جريمة الابتزاز الالكتروني في النظام السعودي "دراسة تحليلية"

The Crime of Electronic Blackmail in Saudi Law
"An Analytical Study"

إعداد

الدكتور/ افضال السيد صديق كردمان

استاذ مساعد – كلية الشريعة والأنظمة – جامعة الطائف

المملكة العربية السعودية

البريد الإلكتروني : afdalkrdaman@gmail.com

١٩- جريمة الابتزاز الالكتروني في النظام السعودي

ملخص البحث

تعد جريمة الابتزاز الالكتروني احدى الجرائم الإلكترونية الحديثة التي تهدد حياة الأفراد والمجتمع نسبة للاستخدام السيء للشبكة المعلوماتية أو الحاسب الآلي أو مواقع التواصل الاجتماعي. فجريمة الابتزاز الالكتروني في النظام السعودي يقصد بها الدخول غير المشروع لتهديد أو ابتزاز الشخص لحمله على القيام بعمل أو الامتناع عن عمل ولو كان هذا القيام بالعمل أو الامتناع عن العمل مشروعاً. وتتمثل أهمية البحث في أهمية وخطورة جريمة الابتزاز الالكتروني وذلك من خلال تهديد الجاني وتخويفه للمجني عليه أو الضحية بنشر صور، أو مقاطع فديو، أو تسجيلات صوتية، أو معلومات شخصية على شبكة الانترنت مالم يحصل على منفعة مادية أو معنوية أو غير أخلاقية. ويهدف البحث إلى حماية المجني عليهم ضحايا هذه الجريمة من الوقوع فيها وتشويه سمعتهم. حيث إن مشكلة البحث تكمن في ضعف الرقابة على مواقع الشبكة المعلوماتية المختلفة وفرض سيطرة الجاني المبتز على الضحية بما يمتلكه تحت يده تهديداً للضحية من اجل تحقيق المنفعة غير المشروعة، إضافة لصعوبة اثبات جريمة الابتزاز الالكتروني وعدم كفاية وعي الضحايا بتقديم شكواهم لملاحقة الجناة وضبطهم وردع هذه الجريمة. وتوصل البحث الى نتيجة مفادها إن جريمة الابتزاز الالكتروني لها طبيعة خاصة من حيث الأركان والعقوبة تتطلب بيان طرق اثباتها وكيفية التعامل معها بالدراسة التحليلية وفق أحكام النظام السعودي. ويوصي البحث بتشديد عقوبة جريمة الابتزاز على المبتز ومساعدة الضحية بتقديم شكواها بكل سرية ويسر عبر وسيلة تبليغ موحدة لبث الطمأنينة في نفس الضحية وملاحقة المبتز ومكافحة الجريمة.

الكلمات المفتاحية:

ابتزاز الكتروني، تهديد، منفعة مادية أو معنوية، المبتز، الضحية ، نشر، شبكة المعلوماتية، مواقع التواصل الاجتماعي.

Abstract:

Cyber blackmail is a modern cybercrime that threatens the lives of individuals and society due to the misuse of the internet, computers, or social media. Under the Saudi system, cyber blackmail refers to unauthorized access to a computer or social networking site to threaten or blackmail someone into doing or abstaining from doing something, even if doing or abstaining from doing something is legal. The importance of this research lies in the importance and seriousness of cyber blackmail, which involves threatening and intimidating the victim by publishing photos, video clips, audio recordings, or personal information online unless they receive a material, moral, or immoral benefit. The research aims to protect victims of this crime from falling victim to it and having their reputations tarnished. The problem with this research lies in the weak oversight of various internet sites and the blackmailer's control over the victim, using the

information they possess to threaten them to achieve an illegal benefit. This is in addition to the difficulty of proving cyber blackmail and the lack of awareness among victims to file complaints, prosecute and apprehend the perpetrators, and deter this crime. The study concluded that the crime of electronic blackmail has a unique nature in terms of its elements and penalty, requiring a detailed explanation of the methods of proof and how to deal with it, based on the provisions of the Saudi legal system. The study recommends imposing harsher penalties for blackmailing the blackmailer and assisting victims by submitting their complaints confidentially and easily via a unified reporting method to reassure victims, prosecute the blackmailer, and combat the crime.

Keywords:

Electronic blackmail / Threat / Material or moral benefit / Blackmailer / Victim / Publication / Information network / social media.

مقدمة:

الجريمة هي ظاهرة اجتماعية قديمة، ومع التطور العلمي والتقني ظهرت أنماط جديدة من الجرائم وأبرزها جريمة الابتزاز الإلكتروني والتي يتخذ فيها الجاني أو المبتز من الوسائل الإلكترونية ما من شأنه أن يهدد ويخوف به المجني عليه وهو ضحية الجريمة بنشر صور، أو مقاطع فديو، أو تسجيلات صوتية، أو اسرار شخصية مقابل الحصول على منفعة مادية أو معنوية أو إقامة علاقة غير مشروعة. لا ننكر أن في عالم التحول الرقمي الذي نشهده اليوم يلجأ الكثير من الأفراد إلى تخزين أسرارهم الشخصية على أجهزة الحاسب الآلي أو الهواتف الذكية مستخدمين في ذلك شبكة الانترنت والتطبيقات الالكترونية ومواقع التواصل الاجتماعية المتاحة بغية الحفاظ عليها بعيداً عن أي اعتداء. وبالرغم من المزايا التي توفرها هذه الوسائط الالكترونية إلا أن الواقع العملي يشير إلى وقوع كثير من الأفراد ضحايا لجريمة انتهاك الخصوصية والحريات مقابل الطمع أو الجشع أو الانتقام أو حتى التشهير بسمعة الأبرياء. وتؤكد الشريعة الاسلامية ان مفهوم الابتزاز متعلق بالتسبب بالحرج لشخص ما من النواحي الاجتماعية او الاسرية او الأدبية، والذي يشمل مفهوم الفضيحة وتشويه السمعة والتهديد للضحية من خلال الضغط عليه وإجباره على القيام بأفعال خارجة عن ارادته، ومنافية لطبيعته، ولدينه، وأخلاقه. لذلك يحرص المنظم السعودي الجنائي في نظام مكافحة جرائم المعلوماتية، وكذلك المجتمع الدولي على التعاون لمكافحة جريمة الابتزاز الالكتروني والحد من خطورتها وتفشيها وملاحقة الجناة ومعاقبتهم نسبة لخصوصية الجريمة من حيث أركانها وعقوبتها وطرق اثباتها وكيفية التعامل معها.

