؛ و "طريقة تبليغ عن الابتزاز"، شركة بصمة أمان، (تم الوصول إليه في 2 يوليو 2025).
2- "أهم 3 طرق لمحاربة الابتزاز الإلكتروني"، شركة بصمة أمان، (تم الوصول إليه في 2 يوليو 2025)؛ و "الأثار النفسية للابتزاز الإلكتروني"، موقع ريسيرش جيت، (2024).

3- العجيل، منصور عبد السلام، "جريمة الابتزاز الإلكتروني: دراسة مقارنة"، المجلة القانونية، (يوليو 2024).

4- "اتفاقية بشأن جرائم الفضاء الإلكتروني"، مجلس أوروبا، 23 نوفمبر 2001؛ و "خدمات التعاون في مجال مكافحة الجريمة السيبرانية"، الإنترنت، (تم الوصول إليه في 2 يوليو 2025).

5- الجمعية العامة للأمم المتحدة تعتمد اتفاقية تاريخية لمكافحة الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 25 ديسمبر 2024.

خاتمة

في ختام هذا البحث، الذي سعى إلى تفكيك أبعاد جريمة الابتزاز والتهديد عبر وسائل التواصل الاجتماعي، يمكن استخلاص مجموعة من النتائج وتقديم عدد من التوصيات التي نأمل أن تساهم في تعزيز جهود المواجهة لهذه الظاهرة المعقدة.

أولاً: النتائج

1. طبيعة الجريمة المركبة: توصل البحث إلى أن الابتزاز الإلكتروني ليس مجرد جريمة تقنية، بل هو ظاهرة "اجتماعية-تقنية-قانونية" مركبة. فهو يجمع بين سلوك إجرامي تقليدي (التهديد) وبيئة رقمية (وسائل التواصل الاجتماعي) تضاعف من خطورته وتسهل انتشاره، مما يجعل مواجهته تتطلب استراتيجيات متعددة الأبعاد تتجاوز الحلول القانونية الصرفة.
2. فعالية الإطار التشريعي السعودي: أظهر التحليل أن الإطار القانوني السعودي، ممثلاً في نظام مكافحة جرائم المعلوماتية، يوفر أساساً تشريعياً صلباً لملاحقة الجناة. وتكمن قوته في سياسة "التجريم الواسع والمرونة العقابية"، التي تمنح القضاء سلطة تقديرية واسعة لتكييف الوقائع وتطبيق العقوبة الأشد عند اقتران الابتزاز بجرائم أخرى كالتمسك بالآداب العامة.
3. تحديات الإثبات والملاحقة: على الرغم من قوة النصوص النظامية، لا تزال هناك تحديات عملية كبيرة في مرحلة الإثبات، خاصة فيما يتعلق بإثبات القصد الجنائي، وصعوبة تتبع الجناة الذين يستخدمون أدوات لإخفاء الهوية أو يعملون من خارج الحدود الإقليمية، مما يجعل التعاون الدولي ضرورة حتمية وليست خياراً.
4. عمق الضرر النفسي والاجتماعي: أكد البحث أن الآثار النفسية والاجتماعية للجريمة لا تقل خطورة عن أي ضرر مادي، بل قد تفوقه. فالجريمة لا تستهدف مال الضحية فحسب، بل تستهدف كرامته وأمنه النفسي وعلاقاته الاجتماعية، مما قد يؤدي إلى العزلة والاكتئاب، ويهدد النسيج الاجتماعي ككل من خلال تقويض الثقة في الفضاء الرقمي.

5. أهمية الوقاية وبناء الوعي: تبين أن خط الدفاع الأول والأكثر فعالية في مواجهة الابتزاز يكمن في الوقاية وبناء الوعي لدى المستخدمين. فالسلوكيات الفردية الحذرة، أو ما يعرف بـ "النظافة الرقمية"، تظل هي الحصن الأقوى لمنع وقوع الجريمة من الأساس.

ثانياً: التوصيات

بناءً على النتائج المستخلصة، يقدم البحث التوصيات التالية:

أ. توصيات تشريعية:

1. إلى المنظم السعودي: يُقترح النظر في إضافة نص خاص في نظام مكافحة جرائم المعلوماتية لتشديد العقوبة بشكل صريح في حالات الابتزاز التي تستخدم تقنيات التزييف العميق (Deepfakes)، نظراً لخطورتها وقدرتها الفائقة على التضليل. كما يوصى بوضع إطار إجرائي واضح للتعامل مع الأدلة الرقمية المفبركة في مراحل التحقيق والمحكمة.
2. على المستوى الإقليمي والدولي: دعوة الدول العربية التي لم تنضم بعد إلى اتفاقية بودابست للجرائم الإلكترونية إلى دراسة الانضمام إليها للاستفادة من آليات التعاون الدولي التي توفرها. وكبديل، العمل على إبرام اتفاقيات ثنائية وإقليمية فعالة لتسهيل إجراءات تسليم المجرمين وتبادل الأدلة الإلكترونية بشكل سريع وآمن.

ب. توصيات قضائية وأمنية:

1. التدريب والتأهيل: عقد دورات تدريبية متخصصة ومستمرة للقضاة وأعضاء النيابة العامة ورجال الضبط الجنائي، تركز على الطبيعة الفنية للأدلة الرقمية، وأحدث أساليب التحقيق في الجرائم السيبرانية، وكيفية التعامل مع التحديات التي يفرضها الفضاء الرقمي.
2. تعزيز التعاون المؤسسي: إنشاء آليات تنسيق أكثر فاعلية بين وحدات مكافحة الجرائم الإلكترونية، وهيئات الاتصالات وتقنية المعلومات، والشركات المالكة لمنصات التواصل الاجتماعي، بهدف تسريع عمليات تحديد هوية الجناة، وحذف المحتوى الضار،

والاستجابة لطلبات السلطات القضائية.

ج. توصيات مجتمعية وتوعوية:

1. الحملات التوعوية: إطلاق حملات توعية وطنية مكثفة ومستمرة، تستخدم لغة بسيطة ومباشرة، وتستهدف بشكل خاص فئات الشباب والمراهقين وأولياء الأمور. يجب أن تركز هذه الحملات على السلوكيات الوقائية، وكيفية التعرف على محاولات الابتزاز، وأهمية وسبل الإبلاغ الفوري.
2. برامج الدعم المتكامل: تطوير وتوفير برامج دعم نفسي وقانوني متكاملة ومتاحة بسهولة لضحايا الابتزاز، يتم تقديمها من خلال منصات سرية وموثوقة تضمن الحفاظ التام على خصوصية الضحايا وتشجعهم على طلب المساعدة دون خوف من الوصمة الاجتماعية.