Comprehensive Journal of Science
Volume (10), Issue (38), (Dec, 2025)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) ملحق العدد 38 ديسمبر 2025
ردمد: 3014-6266

دور الأمن السيبراني في مكافحة الجرائم المالية والالكترونية

(الابتزاز الإلكتروني الموجه ضد النساء نموذجاً)

عائشة إبراهيم صالح

باحثة دكتوراة جامعة الزيتونة ترهونة - ليبيا

Asaabrahm2@gmail.com

تاريخ الاستلام:2025/12/8 –تاريخ المراجعة: 2025/12/12– تاريخ القبول: 2025/12/19– تاريخ للنشر: 2026 /1/20

الملخص:

تهدف هذه الدراسة إلي التعرف على ماهية الابتزاز الإلكتروني، كأحد أخطر الجرائم الإلكترونية والمالية في العصر الحديث، وبيان الدور الكبير الذي يلعبه الامن السيبراني في مكافحتها كونه أحد الطرق الناجعة للحد منها، بالإضافة الي التطرق لدور التقدم التكنولوجي المتسارع والذي سهّل من ارتكاب هذه الجرائم وبكافة أشكالها، إذ يمكن ان يعد هذا التطور نعمة ونقمة في انٍ واحد، وعليه يمكن القول أن هذه التقنيات الحديثة وإن كانت تحسن كفاءة وجودة العمل وتنمي الابتكار، ألا أنها وفي الوقت نفسه تتسبب في ثغرات امنية كبيرة يمكن استغلالها من المجرمين الإلكترونين، مما جعل الامن السيبراني يواجه تحديات كبيرة وجمة ؛ ولعل ظاهرة الابتزاز الالكتروني للنساء أحد اخطرها وابرزها، فقد غزت المجتمع الليبي فالآونة الأخيرة بشكل مخيف وبأساليب مختلف، فالاستخدام الخاطئ للأنترنت ادي الي ظهور مجموعة من المستخدمين الذين يسعون إلى تكريس جهودهم لتطويع هذه التكنولوجيا لخدمة مصالحهم النفعية من خلال ابتزاز مستخدمي الانترنت، وذلك عبر استخدام أساليب مبتذلة قد تكون عاطفية أو مادية لجر الضحايا؛ وتهديدهم بنشر معلومات محرجة او سرية او تعطيل أنظمة هواتفهم أو حواسيبهم ، وذلك لإجبارهم علي دفع الأموال أو تقديم خدمات أو تحقيق مكاسب غير مشروعة مادية كانت أو معنوية، وتتنوع اساليبهم ما بين برامج الفدية وهجمات حجب الخدمة، وتهديدات نشر المعلومات الشخصية، والتي تبدأ عادة بالاستدراج أو الاختراق، وتنتهي بالتهديد والابتزاز بدفع الأموال، ويذكر انها تتضمن صوراً متعددة منها الابتزاز المالي والعاطفي والاجتماعي، مما يتطلب وعيا أمنياً وقوانين صارمة ، وتعاوناً كبيرا بين الافراد والجهات الأمنية لحماية الأشخاص والممتلكات الرقمية من هذا الخطر المحدق، وذلك من خلال تبليغ الافراد عنها وبشكل فوري، مع حفظ الأدلة.

الكلمات المفتاحية: الجرائم المالية الإلكترونية، الابتزاز الالكتروني، الامن السيبراني، التطور التكنولوجي، الفضاء الرقمي.

Abstract

This study aims to identify the nature of electronic blackmail, as one of the most dangerous cyber and financial crimes in the modern era, and to demonstrate the significant role that cybersecurity plays in combating it, as it is one of the effective ways to reduce it. In addition, it addresses the role of rapid technological progress, which has facilitated the commission of these crimes in all their forms. This development can be considered both a blessing and a curse at the same time. Accordingly, it can be said that while these modern technologies improve the efficiency and quality of work and foster innovation, they also cause significant security vulnerabilities that can be exploited by cybercriminals. This has led to cybersecurity facing numerous and significant challenges. Perhaps the phenomenon of electronic blackmail of women is one of the most dangerous and prominent of these. It has recently invaded Libyan

society in an alarming way and through various methods. The misuse of the internet has led to the emergence of a group of users who seek to dedicate their efforts to adapting this technology to serve their self-serving interests by blackmailing internet users, through the use of vulgar methods that may be emotional or material to lure victims. They threaten victims by publishing embarrassing or confidential information, or by disabling their phone or computer systems, to force them to pay money, provide services, or gain illicit benefits, whether material or otherwise. Their methods vary, ranging from ransomware and distributed denial-of-service attacks to threats of publishing personal information. These tactics typically begin with entrapment or hacking and end with threats and extortion. It's worth noting that these tactics encompass various forms, including financial, emotional, and social blackmail. This necessitates heightened security awareness, strict laws, and close cooperation between individuals and security agencies to protect people and digital assets from this imminent danger. Individuals should report such incidents immediately and preserve evidence.
Keywords: Cybercrime, Cyber Extortion, Cybersecurity, Technological Development, Digital Space

المقدمة:

تطورت الجريمة بتطور نمط حياة الإنسان، فمع هذا التقدم التقني المتسارع وتغير المشهد؛ وازدياد التهديدات مما يجعل الواقع أكثر تعقيدا من إي وقت مضي؛ حيث بلغ هذا التطور أوجه مع تطور التكنولوجيا واستخداماتها، فهذا التطور التكنولوجي السريع ادي الي ازدياد التهديدات السيبرانية وبوتيرة غير مسبوقة.

وتعد ظاهرة الابتزاز الالكتروني أحد المخرجات السيئة لاستخدام التكنولوجيا الحديثة، واستغلال للرقمنة في مجالات مشينة ، حيث تم توظيفها في مجالات غير مشروعة وبأساليب مبتذلة، وذلك عبر الاستدراج والاغراء الالكتروني، ومن خلال جمع المعلومات أو الصور أو الفيديوهات الخاصة بالضحية والتي قد تحتوي علي ممارسات غير أخلاقية، ليتم من خلالها بث الرعب والخوف في نفسية الضحية من الفضيحة التي قد تحلق به جراء نشرها، وأيضا هناك من يتم التغرير بيهم عبر الوسائط الرقمية أو إيقاعهم كضحايا عبر التهديد المباشر بسبب قلة الوعي والتثقيف بهذه الجرائم وكيفية التصرف الصحيح فيها، وعليه يمكن الاستدلال بأن هناك فجوة ثقافية وتوعوية كبيرة في المجتمع ينبغي تداركها، خاصة مع تواجد مجموعة كبيرة من القراصنة الرقميين، وانتشار الأجهزة الرقمية بمختلف أنواعها، وتوافر اشتراكات الانترنت في شتي الأماكن والتجمعات ، مما يزيد من مخاطر الممارسات الخاطئة لهذه التكنولوجيا في مجتمع يعاني أغلبه من (أمية رقمية) ، وفي وقت تتسارع فيه جميع الدول لاستخدام هذه التكنولوجيا، مما يحتم ضرورة تعزيز وتامين الخصوصية للعالم السيبراني، وتوعية المستخدمين من خطورته وعدم مشاركة أي معلومات حساسة أو خاصة ، وذلك لحماية خصوصية الأفراد أثناء استخدام هذه المنصات والبرمجيات المختلفة.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في التعرض لموضوع هام يتمثل في الابتزاز الإلكتروني، باعتباره أحد أخطر الجرائم الالكترونية والمالية في الوقت الحاضر، وبيان مدي خطورة هذه الجرائم والتي اعتبرت جديدة ومستحدثة حيث لم تكن معروفة قط ؛ كما أنها لم تستثني أحد؛ وفي مجالا كبير منها كانت موجهة لفئة النساء؛ والتي تعتبر ذات خصوصية كبيرة في مجتمع مثل مجتمعنا يوصف بالمحافظ ، وذلك في وقت تكاثرت وتعاظمت فيه سريعا جرائم الانترنت، مما يجعل لهذه الجريمة آثار في غاية السوء والخطورة علي الضحايا وذويهم والمجتمع في آن واحد، ، خاصة مع التوسع في استخدام الانترنت والخدمات الرقمية، مما جعلها تشهد نمواً ملحوظاً في الآونة الأخيرة لتلقي بظلالها علي المجتمع بأسره وليس الضحايا فحسب، ومن هنا تبرز أهمية الدراسة والتي تسلط الضوء على جريمة الابتزاز الإلكتروني خاصة الموجه للنساء،

كذلك إبراز الدور الهام للأمن السيبراني لمواجهتها وذلك بالنظر لما تشكله من تهديدا كبير يتطلب الاهتمام والمتابعة من كافة الجهات المختصة.

اهداف الدراسة:

تتجلي أهداف الدراسة في التعرف على ماهية الابتزاز الإلكتروني بصفة عامة، كذلك الابتزاز الموجه للمراءة بصفة خاصة، ايضاً التعرض لأبرز صوره وانواعه والأثار المترتبة عليه، كذلك البنيان القانوني الذي تقوم عليه هذه الجريمة، بالإضافة الي التعرض لدور الامن السيبراني في التصدي لها.