مشكلة البحث:

تكمن مشكلة البحث في إن جريمة الابتزاز الالكتروني أصبحت ظاهرة اجتماعية فرضت نفسها خاصة في ظل عدم وجود تشريعات خاصة وعقوبات مغلظة، ومن حيث صعوبة اثبات جريمة الابتزاز الالكتروني وضعف وعي الضحايا بوجوب تقديم شكاوى على المبتزين لردعهم وقطع دابر الجريمة. وسيتم بيان ذلك من خلال تحليل نصوص النظام السعودي وبيان طرق اثبات الجريمة وسبل المواجهة عبر لجان التحقيق والضبط والمكافحة المتخصصة، وتحليل الأحكام القضائية التي ترتبط بهذه الجريمة.

أهمية البحث:

تظهر أهمية البحث من خلال العدد المتزايد لضحايا جريمة الابتزاز الالكتروني باعتبارها ظاهرة عالمية وجريمة معلوماتية عابرة للدول، وذلك باستغلال المبتز لعلمه بالوسائط الالكترونية واختراقه لخصوصية المجني عليه متجاوزاً ذلك بتهديده للحصول على منفعة مادية أو معنوية أو غير اخلاقية بغير وجه حق. وتبدو خطورة الجريمة فيما يمارسه الجاني من تهديد وتخويف للمجني عليه على نحو يجبره على القيام بعمل أو الامتناع عن عمل وهو مسلوب الإرادة والاختيار، وذلك من خلال تحليل الجريمة وأركانها وعقوبتها في النظام السعودي وكيفية اثباتها وسبل مواجهتها.

أهداف البحث:

يهدف البحث إلى تحديد الإطار النظري لجريمة الابتزاز الإلكتروني من حيث المفهوم والمراحل والخصائص والدوافع والأنواع، وتحليل أركانها والعقوبة المقررة لها في النظام السعودي. كما يهدف البحث إلى بيان كيفية اثبات جريمة الابتزاز الالكتروني وطرق مكافحة الجريمة العملية والسوابق القضائية التي أرساها القضاء الجنائي السعودي المختص.

أسئلة البحث:

ويطرح البحث مجموعة من الأسئلة نجيب عليها من خلال دراسة تحليلية لموضوعاته في ظل النظام السعودي وقضاءه العالي، وهي كالتالي:

ما المقصود بجريمة الابتزاز الالكتروني؟

ما هي مراحل وخصائص جريمة الابتزاز الالكتروني؟

ما دوافع جريمة الابتزاز الالكتروني، وما هي أنواعه؟

ما هي أركان جريمة الابتزاز الالكتروني وما هي عقوبتها؟

ما هي طرق اثبات جريمة الابتزاز الالكتروني، وكيف يتم التعامل معها؟

منهج البحث:

اتبع البحث المنهج الوصفي والتحليلي وذلك بوصف الإطار النظري لجريمة الابتزاز الالكتروني من حيث التعريف والخصائص والمراحل ودوافع الجريمة وأنوعها. وأيضا

من خلال تحليل وتكييف نصوص نظام مكافحة جرائم المعلوماتية السعودي من حيث أركان الجريمة والعقوبة المقررة لها، وكيفية اثبات الجريمة ومواجهة الهيئات السعودية المختصة للجريمة وما أوردته المحاكم السعودية من سوابق قضائية.

الدراسات السابقة:

بلا شك هناك كتابات ومؤلفات في موضوع جريمة الابتزاز الالكتروني؛ إلا أن البحث يختلف في دراسته وتحليله للجريمة من جوانب مختلفة نوردها عند تناول بعض الدراسات السابقة بالمناقشة والتحليل، وذلك كالتالي:

في دراسة بعنوان "جرائم الابتزاز الالكتروني- دراسة مقارنة"[١]، تناولت الدراسة الجانب النظري للابتزاز والفرق بين الابتزاز والجريمة الالكترونية وأركان الجريمة والعقوبة وكيفية المواجهة وذلك في التشريع الإماراتي والتشريع المقارن، كما بينت الدراسة دور الشرطة في مواجهة الجريمة. وتختلف الدراسة في موضوعاتها في أن البحث الذي بين أيدينا ركز على دراسة وتحليل جريمة الابتزاز خاصة في ظل النظام السعودي المختص، وكيفية الاثبات والمواجهة في ظل النظام السعودي ولجانه الخاصة بالمكافحة وقضاءه المختص.

[١]- انظر، أنغام سالم سعيد بن غانم، جرائم الابتزاز الالكتروني "دراسة مقارنة"، دار النهضة العلمية، الإمارات، ٢٠٢٤م.

وفي دراسة أخرى بعنوان "جريمة الابتزاز الالكتروني"[١]، ناقشت الدراسة جريمة الابتزاز في الصورة الالكترونية مع تطبيقات القضاء المقارن وتشريعات عدد من البلدان كالعراق ومصر وفرنسا وكندا والولايات المتحدة وعدد من دول الشرق الأوسط، من خلال سرد الوقائع الاجتماعية لجريمة الابتزاز الالكتروني. كما أوردت الدراسة إرشادات قانونية وتقنية للوقاية من الجريمة. ولكن البحث هنا تناول التركيز بالتحليل والوصف لجريمة الابتزاز الالكتروني واركانها وعقوبتها من خلال النظام السعودي خاصة وبين طرق الاثبات العملية والمتبعة في الأنظمة السعودية وسبل المكافحة من خلال الهيئات السعودية المتخصصة وبيان السوابق القضائية واحكام القضاء الجنائي السعودي في هذا الشأن.

دراسة ثالثة بعنوان "جريمة الابتزاز الالكتروني- دراسة مقارنة"[٢]، ركزت الدراسة في جوانب جريمة الابتزاز الالكتروني الموضوعية في القانون المصري مقارنة مع ما بينته التشريعات المقارنة ومكافحة الجريمة في كلٍ، وذلك تأصيلاً وتحليلاً ومقارنةً لموقف التشريع المصري خاصة وأحكام المحاكم الصادرة بشأنها وبحث الآراء الفقهية لوضع الحلول المثالية لمواجهتها. أما البحث المقدم فتناول الجوانب النظرية والعملية لجريمة الابتزاز الالكتروني في ظل النظام السعودي المختص وتحليل نصوصه بالنسبة لأركان الجريمة وعقوبتها. وما أورده النظام السعودي من وسائل لإثبات جريمة

[١]- انظر، عمار عباس الحسيني، جريمة الابتزاز الالكتروني، منشورات زين الحقوقية، بيروت، لبنان، ٢٠٢٢م.

