مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية
Bani Waleed University Journal of Humanities and Applied Sciences
تصدر عن– جامعة بني وليد – ليبيا
Website:https://jhas-bwu.com/index.php/bwjhas/index
ISSN 3005-3900 الصفحات (331 -350) المجلد الحادي عشر – العدد الأول – 2026

The substantive provisions of the crime of electronic extortion in libyan criminal law

Taher Ahmed Abu Ashiba [1]* , Abdulaziz Muftah AlGhafoud [2]
[1] Department of Criminal Law, Faculty of Law - Tarhuna, Al-Zaytuna University, Tarhuna, Libya.
[2] Department of Sharia and Law, Faculty of Sharia and Law, Al-Asmariya Islamic University, Zliten, Libya.
abd.alghafoud@asmarya.edu.ly

الأحكام الموضوعية لجريمة الابتزاز الإلكتروني في التشريع الجنائي الليبي

أ.طاهر أحمد أبو عشيبة [1] *، أ.عبدالعزيز مفتاح الغافود [2]
[1] قسم القانون الجنائي، كلية القانون- ترهونة، جامعة الزيتونة، ترهونة، ليبيا .
[2] قسم الشريعة والقانون، كلية الشريعة والقانون، الجامعة الأسمرية الإسلامية، زليتن، ليبيا.

Received: 20-12-2025	Accepted: 19-01-2026	Published: 25-01-2026
Copyright: © 2026 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

الملخص :
يتناول هذا البحث الأحكام الموضوعية لجريمة الابتزاز الإلكتروني في التشريع الجنائي الليبي، من خلال دراسة شاملة لماهيتها وأركانها والعقوبات المقررة لها. يركز البحث على تحليل النصوص القانونية الموجودة في قانون العقوبات الليبي، وتحديداً المادتين 429 و430، اللتين تشكلان الأساس القانوني الوحيد لتجريم هذه الجريمة في غياب نصوص متخصصة في قانون مكافحة الجرائم الإلكترونية. يناقش البحث الأركان الثلاثة للجريمة: الركن الشرعي (مبدأ الشرعية)، والركن المادي (السلوك الإجرامي المتمثل في التهديد والإرغام)، والركن المعنوي (القصد الجنائي). كما يتناول البحث العقوبات المقررة للجريمة في صورتها التامة وفي حالة الشروع فيها، وأحكام المساهمة الجنائية (الفاعل الأصلي والشريك). ينتهي البحث بتقديم نتائج وتوصيات تهدف إلى تحسين الإطار القانوني لمواجهة هذه الجريمة الخطيرة والمتنامية، بما في ذلك تشديد العقوبات وإصدار نصوص متخصصة وتطوير آليات التحقيق والإثبات.

الكلمات الدالة: الابتزاز،الإجرام، الإلكترونية، التجريم، التشريع.

Abstract:
This research examines the substantive provisions of the crime of electronic extortion under Libyan criminal law, through a comprehensive study of its nature, elements, and prescribed penalties. The research focuses on analyzing the legal texts contained in the Libyan Penal Code, specifically Articles 429 and 430, which constitute the sole legal basis for criminalizing this offense in the absence of specialized provisions in the Law to Combat Cybercrime. The research discusses the three elements of the crime: the legal element (principle of legality), the material element (criminal conduct consisting of threats and coercion), and the mental element (criminal intent). The research also addresses the penalties prescribed for the crime in its completed form

and in cases of attempt, as well as the provisions on criminal participation (principal perpetrator and accomplice). The research concludes by presenting findings and recommendations aimed at improving the legal framework for combating this serious and growing crime, including strengthening penalties, enacting specialized provisions, and developing investigation and proof mechanisms.

Keywords: Extortion, crime, cybercrime, criminalization, legal.

المقدمة

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وعلى آله وأصحابه أجمعين، وبعد

في خضم الثورة المذهلة التي يشهدها العالم في مجال التكنولوجيا والاتصالات، ومع تزايد الاعتماد على الفضاء السيبراني في كافة مناحي الحياة، برزت أنماط إجرامية مستحدثة لم تكن معهودة في السابق، مستغلةً الطبيعة الخاصة للبيئة الرقمية، وتأتي جريمة الابتزاز الإلكتروني في مقدمة هذه الظواهر الإجرامية التي باتت تشكل تهديداً حقيقياً لأمن الأفراد واستقرار المجتمعات، فمن خلال استغلال ضعاف النفوس للوسائل التقنية الحديثة، تحول الفضاء الإلكتروني إلى مسرح لعمليات التهديد والترهيب، حيث يتم استدراج الضحايا والضغط عليهم لكشف أسرارهم أو إفشاء معلومات تمس حياتهم الخاصة، بهدف إجبارهم على الانصياع لمطالب مادية أو معنوية غير مشروعة.

ولم يكن المجتمع الليبي بمنأى عن هذه الظاهرة الخطيرة، بل شهد في السنوات الأخيرة انتشاراً واسعاً لهذه الجريمة التي أخذت أبعاداً مقلقة، وتركت آثاراً سلبية عميقة على النسيج الاجتماعي وتماسك الأسرة، مما يفرض على الباحثين ورجال القانون ضرورة دراستها وتحليلها بعمق لفهم أبعادها ووضع الحلول التشريعية والمجتمعية لمواجهتها.

أهمية البحث

تنبثق أهمية هذا البحث من عدة اعتبارات نظرية وعملية، يمكن إيجازها في النقاط التالية:

1. الأهمية العلمية: يسعى البحث إلى إثراء المكتبة القانونية الليبية بدراسة متخصصة تتناول الأحكام الموضوعية لجريمة الابتزاز الإلكتروني، في ظل حداثة هذه الجريمة وقلة الدراسات التي تناولتها بالتحليل المعمق في السياق التشريعي الليبي، خاصة بعد صدور قانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2022م.
2. الأهمية العملية: تتمثل في تسليط الضوء على جريمة تمثل انتهاكاً صارخاً للحق في الخصوصية وحرمة الحياة الخاصة، وتهديداً لأمن واستقرار المجتمع. ومن خلال تحليل نصوص التجريم والعقاب، يهدف البحث إلى توضيح الإطار القانوني لمواجهة هذه الجريمة، مما يساعد القضاة والمحامين وأعضاء النيابة العامة في تطبيق القانون تطبيقاً سليماً، ويسهم في توعية أفراد المجتمع بمخاطرها وآليات الحماية منها.
3. الأهمية المجتمعية: من خلال فهم الأبعاد القانونية لهذه الجريمة، يمكن اقتراح آليات فعالة لزيادة الوعي المجتمعي، وتشجيع الضحايا على الإبلاغ، وتطوير استراتيجيات وقائية وعلاجية للحد من انتشار هذه الظاهرة المدمرة.

إشكالية البحث:

على الرغم من الجهود التي بذلها المشرع الليبي لمواكبة التطورات التقنية من خلال إصدار قانون خاص بمكافحة الجرائم الإلكترونية، إلا أن الطبيعة الخاصة لجريمة الابتزاز الإلكتروني، وكونها جريمة مركبة

ومعقدة وعابرة للحدود، تثير العديد من التحديات القانونية على مستوى التجريم والعقاب، وعليه، تتبلور الإشكالية الرئيسية لهذا البحث في التساؤل التالي:

ما مدى كفاية وفعالية الأحكام الموضوعية التي وضعها المشرع الليبي لمواجهة جريمة الابتزاز الإلكتروني، تجريماً وعقاباً؟

ويتفرع عن هذه الإشكالية المحورية عدة تساؤلات فرعية يسعى البحث إلى الإجابة عليها:

1. ما المقصود بجريمة الابتزاز الإلكتروني، وما هي خصائصها وأنواعها ؟
2. ما هي الأركان الموضوعية التي تقوم عليها جريمة الابتزاز الإلكتروني؟
3. ما هي السياسة العقابية التي اتبعها المشرع الليبي في مواجهة جريمة الابتزاز الإلكتروني، وما هي العقوبات المقررة لها في صورتها التامة وصور الشروع فيها؟
4. كيف عالج المشرع الليبي أحكام المساهمة الجنائية (الفاعل الأصلي والشريك) في جريمة الابتزاز الإلكتروني، وما هي العقوبات المقررة لكل مساهم؟

منهج البحث

لتحقيق أهداف البحث والإجابة على تساؤلاته، سيتم الاعتماد بشكل أساسي على المنهج الوصفي التحليلي. ويتمثل الجانب الوصفي في استعراض النصوص القانونية ذات الصلة في كل من قانون العقوبات الليبي وقانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2022م، بالإضافة إلى استعراض آراء الفقه القانوني ،أما الجانب التحليلي، فيتجلى في تحليل هذه النصوص والأحكام الفقهية وتفكيكها بهدف استنباط الأحكام الموضوعية المتعلقة بتجريم وعقاب جريمة الابتزاز الإلكتروني، وتقييم مدى كفايتها وانسجامها.

خطة البحث

للإحاطة بكافة جوانب الموضوع ومعالجة إشكاليته الرئيسية، سيتم تقسيم هذا البحث إلى مبحثين رئيسيين، على النحو التالي:

المبحث الأول: الأحكام الخاصة بالتجريم في جريمة الابتزاز الإلكتروني

المطلب الأول: ماهية جريمة الابتزاز الإلكتروني

المطلب الثاني: أركان جريمة الابتزاز الإلكتروني

المبحث الثاني: الأحكام الخاصة بالعقاب في جريمة الابتزاز الإلكتروني

المطلب الأول: العقوبات المقررة لجريمة الابتزاز الإلكتروني

المطلب الثاني: أحكام المساهمة الجنائية وعقوبتها

المبحث الأول: الأحكام الخاصة بالتجريم في جريمة الابتزاز الإلكتروني

يمثل هذا المبحث حجر الزاوية في دراستنا، حيث يتناول الإطار القانوني الذي وضعه المشرع الليبي لتجريم فعل الابتزاز الإلكتروني، فالتجريم هو الخطوة الأولى والأساسية في أي سياسة جنائية تهدف إلى مكافحة سلوك معين، ومن خلاله يتم تحديد الأفعال التي يعتبرها المشرع ضارة بالمجتمع وتستوجب التدخل العقابي، وسنقسم هذا المبحث إلى مطلبين، نتناول في الأول ماهية هذه الجريمة المستحدثة، ونخصص الثاني لدراسة أركانها الموضوعية.

المطلب الأول: ماهية جريمة الابتزاز الإلكتروني قبل الخوض في تحليل الأركان المادية والمعنوية لجريمة الابتزاز الإلكتروني، لا بد من الإحاطة بإطارها المفاهيمي، وذلك بتحديد تعريف دقيق لها، وبيان الخصائص

التي تميزها عن غيرها من الجرائم التقليدية، والوقوف على أبرز صورها وأنواعها في الواقع العملي. وهذا ما سنتناوله في الفرعين التاليين.