إشكالية الدراسة:

وعلى اعتبار أن هذه الجرائم تنشأ في الفضاء الإلكتروني معتمدة على استغلال التكنولوجيا والفضاء الرقمي، لتبرز ظاهرة خطيرة تهدد كيان المجتمع وأمنه، كونها قد تتعلق بالشرف في كثيرً من الأحيان، وغير متوافقة في ذلك مع خصوصية المجتمع الليبي، وعليه فإن مشكلة الابتزاز الإلكتروني فرضت نفسها كقضية حديثة تواجه المجتمعات باختلاف أعراقها، بحيث أصبحت تشكل تحديا جدياً، يتطلب فهم أبعادها وجوانبها للسيطرة عليها، وذلك لما لهذه الجريمة من انعكاسات خطيرة ليس علي الفرد فحسب بل علي الأسرة والمجتمع ككل، ومن هنا تبرز إشكالية الدراسة في تساؤل رئيس وهو: ما هي تداعيات انتشار هذه الجريمة في مجتمعنا الليبي خصوصا كونه مجتمع يوصف بالمحافظ ؟ وماهي طرق الحماية منه؟ كذلك ما هو دور الامن السيبراني في مواجهتها بالشكل الصحيح والملائم، خاصة وأن هؤلاء المجرمون الإلكترونيون يطورون وباستمرار من تقنياتهم وأدواتهم دائماً ما تكون متجددة، ليستغلوها عند وجود أي ثغرة أمنية؟

ووفقاً للإشكالية المطروحة أعلاه ستعتمد هذه الدراسة على المنهج الوصفي عن طريق وصف وتحديد المفاهيم الرئيسة ذات الصلة بالدراسة، بإضافة إلى المنهج التحليلي وذلك بتحليل النصوص التشريعية وأحكام القضاء المتعلقة بموضوع الدراسة.

وبذلك قمنا بتقسيم خطة البحث على النحو التالي:

المبحث الاول: ماهية الجرائم الإلكترونية والمالية (الابتزاز الإلكتروني)، وتداعياته على المجتمع.

المطلب الاول: ماهية الابتزاز الإلكتروني.

المطلب الثاني: تداعيات الابتزاز الإلكتروني على المجتمع.

المبحث الثاني: البنيان القانوني للابتزاز الإلكتروني ودور الامن السيبراني في مكافحتها.

المطلب الاول: البنيان القانوني الذي تقوم عليه جريمة الابتزاز الإلكتروني

المطلب الثاني: دور الامن السيبراني في مكافحة جريمة الابتزازالالكتروني والتصدي لها.

المبحث الاول

ماهية الجرائم الإلكترونية والمالية [1]

تعد الجريمة الالكترونية بصفة عامة والمالية بصفة خاصة إحدى أهم الأخطار التي تواجه الدول المتقدمة والنامية على حد سواء ، فهي عالمية بلا حدود حيث أن التحقيق فيها والحكم عليها يعد عملية معقدة للغاية، فهي ترتكب من قبل الافراد أكثر مما ترتكب من محترفي الحاسوب وشبكات المعلومات ، كما انها قد ترتكب من قبل منظمات بقصد الحصول الربح أو عن معلومات لمنافسيها، كذلك قد ترتكب عن رسائل اعلام تبحث عن معلومات أو أخبار لتضللها، أو بمقابل مادي ، او من قبل حكومات تبحث عن معلومات حساسة، حيث ان هذه الجرائم تعد خطر مجتمعي متزايد وبشكل متسارع، وهو

[1] ومن وجهتنا المتواضعة نري بأن الامن السيبراني هو الذي يقوم بتطبيق التقنيات او العمليات والضوابط بهدف حماية الانظمة او الشبكات او الحواسيب او البرامج او الأجهزة او البيانات من التعرض للهجمات الالكترونية ويطلق عليه اسم "امن التكنولوجيا أو امن المعلومات التكنولوجية"

ما سنسلط الضوء عليه في هذا المبحث، والذي قسمناه إلي مطلبين بحيث نتناول في المطلب الأول ماهية الجرائم المالية الالكترونية وانواعها، بينما نعرج في الثاني علي دور الامن السيبراني في مكافحة هذه الجرائم، وذلك علي النحو التالي:

المطلب الأول: ماهية الجرائم الإلكترونية والمالية (الابتزاز الإلكتروني).

المطلب الثاني: تداعيات هذه الجريمة على المجتمع وطرق الحماية منه.

المطلب الاول

ماهية الجرائم الإلكترونية والمالية (الابتزاز الإلكتروني).

مع دخول الحاسوب والانترنت إلي مجتمعنا ، وتواجدها في كافة جوانب حياتنا، حيث أتاحت للبشر كثيراً من الخدمات التي لم تكن متاحة من قبل، بحيث وفرت له الوقت والجهد في كثير من المجالات، إلا انها وبالرغم من كل ذلك لها سلبياتها والمتمثلة في تغيير نمط الاجرام ،حيث ابتدأ نوع جديد من الجرائم بالظهور ، وبتهديد الكافة وهو ما يسمي بالجرائم الالكترونية، والتي يعد من ابرز صورها ما يعرف بالابتزاز الإلكتروني والمتمثل في الحديث مع الضحية والتعارف عليه بالتدريج وحتي الوصول الي ما يحتاج اليه، لتهديده وابتزازه حتي الوصول لمبتغاه ، كذلك ظهور ما يعرف بالمجرم الإلكتروني ، والذي استغل بدوره هذه التقنية الحديثة لارتكاب جرائمه، محاولاً الإفلات من العقاب بالتخفي وراء أجهزة الاتصالات الذكية، مما يجعل الحاجة ملحة الي التعريف بهذه الجرائم والتوعية والإرشاد بها وبمخاطرها، كذلك سن وتحديث القوانين والتشريعات اللازمة لمكافحتها نظراً لما تتسب به من خسائر مادية ومعنوية كبيره، باعتبار ان العالم متجه الي الرقمنة بالكامل فانه يتعين على الدولة الليبية أن تتجه لي أن يكون لديها مؤسسة قوية في الامن السيبراني لحماية البيانات والاجهزة المتصلة بشبكة المعلومات والشبكة العالمية الموحدة للحفاظ على أمن وسلامة المعلومات.2

ومن هذا المنطلق وجب علينا ابتداءً التعريف بالجريمة الإلكترونية والمالية، ومن ثم تعريف جريمة الابتزاز الإلكتروني بصفة عامة، والابتزاز الموجه للنساء بصفة خاصة، وتوضيح صورها، والآثار المترتبة عليها، وذلك على النحو التالي:

الفرع الأول . المقصود بالجرائم الإلكترونية والمالية وجريمة الابتزاز الإلكتروني:

الفرع الثاني . تداعيات وإثار الابتزاز الإلكتروني الموجه ضد النساء على المجتمع الليبي.

الفرع الأول

المقصود بالجرائم المالية الالكترونية

وجريمة الابتزاز الإلكتروني

يمكن القول أن هذه الجرائم تستهدف الأنظمة والشبكات والبيانات المالية، وذلك باستخدام التكنولوجيا ، مثل الانترنت والهواتف الذكية والأجهزة الالكترونية الأخرى، وتشمل عدة صور ومنها: جرائم سرقة المعلومات المالية الحساسة ، والاحتيال الالكتروني والتلاعب بالبيانات المالية والابتزاز الالكتروني ،والاحتيال المصرفي الالكتروني والجرائم المتعلقة بالعملات الرقمية ، وغسل الأموال الالكتروني 3وغيرها ، ومن الجدير بالذكر ان هذه الجرائم مجتمعة تشكل ما يعرف بالجرائم المالية الالكترونية ، والتي تعد احد اخطر التهديدات التي تواجه الأشخاص و المؤسسات خاصة المالية منها ذات الطبيعة الحساسة.

ومن هنا بات من الضرورة بمكان إيضاح المقصود منها، خاصة أنها وبطبيعتها متغيرة وغير ثابتة بحيث يمكن وصفها، فضلا عن صعوبة إيجاد تعريف يمكن أن يغطي كافة صورها، لذا سنحاول جاهدين أن نلم شعثه؟؟ في النطاق

[2] د. أحمد فاروق زاهر الجريمة المنظمة، ماهيتها وخصائصها واركانها بمركز الدراسات والبحوث، اكاديمية نايف للعلوم الاكاديمية، الرياض، السعودية،2007، ص21.

[3] قانون رقم 2 لسنة 2005، بشأن مكافحة غسيل الاموال، متوافر على الرابط التالي:
Security.legislation.lyتاريخ الزيارة 2025.12.15 الساعة 10:10 مساءاً.