[٢]- انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق- جامعة بني سويف، المجلد ٣٦، العدد ٢، يوليو ٢٠٢٤م.

١٩- جريمة الابتزاز الالكتروني في النظام السعودي

الابتزاز الالكتروني وما هو متبع ومعمول به في ظل المحاكم السعودية وماهية طرق المواجهة المتبعة من ناحية التبليغ وتقديم الشكاوى وملاحقة وضبط الجريمة من قبل الأجهزة السعودية المختصة بالمكافحة.

وفي دراسة أخرى بعنوان "دور الأنظمة في الحد من جريمة الابتزاز الالكتروني- دراسة مقارنة في النظام السعودي والقانون الاماراتي"[١]، بينت الدراسة جريمة الابتزاز الالكتروني في اطارها العام والعقوبات المقررة عليها من خلال دراسة مقارنة بين النظام السعودي والاماراتي. كما تناولت جانب التحقيق الجنائي للجريمة من خلال استقراء النظم والإجراءات وواقع الحال في المجتمع السعودي ودول الخليج العربي وخاصة المجتمع الاماراتي. بينما تناول البحث في اطاره النظري والموضوعي لجريمة الابتزاز الالكتروني من حيث المفهوم والدوافع والأنواع وأركان الجريمة والعقوبة المقررة في نظام مكافحة المعلوماتية السعودي، وبيان طرق الاثبات العملية للجريمة في النظام السعودي وسبل التبليغ عن الجناة المبتزين وكيفية تقديم الشكاوى لمواجهة جريمة الابتزاز الالكتروني في النظام السعودي. ومناقشة ما هو معمول به من لجان التحقيق المختصة وأجهزة مكافحة الجريمة وما أوده القضاء السعودي من تطبيقات في هذا الخصوص.

[١]- انظر، ماجد سعد مرشد العتيبي، دور الأنظمة في الحد من جريمة الابتزاز الالكتروني "دراسة مقارنة في الأنظمة المنظمة للابتزاز الالكتروني في النظام السعودي والقانون الاماراتي"، المجلة العربية للنشر العلمي، العدد ٧٥، الإصدار الثامن، كانون الثاني ٢٠٢٥م.

هيكل البحث:

المبحث الأول: الإطار النظري لجريمة الابتزاز الالكتروني

المطلب الأول: تعريف جريمة الابتزاز ومراحلها

المطلب الثاني: أسباب ودوافع جريمة الابتزاز الالكتروني

المطلب الثالث: خصائص وأنواع جريمة الابتزاز الالكتروني

المبحث الثاني: أركان وعقوبة جريمة الابتزاز الالكتروني في النظام السعودي

المطلب الأول: أركان جريمة الابتزاز الالكتروني في النظام السعودي

المطلب الثاني: عقوبة جريمة الابتزاز الالكتروني في النظام السعودي

المبحث الثالث: اثبات جريمة الابتزاز الالكتروني في النظام السعودي والتطبيق القضائي لمواجهتها

المطلب الأول: كيفية اثبات جريمة الابتزاز الالكتروني في النظام السعودي

المطلب الثاني: التطبيق القضائي لمواجهة جريمة الابتزاز الالكتروني

المبحث الأول

الإطار النظري لجريمة الابتزاز الالكتروني

تمهيد:

تعتبر جريمة الابتزاز الإلكتروني من الجرائم الكبرى في المملكة العربية السعودية التي تهدد أمن وسلامة الأفراد والمجتمعات، وقد شهدت جرائم الابتزاز في الآونة الأخيرة تزايداً ملحوظاً نتيجة لتطور التكنولوجيا وزيادة استخدام وسائل التواصل الاجتماعي وانتشار التطبيقات الإلكترونية والمنصات الرقمية. ونقسم هذا المبحث إلى ثلاثة مطالب، المطلب الأول بعنوان "تعريف جريمة الابتزاز ومراحلها"، والمطلب الثاني تحت عنوان "أسباب ودوافع جريمة الابتزاز الالكتروني"، أما المطلب الثالث فيحمل عنوان "خصائص وأنواع جريمة الابتزاز الالكتروني".

المطلب الأول

تعريف جريمة الابتزاز ومراحلها

الفرع الأول: تعريف جريمة الابتزاز الالكتروني

الابتزاز في اللغة: مأخوذ من الثلاثي بزز، يقال بزَ الشيء بزاً اغتصبه، والبز هو السلب، وابتز الشيء أي استلبه ومن المثل: من عزَ بزَ، أي معناه من غلب سلب[١].

أما الابتزاز في الاصطلاح: هو الحصول على المال والمنافع من شخص تحت التهديد بفضح بعض أسراره[٢]. ويعرف بأنه: "محاولة تحصيل مكاسب مادية أو معنوية من شخص، أو اشخاص طبيعية، أو اعتبارية بالإكراه، أو التهديد وذلك بفضح سر من وقع عليه فعل الابتزاز". ويعرف أيضاً بأنه: "محاول الجاني الإكراه أو سلب الإرادة والحرية والاختيار لإيقاع الأذى الجسدي أو المعنوي على الضحية عن طريق وسائل لحقيق جرائمه الأخلاقية أو المادية أو كليهما"[٣].

وتعرف جريمة الابتزاز بأنها: "الضغط الذي يباشره الجاني على إرادة المجني عليه في محاولة لحمله على ارتكاب جريمة ما، وذلك من خلال قيام الجاني بتهديد المجني

---

[١]- انظر، محمد بن مكرم بن علي أبو الفضل جمال الدين ابن منظور الأنصاري الرويفعي (المتوفي عام ٧١١هـ)، لسان العرب، (٥/ ٣١٢)، دار صادر بيروت، الطبعة الثالثة، ١٤١٤هـ، ص٢٧١.

[٢]- انظر، المرجع نفسه، ص٢٧٥.

[٣]- انظر، علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، مركز باحثات لدراسات المرأة، مكتبة الملك فهد الوطنية للنشر، الرياض، ١٤٣٢هـ، ص١٤.