الفرع الأول: تعريف جريمة الابتزاز الإلكتروني وتمييزها عن الجرائم المشابهة

أولاً: تعريف جريمة الابتزاز الإلكتروني

لم يضع المشرع الليبي-شأنه في ذلك شأن العديد من التشريعات المقارنة- تعريفاً جامعاً مانعاً لجريمة الابتزاز الإلكتروني، لا في قانون العقوبات ولا في قانون مكافحة الجرائم الإلكترونية. ويعود ذلك غالباً إلى رغبة المشرع في عدم تقييد نفسه بتعريفات قد تتجاوزها التطورات التقنية المتسارعة، تاركاً هذه المهمة للفقه والقضاء (علاق، 2024، صفحة 256)؛ لذا، سنستعرض المفهوم اللغوي والاصطلاحي، وصولاً إلى محاولة وضع تعريف قانوني مقترح.

1. **الابتزاز لغة** : ترجع كلمة "ابتزاز" في أصلها اللغوي إلى الفعل الثلاثي "بَزَّ"، ويقال "بَزَّهُ يَبُزُّهُ بَزًّا"، وهو يفيد معنى الغلبة والقهر والاستيلاء على الشيء خفية أو عنوة. جاء في القاموس المحيط أن من معاني "البَزّ" أخذ الشيء بصفة القهر والخفاء. (آبادي، د.ت، صفحة 647)

وجاء في لسان العرب، "ابتززتُ الشيء: استلبته"، و"بَزَّهُ" أي غلبه وغصبه وانتزعه منه. (ابن منظور، 1993، صفحة 312)

يتضح من ذلك أن المفهوم اللغوي للابتزاز يدور حول فكرة سلب الشيء من صاحبه بالقوة والإكراه، وهو المعنى الذي يتوافق مع جوهر هذه الجريمة.

2. الابتزاز اصطلاحا:

تعددت تعريفات الفقهاء لجريمة الابتزاز الإلكتروني، وإن كانت جميعها تتفق على عناصرها الأساسية، فقد عُرّفت بأنها: "عملية تهديد وترهيب للضحية للإضرار بسمعته ومكانته الاجتماعية عن طريق معلومات سرية وحساسة أو صور أو مقاطع فيديو تخص المعني، والتهديد بنشرها عبر وسائل التواصل الاجتماعي مقابل منافع مادية أو معنوية يُجبر الشخص الذي وقع عليه الابتزاز على دفعها مرغماً" (علاق، 2024، صفحة 256)

وعُرّفت أيضاً بأنها "استغلال الطرف الآخر من أجل مقاصد مادية أو شهوانية عن طريق الاحتفاظ بتسجيلات إلكترونية للتهديد بها". (مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية، 2011، صفحة 18).

كما عرفها البعض بأنها: "حصول الجاني علي معلومات سرية أو صور أو مواد فيلميه تتعلق بالمجني عليه، واستغلال ذلك للحصول علي المال أو لإجبار الضحية علي القيام بأعمال غير مشروعة" (صالح، 2018، صفحة 12)

من خلال هذه التعريفات، يمكن استخلاص أن الابتزاز الإلكتروني هو سلوك إجرامي يقوم على التهديد باستخدام وسيلة إلكترونية، بهدف إجبار المجني عليه على القيام بعمل أو الامتناع عنه، تحقيقاً لمنفعة غير مشروعة للجاني.

ثانيا: خصائص جريمة الابتزاز الإلكتروني

تتسم جريمة الابتزاز الإلكتروني بمجموعة من الخصائص التي تمنحها خطورة خاصة وتجعل مواجهتها تحدياً كبيراً، وأبرز هذه الخصائص:

1. جريمة عابرة للحدود: لا يعترف الفضاء السيبراني بالحدود الجغرافية، مما يسمح للجاني بارتكاب جريمته من أي مكان في العالم ضد ضحية في دولة أخرى، هذه الطبيعة العالمية تثير صعوبات جمة تتعلق بتحديد

القانون الواجب التطبيق والاختصاص القضائي وإجراءات الملاحقة وتسليم المجرمين. (أحمد، 2019، صفحة 140)

2. صعوبة الإثبات: تتم الجريمة في بيئة غير مادية، وغالباً ما يسعى الجاني إلى إخفاء هويته الحقيقية واستخدام تقنيات متقدمة لمحو آثاره الرقمية، مما يجعل عملية جمع الأدلة وتحديد هوية مرتكب الجريمة أمراً في غاية الصعوبة والتعقيد. (حجازي، 2009، صفحة 51)

3. خطورة الأثر النفسي والاجتماعي: لا يقتصر ضرر هذه الجريمة على الجانب المادي، بل يمتد ليترك آثاراً نفسية مدمرة على الضحية، كالخوف والقلق والعزلة، وقد يصل الأمر في بعض الحالات إلى الانتحار. كما أنها تهدد السلم الاجتماعي وتؤدي إلى تفكك الأسر وانعدام الثقة (الصول، 2024، صفحة 235).

4. ارتفاع الرقم المظلم : يُقصد به الفجوة بين عدد الجرائم المرتكبة فعلاً وعدد الجرائم المبلغ عنها رسمياً، في جرائم الابتزاز، يحجم الكثير من الضحايا عن الإبلاغ خوفاً من الفضيحة أو من تنفيذ الجاني لتهديداته، مما يجعل الأرقام الرسمية لا تعكس الحجم الحقيقي للظاهرة. (حسان، 2024، صفحة 884)

الفرع الثاني: أنواع جريمة الابتزاز الإلكتروني

تتخذ جريمة الابتزاز الإلكتروني صوراً متعددة، تختلف باختلاف غرض الجاني وطبيعة الضحية، ومن أكثرها شيوعاً:

1. الابتزاز المادي :

هذه هي الصورة النمطية والأكثر شيوعاً للابتزاز، حيث يكون الدافع الأساسي للجاني هو تحقيق كسب مادي غير مشروع، يقوم الجاني بالحصول على معلومات أو صور أو مستندات حساسة تتعلق بالضحية، ثم يساومه عليها مقابل مبلغ من المال، وتتنوع طبيعة المعلومات المستخدمة في التهديد، فقد تكون صوراً شخصية، أو محادثات خاصة، أو مستندات مالية، أو أسراراً تجارية، وتكمن خطورة هذا النوع في أنه قد يتطور إلى سلسلة لا تنتهي من المطالب المالية، حيث يظل الجاني يبتز الضحية كلما نفد المال لديه، مما يدخل الضحية في دوامة من الخوف والاستنزاف المالي. (فتح الله، 2021، صفحة 80)

2. الابتزاز الجنسي:

يعد هذا النوع من أبشع صور الابتزاز وأشدها تأثيراً على الضحية، حيث يستغل الجاني غريزة الخوف من الفضيحة لدى المجني عليه (غالباً من النساء أو القصر) لتحقيق مآرب جنسية. تبدأ الجريمة عادةً بإقامة علاقة عاطفية وهمية عبر الإنترنت، يتم من خلالها استدراج الضحية لإرسال صور أو مقاطع فيديو ذات طبيعة حميمية. وبمجرد حصول الجاني على هذا المحتوى، يبدأ في تهديد الضحية بنشره على الملأ أو إرساله إلى أفراد عائلته وأصدقائه، ما لم تستجب لمطالبه الجنسية، والتي قد تتراوح بين إجباره على القيام بأفعال جنسية عبر الكاميرا، أو إقامة علاقة جنسية فعلية معه. (علاق، 2024، صفحة 257)

ويترك هذا النوع من الابتزاز ندوباً نفسية عميقة لدى الضحية، وقد يؤدي إلى عواقب وخيمة تصل إلى الانتحار. (الصول، 2024، صفحة 236)

3. ابتزاز الأطفال والمراهقين :

يمثل الأطفال والمراهقون فئة مستهدفة بشكل خاص من قبل المبتزين، نظراً لقلة خبرتهم، وسهولة التأثير عليهم، وخوفهم من إخبار والديهم. يستغل الجناة فضول هذه الفئة ورغبتها في إثبات الذات لاستدراجهم في محادثات غير لائقة، أو إقناعهم بإرسال صور خاصة، أو حتى الحصول على معلومات شخصية عن أسرهم. ثم يستخدم الجاني هذه المعلومات لابتزاز الطفل أو المراهق، إما للحصول على المال، أو لإجباره على القيام

بأفعال غير قانونية، أو لاستغلاله جنسياً، وتكمن الخطورة هنا في أن الضرر لا يقتصر على الطفل نفسه، بل قد يمتد ليشمل أسرته بأكملها. (علاق، 2024)

4. ابتزاز الشركات والمؤسسات:

لم يعد الابتزاز الإلكتروني مقتصراً على الأفراد، بل امتد ليشكل تهديداً خطيراً للشركات والمؤسسات الحكومية والخاصة. وتأخذ هذه الجريمة في هذا السياق شكلين رئيسيين:

التهديد بتسريب البيانات: حيث يتمكن المهاجمون من اختراق أنظمة الشركة وسرقة بيانات حساسة (بيانات عملاء، أسرار تجارية، خطط استراتيجية)، ثم يهددون بنشرها على الإنترنت أو بيعها للمنافسين ما لم تدفع الشركة فدية مالية ضخمة. (بعيوي، 2020، صفحة 25)

هجمات الفدية: وهي الصورة الأكثر تدميراً، حيث يقوم المهاجمون بزرع برمجية خبيثة في شبكة الشركة تقوم بتشفير جميع ملفاتها وأنظمتها، مما يؤدي إلى شل عملياتها بالكامل، ثم يطالب المهاجمون بفدية (غالباً بعملات مشفرة لضمان عدم تعقبهم) مقابل إعطاء مفتاح فك التشفير، وتواجه الشركة هنا خياراً صعباً بين دفع الفدية مع عدم وجود ضمان لاستعادة بياناتها، أو تحمل خسائر فادحة قد تؤدي إلى إفلاسها. (حسان، 2024، صفحة 875)

المطلب الثاني: أركان جريمة الابتزاز الإلكتروني

لا قيام لأي جريمة دون توافر أركانها التي يحددها القانون، والتي تمثل قوامها وعناصرها الأساسية. وجريمة الابتزاز الإلكتروني، كغيرها من الجرائم، تستلزم لقيامها توافر الركن المادي والذي يتمثل في السلوك الخارجي الملموس الذي يرتكبه الجاني، والركن المعنوي يتمثل في الإرادة الآثمة التي دفعت الجاني إلى ارتكاب جريمته.

وفي سياق جريمة الابتزاز الإلكتروني، يثور التساؤل حول الأساس القانوني لتجريم هذا الفعل في التشريع الليبي، وكما أسلفنا، لم يفرد المشرع الليبي نصاً خاصاً ومستقلاً لجريمة الابتزاز الإلكتروني باسمها في قانون الجرائم الإلكترونية، بل يمكن استخلاص تجريمها من خلال النصوص العامة في قانون العقوبات، وبالرجوع إلى هذا الأخير نجد أنه نص في المادة ة 429 على أنه: "يعاقب بالحبس أو بغرامة كل من أرغم الغير بالعنف أو بالتهديد على إتيان فعل أو احتماله أو عدم القيام به. ويعاقب بالسجن مدة لا تجاوز ثلاث سنوات إذا كان التهديد موجهاً لإرغام الغير على إتيان فعل يكون جريمة."