الذي تتطلبه الدراسة فضلا عن تبيان المقصود بالابتزاز الإلكتروني بصفة عامة، والابتزاز الموجه للنساء بصفة خاصة، وأبرز صورهِ من حيث الوقوع، وذلك على النحو التالي:

اولاً. تعريف الجريمة المالية الالكترونية:

نظراً لحداثة هذه الجريمة فإن فقهاء القانون لم يتفقوا على تعريف موحد لها، اذ لايزال الخلاف حول تعريفها قائماً، كما لم يقم غالبية مشرعي القانون ومنهم المشرع الليبي، بوضع تعريف محدد وبدقة لها، مما جعلنا نتعرض الي اهم التعاريف الفقهية لهذه الجريمة والتي من أهمها:

التعريف القائل بأنها (السلوك الاجرامي الذي يتم ارتكابه باستخدام تقنيات الحاسوب سواء كان هذا الاستخدام قد تم بشكل مباشر او غير مباشر، أو كان يستهدف بجريمته تلك التقنيات فتكون محل الجريمة.)4

وعرفت كذلك بأنها: (الجرائم التي يتم فيها استخدام وسائل التكنولوجيا الحديثة وشبكة الانترنت للاستيلاء على أموال يكون لها علاقة المصرف من المصارف، او متحصل عليها عن طريق إحدى الخدمات التي يقدمها المصرف لعملائه.)5

وتعتبر هذه الجرائم من أخطر الظواهر الاجرامية التي عرفها العالم في القرن الأخير، حيث أن لها تداعيات وخيمة على مستوي الافراد والدولة، وذلك في حال ما وجهت هذه الهجمات الي الأسواق المالية او المصرفية في البلاد، مما قد يودي الي تدمير اقتصادها، كذلك يمكن ان توثر على الامن القومي للدولة، وذلك من خلال إمكانية اختراق أنظمتها الأمنية حيث يمكن للمهاجمين الالكترونيين، اختراق الأنظمة الأمنية والمالية، مما قد يؤدي الي الوصول لمعلومات حساسة6.

وتتم هذه الجريمة من خلال مهاجمة الجاني لنظام المعلومات الخاص بالمصرف، سواء عن طريق شن هجوم خارجي كإرسال كم من الطلبات على نظام المصرف او حتى الفرد العادي بحيث لا يمكنه ان يتحملها، فيتوقف من عمله بما يسهل على الجاني الهجوم والاستيلاء على قاعدة المعلومات7 أو البيانات لهذا الشخص او تلك الجهة، أو أن يقوم بزراعة برامج التجسس على قاعده بيانات أي مؤسسة من المؤسسات خاصة المالية منها ليصل إلى حسابات العملاء ويتلاعب فيها، مما يعطيه الفرصة للاستيلاء على مبالغ مالية ضخمة.

ثانياً. تعريف الابتزاز الالكتروني:

أن للتطور التكنولوجي محاسنه الكثيرة، إلا أنه وبالرغم من هذه المزايا فإن له مساوي تعيبه، ولعل أبرز هذه المساوي هو الاستخدام غير المشروع لأوجه هذا التطور ووسائله المستحدثة، وذلك بتسخير هذه الوسائل الالكترونية الحديثة لارتكاب الجرائم المختلفة، ومنها الابتزاز الإلكتروني والذي يعد أحد اخطر الجرائم الرقمية التي تهدد الافراد والمجتمعات في العصر الحديث، كونه يعتمد علي استغلال معلومات أو صور شخصية لابتزاز الضحية مالياً او عاطفياً او اجتماعياً ، بحيث أصبحت تشكل تهديداً كبيراً خاصة لفئات الشباب والأطفال، وتعتبر جريمة الابتزاز من الجرائم المستحدثة ، ويطلق عليها في علم الجريمة "الجرائم الناعمة" كونها تخلو من العنف وعليه سنتناول المقصود بالابتزاز الإلكتروني لغة ، واصطلاحاً ،وقانوناً وذلك علي لنحو التالي:

أ. التعريف اللغوي: الابتزاز لغة جاء من المصدر "إبتزَ" بتشديد الزاء، أي محاولة الحصول على المال والمنافع من شخص تحت التهديد بفضح بعض اسراره او غير ذلك، كذلك هو إي سلب أو انتزاع الشي بالقوة أو الحيلة، ويقال "أبتز المال " أي اخذ عنوة او غصباً او بمكر وخداع، وجمعها ابزاز بمعني السلاح8.

---

4 عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر،2002، ج1، ص1.

5 الجرائم الالكترونية المصرفية- مقال متوفر على الرابط التالي: https: lljordan.lawe.com

6 محمد فتحي عيد، الاجرام المعاصر، الطبعة الاولي، اكاديمية نايف العربية للعلوم الامنية، الرياض،1999، ص124.

7 نهله عبد القادر، الجرائم المعلوماتية، دار الثقافة للنشر، عمان، الاردن، الطبعة الاولي،2008، ص49.

8 معجم المعاني الجامع، معجم عربي بتصرف، متوافر على الرابط التالي: https:ll www.almaany.com تاريخ الزيارة 24.12.2025، الساعة 5.30 مساءً.

ب . التعريف الفقهي: تتعدد المفاهيم الفقهية للابتزاز حيث عرفه جانب من الفقهاء: بأنه (اخذ شيء من شخص بغير رضاه، أي أن يسخر مجرم طاقاته وابداعاته لارتكاب جرم سواء تعلق به شخصياً من باب الانتقام او تعلق بأناس يدفعون له مقابل تنفيذه ما يطلبون، وهنا يتدخل الجانب التقني، إذ تشكل الاتصالات الحديثة من حاسوب وبرامج وشبكات، أدوات تنفيذ للجريمة الإلكترونية). 9

ويذكر في هذا المجال أن محكمة النقض المصرية لم تقدم تعريفاً محدداً ومباشراً للابتزاز الإلكتروني، بل ارست مبادئ قضائية تؤكد عليه، وقد قضت في هذا الشأن بقولها (ان التهديد والتشهير عن الطريق الالكتروني للحصول على مقابل يشكل جريمة ابتزاز)10 فالهدف منها هو الحصول على مكاسب غير مشروعة، عبر التهديد بنشر معلومات شخصية أو صور أو مواد حساسة مقابل المال او خدمات غير قانونية، او معلومات سريه خاصة بشخص او شركة أو مؤسسة او يحدث هذا الابتزاز باستدراج الضحايا عن طريق روابط وهمية11، او عن طريق البريد الالكتروني، أو مواقع التواصل الاجتماعي، والتي أصبحت تستخدم اليوم من قبل جميع الفئات العمرية.

ج . التعريف القانوني للابتزاز: وبحسب قانون مكافحة الجرائم الالكترونية رقم 5 لسنة 2022 بشأن مكافحة الجرائم الالكترونية فهي (كل فعل يستخدم فيه الجاني وسائل تقنية المعلومات او الشبكات الالكترونية لتهديد شخص او الضغط عليه للحصول على مكاسب غير مشروعة.) 12

كما عرفها القانون المصري في المادة 375مكرر من قانون العقوبات المصري بأنه: (يعاقب بالحبس مدة لا تقل عن سنة كل من قام بنفسه او بواسطة الغير باستعراض القوة أو التلويح بالعنف او التهديد باءيهما او استخدامه ضد المجني عليه أو مع زوجه أو أحد اصوله أو فروعه، وذلك بقصد ترويعه أو التخويف بالحاق أي اذي مادي او معنوي به أو الإضرار بممتلكاته أو سلب ماله أو الحصول على منفعة.)

كذلك عرفها القانون السعودي بموجب قانون مكافحة الجرائم المعلوماتية أين السنة التي أصدر بها القانون بأنها: (تهديد الشخص بنشر معلومات خاصة او الحاق الضرر به، أو بفضح أمور مخلة بالشرف، لإجباره على القيام بفعل معين او الامتناع عنه مثل: دفع المال؛ او تقديم الخدمات؛ او إقامة علاقة.) 13.

الفرع الثاني . الابتزاز الإلكتروني الموجه ضد النساء واسبابه.

أن ظاهرة الابتزاز الإلكتروني تعتبر من أكثر أنواع الجرائم الإلكترونية انتشاراً في الوقت الحاضر في مجتمعنا، حيث تتم باستخدام الفضاء الإلكتروني، ويتضح من خلال البحث والتقصي ان أحد أبرز أنواع الابتزاز شيوعاً في المجتمع هو ابتزاز النساء، وترجع ظاهرة الابتزاز الإلكتروني في المجتمع الليبي الي أسباب عديدة لعل أبرزها الجهل بالتكنولوجيا وطرق التعامل معها، وضعف الوازع الديني، كما يتضح ايضاً من خلال البحث ان أكثر الدوافع وراء الابتزاز هو الدافع المالي والمادي بالدرجة الأولى، ومن الحري بالذكر ان أبرز الجرائم الإلكترونية والمالية واكثرها وقوعا على ارض الواقع هو جريمة الابتزاز الإلكتروني، وعليه سنتعرض في هذا المقام لجريمة الابتزاز الإلكتروني الموجه ضد النساء، والأسباب الدافعة اليه تباعاً وعلي النحو التالي:

---

9 د. حمود بن خميس النوفلي، الآثار الاجتماعية للابتزاز الإلكتروني، ندوة حول الابتزاز الإلكتروني بين التوعية والتجريم، المعهد العالي للقضاء، سلطنة عمان،2019، ص22.

10 طعن جنائي مصري رقم 17036لسنة 91 قضائية متوافر عبر الرابط:http\\ www>youm7>com

11 محمد سلامه الصول، ظاهرة الابتزاز الإلكتروني في المجتمع الليبي، مجلة علوم التربية، العدد السابع عشر، ص240.

12 قانون رقم 5 لسنة 2022ف بشأن مكافحة الجرائم الالكترونية، متوفر على الرابط التالي:
https://lawsociety.ly، بتاريخ الزيارة: 15-12-2025 الساعة 10:00 مساءاً

13 نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي رقم 17 لسنة 1428 المادة 3: منه متوافر عبر الرابط الالكتروني smwalinsaf.com تاريخ الزيارة يوم 25.12. 2025.الساعة9.30. مساءً.