عليه بنشر معلومات أو صور أو اسرار لا يريد نشرها بقصد التشهير به للثأر من المجني عليه للحصول على مكاسب منه أو تنازلات"[١].

ومع استخدامات الحاسوب المختلفة على نحو واضح؛ أصبح كل فرد يمتلك حاسوب وانتقلنا من مرحلة المعالجة البشرية إلى مرحلة المعالجة الالكترونية، فبرزت جريمة الابتزاز الالكترونية كإحدى جرائم المعلوماتية التي تقع عبر اختراق المجال الالكتروني والوصول لأسرار الناس وابتزازهم بها. وتعرف جريمة الابتزاز الالكتروني وفقاً للفقه القانوني تعريف ضيق وتعريف آخر واسع، فتعرف جريمة الابتزاز الالكتروني من حيث النطاق القانوني الضيق بأنها: "جريمة تأخذ صورة التهديد من الجاني إلى المجني عليه وذلك بفضحه في أمور يخشى من كشفها بغرض الحصول على منفعة مادية أو غير مادية"[٢]. وتعرف بأنها: "عملية تهديد وتخويف الضحية بنشر صور أو فيديوهات أو تسريب معلومات سرية بفضحها عبر الإنترنت بهدف الحصول على مبالغ مالية أو اجبار الضحية على القيام بأعمال غير مشروعة لصالح المبتز"[٣]. وتعرف ايضاً بأنها: "توصل الجاني إلى الاستحواذ على بيانات ومعلومات شخصية لشخص المجني عليه ثم تهديده بكشفها أو نشرها إذا لم يقم الأخير بالقيام بعمل أو

---

[١]- انظر، أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣م، ص٥٥٦.

[2]- Omer Abdulsalam Hussein, prof, Dr. Nazura Abdul manap, prof, Dr. Mohammed Rizal, Cyber blackmail crime against women- A case study, journal of positive school psychology, 2022 Vol No3,6882- 6893, P3.

[٣]- انظر، أشرف عبد لسلام علي كيلاني، الابتزاز الالكتروني والآثار المترتبة عليه "دراسة فقهية مقارنة"، مجلة البحوث الفقهية والقانونية، العدد ٤٦، يوليو ٢٠٢٤م، ص١٤.

الامتناع عنه أو أداء مبالغ مالية للجاني". فهي تعد احدى الطرق التي يمارس بها الجاني تهديده وتخويفه للمجني عليه بنشر المعلومات أو البيانات أو الصور الشخصية الخاصة به والتي لا يرغب في نشرها؛ وذلك إذا امتنع المجني عليه عن تنفيذ ما يطلبه الجاني من منافع مادية أو غير مادية[١].

يتضح للباحث من التعريفات السابقة أنها تتركز في مضمون الابتزاز والغرض منه عندما تحصل من خلال وسائل الكترونية عبر التهديد وايقاعه؛ مالم يمتثل المجني عليه بدفع المبالغ المالية أو القيام بالعمل أو الامتناع عنه أو تحصيل المنفعة غير المادية.

وتعرف جريمة الابتزاز الالكتروني تعريفاً واسعاً بأنها: "محاولة الجاني تحقيق مكاسب سواء كانت مادية أم غير مادية وذلك عن طريق تهديد المجني عليه بإلحاق الأذى بنفسه أو بماله أو بشخص آخر يهمه من خلال نشر معلوماته أو اسراره الخاصة"[٢]. وتعرف أيضاً بأنها: "كل تهديد يرتكبه الجاني بنفسه أو من خلال وسيط الكتروني ضد المجني عليه على نحو يؤثر في نفسه ليحمله على القيام بما يكلفه به الجاني من أفعال مشروعة أو غير مشروعة"[٣]. وتعرف بأنها: "جريمة تتحقق من خلال قيام

[١]- انظر، سامي مرزوق نجا، المسؤولية الجنائية عن الابتزاز الالكتروني في النظام السعودي، رسالة ماجستير- جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٥م، ص٢٧.

[2]- John. Dr. Mercer, Cybersquatting: blackmail on the information superhighway, Hein onlin68. U. J. SCI& Tech L. 290,2000, P.11.

[٣]- انظر، تامر صالح، الابتزاز الالكتروني "دراسة تحليلية مقارنة"، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد١، ٢٠١٨م، ص٢٢.

الجاني باستخدام وسائط الكترونية والتوصل لمعلومات أو صور أو بيانات سرية تخص المجني عليه لأداء عمل غير مشروع"[١].

عرف المنظم السعودي في نظام مكافحة جرائم المعلوماتية جريمة الابتزاز الالكتروني بأنها: "الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولوكان القيام بهذا الفعل أو الامتناع عنه مشروع"[٢]. والشخص من خلال النظام يقصد به: "أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة"[٣]. يظهر للباحث أن المنظم السعودي أن فعل الابتزاز يأخذ شكل التهديد الذي يتضمن مضموناً معيناً مثل العنف أو افشاء أمور مخلة بالشرف أو الاعتبار، بهدف حصول الجاني على المال أو الكسب غير المادي كما واعتبرها النظام جريمة حتى وان كان الفعل أو الامتناع مشروعاً.

الفرع الثاني: مراحل جريمة الابتزاز الالكتروني

عرفنا مما سبق أن جريمة الابتزاز الالكتروني عبارة عن تهديد الجاني للمجني عليه بكشف اسراره في حال عدم استجابة المجني عليه لطلب الجاني. ويتضح أن جريمة الابتزاز الالكتروني تمر بعدد من المراحل تتمثل في التالي:

---

[١]- انظر، ممدوح رشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الأمنية، المجلد٣٣، العدد٧٠، الرياض، ٢٠١٧م، ص١٩٩.

[٢]- انظر، المادة رقم ٣، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

[٣]- انظر، المادة رقم ١، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

أولاً: الطلب، ويقصد به عندما يطلب الجاني من المجني عليه القيام بعمل أو الامتناع عن عمل أو الحصول على مكاسب مادية أو معنوية أو أي عملٍ غير مشروع.

ثانياً: المقاومة، وتظهر على الضحية في شكل قلق أو خوف بناء على الخوف والتهديد من افتضاح اسرار المجني عليه أو نشر صوره أو مقاطع الفيديو المرئية أو حتى التسجيلات الصوتية والتي تفتضح أموراً شخصية ما كان ليطلع أحداً عليها.