فهذه المادة تشكل في حقيقتها الأساس القانوني الأول لتجريم جريمة الابتزاز الإلكتروني، حيث تتضمن العناصر الأساسية التي تميز الابتزاز عن مجرد التهديد. فهذه المادة تجرم الإرغام بالتهديد، وهو ما يعني أن الجاني لا يقتصر على مجرد التهديد، بل يسعى إلى إرغام الضحية على القيام بفعل معين أو الامتناع عنه. وفي حالة الابتزاز الإلكتروني، يكون الفعل المطلوب عادة هو تسليم مبلغ من المال أو ممتلكات ذات قيمة مالية.

كما أن المادة 430 من قانون العقوبات تنص على أنه : " يعاقب بغرامة لا تزيد على خمسة جنيهات كل من هدد الغير بإنزال ضرر غير مشروع به، ... وإذا كان التهديد بارتكاب جريمة ضد النفس أو المال أو بإفشاء أمور مخدشة بالشرف ..."

يظهر من هذا النص أنه يشمل جوهر فعل الابتزاز، وهو التهديد (بجريمة أو بأمور شائنة) المقترن بطلب أو شرط (وهو ما يمثل الإجبار على القيام بعمل أو الامتناع عنه). إلا أن هذه النصوص وُضعت في زمن لم تكن فيه الجرائم الإلكترونية بالصورة التي هي عليها اليوم، مما قد يثير صعوبات في تطبيقها على الحالات التي تتم عبر وسائل تقنية معقدة (علاق، 2024، صفحة 260)، وبعد أن بينا الأساس القانوني لهذه الجريمة في التشريع الجنائي الليبي ننتقل لبيان الركن والمادي والمعنوي في الفروع التالية:

الفرع الثاني: الركـن المادي لجريمة الابتزاز الإلكتروني

لكي يتدخل المشرع بوضع قوانين وجزاءات ضمن نصوص قانونية محددة، ولكي يقرر القاضي المسؤولية الجنائية الناشئة عن الأفعال والعقاب الواجب توقيعه على شخص معين، لا بد أن يرتكب المتهم أفعالاً معينة تشكل الركن المادي للجريمة.

وكما هو معروف في الفقه الجنائي، فإن الركن المادي يتمتع بطبيعة مادية ملموسة يمكن إدراكها بالحواس، بحيث لا يعترف القانون بوجود جريمة دون توافر هذا الركن. ويعبر عن الركن المادي بالواقعة المادية التي تنطبق على النموذج القانوني المحدد للجريمة التامة. (بارة، 2022، صفحة 127) ويتمثل الركن المادي في النشاط الخارجي الملموس الذي تتحقق به الجريمة في العالم الواقعي. ويتكون هذا الركن في جريمة الابتزاز الإلكتروني من ثلاثة عناصر متكاملة: الفعل (النشاط الإجرامي)، والنتيجة الإجرامية، وعلاقة السببية التي تربط بينهما.

1. الفعل (النشاط الإجرامي):

بقراءة نص المادة 429 و 430 من قانون العقوبات الليبي يتبين لنا أن فعل الابتزاز يتمثل في كل قول أو فعل يصدر عن الجاني ويكون من شأنه إلقاء الرعب في نفس المجني عليه وحمله على الاعتقاد بأنه سيتعرض لضرر محدق في نفسه أو ماله أو شرفه إذا لم يستجب لمطالب الجاني. (حسني، 2018، صفحة 1105)

ولا يهم أن يكون الجاني قادراً فعلاً على تنفيذ تهديده أو عازماً على ذلك، بل يكفي أن يكون التهديد في حد ذاته جاداً ومناسباً لإحداث الأثر النفسي المطلوب لدى المجني عليه. ويجب أن يتم هذا التهديد باستخدام وسيلة إلكترونية، كرسائل البريد الإلكتروني، أو تطبيقات المراسلة الفورية (واتساب، تليجرام)، أو منشورات على وسائل التواصل الاجتماعي، أو حتى من خلال المكالمات الهاتفية عبر الإنترنت. (سعيد، 2025، صفحة 290)

وهذا هو ما أشارت إليه المحكمة العليا الليبية في أحد أحكامها حيث قضت على أنه : " جريمة التهديد المنصوص عليها في المادة 430 من قانون العقوبات تتحقق بوجه عام بكل قول أو فعل يوجه من الجاني إلى المجني عليه ويكون من شأنه إزعاجه وإلقاء الرعب في نفسه وإحداث الخوف لديه وذلك بتوعده بإنزال ضرر غير مشروع به أو بارتكاب جريمة ضد النفس أو المال أو بأية حالة من الحالات الأخرى المبينة في الفقرة الثانية من المادة السالفة الذكر..." (طعن جنائي رقم 729 / 39 ق، 1995)

ويمكن أن يتخذ التهديد شكلين أساسيين في جريمة الابتزاز الإلكتروني. الشكل الأول هو التهديد الصريح والمباشر، والذي يتمثل في استخدام عبارات واضحة وصريحة تتضمن تهديداً مباشراً بارتكاب فعل معين أو بإفشاء معلومات حساسة. في هذه الحالة، يكون التهديد جلياً وواضحاً لا يحتمل اللبس أو التأويل. (علاق، 2024، صفحة 260)

أما الشكل الثاني فهو التهديد الضمني والمستتر، والذي يتمثل في إرسال إشارات أو عبارات معينة يفهم منها التهديد بشكل غير مباشر، وفي هذا الشكل، يكون التهديد مستتراً لكن يمكن استخلاصه من السياق العام للرسائل والتواصل بين الجاني والضحية. وفي كلا الشكلين، يعكس التهديد رغبة المبتز في الحصول على مقابل مادي أو معنوي نظير عدم تنفيذ التهديد.

من المهم التأكيد على أن نصي المادة سالفي الذكر لا يفرقا بين كون الفعل المطلوب من الضحية مشروعاً أو غير مشروع. فالعبرة الحقيقية في تحقق جريمة الابتزاز تكمن في الضغط والإكراه الذي يقترن بالتهديد، وفي إرغام وإجبار الضحية على القيام بفعل معين. فعلى سبيل المثال، قد يقوم المبتز بتهديد رب العمل بنشر صور خاصة له عبر وسائل التواصل الاجتماعي نظير توقيعه على معاملة مالية. وفي هذه الحالة، قد تكون المعاملة

المالية مشروعة من حيث الأصل، لكن الطريقة التي تم بها إجبار رب العمل على التوقيع عليها عبر التهديد هي التي تجعل الفعل جريمة. (علاق، 2024، صفحة 260)

ويتحقق التهديد بمجرد توجيهه من الجاني إلى الضحية بقصد إحداث أثر الخوف والرعب في نفس من وجهت إليه. وليس هناك اعتداد بالأسلوب أو القالب الذي تصاغ فيه عبارات التهديد، سواء كانت صريحة أو ضمنية، مباشرة أو غير مباشرة، فالمهم هو أن يفهم الضحية من التهديد أنه يواجه خطراً معيناً إذا لم يستجب لمطالب المبتز.

وعلى هذا تتضح التفرقة بين الابتزاز الإلكتروني والابتزاز التقليدي من هذه الناحية فالابتزاز التقليدي يتم عادة من خلال التواصل المباشر بين الجاني والمجني عليه، سواء كان هذا التواصل شفاهياً أو من خلال رسائل مكتوبة أو أي وسيلة تقليدية أخرى، بينما الابتزاز الإلكتروني يتم من خلال الوسائل الإلكترونية الحديثة مثل البريد الإلكتروني وتطبيقات التواصل الاجتماعي والرسائل النصية وغيرها من الوسائل الرقمية، وهذا الاختلاف في الوسيلة ينعكس على طبيعة الركن المادي للجريمة، فالابتزاز الإلكتروني يتميز بسهولة التنفيذ والتكرار، حيث يمكن للجاني أن يرسل التهديدات لعدد كبير من الضحايا في نفس الوقت دون الحاجة إلى التواجد الفعلي في نفس المكان، كما أن الابتزاز الإلكتروني يتميز بإمكانية إخفاء هوية الجاني بسهولة أكبر من الابتزاز التقليدي، مما يجعل من الصعب على الضحايا تحديد الجاني والإبلاغ عنه. (الصول، 2024)

وبالتالي، فإن الابتزاز الإلكتروني يتطلب نصوصاً قانونية متخصصة وعقوبات أكثر ردعاً من تلك المقررة للابتزاز التقليدي، لكي تتناسب مع خطورة الجريمة وآثارها الضارة على الضحايا والمجتمع.

2. النتيجة الإجرامية:

يشكل العنصر الثاني من الركن المادي لجريمة الابتزاز الإلكتروني ما يطلق عليه بالنتيجة الإجرامية، وهي الحالة التي ينتج عنها السلوك الإجرامي للجاني. فالابتزاز بطبيعته لا يقتصر على مجرد التهديد البسيط، بل يتطلب أن يكون هذا التهديد موجهاً نحو تحقيق غرض محدد، ألا وهو إرغام الضحية على القيام بعمل معين أو الامتناع عن القيام به. وهذا الجانب هو الذي يميز الابتزاز عن غيره من الجرائم ذات الصلة.

وتتعدد صور الأعمال التي قد يسعى المبتز إلى إرغام الضحية على القيام بها. فقد يكون الهدف الحصول على مبلغ مالي، وهو ما يعتبر الصورة الأكثر انتشاراً في الممارسة العملية. وقد يتجاوز الأمر ذلك ليشمل إرغام الضحية على تنفيذ أفعال أخرى، سواء كانت ذات طبيعة جنسية أو اقتصادية أو إدارية، كما قد يقتصر الهدف على إرغام الضحية على الامتناع عن القيام بفعل معين، مثل عدم الإدلاء بشهادة أمام الجهات المختصة أو الامتناع عن تنفيذ واجب وظيفي. (علاق، 2024)

من الناحية القانونية، لا يتطلب القانون أن يستجيب المجني عليه فعلاً للتهديد ويقوم بتسليم الأموال أو تنفيذ الفعل المطلوب. فالجريمة تتحقق بمجرد صدور التهديد بقصد تحقيق هذه النتيجة، بغض النظر عما إذا كان الجاني قد حقق هدفه أم لا. وبالتالي، فإن عدم استجابة الضحية للتهديد لا يؤدي إلى انتفاء الجريمة، بل قد يرقيها إلى مرتبة الشروع في الجريمة إذا توافرت باقي أركانها. (حسان، 2024، صفحة 880)

ويرى البعض أن جريمة الابتزاز الإلكتروني تندرج ضمن فئة ما يعرف بجرائم الخطر، وليس جرائم الضرر. فجرائم الخطر هي تلك التي يكفي فيها مجرد تعريض المصلحة المحمية قانوناً للخطر، دون الحاجة إلى حدوث ضرر فعلي ومباشر، وفي حالة الابتزاز الإلكتروني، فإن مجرد استخدام الوسائل الإلكترونية في توجيه التهديد والإرغام يشكل اعتداءً على حقوق الضحية ومصالحه الشخصية، بصرف النظر عما إذا كان قد