اولاً. جريمة الابتزاز الإلكتروني الموجه ضد النساء: يعد انتشار منصات التواصل الاجتماعي بالنسبة للنساء سلاح ذو حدين، إذ ومنذ ظهور هذه المنصات استخدمتها العديد من النساء للتعبير عن أنفسهن؛ وذلك للدفاع عن حقوقهن والمطالبة بها، كما استخدمتها نساءً اخريات كوسيلة للتكسب الشريف وكمصدر للرزق، وباعتبار وسائل التواصل الاجتماعي والانترنت منصة يسهل الوصول اليها، مما يجعلهن عرضة للتحرش عبر الانترنت او الوقوع كضحايا بسببه.

حيث تكون المراءة المستخدمة لشبكات التواصل الاجتماعي يومياً، عرضة للابتزاز أكثر من النساء اللواتي لا يستخدمن الانترنت، ويعد الابتزاز الإلكتروني شكل من اشكال العنف الرقمي، حيث يقوم شخص ما بتهديد المراءة بنشر معلومات عنها او صور أو فيديوهات خاصة بها ، اذ لم تنفذ ما يريده ، ومن الجدير بالذكر في هذا المقام أن الابتزاز الإلكتروني قد يؤدي إلى عواقب وخيمة علي الضحية والأسرة والمجتمع في ذات الوقت، ومن ذلك الضرر النفسي الذي قد يلحق بالضحية ، إضافة الي الضرر الاجتماعي للأسرة بل وللمجتمع بأسره، يضاف اليهما الضرر المادي والمتجسد في المقابل المادي والذي قد يكون كبيرا ومبالغاً فيه.

ثانياً. الأسباب الدافعة للابتزاز الإلكتروني الموجه ضد النساء: ولعل أبرز أسبابه ودوافعه إضافة إلي الأسباب المادية، محاولة تشويه السمعة، وتراجع منظومة القيم الأخلاقية والاجتماعية الراسخة في المجتمع، والتي يمكن أن نلخصها في النقاط الاتية:

أ. ضعف الوازع الديني: أن من أكثر العوامل المؤدية لارتكاب الجرائم عامة، وهذه الجريمة خاصة، هو البعد عن الله وضعف الالتزام بالواجبات الدينية والعبادات، وعدم الرضا من بعض الأشخاص بما رزقهم الله فيتجهون للأجرام كمحاولة لتحقيق الكسب السريع، مع عدم وجود الإحساس بالرقيب أو الحسيب في التصرفات او الأفعال والسلوكيات، وقلة الوعي بمراقبة الله تعالي لنا في كل تصرفاتنا، كذلك عدم وجود مراقبة شخصية للشخص من اسرته، مما يجعله معتاد علي المحرمات وغير مكترث بها ، وربما يفاخر بها ،مما يشجع كثير من ضعاف النفوس للاقتداء به، والإقدام علي ارتكاب نفس السلوك ونشره.

ب .العوامل الاقتصادية: حيث تلعب الجوانب الاقتصادية دوراً هاماً ومحركا لسلوك هؤلاء المجرمون الالكترونيون، إذ تعد سبباً رئيسا في الابتزاز الإلكتروني، والذي يكون في أغلبه لأسباب مادية محضة، فالمبتز المنحرف غالباً ما يدفعه الي اللجوء للابتزاز هو الرغبة في الحصول على الأموال من الضحية، وذلك لتحقيق الثراء السريع باقل جهد، ويكون ذلك من خلال تهديد المبتز للضحية واستغلاله إياه للاستسلام لرغباته في دفع مبالغ مالية له، أو القيام بأعمال غير مشروعة ،او الدخول في علاقة غير شرعية، أو تقديم تنازلات غير أخلاقية مقابل امتناعه عن نشر محادثات أو صور أو فيديوهات سرية او خاصة بالضحية، سبق وإن تحصل عليها الجاني بطرق متعددة .

ج . تشويه سمعة الضحية: إذ قد يكون هدف المبتز هو تشويه سمعة الفتاة وإثارة الفتنة والمشاكل لها، سواء في داخل الأسرة أو بين الأصدقاء، كما قد يكون الهدف منه تحقيق غايات عدائية او تجسسية، بحيث يجبر المبتز الضحية على تقديم معلومات سرية تتعلق بعملها او مؤسستها، مما يضر بمصلحة الجهة المستهدفة. 14

المطلب الثاني

تداعيات واثار الابتزاز الإلكتروني الموجه ضد النساء على المجتمع الليبي.

كثيرا ما نجد أن أغلب ضحايا هذه الظاهرة هم من فئة النساء وخاصة الفتيات المراهقات، ويعتبر هذا النوع منتشر وبشكل كبير في المجتمع الليبي في الآونة الأخيرة، وهو النموذج الأكثر وقوعاً للجريمة، خاصة إذ كان مرتكبها رجلاً، إذ وفي كثير من الأحيان تبدأ العلاقة بين الطرفين بالثقة التامة التي تتزين من خلالها العاطفة والحب والحنان، بحث يقوم الجاني بعد التعرف علي الفتاة والتواصل معها واكتساب ثقتها ، فتنشأ تلك العلاقة الوهمية بإغراء الضحية ليتبين في ما بعد أنه يستغلها

14 تتنوع أسباب الابتزاز الإلكتروني ما بين الدوافع المادية " طلب المال او الفدية" والأخلاقية "الضغط او طلب الخول في علاقة غير مشروعة او التشهير، او لابتزاز الهوية الشخصية وذلك بسرقة البيانات الشخصية او الحسابات البنكية.

للحصول علي معلومات او وثائق او مستندات او صور خاصة، أو مقاطع خادشه فيها ما يسيء للفتاة، ومن ثم يقوم بتهديدها وابتزازها ، بأنها إذ لم تقم بتلبية مطالبه المادية أو الجنسية، فانه سيقوم بنشر هذه المحادثات علناً، وكثيراً ما تلجأ الفتاة إلى الامتثال لهذه المطالب ، خوفاً من الفضيحة والتشهير بها، وفضحها أمام أهلها وأقاربها، بل وامام المجتمع بأسره، وعليه سوف نسلط الضوء في هذا المطلب علي تداعيات هذه الجريمة على المجتمع الليبي في فرعاً اول ، ونعرج علي ابرز الاثار المترتبة عليها في الفرع الثاني، وذلك علي النحو التالي:

الفرع الأول . تداعيات الابتزاز الإلكتروني الموجه ضد النساء على المجتمع الليبي.

الفرع الثاني . أنواع الابتزاز الإلكتروني.

الفرع الأول

تداعيات والاثار المترتبة على الابتزاز الإلكتروني

للابتزاز إلكتروني تداعيات خطيرة على الفرد والمجتمع، كما أن له اثاراً مدمرة على الفرد تشمل ضغوطاً نفسية هائلة من قلق وخوف واكتئاب قد تصل بالمرء للانتحار، من جراء تهديدات للأضرار بسمعته، أو المطالبة بمبلغ مادية تفوق قدرته، مما قد يدفعه لارتكاب جرائم اخري.

كما أنه يشكل انتهاكاً صارخاً للخصوصية الأشخاص؛ وذلك باختراق أجهزتهم بواسطة روابط مشبوهة أو مزيفة؛ قد يكلف مجرد النقر عليها ثمناً باهضاً، مما يؤدي إلى فقدان الثقة في الفضاء الإلكتروني ، كما انه يهدد المجتمع بتفكك الأسر وانتشار الجريمة وازدياد معدلاتها، مما من شأنه تهديد أمن واستقرار المجتمع، مما يتطلب وعياً مجتمعياً وجهوداً حكومية للتوعية بمخاطر مثل هذه الجرائم والتي تهدد المجتمع في عمقه ، فالابتزاز وخاصة الموجه ضد النساء له مخاطر كبيرة لا تهدد الضحية فحسب بل الاسرة والمجتمع بأكمله ، كون المجتمع الليبي مجتمع محافظ ، وأكثر الجرائم فيه تعقيدا هي تلك المتعلقة بالشرف ، وللنساء فيه مكانة مقدسة لا يمكن تجاوزها، وعليه يتعين تعاون و تكاثف كافة الجهود، للتوعية والتثقيف بهذه الأخطار المحدقة والمتزايدة ، وذلك بالتبليغ فوراً على هذه الجرائم وتوفير الحماية للضحايا، ولعل أبرز هذه التداعيات وعلي مستوي الفرد والمجتمع ما سنتناوله وعلي النحو التالي:

اولاً . تداعيات الابتزاز على الفرد:

أ . التداعيات النفسية: يسبب الابتزاز الالكتروني الموجه للأشخاص أضرارًا نفسية مدمرة، تتمثل في القلق المستمر، والاكتئاب، وارتفاع نسب الانتحار، والشعور بالعجز نتيجة السيطرة على إرادته من طرف المبتز، كذلك انعدام الثقة في النفس والتصرفات، جراء انتهاك الخصوصية والتهديد بنشر معلومات حساسة او صور وفيديوهات خاصة، مما يخرق حقوق الفرد الشخصية، ويؤدي إلى اضرار جسيمة قد تصل بالشخص لإنهاء حياته للتخلص من هذه الضغوطات.