ثالثاً: الضغط، يقوم المبتز أو الجاني بالإصرار على المجني عليه وتضييق الخناق عليه ومحاصرته بصورة تضغط عليه نفسياً وتدفعه لتلبية طلبات المبتز.

رابعاً: التهديد، والتهديد يقصد به: "كل قول أو كتابة يكون من شأنه القاء الرعب والذعر في نفس الشخص المهدد في ارتكاب جريمة في حقه أو افشاء ما يخدش شرفه أو سمعته ويحمل المهدد لإجابة الجاني إلى مبتغاه"[١]. ويظهر التهديد جلياً في جريمة الابتزاز الالكتروني كأحد أهم الأفعال المادية التي يمارسها الجاني على الضحية بالتخويف والتهديد سواء كان بالقول أو الكتابة لحمله على تنفيذ طلبه، وأن يهدده بأنه إن لم يفعل ما يطلبه سوف ينشر ما تحت يده ويفضح سره.

خامساً: الإذعان، نتيجة للخوف الذي ينتاب المجني عليه فإنه يستسلم ويذعن لطلبات ورغبات الجاني المبتز لكيلا يفتضح أمره أو يشهر بسمعته.

[١]- انظر، حسن صادق المرصفاوي، شرح قانون العقوبات –القسم الخاص، منشأة المعاف، الإسكندرية، ١٩٩٠م، ص١٤.

سادساً: التكرار، يتكرر فعل الابتزاز للضحية مرة وأخرى، فمطالب المبتز لا تنتهي بمجرد تنفيذ المجني عليه أول مرة لطلب الجاني المبتز[١].

يخلص الباحث إلى أن جريمة الابتزاز الالكتروني تمر بمجموعة من المراحل تكون في مجموعها جريمة الابتزاز الالكتروني الكاملة والتي تتكون من الفعل المادي والمعنوي.

المطلب الثاني

أسباب ودوافع جريمة الابتزاز الالكتروني

الفرع الأول: أسباب جريمة الابتزاز الالكتروني

جريمة الابتزاز الالكتروني هي صورة مستحدثة للابتزاز التقليدي وأحد افرازات التكنولوجيا والتطور التقني الذي يشهده عالمنا اليوم. فهي أسلوب يقوم على الضغط والتهديد الذي يقوم به المبتز على شخص آخر وهو المجني عليه بتوعده وتخويفه بنشر صور تخصه أو معلومات شخصية أو مقاطع مرئية لا يرغب المجني عليه في نشرها، والسبب وراء كل هذا وذاك هو اشباع الجاني لرغباته المادية أو المعنوية أو

[١] - انظر، افراح بن خميس بن عامر، مشكلة الابتزاز الالكتروني لدى طلبة مرحلة التعليم ما بعد الأساس ودور الخدمة الاجتماعية في المجال المدرسي في التعامل معه، رسالة ماجستير - كلية الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، سلطنة عمان، ٢٠١٨م، ص٢١.

الجنسية أو حتى الانتقام من الضحية[١]. وتتمثل أسباب جريمة الابتزاز الالكتروني في النقاط التالية:

أولاً: ضعف الوازع الديني والفراغ

إن عدم استشعار مراقبة المولى عز وجل للعبد والخوف منه وضعف الالتزام بالعبادات التي تعين على اجتناب المعاصي، وكثرة الفراغ مع سهولة الحصول على المحتويات المختلفة على شبكة الانترنت لهو أحد أهم الأسباب التي أدت لظهور وتفشي جريمة الابتزاز الالكتروني. كما أن الاحصائيات مؤخراً تؤكد أن فئة الشباب هي أكثر الفئات عرضة للوقوع في جريمة الابتزاز الالكتروني. وقد أرجع بعض المسؤولين المطلعين في المملكة العربية السعودية إلى أن ٨٨% من جرائم الابتزاز تقع ضحيتها النساء، وغالباً ما تكون المرأة هي السلاح الذي يستخدمه المبتز لما تقدمه بضعف منها وقلة وازع ديني واتباعٍ للشهوات والفراغ بإعطاء الصور أو الفيديوهات وغيره مما يجعلها ضحية لهذه الجريمة[٢].

ثانياً: اختراق الخصوصية في الأماكن العامة وعبر مواقع التواصل الاجتماعي

من أبرز أسباب وقوع جريمة الابتزاز الالكتروني هو عدم احترام الحريات والتطفل على خصوصيات الغير، ومؤدى ذلك يرجع إلى التطور الهائل لوسائل النظم المعلوماتية وخاصة الكاميرات المزودة في المحلات التجارية والشركات والأماكن

[١]- انظر، سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم التواصل الاجتماعي "دراسة مقارنة"، دور المعرفة للنشر والتوزيع، الإسكندرية، ٢٠٢٢م، ص١١١.

[٢]- انظر، علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، مرجع سابق، ص ١٥ وما بعدها.

العامة والتي تسمح بالتقاط الصور دون اذن أو علم صاحبها[١]. كما أن وسائل التواصل الاجتماعي ومختلف التطبيقات الالكترونية ألغى حاجز الخصوصية والحشمة وفتح باب الدخول في الحياة الخاصة للأسر والشباب على مصراعيه[٢]. ومن أهداف نظام مكافحة جرائم المعلوماتية السعودي المساعدة على تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية المصلحة العامة، والأخلاق، والآداب العامة[٣].

ثالثاً: الاستخدام السيء للوسائل الالكترونية

تدخلت وسائل الاتصال الالكتروني في حياة الشباب والشابات بطريقة واضحة وملموسة حيث جمعت الفريقين في حجرة افتراضية لا رقابة عليهم فيها، إضافة لما يتسبب به أصدقاء السوء وما يغمر الشباب من حب المغامرة والتقليد وبالتالي الوقوع في الخطأ. وقد أصبح الاستخدام السيء لهذه التطبيقات والتقنية بتبادل الصور والتسجيلات الصوتية والمقاطع المرئية سبباً للمبتزين بتخزين هذه المعلومات وحفظها

[١]- انظر، ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دار النهضة العربية، القاهرة، بدون سنة نشر، ص١١ وما بعدها.

[٢]- انظر، علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، المرجع السابق، ص١٩.

[٣]- انظر، المادة رقم ٢، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ.