لحق به ضرر مادي أو معنوي فعلي. فالقانون يحمي هنا من احتمالية الضرر وليس من الضرر الفعلي الذي قد لا يتحقق أبداً. (حنش، 2020، صفحة 28)

ويترتب على هذا التصنيف أن النتيجة الإجرامية لا تتطلب تزامناً زمنياً مع السلوك الإجرامي. فقد يتأخر حدوث النتيجة بفترة طويلة أو قصيرة عن لحظة ارتكاب فعل التهديد. وعلاوة على ذلك، فإن الركن المادي قد يتحقق دون أن تترتب عليه النتيجة الإجرامية بالكامل، فعلى سبيل المثال، قد يتم اكتشاف جريمة الابتزاز بمجرد تحديد الضحية والتهديد به، دون أن يكون الجاني قد حقق الهدف الذي سعى إليه. وفي هذه الحالات، يستحق الجاني العقاب بموجب القانون، حيث أن الجريمة قد تحققت بعناصرها الأساسية. (علاق، 2024، صفحة 262)

فتتحقق جريمة الابتزاز الإلكتروني عندما يقوم الجاني بأفعال من شأنها أن تثير الخوف والقلق لدى الضحية وتسيء إلى سمعته وشرفه وهذه الأفعال وحدها، بغض النظر عن نتيجتها الفعلية، تشكل جريمة كاملة الأركان، فالمشرع الليبي، من خلال نصوص قانون العقوبات، وتحديداً المادة 429 و430 منه، قد اعترف بخطورة هذا السلوك وأقرر عقوبات مشددة عند توافر عناصر معينة، مثل التهديد بارتكاب جريمة أو بإفشاء أسرار وأمور مخدشة بالشرف، وهذا الموقف التشريعي يعكس إدراكاً واضحاً لطبيعة جريمة الابتزاز وخطورتها على الفرد والمجتمع.

3. علاقة السببية:

يجب أن تتوافر رابطة سببية مباشرة بين فعل التهديد الذي ارتكبه الجاني والنتيجة المتمثلة في إجبار المجني عليه على التصرف على غير إرادته. بمعنى آخر، يجب أن يكون التهديد هو العامل الحاسم الذي دفع المجني عليه إلى التفكير في الاستجابة لمطالب الجاني. فإذا كان قرار المجني عليه نابعاً من سبب آخر غير التهديد، فإن علاقة السببية تنتفي. (بهنام، 2000، صفحة 450)

الفرع الثاني: الركن المعنوي لجريمة الابتزاز الإلكتروني

يمثل الركن المعنوي العنصر الثالث من أركان جريمة الابتزاز الإلكتروني، وهو يتعلق بالحالة النفسية للجاني وتوجه إرادته نحو ارتكاب الفعل المجرم، فالركن المعنوي يشكل الرابط بين السلوك المادي للجاني وشخصيته، ويتجسد في القصد الجنائي الذي يعكس أعلى درجات الإثم الجنائي، لما يعكسه من اتجاه واضح من جانب الجاني نحو مخالفة القانون وتجاوز حدوده. (باره، 2014، صفحة 315)

وتتطلب جريمة الابتزاز الإلكتروني توافر القصد الجنائي العام، والذي يتكون من عنصرين أساسيين: العلم والإرادة، فيجب أن يعلم الجاني بأنه يستخدم وسائل إلكترونية أو شبكة الإنترنت أو منصات التواصل الاجتماعي، وأن فعله هذا يشكل ابتزازاً وتهديداً للمجني عليه. كما يجب أن يعلم بأن حصوله على المعلومات والبيانات والصور الحساسة عن شخص ما وتهديده بها يمثل اعتداءً على حقوقه الشخصية، وأن هذا التهديد من شأنه إيقاع الخوف والرعب في نفس الضحية وإرغامه على الامتثال لطلباته، وعلى الرغم من توافر هذا العلم، فإن الجاني يتجه بإرادته نحو تحقيق هذا الفعل دون أي اعتبار لعواقبه أو تبعاته على الضحية. (علاق، 2024، صفحة 263)

بالإضافة إلى القصد الجنائي العام، تتوافر في جريمة الابتزاز الإلكتروني أيضاً عناصر من القصد الجنائي الخاص، فالجاني يسعى بنية محددة إلى الحصول على مقابل أو منفعة معينة، سواء كانت مادية أو معنوية، قد يكون هذا المقابل عبارة عن مبلغ مالي أو تنفيذ معاملة مالية معينة أو توقيع أوراق تحمل قيمة مالية، وقد يتخذ المقابل شكلاً معنوياً، مثل إقامة علاقة غير مشروعة أو القيام بفعل معين لا يتعلق بالمال، وهذا الجانب من النية يميز جريمة الابتزاز عن مجرد التهديد البسيط. (حسني، 2018، صفحة 1108)

من المهم التأكيد على أنه لا يشترط لقيام جريمة الابتزاز أن يقصد الجاني فعلاً تحقيق الشيء المهدد به، فمجرد التهديد ذاته يشكل جريمة قائمة بذاتها يعاقب عليها القانون، لما يحدثه من قلق واضطراب في نفس المجني عليه، فالركن المعنوي هو مسلك ذهني ونفسي من جانب الجاني، وبتوافره تتحقق جميع مقومات المسؤولية الجنائية، مما يترتب عليه حق الدولة في العقاب، وهذا الحق يستند بشكل أساسي إلى توافر هذه المقومات. (حسان، 2024، صفحة 910).

يتحقق القصد الجنائي في جريمة الابتزاز الإلكتروني في عدة حالات: **الحالة الأولى**: هي عندما يتوقع الجاني ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي يعلق عليه القانون وجود الجريمة، **والحالة الثانية:** هي عندما ينجم عن فعل الجاني أو امتناعه ضرر أو خطر أكثر جسامة مما كان يقصده، وهي ما يعرف بحالة تجاوز القصد. **أما الحالة الثالثة**: فهي تلك الحالات التي ينسب فيها القانون الفعل إلى الفاعل نتيجة لفعله أو امتناعه، أو الحالات التي يفترض فيها القانون توافر القصد الجنائي افتراضاً قانونياً. وهذا الافتراض مستمد من مبدأ أنه طالما أن النتيجة الجسيمة قد تحققت نتيجة لفعل الجاني، فإن هذا الفعل كان كافياً لإحداثها، وبالتالي يجب أن يتحمل الجاني نتائجه سواء توقعها أم لم يتوقعها. (حسان، 2024، صفحة 910).

والأمر الجدير بالذكر هنا أن الدافع أو الباعث على ارتكاب الجريمة (كسوء الحالة المادية أو الرغبة في الانتقام) لا عبرة له في قيام الركن المعنوي، طالما توافرت لدى الجاني نية تحقيق الكسب غير المشروع من وراء تهديده.

المبحث الثاني: الأحكام المتعلقة بالجزاء في جريمة الابتزاز الإلكتروني

بعد أن فرغنا في المبحث الأول من تحديد ماهية جريمة الابتزاز الإلكتروني وبيان أركانها الموضوعية، ننتقل في هذا المبحث إلى الشق الثاني من الأحكام الموضوعية، وهو شق العقاب، فالسياسة الجنائية لا تكتمل بمجرد تجريم الأفعال الضارة، بل لا بد من وضع جزاءات رادعة تتناسب مع خطورة هذه الأفعال وتحقق أهداف العقوبة في الردع العام والخاص، وسنتناول في هذا المبحث العقوبات المقررة لهذه الجريمة، ثم أحكام المساهمة الجنائية فيها.

المطلب الأول: العقوبات المقررة لجريمة الابتزاز الإلكتروني

تتحدد السياسة العقابية التي يتبعها المشرع في مواجهة ظاهرة إجرامية معينة من خلال طبيعة ونوع ومقدار العقوبات التي يفرضها على مرتكبيها. وقد تعامل المشرع الليبي مع جريمة الابتزاز الإلكتروني من خلال نصوص متفرقة، سواء في قانون العقوبات التقليدي أو في قانون مكافحة الجرائم الإلكترونية المستحدث. وسنخصص هذا المطلب لدراسة العقوبات المقررة لهذه الجريمة في صورتها التامة، ثم نتطرق إلى عقوبة الشروع فيها.

الفرع الأول: عقوبة الجريمة التامة في جريمة الابتزاز الإلكتروني

الجريمة التامة هي التي استكملت جميع أركانها وتحققت نتيجتها الإجرامية التي هدف إليها الجاني، وفي جريمة الابتزاز، تعتبر الجريمة تامة بمجرد أن يؤدي التهديد إلى حمل المجني عليه على تسليم المال أو القيام بالعمل أو الامتناع عنه. (حسني، 2018، صفحة 1107) وتختلف العقوبة المقررة باختلاف النص القانوني المطبق.

ومن الضروري التأكيد في البداية على أن قانون مكافحة الجرائم الإلكترونية الليبي رقم (5) لسنة 2022م لم ينص على جريمة الابتزاز الإلكتروني كجريمة مستقلة ومحددة بشكل صريح. وبالتالي، فإن تجريم هذا الفعل

والعقوبات المقررة له تستند إلى القواعد العامة الموجودة في قانون العقوبات الليبي، وتحديداً المادتين 429 و430، اللتين توفران الإطار القانوني الشامل لمعاقبة جريمة الابتزاز الإلكتروني.

أولا : العقوبة بموجب المادة 429 (الإرغام بالعنف أو التهديد)

تنص المادة 429 من قانون العقوبات الليبي على أنه : " يعاقب بالحبس مدة لا تزيد على سنتين كل من أرغم الغير بالعنف أو بالتهديد على اتيان فعل أو احتماله أو عدم القيام به.

ويعاقب بالحبس إذا كان التهديد موجهاً لإرغام الغير على اتيان فعل يكون جريمة، أو كان التهديد كتابة.

فإذا حصل الجاني على نفع غير مشروع إضراراً بالغير تكون العقوبة السجن مدة لا تجاوز خمس سنوات.

يتضح من هذا النص أنه جعل ثلاث صور للعقاب على جريمة التهديد وهي:

الصورة الأولى: الإرغام البسيط بالعنف أو التهديد:

تتمثل هذه الصورة في قيام الجاني بإرغام الغير بالعنف أو بالتهديد على إتيان فعل معين أو احتماله أو عدم القيام به، دون توافر أي ظروف مشددة أخرى. وفي هذه الحالة البسيطة، تكون العقوبة المقررة هي الحبس لمدة لا تزيد على سنتين. وهذه الصورة تشمل جميع حالات الإرغام التي لا ترقى إلى مستوى الصور المشددة، سواء كان الإرغام بالعنف المادي أو بالتهديد الشفاهي البسيط. والمشرع هنا قد حدد عقوبة معقولة تعكس خطورة الفعل لكن دون الوصول إلى الصور الأشد.

الصورة الثانية: الإرغام المشدد بالعنف أو التهديد:

تتمثل هذه الصورة في حالتين مختلفتين يتم تشديد العقوبة فيهما، **الحالة الأولى**: هي عندما يكون التهديد موجهاً لإرغام الغير على إتيان فعل يكون جريمة، وفي هذه الحالة، يقصد الجاني إرغام الضحية على ارتكاب فعل إجرامي معين، مما يعكس خطورة أكبر من مجرد الإرغام على فعل مشروع.