ب . التداعيات الاجتماعية: يؤدي الابتزاز الالكتروني بالشخص الي العزلة من جراء تدمير سمعته؛ كما قد تؤدي الي التفكك الاسري؛ بسبب الضغوط على الأفراد خاصة إذ كانت أمراءه، فكثيراً ما طلق الرجل زوجته أو ضربها او حتي يقتلها بسبب الفضيحة ، سواء كانت بذنب او بدون ذنب ونتيجة للاستخدام الخاطئ للوسائل التواصل الاجتماعي مما نتج عنه هذا الابتزاز الإلكتروني ، وما ينتج عن هذا التفكك من اضرار كبيرة تتجاوز الاسرة للمجتمع في مجموعه، ليتحول افرادها الي اشخاص منحرفين ومجرمين، لا يقتصر ضررهم على أنفسهم فحسب بل على المجتمع باسره، فبدل من انشاء جيل سوي يكون منتج ومفيد للمجتمع، ننشي جيلاً معرض للانحراف والاجرام.

ج . التداعيات المادية: ينتج عن الابتزاز الإلكتروني وفي أغلب الأحيان، خسائر مالية مباشرة نتيجة الدفع للشخص المبتز، سواء تمثل الدفع في الفدية او مقابل خدمات غير مشروعة، او غيرها من المطالب والتي تكون في أغلبها مادية محضة.

ثانياً . تداعيات الابتزاز الإلكتروني على المجتمع:

أ. انتشار معدلات الجريمة: إذ قد يدفع الابتزاز بالشخص لارتكاب جريمة ما كان ليقدم على ارتكابها لولا هذا المبتز، مما من شأنه ازدياد معدلات الجريمة، من سرقة واحتيال، واغتصاب وقتل وغيرها من الاعتداءات الماسة بأمن المجتمع واستقراره.

ب . فقدان الثقة: تؤدي الاختراقات وعدم الوعي بمخاطر الانترنت والاستخدام الخاطئ له، الي فقدان الثقة في وسائل التواصل الاجتماعي والمنصات الرقمية بشكل عام، من قبل الأشخاص في وقت تتجه فيه اغلب الدول الي التكنولوجيا في شتي نواحي الحياة مما يحتم على الناس استخدامها، وعليه وجب توعيتهم بكيفية الاستخدام الصحيح لها، وتنبييهم بمخاطرها وتجنب النقر على الروابط الوهمية أو المشبوهة المصدر، وتجنب التعامل مع الأشخاص الغرباء وأيا كانوا لاحتمال أن يكونوا مخترقين أي مجرمون الإلكترونيون.

ج . التهديد الأمني: 15 فاستغلال هؤلاء المجرمون الإلكترونيون لأي ثغرات أمنية، أو ابتزازهم لأشخاص يعملون في جهات حساسة بالدولة، قد يؤدي إلى الوصول لمعلومات حساسة وحيوية، مما من شأنه التأثير على استقرار المجتمع وامنه.

الفرع الثاني

انواع الابتزاز الإلكتروني

بعد ما بينا اثار وتداعيات التي يخلفها الابتزاز الإلكتروني يتضح لنا أن للابتزاز أنواع متعددة، تختلف باختلاف الطريقة والهدف من حيث كل نوع من هذه الأنواع، فقد يكون مادياً او عاطفياً وفي بعض الأحيان يكون ابتزاز للمطالبة بفدية، وايضاً الابتزاز الجنسي والاجتماعي والوظيفي، نوجزها وذلك على النحو التالي:

الابتزاز المالي: ويتجسد في مطالبة المبتز من الضحية بدفع مبالغ مالية مقابل عدم نشر معلومات خاصة او حساسة، او فيديوهات أو صورة شخصية، وهو النوع الشائع للاحتيال على الأشخاص وخاصة النساء، ذلك باختراق او سرقة بياناتهم.

الابتزاز العاطفي: وتتمثل في قيام المبتز باستغلال مشاعر الضحية بعلاقات عاطفية زائفة، ليتمكن خلال هذه الفترة من الحصول علي أكبر قدر من الأسرار والمعلومات الشخصية أو المستندات أو صور وفيديوهات خاصة، وتهديده بنشر الصور ومقاطع الفيديو عبر وسائل التواصل الاجتماعي في حال لم يستجب لمطالبه.

الابتزاز الجنسي: حيث يتم من خلاله استدراج الضحية لاماكن مشبوهة وتصويرها داخلها والتهديد بمشاركة هذه الصور والمقاطع الحساسة ذات الطبيعة الجنسية، بحيث يتمكن فيما بعد من ابتزاز الضحية، بأفعال غير أخلاقية مثل الأشياء الإباحية أو الأنشطة الجنسية، كما قد يستخدم هؤلاء المبتزون او المجرمون الإلكترونيون التقنيات الحديثة، كالذكاء الاصطناعي لإنشاء صور ومقاطع مفبركة لإقناع الضحية بالخضوع لمطالبهم.

الابتزاز الوظيفي: ويتجسد هذا النوع في تهديد الموظف بنشر معلومات قد تؤثر على مستقبله الوظيفي مالم ينفذ مطالب معينة، بحيث يكون مصدر هذا التهديد مدير فاسد أو زميل عمل غير نزيه. 16

المبحث الثاني

البنيان القانوني لجريمة الابتزاز الإلكتروني ودور الامن السيبراني في مكافحتها

مع الاعتماد المتزايد في حياتنا اليومية على الأنظمة الإلكترونية، والأجهزة المتصلة بالشبكة العالمية للمعلومات، وتشعب عمل هذه الأجهزة من هواتف خلوية وأجهزه حوسبة شخصية مما يزداد معه عدد المتصلين بالفضاء السيبراني؛ وتزداد معه احتمالات الاعتداءات والجريمة؛ ومع وجود حوادث تتمثل في اختراق الأنظمة وسرقة البيانات وتسربها، واستغلالها

---

[15] . لعل أبرز أنواع التهديدات السيبرانية الأكثر شيوعاً، والمتمثلة في البرمجيات الخبيثة، الفيروسات، برامج الفدية، برامج التجسس، احصنة طروادة، التصيد الاحتيالي، هجمات الحرمان من الخدمة، هجمات الوسيط، الحقن، استغلال الثغرات غير المكتشفة.

[16]. ماهي أنواع الابتزاز الإلكتروني؟ وكيف نتعامل معها، مقال الإلكتروني متوافر عبر الرابط الإلكتروني: cyperone.co تاريخ الزيارة 25.12.2025، الساعة 10.00مساءً.

فيما بعد والتهديد بها، حيث أن كل فعل من هذه الأفعال يشكل قد جريمة أو يدخل في البناء القانوني لها، فالمعلومات التي تضخ وتنساب وتحفظ في الفضاء السيبراني وعبره، متعلقة بأسرار الأشخاص وحياتهم الخاصة التي لا ينبغي باي حال من الأحوال اختراقها والعبث بها ، إذ تعتبر هامة وماسه بكل شخص معنى بهذا الفضاء وبدون استثناء، مما يجعل الحفاظ عليها وعلى سريتها من أهم الاخطار[17]، فالحفاظ عليها وسلامتها ضرورة قصوي لا يمكن الاستغناء عنها ، وهنا يبرز الأمن السيبراني كحجر الزاوية الذي يرتكز عليها لتحقيق استقرار واستمرارية في هذا العالم المترابط، ومن هذا المنطلق سوف نقسم هذا المبحث الي مطلبين نتناول في الأول البنيان القانوني لجريمة الابتزاز الإلكتروني، ونسلط الضوء في المطلب الثاني علي دور الامن السيبراني في مكافحتها وذلك علي النحو التالي:

المطلب الأول . البنيان القانوني الذي تقوم عليه جريمة الابتزاز الإلكتروني.

المطلب الثاني . دور الامن السيبراني في مكافحة جريمة الابتزاز الإلكتروني والتصدي لها.

المطلب الاول

البنيان القانوني الذي تقوم عليه جريمة الابتزاز الإلكتروني

الابتزاز الإلكتروني والذي يتم عبر الوسائل الإلكترونية هو نوع من أنواع تهديد الأشخاص والضغط عليهم، بهدف ابتزازه اجباره على القيام بفعل او الامتناع عنه، وتقتضي هذه الجريمة وجود شخصين فأكثر، بحيث يكون أحدهما الجاني والآخر المجني عليه، وبالرغم من حداثة عهدها الا انها في الأساس والاركان شانها شأن سائر الجرائم الأخرى.

ولقيام جريمة الابتزاز الإلكتروني، ينبغي توافر الأركان المطلوبة في كل جريمة، كي تصبح معاقباً عليها، والمتمثلة في الركن الشرعي، والمتمثل في الركن الشرعي وهو وجود النص القانوني الذي يحدد الفعل المجرم والجزاء الجنائي، أما الركن المادي فهو كل ما يدخل في كيان جريمة الابتزاز الالكتروني، وتكون له طبيعة مادية ملموسة سواء كان فعلاً أو امتناعاً، والركن المعنوي لها يعتبر داخلياً كامناً في نفسية الجاني، وبهذا المعني والاتجاه سنعني بالبحث في هذه الأركان المكونة لجريمة الابتزاز وفق ثلاث فروع، وذلك علي النحو التالي: **الفرع الأول . الركن الشرعي**

الفرع الثاني . الركن المادي

الفرع الثالث . الركن المعنوي

الفرع الأول

الركن الشرعي

وهو النص الجنائي لجريمة الابتزاز والذي بموجبه جرم الفعل استناداً لمبدأ "لا جريمة ولا عقوبة الإ بنص" قانوني يجرم هذا الفعل أو النشاط، المادة الاولي من قانون العقوبات الليبي، وعليه يعد الفعل مجرماً استنادا لما نص عليه قانون مكافحة الجرائم الإلكترونية رقم 5 لسنة 2022والتي نصت على انه " كل فعل يستخدم خلاله الجاني وسائل تقنية المعلومات او الشبكات الإلكترونية لتهديد شخص او الضغط عليه للحصول على مكاسب غير مشروع."