للقيام بجرائمهم والتهديد والمساومة بها للمجني عليهم لاحقاً للحصول على مقابل مالي أو منفعة أو علاقة غير مشروعة[١].

رابعاً: الجهل بالأمور التقنية وضعف الرقابة الاسرية

إن الجهل وعدم المعرفة والالمام بالأمور التقنية على شبكة الانترنت وعدم تقدير العواقب يوقع كثير من الشباب والأحداث ضحايا الابتزاز. كما إن غياب رقابة الأسر ومتابعتهم وتوجيههم أدى إلى انحراف الأبناء واتباعهم لطرق غير سوية بقضائهم ساعات طوال أمام المواقع الالكترونية ومواقع التواصل الاجتماعي المختلفة بلا فائدة تضيعاً للوقت واتباعاً للشهوات وصولاً لتشويه سمعة الأسر وشرفهم[٢].

الفرع الثاني: دوافع جريمة الابتزاز الالكتروني

إن محاولة الجاني أو المبتز للحصول على المكاسب المادية أو المعنوية بتهديد المجني عليه بنشر صوره أو معلومات سرية تخصه أو بتشويه سمعته وشرفه أو الحاق الأذى به إذا لم يحصل على ما يطلبه من المجني عليه؛ يمثل الأفعال التي تقوم عليها جريمة الابتزاز الالكتروني[٣]. وتتمثل دوافع جريمة الابتزاز الالكتروني في الدوافع التالية:

[١]- انظر، أشرف عبد لسلام علي كيلاني، الابتزاز الالكتروني والآثار المترتبة عليه "دراسة فقهية مقارنة"، مرجع سابق، ص٢٣.

[٢]- انظر، علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، مرجع سابق، ص٢٢.

[٣]- انظر، تامر صالح، مرجع سابق، ص١٢.

الدافع الأول: الحصول على كسب أو مقابل مالي

إن فعل التهديد الذي يصدر من الجاني المبتز تجاه المجني عليه تدفعه رغبة الحصول على مبلغ مالي يوفر له سبل المعيشة والعيش الرغد ويكون ذلك عبر ارسال المبتز رسائل الكترونية مكتوبة أو تسجيل صوتي أو اتصال من خلال شبكة الانترنت أو بأي وسيلة الكترونية كالماسنجر، أو الواتساب، أو فيس بوك، أو أي موقع للتواصل الاجتماعي إخفاء لحقيقة الجاني المبتز وتهديداً للمجني عليه بتنفيذ طلبه والا سوف ينشر ما هدد به على الملأ[١]. والرغبة المادية التي تحرك المبتز نحو السلوك الاجرامي وتحقيقه لكسب مادي من ورائها يلجأ المبتز بتحديد مهلة زمنية للمجني عليه لتنفيذ طلبه تحت التهديد له بنشر أو تسريب معلومات تخص المجني عليه[٢].

الدافع الثاني: تحقيق منفعة معنوية أو إقامة علاقة غير مشروعة

قد يتمثل دافع جريمة الابتزاز الالكتروني في التهديد بإفشاء أمور فاضحة أو نسبتها إلى المجني عليه؛ من أجل تحيق منفعة معنوية أو إقامة علاقة غير مشروعة مع المجني عليه احتقاراً للضحية وتشويها لسمعتها. ولا تتحقق الجريمة إذا كان التهديد بإذاعة سر اختراع أو أرباح، انما تقع جريمة الابتزاز بالتهديد بنشر أو فضح أمور

[١]- انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، المجلة القانونية، بدون سنة نشر، ص٩٠٤.

[٢]- انظر، ديب أرم بن بو عبد الله نورة، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مجلة الحقوق والعلوم الإنسانية، المجلد ٦، العدد ١، ٢٠٢٣م، ص٤٠٥.

تخل بشرف أو سمعة المجني عليه[١]. ومن قبيل دوافع الجريمة رغبة الجاني في تحقيق منفعة معنوية أو إقامة علاقة جنسية مع الضحية وقد يتكرر الابتزاز مرة تلو الأخرى وذلك ان لم تقم الضحية بتلبية رغبة الجاني المبتز والا قام بنشر ما هددها به من صور أو غيرها[٢]. والرغبات الجنسية قد يكون محلها النساء أو الرجال أو الأطفال وخاصة في البيئة الرقمية، حيث يستغل المبتز المجني عليه لتلبية رغباته الجنسية من خلال التهديد والتخويف ابتزازاً له بنشر صور أو معلومات سرية وشخصية. وقد يكون الابتزاز نتيجة لارتباط عاطفي أو علاقة وهمية عبر وسائل التواصل الاجتماعي أو المواقع الالكترونية تنتهي باستغلال الجاني للضحية تحت التهديد والاكراه لإقامة علاقة جسدية غير أخلاقية معه تلبية لرغبته في ذلك[٣].

الدافع الثالث: الدوافع العاطفية

قد يكون الانتقام، أو الكره، أو الحقد، أو الضغينة الشخصية دافعاً لارتكاب جريمة الابتزاز الالكتروني، وقد يكون حب الذات أو التسلط دافعاً باستدراج الضحية عبر الوسائط الافتراضية وغالبا يكون في محيط القرابة الاسرية أو المهنية أو الاجتماعية[٤]. ورغبة الانتقام هي أكبر الدوافع العاطفية تجاه الضحية، سواء كانت حقداً على شخص أجنبي عن الجاني لا علاقة له به ولا تربطه به صداقة أو قرابة أو حتى زمالة

[١]- انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، المرجع السابق، ص٩٠٤ وما بعدها.

[٢]- انظر، المرجع نفسه، ص٨٨٢.

[٣]- انظر، ديب أرم بن بو عبد الله نورة، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مرجع سابق، ص ٤٠٥.

[٤]- انظر، المرجع نفسه، ص ٤٠٥.

وذلك بالحاق الضرر به بنشر صور أو فيديوهات له تشويهاً لسمعته وحرماناً له من حقوقه واحتقاراً له في المجتمع. وهو أخطر أنواع الابتزاز وأشده أثراً على الضحية خاصة الأبرياء منهم حقدا من الجناة واضراراً بمالهم أو نفوذهم أو سمعتهم النظيفة. والانتقام بين الأزواج هو أحد الدوافع لوقوع جريمة الابتزاز، ويقصد به الثأر من شخص الزوج أو الزوجة بنشر صور أو مقاطع حميمية عقاباً له أو ليشفي الجاني غليله من جراء انفصاله عنه، وهذا الدافع ينم عن شخصية مضطربة تتباهى بأفعالها الانتقامية وتتلذذ برؤية الطرف الآخر وهو يعاني وتكون النتيجة الغلبة من هذا النوع من الابتزاز انتحار الضحية[١].