والحالة الثانية: هي عندما يكون التهديد كتابة، أي أن الجاني يوجه التهديد للضحية عبر الكتابة بدلاً من الطريقة الشفاهية. والتهديد الكتابي يعتبر أشد خطورة لأنه يترك أثراً مادياً واضحاً ويعكس نية مبيتة من الجاني. وفي كلا الحالتين، تكون العقوبة المقررة هي الحبس، دون تحديد مدة معينة في النص، مما يعني أن المشرع ترك للقاضي سلطة تقديرية في تحديد مدة الحبس المناسبة حسب ظروف كل حالة.

الصورة الثالثة: الإرغام المشدد مع تحقق النفع غير المشروع

تتمثل هذه الصورة في الحالة التي يحصل فيها الجاني على نفع غير مشروع إضراراً بالغير نتيجة لفعل الإرغام. وهذه الصورة تعتبر الأشد خطورة من بين جميع صور الجريمة، لأنها تجمع بين الإرغام والحصول على فائدة غير مشروعة.

وفي هذه الحالة، يكون الجاني قد استخدم الإرغام كوسيلة للحصول على منفعة معينة، سواء كانت مالية أو معنوية أو جنسية، مما يعكس نية واضحة من الجاني للإثراء على حساب الضحية، والعقوبة المقررة لهذه الصورة المشددة هي السجن لمدة لا تجاوز خمس سنوات، وهي عقوبة شديدة تعكس خطورة هذا السلوك الإجرامي والضرر الذي يلحقه بالضحية.

وعلاوة على هذه الصور الثلاث، نص المشرع على تشديدات إضافية للعقوبة في حالات معينة، فتزاد العقوبة بمقدار لا يجاوز الثلث إذا ارتكب العنف أو التهديد باستعمال السلاح، وهذا التشديد يعكس خطورة استخدام الأسلحة في ارتكاب الجريمة، حيث أن السلاح يزيد من حدة التهديد ويعكس نية الجاني في إلحاق ضرر جسيم بالضحية.

كما تزاد العقوبة بنفس المقدار (الثلث) إذا قام بالعنف أو التهديد عدة أشخاص معتصبين، أي أنهم اجتمعوا بنية محددة لارتكاب الجريمة. وهذا التشديد يعكس خطورة الجريمة الجماعية والضغط النفسي الإضافي الذي يقع على الضحية عند مواجهة عدة أشخاص.

وأخيراً، تزاد العقوبة بنفس المقدار أيضاً إذا قام بالعنف أو التهديد شخص متنكر، أي أنه أخفى هويته أو ملامحه. وهذا التشديد يعكس خطورة الجريمة التي يرتكبها شخص متنكر، حيث أن ذلك يعكس نية مبيتة وحرص الجاني على عدم الكشف عن هويته، مما يزيد من الخطورة والضرر النفسي للضحية.

وبالتالي، فإن العقوبة المقررة لجريمة الإرغام قد تزاد بمقدار الثلث في الحالات المشددة السابقة، مما يعني أن العقوبة الأصلية قد تضاعف تقريباً. فمثلاً، إذا كانت العقوبة الأصلية هي الحبس لمدة سنتين (في الصورة البسيطة)، فقد تصل إلى حوالي سنتين وثمانية أشهر عند توافر أحد ظروف التشديد. وإذا كانت العقوبة الأصلية هي السجن لمدة خمس سنوات (في الصورة المشددة مع النفع غير المشروع)، فقد تصل إلى حوالي ستة سنوات وثمانية أشهر عند توافر ظروف التشديد الإضافية.

ثانيا: العقوبة بموجب المادة 430 (جريمة التهديد)

تنص المادة 430 على أنه : " يعاقب بالحبس مدة لا تجاوز ستة أشهر او بغرامة لا تزيد على خمسين جنيهاً كل من هدد الغير بإنزال ضرر غير مشروع به، ولا تقام الدعوى إلا بشكوى الطرف المتضرر .

وإذا كان التهديد بارتكاب جريمة ضد النفس أو المال أو بإفشاء أمور مخدشة بالشرف أو بأحد الأشكال المذكورة في الفقرة الأخيرة من المادة السابقة تكون العقوبة الحبس مدة لا تزيد على سنة ولا تتوقف إقامة الدعوى على شكوى الطرف المتضرر"

وتقسم هذه المادة التهديد إلى صورتين مختلفتين، يختلف التكييف القانوني والعقوبة المقررة لكل منهما بحسب طبيعة التهديد وموضوعه.

الصورة الأولى: التهديد البسيط بضرر غير مشروع

تتمثل هذه الصورة في قيام الجاني بتهديد الغير بإنزال ضرر غير مشروع به، دون أن يكون هذا التهديد متعلقاً بارتكاب جريمة أو بإفشاء أمور مخدشة بالشرف، وهذه الصورة البسيطة من التهديد تشمل جميع حالات التهديد العام بأضرار لا ترقى إلى مستوى الجرائم أو الأمور المخدشة بالشرف، والعقوبة المقررة لهذه الصورة البسيطة هي الحبس لمدة لا تجاوز ستة أشهر أو بغرامة لا تزيد على خمسين جنيهاً، وهذه عقوبة خفيفة نسبياً تعكس أن المشرع اعتبر هذه الصورة من التهديد أقل خطورة من الصور الأخرى. وعلاوة على ذلك، فإن الدعوى الجنائية لا تقام إلا بشكوى من الطرف المتضرر، مما يعكس أن المشرع اعتبر هذه الجريمة من الجرائم التي تمس المصالح الخاصة للأفراد وليس النظام العام، وبالتالي ترك للمجني عليه الحق في تحريك الدعوى من عدمه.

الصورة الثانية: التهديد المشدد بارتكاب جريمة أو بإفشاء أمور مخدشة بالشرف

تتمثل هذه الصورة المشددة في حالات معينة يتم فيها تشديد العقوبة بشكل ملحوظ. الحالة الأولى هي عندما يكون التهديد بارتكاب جريمة ضد النفس، أي أن الجاني يهدد الضحية بالقتل أو الإيذاء أو الاعتداء الجسدي. والحالة الثانية هي عندما يكون التهديد بارتكاب جريمة ضد المال، أي أن الجاني يهدد الضحية بالسرقة أو الإتلاف أو الاختلاس. والحالة الثالثة هي عندما يكون التهديد بإفشاء أمور مخدشة بالشرف، أي أن الجاني يهدد الضحية بكشف أسرار شخصية أو صور حميمية أو معلومات محرجة. والحالة الرابعة هي عندما يكون التهديد بأحد الأشكال المذكورة في الفقرة الأخيرة من المادة السابقة (المادة 429)، والتي تتعلق بالتشديدات الإضافية مثل استعمال السلاح أو قيام عدة أشخاص معتصبين أو شخص متنكر.

والعقوبة المقررة لهذه الصورة المشددة هي الحبس لمدة لا تزيد على سنة واحدة. وهذه عقوبة أشد من الصورة البسيطة، حيث أن المشرع رفع الحد الأقصى من ستة أشهر إلى سنة واحدة. وهذا التشديد يعكس إدراك المشرع لخطورة أكبر لهذه الصور من التهديد، خاصة عندما يتعلق الأمر بتهديدات بجرائم ضد النفس أو المال أو بإفشاء أمور مخدشة بالشرف. وعلاوة على ذلك، فإن الدعوى الجنائية لا تتوقف إقامتها على شكوى من الطرف المتضرر، بل تصبح من جرائم الشكوى ذات الطبيعة الخاصة التي يمكن للنيابة العامة تحريكها من تلقاء نفسها. وهذا يعكس أن المشرع أعطى أهمية خاصة لهذه الصور المشددة من التهديد، حيث أنها تمس مصالح أساسية للأفراد مثل الحياة والمال والشرف.

وفي سياق جريمة الابتزاز الإلكتروني، فإن معظم الحالات تندرج ضمن الصورة الثانية المشددة من المادة 430، حيث أن الجاني عادة ما يهدد الضحية بإفشاء معلومات أو صور حساسة مخدشة بالشرف. وبالتالي، فإن العقوبة المقررة لجريمة الابتزاز الإلكتروني بموجب المادة 430 ستكون الحبس لمدة لا تزيد على سنة واحدة، وهي عقوبة تعكس خطورة هذه الجريمة. وعلاوة على ذلك، فإن النيابة العامة تستطيع تحريك

الدعوى من تلقاء نفسها دون الحاجة إلى شكوى من المجني عليه، مما يعكس التزام المشرع بحماية الأفراد من هذه الجريمة الخطيرة.

غير أنه يجدر الملاحظة أن هناك فرقاً مهماً بين المادة 429 والمادة 430. فالمادة 429 تتعلق بجريمة الإرغام بالعنف أو التهديد، حيث يكون الهدف من الجريمة هو إرغام الضحية على إتيان فعل معين أو الامتناع عن فعل. بينما المادة 430 تتعلق بجريمة التهديد البسيط، حيث يكون الهدف من الجريمة هو مجرد التهديد دون أن يكون هناك إرغام على فعل معين. وفي حالة جريمة الابتزاز الإلكتروني، فإن الجريمة تجمع بين عنصري الإرغام والتهديد، حيث أن الجاني يهدد الضحية بإفشاء معلومات أو صور حساسة بقصد إرغامها على تسليم مبلغ من المال أو القيام بفعل معين. وبالتالي، فإن جريمة الابتزاز الإلكتروني قد تندرج تحت أحكام المادة 429 (جريمة الإرغام) أو المادة 430 (جريمة التهديد)، أو قد تندرج تحت أحكام كليهما معاً، حسب الظروف المحددة لكل حالة وتقدير المحكمة

غير أنه يجدر بالملاحظة أن المشرع الليبي رغم إصداره قانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2022م، لم يتضمن هذا القانون نصوصاً مشددة وخاصة تجرم جريمة الابتزاز الإلكتروني بشكل مباشر وصريح. فالقانون الإلكتروني جاء عاماً ، وافتقد إلى نصوص متخصصة تعكس الخطورة الحقيقية لجريمة الابتزاز الإلكتروني في العصر الحالي وهذا النقص التشريعي يعتبر قصوراً واضحاً، خاصة وأن جرائم الابتزاز الإلكترونية أصبحت ظاهرة منتشرة بشكل متزايد في المجتمع الليبي، مما يهدد أمن واستقرار الأفراد والعائلات (علاق، 2024).