ويذكر أن الشارع الليبي قد أولى أهمية بالغة لخصوصية الافراد بحيث اعتبر الاعتداء عليها جريمة شانها في ذلك شأن سائر الجرائم الأخرى، حيث ان الجانب الأخلاقي هو اول ما قد تستهدفه جريمة الابتزاز الإلكتروني والذي يعد من اهم جوانب الحياة في المجتمع الليبي والذي طالما اعتز بمبادئه وأخلاقه وقيمه الفاضلة، ولذا اعتبر هذا الفعل جريمة ورتب عليها أقسي العقوبات كونها كفيلة وحدها بتدمير حياة الضحية، أو تفكيك عائلته، وافقاده الانتماء لمجتمعه.

[17] برايح ـ هدي، مرابط حبيبة، التحول الرقمي وأثره على الجرائم المالية (التحديات والحلول القانونية)، مجلة القانون الدستوري والمؤسسات السياسية، العدد2 ،2025، ص231.

ويعد التشريع الليبي من بين عدة تشريعات عربية عنيت بتجريم الافعال المادية المكونة لجريمة الابتزاز، واتجهت إلى إصدار قوانين خاصة لضمان تجريم الابتزاز الإلكتروني بكافة صوره، ووضع ركن شرعي لها ومن بينها التشريع الجزائري والمصري والسعودي وغيرها.

الفرع الثاني

الركن المادي

ويتمثل الركن المادي للجريمة في السلوك الذي تظهر به إلى حيز الوجود أو للعالم الخارجي، فهو يبرز الجريمة ويجعلها تخرج إلى العالم الخارجي، ولا تختلف جريمة الابتزاز الالكتروني في أركانها عن جريمة الابتزاز التقليدي، فهي تتطلب سلوك اجرامي يصدر عن الجاني سواء بالقول أو بالفعل أو بالكتابة او أي شي آخر قد يمثل تهديداً بنشر البيانات أو الصور أو المعلومات او مقاطع فيديو للضحية.

فالركن المادي في هذه الجريمة يتمثل في تهديد الشخص بفعل معين أو الامتناع وبشكل غير قانوني، أي كانت طريقته سواء كان بالفعل أو القول أو الكتابة، كالتهديد بنشر معلومات او بيانات سرية او صور وفيديوهات خاصة وحساسة، وغيرها من الأفعال أو التصرفات التي تبدأ بها الجريمة، إذ ترتبط طبيعة الركن المادي في هذه الجريمة باستخدام الأدوات والتقنيات لارتكاب الجريمة، غير ان المشكلة الأساسية التي يثيرها هذا السلوك الاجرامي هو أن الوقائع المادية المكونة له غير واضحة، ويصعب اكتشافها بخلاف الجرائم العادية، فهي تتطلب سلوك اجرامي يتم عبر وسائل التواصل الاجتماعي او الحاسب الالي وان يعتبر تهديداً سواء بالقول أو بالكتابة أو بالرموز أو صور أو إشعارات من شانها إلقاء الرعب والخوف في نفس الضحية، ولا يهم ما إذ كان الجاني ينوي تنفيذ الأمر المهدد به أم لا ، بل يشترط فقط أن يكون التهديد جدياً وليس هزل ، ويقوم الركن المادي في هذه الجريمة بعديد الصور ومنها:

الابتزاز بالصور والفيديوهات: بحيث يتم تهديد الشخص بنشر الصور ومقاطع الفيديو الخاصة به، حقيقية كانت أم مفبركة، مالم يتم تنفيذ طلب معين من الضحية.

الابتزاز بالمحادثات الخاصة: ويتجسد فيه السلوك الاجرامي بالقيام باستغلال رسائل او تسجيلات صوتية خاصة وحساسة، للحصول على مقابل مادي أو معنوي أو لغاية غير مشروعة، في حال لم يقم الشخص بتلبية مطالب المبتز.

ابتزاز التشهير: ويتخذ فيه السلوك الاجرامي مظهر التهديد الموجه للشخص بنشر شائعات عنه، او معلومات سيئة تسيء بسمعته او شرفه، سواءً كانت هذه المعلومات صحيحة أو كاذبة.

الفرع الثالث

الركن المعنوي

تتطلب جريمة الابتزاز الإلكتروني لقيامها ركناً معنوياً إلى جانب الركن الشرعي والمادي لها، فهي تعد من الجرائم العمدية التي يلزم ان يتوافر فيها القصد الجنائي العام والتي لا يتصور ان تكون الا عمدية، وذلك بان تنصرف إرادة الجاني الي ارتكاب الفعل المادي مع العلم بأن القانون يمنعه ويعاقب عليه.

فجريمة الابتزاز الإلكتروني بطبيعتها تأبى أن تكون إلا كذلك، مما يوجب توافر القصد الجنائي العام إلي جانب القصد الجنائي الخاص، ويقصد من ذلك أن القصد الجنائي العام يتوافر بمجرد الاتجاه لارتكاب هذه الجريمة من العلم بخطورتها.

بمعني أنه يلزم ان يعلم الجاني بنتيجة السلوك الذي اقترفه وأن ينصب علمه على ان ما يقوم به، من حصوله على الصور الفاضحة وبيانات سرية ومعلومات حساسة لأحد الأشخاص هو لتهديده بها مقابل الحصول أموال او منفعة وانه يعد جريمة معاقب عليها.

كذلك وإلي جانب علم الجاني بسلوكه يلزم توافر عنصر آخر حتى تتحقق الجريمة، وهو أن تكون إرادته منصرفة الي السلوك الاجرامي، مع توقع النتيجة الاجرامية في الوقت نفسه، وإلى جانب هذا القصد الجنائي العام يلزم توافر قصد جنائي خاص يتمثل في أن يكون الهدف أو النية من هذه الجريمة هو الحصول علي منفعة أو أموال أو أعمال غير مشروعة، وقد قضت في هذا الشأن محكمة النقض المصرية بأنه: " تقوم جريمة الابتزاز والتهديد علي قصد خاص ، يتمثل في إرغام المجني عليه علي أداء مبلغ من المال أو القيام بفعل أو الامتناع عنه، ويجب اثبات هذا القصد اثباتاً يقينياً".. 18

المطلب الثاني

دور الأمن السيبراني 19

في مكافحة جريمة الابتزاز الإلكتروني والتصدي لها.

تشهد ليبيا تحول رقمياً سريعاً، أصبح فيه الامن السيبراني ضرورة ملحة لحماية الأفراد والأنظمة الرقمية والبيانات الحساسة من اي هجمات الإلكترونية محتملة، قد تهدد الافراد او حتي المؤسسات، مما يجعل البلاد تواجه تحديات كبيره وغير مسبوقة في مجال تعزيز الامن السيبراني، خاصه انها تفتقر إلى الخطط الأمنية المتكاملة لحماية البيانات او المعلومات الرقمية، مما قد يسهم في سهولة وسرعة اختراق البيانات الخاصة بالاشخاص وسرقتها واستخدامها في اعمال غير مشروعة ، كابتزازهم وتهديدهم بها، للحصول علي أموال أو أي منفعة أخري، خاصة مع ازدياد هذه الأعمال في الآونة الأخيرة وبشكل مطرد، كذلك كثرة وانتشار المجرمون الإلكترونيون مما يتطلب وجود أمن سيبراني قوي لمواجهة هذه الهجمات السيبرانية المتزايدة والخطيرة ، إذ يمكن القول إن المؤسسات في ليبيا غير جاهزة لمواجهة هذه التهديدات، مثل هجمات الفدية وهجمات ديدوس، والتي تعتبر من بين أخطر الهجمات التي لا يقتصر تهديدها للأمان الرقمي فحسب، بل وبسمعة المؤسسات الوطنية جمعاء.

ويذكر أن الامن السيبراني يلعب دوراً محورياً وهاماً في مكافحة الابتزاز الإلكتروني؛ وذلك عبر حماية وتأمين الانظمة والبيانات، اذ ومع التحول الرقمي والاتجاه نحو النماذج الرقمية والإلكترونية في أغلب مجالات الحياة، مما يؤدي إلي تنامى التهديدات بشكل متسارع أكثر من أي وقت مضي.

وعليه فانه يتعين تجاوز الأساليب التقليدية المتبعة لأمن البيانات والمعلومات وأكثر من أي وقت مضي، مما يدفع الجميع افراداً ومؤسسات بان يكون كلاً منهم سباق في إنشاء أنظمة حماية وتامين لكافة البيانات أو المعلومات الخاصة به ضد أي هجمات الالكترونية متوقعة.20

فالأمن السيبراني في بلادنا يحتاج الي وقفة جادة من مؤسسات قوية تنفذ العقوبات على القراصنة والمخترقين بحيث تضم فنيين في مجال الآمن، كذلك خبراء في الانترنت يتعاونون لإقامة نظام حماية فعال، ولتنسيق الجهود كافة لمكافحة اي هجمات الإلكترونية، ويضاف الي ذلك ضرورة تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية العابرة للحدود21، ومن هنا يمكن القول بأن للأمن السيبرني مزايا عديدة لا يمكن انكارها باي حال من الأحوال ، بحيث توفر حماية أكثر للأفراد،

---

[18]. طعن جنائي مصري، رقم 6943 لسنة 63 قضائية، جلسة 6.5. 1996

[19] الامن السيبراني: أهمية الحماية البيانات في العصر الرقمي مقال متوفر عبر الرابط تاريخ الزيارة 12.16 2015 :https//sphills.com 7:30 صباحا

[20] الامن السيبراني في العصر الرقمي، التحديات والاستراتيجيات، مقال الالكتروني متوافر عبر الرابط التالي: https: \\ khalieah>com تاريخ زيارة الموقع 16.12. 2025 الساعة 12.40 دقيقه مساءً.