المطلب الثالث

خصائص وأنواع جريمة الابتزاز الالكتروني

الفرع الأول: خصائص جريمة الابتزاز الالكتروني

تختص جريمة الابتزاز الالكتروني بمجموعة من الخصائص التي تميزها عن غيرها من جرائم المعلوماتية أو جريمة الابتزاز العادية؛ وذلك نسبة لاستخدام البيئة الافتراضية كوسيلة لوقوع الجريمة. ويمكن اجمال خصائص الجريمة في الخصائص الآتية:

[١]- انظر، أشرف عبد لسلام علي كيلاني، الابتزاز الالكتروني والآثار المترتبة عليه "دراسة فقهية مقارنة"، مرجع سابق، ص ٤٥-٤٧.

١- جريمة معلوماتية خطيرة تمس حرمة الحياة الخاصة

تعرف الجريمة المعلوماتية في النظام السعودي بأنها: "أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[١]. وتظهر خطورة جريمة الابتزاز الالكتروني نسبة لما يتم الحاقه من أذى أو ضرر بمصلحة المجني عليه واسرته والمجتمع ككل، وما يتعرض له المجني عليه من دفع مبالغ مالية كبيرة منعاً لافتضاح سره أو ما يشين سمعته أو ينتهك حرمة حياته الخاصة ويمس بأمن الأفراد والأمن القومي للدولة على نحن يتوجب معه المكافحة والردع للمبتزين[٢]. وهي جريمة خطيرة لأنها تؤثر في شعور الضحية بالخوف على سمعته وبالتالي تؤدي إلى انتشار الفساد الأخلاقي. فلا يأمن الناس على أموالهم ولا على أعراضهم ولا على سمعتهم من الابتزاز، وما قد ينتج عنه من جرائم عنف تقع من قبل المجني عليهم حفاظاً على حرماتهم وانتقاماً من المبتزين أو انتحاراً ظناً منهم أنها سبيل الخلاص من هذا التهديد[٣]. وترتبط جريمة الابتزاز الالكتروني بالاعتداء على حرمة الحياة الخاصة للمجني عليه ونشر خصوصياته مالم ينفذ ما يطلبه المبتز منه[٤].

---

[١]- انظر، المادة رقم ١، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

[٢]- انظر، زهراء عادل عبد الحميد، جريمة الابتزاز الإلكتروني "دراسة مقارنة"، رسالة ماجستير، كلية الحقوق- جامعة عمان الأهلية، الأردن، ٢٠١٩م، ص٥٠.

[٣]- انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مرجع سابق، ص ٤٧٦.

[٤]- انظر، زهراء عادل عبد الحميد، جريمة الابتزاز الإلكتروني "دراسة مقارنة"، المرجع السابق، ص ٥٨.

وجريمة الابتزاز الإلكتروني بالغة الخطورة على المجتمع؛ وهذا يظهر من خلال الخسائر المادية التي تنتج عن هذه الجريمة حيث يصعب معرفة حجم الخسائر المادية الحقيقية التي ترتبت عليها. ونتيجة لذلك فإن الكثير من الشخصيات الاعتبارية التي تتعرض للابتزاز الإلكتروني لا تقوم بإبلاغ الجهات المختصة خشية التعرض لإساءة السمعة أو التأثير على الوضع المالي لهذه المؤسسات وأسهمها في سوق الأوراق المالية. وتظهر خطورة الجريمة على الأفراد الطبيعيين من خلال ما يمس شرفهم وسمعتهم وتنتهك خصوصياتهم، إضافة إلى أن هذه الجريمة الخطيرة تمس أمن الدولة القومي وبالتالي ضرورة مواجهتها من المجتمع الدولي[١]. وقد نص النظام السعودي على فعل الدخول غير المشروع إلى الأنظمة المعلوماتية واعتبرها جريمة الكترونية معاقب عليها وذلك بقوله: " الدخول غير المشروع يقصد به دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"[٢].

٢- جريمة عابرة للحدود

لا تعد جريمة الابتزاز الالكتروني من الجرائم التقليدية وإنما الجرائم التي لا تحترم حدود الدولة الجغرافية الواحدة، بل تتعداها الى دولس أخرى، حيث ترتكب الجريمة عن بعد لذلك يعد العالم بأسره مسرحاً لهذه الجريمة مما يتطلب التعاون الدولي

[١]- انظر، طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الالكتروني عبر وسائل التواصل الاجتماعي،٢٠٢٢م، ص ٤٠-٤٦، مقال على موقع المرجع الالكتروني للمعلوماتية، https://almerja.com/reading.php?idm=187687

[٢]- انظر، المادة رقم ١، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

لمواجهة الجريمة[١]. أيضاً سن القوانين الداخلية ذات العقوبات الصارمة والمناسبة لكيلا يفلت الجناة المبتزون بجريمتهم والحد من انتشارها، وكذلك بإبرام المعاهدات الدولية لمواجهة هذه الجريمة العالمية [٢].

٣- تعد من جرائم الضرر

جريمة الابتزاز الالكتروني من الجرائم التي لا تقع كاملة وترتب آثارها وتستوجب عقوبتها إلا إذا قامت الضحية بتنفيذ طلبات المبتز. فهي تنطوي على التهديد عبر استعمال وسائل الكترونية بالإيذاء الجسدي أو المعنوي أو الاضرار بالسمعة ونشر الخصوصية أو الكذب مما يدفع المجني عليه لتنفيذ رغبات الجاني المبتز وبذلك تقع الجريمة التامة[٣].

٤- جريمة جاذبة للجناة

هي جريمة لا تحتاج إلى جهد عضلي أو بذل مجهود جسماني لأن مسرح الجريمة فيها افتراضي وكل ما يحتاجه الجاني هو جهاز الكتروني سواء كان هاتف ذكي أم حاسوب متصل بشبكة الانترنت. إضافة لقلة المخاطر التي يمكن أن تواجه الجاني

[١]- انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، المرجع السابق، ص ٤٧٢-٤٧٣.