وفيما يتعلق بالمادة 429 من قانون العقوبات الليبي، والتي تتناول جريمة الإرغام بالعنف أو التهديد، فإن العقوبات المقررة بموجبها تتدرج من الحبس لمدة لا تزيد على سنتين في الصورة البسيطة، إلى السجن لمدة لا تجاوز خمس سنوات في الصورة المشددة التي يحصل فيها الجاني على نفع غير مشروع. وبينما تعكس هذه العقوبات درجة معقولة من الردع، إلا أنها قد لا تكون كافية في حالات الابتزاز الإلكتروني المعقدة والمتكررة، فالمبتز الإلكتروني غالباً ما يستهدف ضحايا متعددين ويحقق بذلك أرباحاً كبيرة من جرائمه، مما يجعل العقوبة المقررة غير متناسبة مع الفائدة التي يحصل عليها، وعلاوة على ذلك، فإن الطبيعة الإلكترونية للجريمة تسهل تكرارها وتكثيفها، حيث يمكن للجاني استهداف عدد كبير من الضحايا بجهد أقل وتكاليف أقل مقارنة بالجرائم التقليدية. وبالتالي، فإن العقوبات المقررة بموجب المادة 429 قد لا تحقق الردع الفعال المطلوب لمواجهة هذه الظاهرة المتنامية.

أما فيما يتعلق بالمادة 430 من قانون العقوبات، والتي تتناول جريمة التهديد بشكل مباشر، فإن العقوبة المقررة في الصورة المشددة (التهديد بجريمة أو بإفشاء أمور مخدشة بالشرف) تقتصر على الحبس لمدة لا تزيد على سنة واحدة، وهذه العقوبة، رغم أنها أشد من الصورة البسيطة، تعتبر غير رادعة بشكل كافٍ في سياق جريمة الابتزاز الإلكتروني، فمعظم حالات الابتزاز الإلكتروني تندرج ضمن هذه الصورة المشددة، حيث يهدد الجاني الضحية بإفشاء صور أو معلومات حساسة مخدشة بالشرف، والعقوبة المقررة بسنة واحدة فقط قد لا تشكل رادعاً حقيقياً لمرتكبي هذه الجريمة، خاصة وأن الأرباح التي يجنيها المبتزون قد تكون كبيرة جداً. فالفائدة المالية التي يحصل عليها الجاني قد تفوق بكثير العقوبة السالبة للحرية التي قد يتعرض لها، مما يخلق حالة من عدم التوازن بين الجريمة والعقوبة، وهذا عدم التوازن يقلل من فعالية الردع ويشجع المبتزين على الاستمرار في ارتكاب جرائمهم.

ومن هنا فإننا نأمل من المشرع الليبي أن يعيد النظر في هذا الموضوع بشكل عاجل، فيجب أن يتضمن قانون مكافحة الجرائم الإلكترونية نصوصاً مشددة وخاصة تجرم جريمة الابتزاز الإلكتروني بشكل صريح، وتفرض عقوبات أكثر ردعاً وتناسباً مع خطورة الجريمة وانتشارها الواسع، كما يجب أن تأخذ هذه النصوص في الاعتبار الطبيعة الخاصة للجريمة الإلكترونية وسهولة ارتكابها وتكرارها، وكذلك الأضرار النفسية والاجتماعية الجسيمة التي تلحق بالضحايا، فتشديد العقوبات سيساهم بلا شك بشكل فعال في حماية المجتمع الليبي من هذه الظاهرة الخطيرة والمتنامية.

الفرع الثاني: الشروع في جريمة الابتزاز الإلكتروني

تثير مسألة الشروع في الجرائم الإلكترونية، ومنها جريمة الابتزاز، نقاشاً فقهياً وقانونياً عميقاً، نظراً للطبيعة الخاصة للبيئة الرقمية التي تتميز بالسرعة واختصار المسافة الزمنية والمكانية بين الفعل والنتيجة. وسنتناول هذه المسألة من خلال محورين: النقاش الفقهي حول إمكانية تصوره، عقوبته المقررة قانوناً.

أولا: النقاش الفقهي حول إمكانية تصور الشروع

يدور الجدل الفقهي حول ما إذا كان الشروع متصوراً أصلاً في جريمة الابتزاز الإلكتروني. ويمكن عرض هذا النقاش من خلال اتجاهين رئيسيين:

الاتجاه الأول: صعوبة أو استحالة تصور الشروع

يرى جانب من الفقه، وإن كان مرجوحاً، أن الطبيعة الفورية للجرائم الإلكترونية تجعل من الصعب تصور وجود مسافة زمنية فاصلة بين البدء في التنفيذ وتحقق النتيجة، وهي المسافة التي تمثل "منطقة الشروع". يستند هذا الرأي إلى أن إرسال رسالة تهديد عبر الإنترنت واستلامها من قبل المجني عليه يحدث في أجزاء من الثانية، وبالتالي فإن الجريمة إما أن تقع تامة باكتمال فعل التهديد، أو لا تقع أصلاً. (شتا، 2007، صفحة 115)

وفقاً لهذا المنظور، فإن جريمة الابتزاز هي جريمة شكلية أو جريمة سلوك، تكتمل بمجرد إتيان السلوك المادي (التهديد) بغض النظر عن نتيجته.

الاتجاه الثاني: إمكانية تصور الشروع:

يرد الاتجاه الغالب في الفقه على الرأي السابق بأن جريمة الابتزاز، حتى في شكلها الإلكتروني، ليست مجرد جريمة سلوك، بل هي جريمة ذات نتيجة أو على الأقل جريمة مقيدة بغاية. (علاق، 2024) فالركن المادي لا يكتمل بمجرد إرسال التهديد، بل لا بد أن يكون هذا التهديد مصحوباً بطلب يهدف إلى حمل المجني عليه على القيام بعمل أو الامتناع عنه. فالنتيجة الإجرامية التي يسعى إليها الجاني ليست مجرد إخافة المجني عليه، بل إجباره على التصرف بشكل معين (حسني، 2018، صفحة 1108)

وبناءً على ذلك، فإن المسافة بين البدء في التنفيذ وتحقق هذه النتيجة النهائية موجودة ومتصورة تماماً، وهي التي تسمح بوقوع الشروع. ويمكن تصور ذلك في صور عديدة لا حصر لها، منها:

1. الجريمة الموقوفة : وهي الصورة الكلاسيكية للشروع، حيث يتدخل عامل خارجي يوقف نشاط الجاني رغماً عنه. مثال: أن يبدأ الجاني في كتابة رسالة التهديد وتحميل الصور، ولكن تنقطع خدمة الإنترنت فجأة قبل أن يتمكن من الضغط على زر الإرسال، أو أن تداهم الشرطة المكان وتقبض عليه متلبساً قبل إتمام فعله. هنا، بدأ الجاني في التنفيذ ولكن فعله أُوقف. (علاق، 2024)
2. الجريمة الخائبة : هنا، يقوم الجاني بكل ما في وسعه لإتمام الجريمة، ولكنه يفشل في تحقيق النتيجة لسبب خارج عن إرادته. مثال: أن يرسل الجاني رسالة التهديد بنجاح، ولكن المجني عليه، وبسبب شجاعته أو وعيه القانوني، يرفض الانصياع للطلب ويقوم بإبلاغ السلطات فوراً. في هذه الحالة، أتى الجاني كل نشاطه الإجرامي، ولكن النتيجة (إجبار المجني عليه) لم تتحقق، مما يجعل الجريمة في مرحلة الشروع. (علاق، 2024)
3. الجريمة المستحيلة: كأن يرسل الجاني التهديد إلى عنوان بريد إلكتروني خاطئ أو إلى حساب تم حذفه، فلا تصل الرسالة أبداً إلى المجني عليه المقصود، هنا، استحال تحقيق النتيجة استحالة نسبية تتعلق بموضوع الجريمة، ويعاقب الفاعل على الشروع لأن إرادته الإجرامية قد تجسدت في سلوك مادي لا لبس فيه. (سعيد، 2025، صفحة 292)

يتضح من هذا التحليل أن الشروع ليس فقط متصوراً في جريمة الابتزاز الإلكتروني، بل هو شائع الحدوث في الواقع العملي، وأن القول باستحالته يتجاهل الطبيعة المركبة لهذه الجريمة والغاية التي يسعى إليها الجاني.

ثانيا: عقوبة الشروع في جريمة الابتزاز الإلكتروني

فيما يتعلق بعقوبة الشروع في جريمة الابتزاز الإلكتروني، فإن القانون الليبي لم يفرد نصاً خاصاً لهذه الجريمة، وبالتالي تطبق عليها القواعد العامة المنصوص عليها في قانون العقوبات الليبي. وتحديداً، تطبق أحكام المادة 60 من قانون العقوبات بشأن عقوبة الشروع في الجنايات، والمادة 61 بشأن عقوبة الشروع في الجنح.

وتنص المادة 60 من قانون العقوبات على أنه: "يعاقب على الشروع في الجناية بالعقوبات الآتية إلا إذا نص القانون على خلاف ذلك: بالسجن المؤبد إذا كانت عقوبة الجناية الإعدام، بالسجن الذي لا تقل مدته عن ثماني سنوات إذا كانت عقوبة الجناية السجن المؤبد، وفي الأحوال الأخرى يحكم بعقوبة السجن مع خفض حديها إلى النصف."

وبناءً على هذا النص، فإن تطبيق عقوبة الشروع في جريمة الابتزاز الإلكتروني يتوقف على تصنيف الجريمة الأساسية، فإذا كانت جريمة الابتزاز الإلكترونية تندرج تحت نص المادة 429 من قانون العقوبات (جريمة الإرغام بالعنف أو التهديد)، والتي تتضمن الصورة المشددة بعقوبة السجن لمدة لا تجاوز خمس سنوات (في حالة الحصول على نفع غير مشروع)، فإن عقوبة الشروع في هذه الجريمة ستكون السجن مع خفض حديها إلى النصف، أي أن الحد الأقصى للعقوبة سيكون حوالي سنتين ونصف بدلاً من خمس سنوات.

أما إذا كانت جريمة الابتزاز الإلكترونية تندرج تحت المادة 430 من قانون العقوبات (جريمة التهديد)، والتي تتضمن صورة مشددة بعقوبة الحبس لمدة لا تزيد على سنة واحدة (في حالة التهديد بجريمة أو بإفشاء أمور مخدشة بالشرف)، فإن هذه الجريمة تعتبر جنحة وليست جناية. وفي هذه الحالة، تطبق أحكام المادة 61 من قانون العقوبات، والتي تنص على أنه: "يعاقب على الشروع في الجنح بالعقوبات المقررة للجنحة الكاملة مع خفض حديها إلى النصف."

وبناءً على هذا النص، فإن عقوبة الشروع في جريمة الابتزاز الإلكتروني بموجب المادة 430 ستكون الحبس لمدة لا تزيد على ستة أشهر بدلاً من سنة واحدة. وهذا يعني أن المشرع الليبي قد أقر بمبدأ تخفيف العقوبة في حالة الشروع، مما يعكس إدراكه لأن الشروع في الجريمة يعتبر أقل خطورة من الجريمة التامة، نظراً لعدم تحقق النتيجة الإجرامية بالكامل.

وبالتالي، فإن عقوبة الشروع في جريمة الابتزاز الإلكتروني تتوقف على طبيعة الجريمة الأساسية وتصنيفها كجناية أو جنحة، وعلى الحد الأقصى للعقوبة المقررة لها. وفي جميع الأحوال، فإن عقوبة الشروع ستكون أخف من عقوبة الجريمة التامة، مما يعكس مبدأ التناسب بين الجريمة والعقوبة في القانون الجنائي الليبي.