[21] ومن الجدير بالذكر ان ليبيا قد احتلت في العام 2023 المرتبة 90 عالمياً في الامن السيبراني، بمعدل 28.78 على مؤشر الامن السيبراني العالمي، حيث تم الكشف عن الثغرات عندما ادي هجوم سيبراني في مايو 2023 الي اختراق بيانات العملاء في قطاع الاتصالات، بما في ذلك المعلومات المالية وجوازات سفر المستخدمين، أشار اليه البيبسي، اية، تطور التهديدات السيبرانية في 2025، فهم التحديات الرقمية، متوافر عبر الرابط: lipyanspider>comتاريخ الزيارة 16.122025 الساعة 7.21صباحاً.

وعليه سنسلط الضوء في هذا المطلب علي أهم ميزات الأمن السيبراني وفق الفرع الأول، في حين نتطرق من خلال المطلب الثاني إلي كيفية الحماية من هذه الجريمة، وذلك علي النحو الاتي:

الفرع الأول . ميزات الامن السيبراني.

الفرع الثاني . كيفية الحماية من الابتزاز الإلكتروني.

الفرع الأول

ميزات الامن السيبراني

إذ يمكن القول إن الأمن السيبراني أصبح اليوم ضرورة لا غنى عنها، في عالم يعتمد بشكل متزايد على التقنية، فتعزيز الأمن السيبراني يمكننا من حماية بياناتنا وخصوصيتنا وأمننا القومي من التهديدات الإلكترونية المتزايدة، سواء كنا إفراداً او شركات او مؤسسات أو حكومات، فميزاته تجعله ضرورياً في عالمنا الرقمي، ولعل أبرز هذه الميزات: –

. حماية البيانات الشخصية والعامة:

فالأمن السيبراني يساعد في حماية البيانات الشخصية للمستخدمين، مثل المعلومات المصرفية أو كلمات المرور والبيانات الخاصة، بالإضافة إلى ذلك يحمي البيانات العامة للشركات من الاختراقات التي قد تؤدى إلى خسائر مالية كبيرة، وذلك باعتماد انظمه كشف التسلل، والتشفير.22

– ضمان استمرارية الاعمال ومنع الهجمات:

إذ ومن خلال تعزيز الأمن السيبراني يمكن للشركات والمؤسسات ضمان استمرارية أعمالها دون انقطاع بسبب الهجمات الإلكترونية، وهذا يساعد في الحفاظ على سمعة المؤسسة وثقة العملاء، حيث تساعد الاستراتيجيات الأمنية القوية في منع انقطاع العمليات، وتقليل وقت التوقف عن العمل، وحماية الإنتاجية، وضمان استمرار تقديم الخدمات، مما يحمي سمعة المؤسسات، ويحافظ على إيراداتها وأموالها من خلال الاستجابة السريعة للهجمات والتعافي منها.

. تعزيز الثقة في التقنية:

عندما يكون الأمن السيبراني قوياً، تزداد ثقة المستخدمين في استخدام التقنية والخدمات الرقمية، وهذا يشجع على تبني المزيد من الابتكارات التقنية التي تعتمد على الانترنت، كما أنه يوفر حماية للمعاملات المالية عبر الانترنت والتطبيقات المصرفية مما من شأنه حماية حسابات العملاء وبياناتهم من الاحتيال.

. التوعية وبناء القدرات:

ويكون ذلك بتثقيف المستخدمين، وزيادة الوعي عندهم حول مخاطر التصيد الاحتيالي، والروابط المشبوهة، لحماية الإفراد والمؤسسات من أي ثغرات قد تتواجد لديهم، كذلك تدريب المختصين، وتطوير مهاراتهم في مجال الأمن السيبراني لمواجهة التهديدات المتطورة.23

وعليه يتعين علينا تطوير استراتيجيتنا الوطنية للأمن السيبراني على مستوى الدولة، وتحديث البنية التحتية الرقمية لتواكب التطورات الدولية في هذا المجال، كذلك تظهر الحاجة الماسة على ضرورة توعية المسؤولين في كافة المؤسسات بأهمية الأمن السيبراني، حيث لا يزال يعتبره البعض من الوظائف الثانوية رغم الأضرار الكبيرة التي قد تنجم عن إغفاله.

---

[22] نذكر ان معهد ماساتشوستس للتقنية قام في العام 1983، باعتماد أول نظام الاتصالات يعتمد على التشفير، ليصبح أساساً لتطوير تقنيات الامن السيبراني الحديث.

[23] شاتر، دانيال بشروش، جولي ربيع وول، نحو تعريف أكثر تمثيلاً للأمن، مجلة الطب الشرعي الرقمية، المجلد3، العدد3 , يوليو 2017، ص196

الفرع الثاني
كيفية الحماية من الابتزاز الإلكتروني

وفيما يتعلق بكيفية الحماية من الابتزاز الإلكتروني، يمكن الإشارة الي انه قد انتشرت في الآونة الأخيرة هذه الجريمة وبكثرة، مما يدعو الي التساؤل عن كيفية حماية الشخص لنفسه وبنفسه، إذ يعد أحد أبرز أسبابها وجود ثغرات في نظام الأمان، نتيجة لإهمال تحديث برامج الحماية وأنظمة التشغيل، كذلك قلة الوعي الأمني لدي الافراد، وتجاهلهم لمشكلات الأمان الأساسية، وعليه يمكن إجمال النقاط التي قد تضمن الحماية من مخاطر الجرائم الالكترونية بصفة عامة في مجموعة من الأسباب لعل أهمها ما نوجزه فيما يلي:

اولاً. الحماية من التعرض لابتزاز الإلكتروني:

– استعمال كلمات مرور قوية للحسابات الالكترونية؛ حيث يعد استخدام كلمات مرور قوية من أفضل الإجراءات لحماية الحسابات الإلكترونية من الاختراق والانتهاك، كذلك ضرورة تحديثها باستمرار، وتجنب النقر على الروابط المشبوهة أو مجهولة المصدر.

. عدم فتح رسائل البريد الكتروني والمرفقات العشوائية الغير موثوقة مطلقا، حيث يعمد الجاني الي إرسال ملفات قد تسبب بالأضرار في الجهاز المحمول او الجهاز اللوحي.

. عدم مشاركة المعلومات الشخصية الخاصة مع أي شخص غير معروف، إذ يعد من أهم اجراءات الحماية من جرائم الاحتيال الإلكتروني هو عدم مشاركة أي معلومات الشخصية مع شخص غريب.

. مراقبة البيانات المصرفية، إذ يتعين وفي حال وقوع الشخص كضحيه لجريمة الالكترونية أن يقوم مباشرةً بمراقبه البيانات المصرفية.

– الابلاغ عن الجرائم الإلكترونية مباشره فور وقوعها، سواء كان للشرطة أو الهيئة المختصة بهذه الجرائم

ثانياً . طرق الوقاية من الجرائم المالية الالكترونية:

ويعد من أبرز طرق الوقاية من هذه الجريمة 24، وصدها قبل وقوعها، بعض الاجراءات التي وإن كانت بسيطة إلا أنها غاية في الأهمية ومنها:

– خدمات أمان للأنترنت، حيث أن هناك العديد من الشركات التي تقدم خدمات للأفراد أو المؤسسات تتمثل في برامج كاملة لحماية شبكة الانترنت الخاصة بالفرد أو المؤسسة، مما من شأنه تحقيق أمان تام للجميع، من خلال ما تحققه هذه الإجراءات من الحماية والوقاية من هذه البرامج الضارة.

– استخدام كلمات مرور قوية مع الحرص على أن تكون سرية بأن تتكون على الاقل من 10 أحرف، أو الأرقام او رموز، وجعلها معقده بحيث لا يمكن تخطيها او تخمينها بسهولة.

. تحديث البرامج باستمرار، إذ كثيراً ما يستخدم المخترقون والمهكرون عبر الانترنت الثغرات في البرامج، والتغلغل من خلالها، لذلك يتعين على الشخص أن يكون حريصاً على تحديث أنظمة التشغيل الخاصة به، وبرامج الامان وباستمرار

.المحافظة على الخصوصية، إذ غالباً ما يصل المجرمون الالكترونيون للمعلومات الشخصية الخاصة بالشخص من خلال عدد قليل من نقاط البيانات، لذلك يتعين على كل شخص ألا ينشر الكثير من معلوماته الخاصة، ويحافظ على هذه المعلومات سرية ومغلقة.