غير أنه يجدر الملاحظة أن هذا المبدأ العام بشأن تخفيف عقوبة الشروع قد لا يكون مناسباً في سياق جريمة الابتزاز الإلكتروني. فهذه الجريمة تتمتع بخصائص فريدة تجعلها تستحق معاملة تشريعية خاصة، فالشروع في جريمة الابتزاز الإلكتروني قد لا يختلف كثيراً عن الجريمة التامة من حيث الخطورة والضرر النفسي والاجتماعي الذي يلحق بالضحية، فمجرد إرسال التهديدات الأولية والبدء في جمع المعلومات الحساسة قد يسبب ضرراً نفسياً جسيماً للضحية، حتى وإن لم تتحقق الجريمة بالكامل، وعلاوة على ذلك، فإن الطبيعة الإلكترونية للجريمة تسهل تكرار الشروع والعودة إلى محاولة إتمام الجريمة بسهولة، مما يجعل تخفيف العقوبة في حالة الشروع غير فعال كرادع.

وبالتالي، يرى الباحثان أن المشرع الليبي بحاجة إلى إعادة النظر في معاملة الشروع في جريمة الابتزاز الإلكتروني. فيجب أن ينص القانون على أن عقوبة الشروع في هذه الجريمة يجب أن تكون مساوية لعقوبة الجريمة التامة، وذلك نظراً للخطورة الحقيقية لهذه الجريمة على المجتمع الليبي وانتشارها الواسع والمتزايد في الآونة الأخيرة، فالعقوبات المخففة للشروع قد لا تحقق الردع الفعال المطلوب لمواجهة هذه الظاهرة الخطيرة.

المطلب الثاني: المساهمة الجنائية في جريمة الابتزاز الإلكتروني

تتسم جريمة الابتزاز الإلكتروني بطبيعة معقدة ومتشعبة تتطلب غالباً تضافر جهود عدة أشخاص، كل منهم يقوم بدور محدد في تنفيذ الجريمة، فقد يقوم شخص بجمع المعلومات والبيانات الحساسة، وآخر بتصميم البرمجيات الخبيثة والأدوات التقنية، وثالث بالتواصل مع الضحية وتهديده، ورابع بتحويل الأموال وغسيلها، هذا التقسيم المعقد للعمل الإجرامي يثير تساؤلات قانونية عميقة حول كيفية توزيع المسؤولية الجنائية بين المساهمين المختلفين، وهنا تتدخل نظرية المساهمة الجنائية كإطار قانوني شامل لتحديد مسؤولية كل فرد عن النتيجة الإجرامية الواحدة، بناءً على درجة إسهامه وسيطرته على مسار الجريمة ودوره الفعلي في تنفيذها.

الفرع الأول: الفاعل الأصلي في جريمة الابتزاز الإلكتروني

عرّفت المادة 99 من قانون العقوبات الليبي الفاعل بأنه "من يرتكب الجريمة وحده أو مع غيره، أو من يأتي عمداً عملاً من الأعمال المكونة له..."، وتعتبر هذه التعريفات الأساس القانوني لتحديد الفاعل الأصلي، الذي يتمتع بسيطرة مباشرة على تنفيذ الجريمة، وفي جريمة الابتزاز الإلكتروني يمكن تحديد صور الفاعل الأصلي بدقة كالتالي:

1- **الفاعل المنفرد**: هو من يرتكب جريمة الابتزاز بمفرده، دون مساعدة من أحد (فرحات، 2020، صفحة 18)، ومثال ذلك الشخص الذي يخترق حساب الضحية على البريد الإلكتروني أو وسائل التواصل الاجتماعي، يحصل على صور خاصة وحساسة، ثم يهدده بنفسه عبر البريد الإلكتروني أو تطبيقات المراسلة بنشر هذه الصور إن لم يسلم مبلغاً من المال، ويستلم الأموال مباشرة في محفظته الرقمية، أو عبر تحويله إلى حسابه المصرفي، هذا الشخص يعتبر فاعلاً أصلياً لأنه قام بجميع الأعمال المكونة للركن المادي للجريمة بمفرده.
2- **الفاعلون المشاركون:** وهي الصورة الأكثر شيوعاً وانتشاراً في عصابات الابتزاز الإلكترونية والمنظمة، فقد تتكون العصابة من عدة أشخاص، لكل منهم دور محدد ومتخصص يساهم في نجاح العملية الإجرامية (علاق، 2024).
3- **من يأتي عملاً من الأعمال المكونة للجريمة**: هذه الصورة تعالج جريمة الابتزاز كجريمة مركبة تتكون من عدة أعمال متتالية (عطية، 2022)، فإذا قام شخص (أ) بتهديد الضحية بنشر صوره الخاصة، وقام شخص آخر (ب) باستلام الأموال من الضحية بناءً على هذا التهديد، فإن كلاً من (أ) و(ب) يعتبر فاعلاً أصلياً. الأول لأنه أتى بفعل التهديد والإرغام، والثاني لأنه أتى بفعل الحصول على المنفعة المالية، وكلاهما من الأعمال المكونة للركن المادي للجريمة.
4- **الفاعل المعنوي**: تتجلى هذه الصورة بوضوح في جرائم الابتزاز الإلكترونية، خاصة عندما يكون هناك تفاوت كبير في القدرات أو الأهلية بين المساهمين، والمثال على ذلك زعيم عصابة يجبر أحد القاصرين تحت التهديد والضغط النفسي على إنشاء حسابات وهمية وإرسال رسائل الابتزاز للضحايا، فهذا القاصر هو مجرد "أداة" غير مسؤولة جنائياً (بارة، 2022، صفحة 404)، بينما الزعيم هو الفاعل المعنوي الحقيقي؛ لأنه يسيطر سيطرة كاملة على مسار الجريمة من خلال سيطرته المطلقة على إرادة المنفذ والتحكم به.

الفرع الثاني: الشريك في جريمة الابتزاز الإلكتروني

الشريك هو من يساهم في الجريمة دون أن تصل مساهمته إلى حد السيطرة الكاملة على مسارها (محمد، 2020، صفحة 205) وقد حددت المادة 100 من قانون العقوبات الليبي صور الاشتراك في ثلاث حالات رئيسية، وكل حالة لها خصائصها وآثارها القانونية:.

1- **التحريض**: يعرّف التحريض بأنه دفع الغير لارتكاب الجريمة بخلق الفكرة لديه أو تعزيز فكرة موجودة بالفعل (سرور، 2015، صفحة 421). يشترط في التحريض أن يكون مباشراً وفعالاً في دفع الجاني لارتكاب جريمة معينة، وأن تقع الجريمة فعلاً بناءً على هذا التحريض.، والمثال على ذلك أن يعلم شخص أن صديقه يمتلك صوراً خاصة لزميل لهما، فيقوم بإقناعه وتحريضه بشكل مباشر على استغلال هذه الصور وابتزاز الزميل للحصول على المال، إذا قام الصديق فعلاً بالابتزاز بناءً على هذا التحريض، فإن المحرض يعتبر شريكاً في الجريمة بالتحريض.

2- **الاتفاق**: يعرّف الاتفاق بأنه توافق إرادتي شخصين أو أكثر على ارتكاب جريمة معينة. (علاق، 2024) ويشترط أن يكون الاتفاق صريحاً أو ضمنياً، وأن تقع الجريمة فعلاً بناءً على هذا الاتفاق. والمثال على ذلك أن يتفق شخصان (أ) و(ب) على تنفيذ جريمة ابتزاز ضد شركة معينة، ويتقرر أن يقوم (أ) باختراق خوادم الشركة وسرقة بيانات العملاء والمعلومات السرية، وأن يقوم (ب) لاحقاً بالتواصل مع الشركة وتهديدها بتسريب البيانات ما لم تدفع مبلغاً محدداً من المال، وإذا وقعت الجريمة بناء على هذا الاتفاق، فإن كلاً منهما يعتبر شريكاً بالاتفاق.

3- **المساعدة**: تعرّف المساعدة بأنها تقديم العون والدعم للفاعل بوسائل مادية أو معلومات تسهل ارتكاب الجريمة (الغريب، 2003، صفحة 580). وتتخذ المساعدة العديد من الصور في جريمة الابتزاز الإلكتروني منها:

- المساعدة السابقة على الجريمة (أعمال مجهزة): وهي الأعمال التي تسبق الجريمة مباشرة وتهيئ لها.
- المساعدة المعاصرة للجريمة (أعمال مسهلة): وهي الأعمال التي تتزامن مع تنفيذ الجريمة وتسهل من سيرها.
- المساعدة اللاحقة للجريمة (أعمال متممة): وهي الأعمال التي تتم بعد ارتكاب الجريمة وتساهم في إتمامها أو إخفاء آثارها. مثال: شخص يساعد المبتز في عملية غسيل الأموال المحصلة من الجريمة، بأن يستلمها في حسابه البنكي الشخصي ثم يحولها إلى عملات رقمية لإخفاء مصدرها، طالما كان هناك اتفاق مسبق وواضح على ذلك.

أما من حيث عقوبة الشريك في جريمة الابتزاز الإلكتروني فقد نصت الفقرة الأولى من المادة 101 من قانون العقوبات على أن "من اشترك في جريمة فعليه عقوبتها إلا ما استثني قانوناً بنص خاص". هذا النص يقرر مبدأ المساواة الحتمية والكاملة في العقوبة بين الفاعل الأصلي والشريك، فكلاهما يستحق نفس العقوبة المقررة للجريمة، لأن كلاً منهما ساهم بإرادة آثمة واعية في الاعتداء على الحق الذي يحميه القانون.

وقد وضعت المادة 101 بعض الاستثناءات الواردة على عقوبة الشريك وتهدف إلى تحقيق العدالة الحقيقية من خلال مراعاة الظروف الشخصية والموضوعية لكل مساهم وهذه الاستثناءات تتمثل في الآتي :

الاستثناء الأول ـ الأحوال الخاصة بالفاعل (الظروف المادية): نصت الفقرة الثانية من المادة 101 على أنه "لا تأثير على الشريك من الأحوال الخاصة بالفاعل التي تقتضي تغيير وصف الجريمة إذا كان الشريك غير عالم بتلك الأحوال..."

الاستثناء الثاني ـ القصد الجنائي الخاص بالفاعل (الظروف الشخصية):

نصت الفقرة الثالثة من المادة 101 على أنه "إذا تغير وصف الجريمة نظراً إلى قصد الفاعل منها أو كيفية علمه بها يعاقب الشريك بالعقوبة التي يستحقها لو كان قصد الفاعل من الجريمة أو علمه بها كقصد الشريك منها أو علمه بها".

الخاتمة

في نهاية هذا البحث الذي تناولنا فيه بالدراسة والتحليل الأحكام الموضوعية لجريمة الابتزاز الإلكتروني في التشريع الجنائي الليبي، توصلنا إلى مجموعة من النتائج والتوصيات التي نأمل أن تسهم في إثراء النقاش القانوني حول هذه الظاهرة الإجرامية الخطيرة.

أولاً: النتائج

1- رغم صدور قانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2022م، إلا أن المشرع الليبي لم يتضمن هذا القانون نصوصاً صريحة ومتخصصة تجرم جريمة الابتزاز الإلكتروني كجريمة مستقلة. بل يتم الاعتماد على القواعد العامة في قانون العقوبات، وتحديداً المادتين 429 و430، مما يعكس قصوراً تشريعياً واضحاً.

2- تبين أن جريمة الابتزاز الإلكتروني تتميز بخصائص فريدة (عابرة للحدود، صعوبة الإثبات، الأثر النفسي، الرقم المظلم) تجعل من مواجهتها تحدياً كبيراً يتطلب آليات غير تقليدية.

3- تشكل المادتان 429 و430 من قانون العقوبات الليبي الأساس القانوني الوحيد لتجريم الابتزاز الإلكتروني، غير أن العقوبات الواردة فيهما لا تكون كافية للردع في ظل انتشار هذه الجريمة وسهولة ارتكابها.

4- الابتزاز الإلكتروني يتخذ صوراً متعددة (مادي، جنسي، استهداف الأطفال، ابتزاز الشركات)، وكل منها يتطلب معالجة قانونية متخصصة. وترك هذه الجريمة آثاراً نفسية وجسدية مدمرة على الضحايا، تفوق بكثير الآثار المترتبة على الجرائم التقليدية، خاصة عندما يتعلق الأمر بنشر محتوى حميمي أو صور شخصية على الإنترنت.

5- العقوبات المقررة حالياً في التشريع الجنائي الليبي حتى في صورتها المشددة، لا تشكل رادعاً فعالاً للمجرمين، خاصة وأن الأرباح التي يجنيها المبتزون قد تكون كبيرة جداً، وخطر الاكتشاف والملاحقة قد يكون منخفضاً نسبياً.

.ثانياً: التوصيات

بناءً على النتائج التي تم التوصل إليها، نوصي بما يلي:

1- ندعو المشرع الليبي إلى التدخل لتعديل قانون مكافحة الجرائم الإلكترونية ، وذلك بإضافة نص خاص ومستقل يجرم ويعاقب على جريمة الابتزاز الإلكتروني بكافة صورها، ويشدد العقوبة المقررة لها، لما لها من آثار خطيرة على المجتمع الليبي .

2- نوصي المشرع الليبي بإضافة نصوص خاصة في قانون مكافحة الجرائم الإلكترونية تنظم أحكام الشروع والمساهمة الجنائية في الجرائم الإلكترونية، بما يتناسب مع طبيعتها التقنية والعابرة للحدود.

3- نوصي بإطلاق حملات توعية وطنية شاملة عبر وسائل الإعلام المختلفة ومنصات التواصل الاجتماعي، لتوعية كافة فئات المجتمع بمخاطر الابتزاز الإلكتروني وكيفية الوقاية منه، وتشجيع الضحايا على كسر حاجز الصمت والخوف والإبلاغ عن الجرائم التي يتعرضون لها، مع توفير آليات إبلاغ آمنة وسرية.

وختاماً، نأمل أن يكون هذا البحث قد ألقى الضوء على الأبعاد القانونية لهذه الجريمة المعقدة، وأن تكون نتائجه وتوصياته لبنة في صرح الجهود الوطنية لمكافحة الجريمة الإلكترونية وحماية أمن وسلامة المجتمع الليبي.

والله من وراء القصد وهو يهدي السبيل.

قائمة المصادر والمراجع

أولا : الكتب :

1. ابن منظور. (1993). *لسان العرب*. بيروت -لبنان: دار صادر.
2. أبو المعاطي شتا. (2007). *جرائم الحاسب الآلي والإنترنت*. د.د.ن.
3. أحمد فتحي سرور. (2015). *الوسيط في قانون العقوبات: القسم العام*. القاهرة: دار النهضة العربية.
4. الفيروز آبادي. (د.ت). *القاموس المحيط*. د.م: د.ن.
5. أمين مصطفى محمد. (2020). *قانون العقوبات القسم العام*. الاسكندرية: دار المطبوعات الجديدة.
6. إيمان صالح علاق. (2024). "جريمة الابتزاز الإلكتروني في التشريع الليبي". *مجلة الحكمة للدراسات والأبحاث*(العدد 19).
7. تامر محمد صالح. (2018). ابتزاز الإلكتروني، دراسة تحليلية مقارنة. *مجلة كلية الحقوق*.
8. خالد حسن أحمد. (2019). *جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دراسة مقارنة*. الإسكندرية: دار الفكر الجامعي.
9. رمسيس بهنام. (2000). *النظرية العامة للقانون الجنائي*. الإسكندرية: منشأة المعارف.
10. سارة محمد حنش. (2020). *لمسئولية الجزائية عن التهديد عبر الوسائل الالكترونية، رسالة ماجستير*. كلية الحقوق جامعة الشرق الاوسط.
11. طارق ابراهيم دسوقي عطية. (2022). *مسرح الجريمة في ضوء القواعد الاجرائية والأساليب الفنية*. الاسكندرية: دار الجامعة الجديدة.
12. عبد الفتاح بيومي حجازي. (2009). *التجارة الإلكترونية وحمايتها القانونية*. الإسكندرية: دار الفكر الجامعي.
13. علي حمود ومحمود بعيوي. (2020). جرائم الابتزاز الإلكتروني المستحدثة. *مجلة الدراسات القانونية*.
14. كريمة فرحات. (2020). *المساهمة الاصلية في الجريمة، رسالة ماجستير*. الجزائر: كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي.
15. محمد رمضان بارة. (2022). *شرح قانون العقوبات الليبي، القسم العام، الاحكام العامة للجريمة،*. طرابلس: مكتبة الوحدة.
16. محمد رمضان باره. (2014). *شرح قانون العقوبات - القسم الخاص- جرائم الاعتداء على الأشخاص*. طرابلس: مكتبة الوحدة .
17. محمد سلامة الصول. (9، 2024). ظاهرة الابتزاز الإلكتروني في المجتمع الليبي(الأسباب، الآثار، آليات الحد منه). *مجلة علوم التربية*(العدد 17)، الصفحات 234-249.
18. محمد عيد الغريب. (2003). *شرح قانون العقوبات القسم الخاصلنسخة الرابعة وفقاً لأخر التعديلات التشريعية وأحدث الاحكام القضائية*. دار الفكر العربي.
19. محمود فتح الله. (2021). *الجرائم المعلوماتية*. مصر: دار الجامعة الجديدة ،.
20. محمود نجيب حسني. (2018). *شرح قانون العقوبات: القسم الخاص*. القاهرة: دار النهضة العربية.
21. مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية. (2011). *الابتزاز: الأسباب والعلاج*. الرياض- السعودية.
22. منصور عبد السلام عبد الحميد حسان. (2024). جريمة الابتزاز الإلكتروني: دراسة مقارنة. *المجلة القانونية، المجلد 17*(العدد 5).
23. نجاة سالم عبدالرحمن سعيد. (2025). التعدي الإلكتروني والأمن المعلوماتي. *مجلة جامعة الزيتونة، العدد 53*.

References:

1. Ibn Manzur. (1993). Lisan al-Arab. Beirut, Lebanon: Dar Sader.
2. Abu al-Ma'ati Shata. (2007). Computer and Internet Crimes. [Publisher not specified].
3. Ahmed Fathi Sorour. (2015). Al-Wasit fi Qanun al-Uqubat: Al-Qism al-'Amm. Cairo: Dar al-Nahda al-'Arabiya.
4. Al-Fayruzabadi. (n.d.). Al-Qamus al-Muhit. [Place of publication not specified].
5. Amin Mustafa Muhammad. (2020). Qanun al-Uqubat al-Qism al-'Amm. Alexandria: Dar al-Matbu'at al-Jadida.
6. Iman Saleh Alaq. (2024). "The Crime of Electronic Extortion in Libyan Legislation." Al-Hikma Journal for Studies and Research (Issue 19).
7. Tamer Muhammad Saleh. (2018). Electronic Extortion: A Comparative Analytical Study. Journal of the Faculty of Law.
8. Khaled Hassan Ahmed. (2019). Internet Crimes Between Cyber Piracy and Electronic Extortion: A Comparative Study. Alexandria: Dar al-Fikr al-Jami'i.[Note: The last sentence appears to be incomplete and possibly contains errors. It has been omitted.]
9. Ramses Behnam. (2000). General Theory of Criminal Law. Alexandria: Dar Al-Maaref.

10. Sarah Mohamed Hanash. (2020). Criminal Liability for Threats via Electronic Means, Master's Thesis. Faculty of Law, Middle East University.
11. Tarek Ibrahim Desouki Attia. (2022). The Crime Scene in Light of Procedural Rules and Technical Methods. Alexandria: Dar Al-Jami'a Al-Jadeeda.
12. Abdel Fattah Bayoumi Hegazi. (2009). E-Commerce and its Legal Protection. Alexandria: Dar Al-Fikr Al-Jami'i.
13. Ali Hammoud and Mahmoud Ba'awi. (2020). Emerging Cyber Extortion Crimes. Journal of Legal Studies.
14. *Al-Abbar, S. K. (2025). Towards a disciplined mechanism for fatwa on Hajj issues. Al-haq Journal for Sharia and Legal Sciences, 167-184.*
15. Karima Farhat. (2020). Principal Participation in Crime, Master's Thesis. Algeria: Faculty of Law and Political Science, Mohamed El-Bachir El-Ibrahimi University.
16. Mohamed Ramadan Bara. (2022). Explanation of the Libyan Penal Code, General Section, General Provisions of Crime. Tripoli: Al-Wahda Library.
17. Muhammad Ramadan Barah. (2014). Explanation of the Penal Code - Special Section - Crimes of Assault Against Persons. Tripoli: Al-Wahda Library.
18. Muhammad Salama Al-Soul. (9, 2024). The Phenomenon of Electronic Blackmail in Libyan Society (Causes, Effects, and Mechanisms for Reducing It). Journal of Educational Sciences (Issue 17), pp. 234-249.
19. Muhammad Eid Al-Gharib. (2003). Explanation of the Penal Code, Special Section, Fourth Edition, According to the Latest Legislative Amendments and Judicial Rulings. Dar Al-Fikr Al-Arabi.
20. Mahmoud Fathallah. (2021). Cybercrimes. Egypt: Dar Al-Jami'a Al-Jadeeda.
21. Mahmoud Najib Hosni. (2018). Explanation of the Penal Code: Special Section. Cairo: Dar Al-Nahda Al-Arabiya.
22. Researchers Center for Women's Studies in cooperation with the Department of Islamic Culture. (2011). Blackmail: Causes and Treatment. Riyadh, Saudi Arabia.
23. Mansour Abdel Salam Abdel Hamid Hassan. (2024). Cyber Extortion: A Comparative Study. The Legal Journal, Volume 17 (Issue 5).
24. Najat Salem Abdel Rahman Saeed. (2025). Cybercrime and Information Security. Al-Zaytuna University Journal, Issue 53.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **JLABW** and/or the editor(s). **JLABW** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.