[24] Katrina.mykil. c.Atriad. confiden tiality.ntgrity.Availabity.gournal of compul;ny and security.intheorelicolly amd piaclee634.31

– تجنب استخدام الأجهزة العامة للأعمال الخاصة، فعند القيام بهذه الاعمال الخاصة والشخصية والتي قد تكون حساسة وخاصة، وعليه يفضل أن تكون في الاجهزة خاصة بالشخص نفسه، والابتعاد عن تلك العامة فيما يتعلق بها.

الخاتمة:

بعد الانتهاء من هذه الدراسة يتضح لنا مدى التهديد الكبير الذي تشكله هذه الجريمة وعلى الكافة، أفراد أو مؤسسات فواقع هذه الجرائم معقد ومتعدد الاوجه ، وله تبعات ونتائج خطيرة أن لم تكبح جماحها، كما أن لها تداعيات خطيرة ومدمرة علي المجتمع بأسره، وتشتمل اضراراً نفسية واجتماعية ومادية جسيمة ، وهو ما يتطلب ضرورة مواجهتها بحلول قانونية حازمة، كذلك التعامل بجدية معها، من خلال تعزيز قدرة الأمن السيبراني ،كذلك بتبني إستراتيجيات فعالة ومتطورة لصد أي تهديدات جديدة او محتملة، ومن جانب اخر ضرورة التوعية والتثقيف بمخاطر هذه الجريمة ، من حيث كيفية تجنبها وعدم الوقوع فيها، أو بالإبلاغ عنها فورًا حال وقوعها وعدم الرضوخ لإرادة المبتز، وبالمحصلة خلصت هذه الدراسة الي مجموعة من النتائج التي توصلنا اليها، وانتهت بجملة من التوصيات نوردها فيما يلي :

اولاً . النتائج:

1. ان الابتزاز هو محاولة لتحصيل مكاسب او منافع مادية او معنوية او جنسية من الضحايا؛ وذلك من خلال التهديد والضغط والاكراه والمساومة، بفضح ونشر معلومات او صور او فيديوهات خاصة، من شأنها تحقير الشخص وإهانته اما عائلته ومجتمعه؟ إعادة صياغة، ويذكر ان هذا التهديد قد يكون مباشراً وقد يكون غير مباشر.

2- أن أهم الأسباب وراء الابتزاز هو ضعف الوازع الديني لدي الشخص، وابتعاده عن تعاليم الدين الإسلامي السمحة، والتي تحثنا محاسن الاخلاق، فالابتعاد عن الدين وكثرة الاختلاط ورفاق السوء والرد على الاتصالات المشبوهة والتجاوب مع أصحابها ومنحه الثقة، كلها أسباب، وتؤدي في نهاية المطاف لعواقب وخيمة.

3. إن دوافع الابتزاز مختلفة ولكنها في مجملها غير أخلاقية وغير مشروعة، فقد تكون مادية أو نفسية أو جنسية أو لمصالح أخري غير مشروعة، مما يرتب آثاراً نفسية واجتماعية خطيرة على الفرد والمجتمع.

4. تعد مكافحة هذه الجرائم خطوة هامة نحو حماية المجتمع الليبي من مخاطر الفضاء الالكتروني، إذ يتعين ضمان حماية استخدام شبكة المعلومات ووسائل التقنية الحديثة بشكل مشروع، للحفاظ على النظام العام، وضمان عدم الإساءة للآخرين أو الاضرار بهم أو استغلالهم، ولكن تبقي فاعلية القانون مرتبطة دائما بوعي المواطنين، كذلك بتعاونهم مع الجهات المختصة.

ثانياً. التوصيات:

1. نهيب بالمشرع الليبي بضرورة إعادة النظر في النصوص القانونية، ومحاولة سد أي ثغرات قد توجد بها وذلك من خلال إعداد واعتماد تشريع متكامل لمواجهة هذه الجريمة وإيجاد قانون يطبق علي المخترقون سواء كانوا في البلاد أو خارجها، بحيث ينالوا جزأهم أينما كانوا، فقد لوحظ أن المجرمون الالكترونيون غالبًا ما يفضلون العمل في الدول التي تفتقر إلي وجود قوانين وتشريعات قوية وصارمة ، حتي يفلتوا من العقاب ، يضاف إليه ضرورة تحديثه وبشكل مستمر لضمان فاعليته ومواكبته لاي تطور مصاحب لهذا الاجرام، فالتطور التقني والتكنولوجي المتسارع ينبغي أن يصاحبه تطور مستمر في المجال التشريعي والأمني والقضائي.

2. نري بضرورة تكثيف التوعية المجتمعية حول مخاطر هذا النوع من الاجرام وخطورته على الافراد والمجتمع وعلى حد سواء، اذ يعد من أبرز أسبابها الجهل بها او اهمالها، ومن ذلك وجود ضعف او ثغرات في الأنظمة، نتيجة إهمال تحديث برامج الحماية وأنظمة التشغيل، كذلك تجاهلهم لمشكلات الأمان الأساسية كضرورة تحديث كلمات المرور وتجنب النقر على الروابط المشبوهة او مجهولة المصدر.

3. نوصي بتهيئة وتعيين مختصين لهم الخبرة في مجال التقنية الحديثة والتكنولوجيا، كذلك ارسالهم لدورات وندوات وملتقيات دولية للاستفادة من تجارب الدولة خاصة تلك المتقدمة في هذا المجال، ايضاً وضع ميزانيات تتناسب مع تحسين الخدمات الرقمية، كونها موضوع حساس قد يصل الي حد المساس بالمجتمع باسره.

4. كما نوصي بتبني أساليب عقابية مشددة وقاسية تتماشي مع هذا الصنف الخطير من الاجرام، وحتى تكون رادعة وكفيلة بالترهيب منها، لضمان عدم العودة اليها

قائمة المراجع:

اولاً: الكتب العربية:

1- المؤمني – نهلا عبد القادر، الجرائم المعلوماتية، دار الثقافة للنشر. عمان، الاردن، الطبعة الأولى، 2008.

2 حجازي – عبد الفتاح – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، ج1، 2002.

3 زاهر – أحمد فاروق، الجريمة المنظمة وماهيتها وخصائصها واركانها، مركز الراسات والبحوث الاكاديمية، اكاديمية نايف للعلوم الأمنية، الرياض، السعودية، 2007.

4 عيد . محمد فتحي، الاجرام المعاصر، اكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، الطبعة الاولى، 1999.

ثانياً. من المراجع الاجنبية.

1- Katrina may Kil CIA Triad Confidentiality Intgrity. Availability. Journal of Computing and security intheoretically and practice-634.31

ثالثاً . البحوث والمجلات والدوريات:

1.. النوفلي . حمود بن خميس، الاثار الاجتماعية للابتزاز الإلكتروني، ندوة حول الابتزاز الإلكتروني بين التوعية والتجريم، المعهد العالي للقضاء، سلطنة عمان،2019.

2. الصول . محمد سلامة، ظاهرة الابتزاز الالكتروني في المجتمع الليبي، مجلة علو التربية، العدد السابع عشر.

3. برايح . هدي، المرابط . حبيبة، التحول الرقمي وأثره على الجرائم المالية (التحديات والحلول القانونية)، مجلة القانون الدستوري والمؤسسات السياسية، العدد الثاني، 2025.

4. شاتر. دانيال بشروش، جولي . ربيع وول، نحو تعريفاً أكثر تمثيلا للأمن، مجلة الطب الشرعي الرقمية، المجلد الثالث، العدد الثالث 2017.

رابعاً. الشبكة العنكبوتية:

1. الجرائم الإلكترونية المصرفية، مقال متوفر عبر الرابط التالي: hitts;gordan lawer.com

2. الامن السيبراني في العصر الرقمي ، التحديات ،و الاستراتيجيات، مقال متوفر عبر الرابط التالي: https; llkhaleah.com.

3. ما هو مستقبل الامن السيبراني، الاكاديمية البريطانية للتدريب والتطوير، مقال الإلكتروني متوفر عبر الرابط التالي: batdacademy.

4. البيبيسي . أية، تطور التهديدات السيبرانية في عام 2025، فهم التحديات الرقمية متوفر عبر الرابط الإلكتروني التالي: Libyan spider.com.

5. الامن السيبراني، أهمية حماية البيانات في العصر الرقمي، مقال متوفر عبر الرابط الإلكتروني التالي: httpsll spskills.

6. معجم المعاني الجامع، معجم عربي بتصرف، متوافر على الرابط التالي: https: ll www.almaany.com تاريخ الزيارة 24.12.2025، الساعة 5.30 مساءً.

7. ماهي أنواع الابتزاز الإلكتروني؟ وكيف نتعامل معها، مقال الإلكتروني متوافر عبر الرابط الإلكتروني: cyperone.co، تاريخ الزيارة 25.12.2025، الساعة 10.00مساءً.

خامساً. التشريعات:

1. قانون رقم 5 لسنه 2022 بشأن مكافحة الجرائم الالكترونية، متوفر على الربط التالي https: ll Law society. Ly:

2 قانون رقم 2 لسنة 2005 بشأن مكافحة غسيل الاموال متوافر عبر الرابط التالي: Security – Leyi. Lation. Ly.

3. نظام مكافحة الجرائم المعلوماتية، المرسوم الملكي رقم 17 لسنة 1428 هجري، متوافر عبر الرابط الالكتروني smwalinsaf.com

سادساً . الاحكام القضائية:

1. مجموعة أحكام محكمة النقض المصرية متوافر عبر الرابط التالي: https//;www.youm7.com