[٢]- انظر، خالد حسن أحمد، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م، ص ١٤٠.

[٣]- انظر، تامر صالح، مرجع سابق، ص٢٤.

وكذلك المقابل مادي الضخم الذي سيعود عليه لقاء جريمته أو المنفعة المعنوية أو غير ذلك اشباعاً لرغبته والتي سيتحصل عليها بكل يسر وسهولة[١].

٥- صعوبة اثبات الجريمة

إن طبيعة جريمة الابتزاز الالكتروني تتمثل في أنها جريمة ليس لها آثار مادية وتعتمد في الأصل على التقنيات الحديثة، والتي يمكن للجاني إخفاء أثرها واخفاء هويته مما يصعب الأمر على جهات التحقق والمحاكمة لإثبات الجريمة. وبغياب الدليل الرقمي المادي الكافي لا تستطيع الجهة المختصة اثبات الجريمة على الجاني وبالتالي ملاحقته وضبطه واحضاره ومن ثم توقيع العقوبة المقررة عليه[٢]. وصعوبة اكتشاف الجريمة يجعل من الصعب الحصول على دليل مادي وبالتالي صعوبة اثباتها، مما يتطلب ضرورة الاعتراف بالدليل الرقمي وأهميته في الاثبات الجنائي وأخذ القضاء بحجيته لما له من دور مهم في اثبات جرائم المعلوماتية وخاصة جريمة الابتزاز الالكتروني ودعم الجهات التقنية المختصة بالمساعدة في اكتشاف الأدلة التي تثبت هذه الجريمة. وتأكيداً لضرورة ذلك فقد نص النظام السعودي المختص على أن: "تتولى هيئة الاتصالات وتقنية المعلومات وفقًا لاختصاصها تقديم الدعم والمساندة

[١]- انظر، زينب محمود حسين، المواجهة الجنائية للابتزاز الالكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ١٠، العدد ٣٧، ٢٠٢١م، ص ٨٧٥.

[٢]- انظر، جاسم ناصر السلماني، التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري، رسالة ماجستير، جامعة قطر، ٢٠٢٣م، ص ١٢. وانظر، طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الالكتروني عبر وسائل التواصل الاجتماعي،٢٠٢٢م، مرجع سابق، ص ٤٠-٤٦.

الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة"[١].

٦- الوسائط الالكترونية هي الوسيلة المستخدمة في الجريمة

تتسم جريمة الابتزاز الالكتروني بأنها تتم عبر استخدام الجاني المبتز للوسائل الكترونية كالهواتف الذكية أو الحواسيب الآلية أو أي وسيط الكتروني حديث. حيث تتم عندما يتمكن الجاني من الحصول على المعلومات الشخصية للمجني عليه وتهديده بالنشر والفضح لها ما لم ينفذ له طلبه أو رغبته؛ وذلك لأن الجريمة لا تتم إلا إذا توفرت الوسيلة التقنية الالكترونية الحديثة[٢]. ويتم النشاط الاجرامي بالاستيلاء أو الاطلاع غير المشروع على المعلومات الخاصة بالضحية والتي تعتبر محلاً للجريمة، والتي يتم التهديد بها من قبل الجاني وابتزاز المجني عليه مستخدماً في سبيل الوصول إليها وسائل تقنية حديثة[٣].

الفرع الثاني: أنواع جريمة الابتزاز الالكتروني

أصبحت شبكات التواصل الاجتماعي بديلاً للأنشطة الاجتماعية التقليدية إلى حد ما وعلى غير ما كان سائداً في الماضي ظهرت الأفلام القصيرة ومقاطع التسجيل الصوتية والمرئية وكذلك الصور، وظهرت في المقابل جريمة الابتزاز الالكتروني

[١]- انظر، المادة رقم ١٤، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

[٢]- انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مرجع سابق، ص ٤٧٢.

[٣]- انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، مرجع سابق، ص ٨٨٤-٨٨٥.

باستيلاء الجاني على ما يخص الضحية من معلومات شخصية مهدداً أيها بنشرها وافتضاحه ما لم يقم بتلبية طلبات الجاني[١]. وجريمة الابتزاز الالكتروني لها طرفان الأول وهو الجاني أو المبتز والذي يكون شخصاً طبيعياً في الغالب من الأحوال. والطرف الثاني وهو المجني عليه أو الضحية وقد تقع على الشخص الطبيعي حدثاً كان أم امرأة أم رجل، وقد تقع على الأشخاص الاعتبارية حين يحصل المبتز على معلومات سرية تخص الشخص الاعتباري فيقوم بتهديده بنشر هذه المعلومات وافتضاحها للمساس باعتباره[٢].

وتتمثل أنواع جريمة الابتزاز الالكتروني في التالي:

النوع الأول: بالنظر إلى المجني عليه.

قد تقع جريمة الابتزاز الالكتروني على الأحداث أو الرجال أو النساء أو على الأشخاص الاعتبارية. فإذا وقعت على الأحداث فإن المبتز يقوم بالتهديد بنشر صور أو فيديوهات أو محادثات للحدث من شأنها أن تمس من شرفه أو سمعة أسرته وذلك بغية الحصول على المال أو اجبار الحدث على إقامة علاقة غير مشروعة. وانتشار ظاهرة الابتزاز الالكتروني للأحداث مرجعها إلى ضعف الحدث وخوفه وسهولة استدراجه، ويتم ذلك من خلال الوسائل الالكترونية مما يجعلهم مطمع لكل جاني أو

---

[١]- انظر، أيمن العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، المملكة العربية السعودية، ٢٠١٥م، ص ٥٥.

[٢]- انظر، أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، دار النهضة العربية للطباعة والنشر، مصر، ٢٠٠٦م، ص ٤٨.

مبتز اعتبار أنه قاصر وينبغي تشديد العقوبة على الجاني[١]. وقد يكون المجني عليه رجلاً خاصة إن كان غنياً أو ذو منصب سياسي فيكون عرضة للمكيدة أو الوقوع في الخطأ من خلال المواقع الالكترونية فيتم تهديده بنشر صور أو فيديوهات تخصه ما لم يدفع مقابل ذلك أموال طائلة أو بنشر أسرار عمله أو عائلته وابتزازه بذلك[٢]. وقد يكون المجني عليه انثى وابتزاز النساء هو الأكثر انتشاراً، حيث تعد الأنثى نموذجاً للابتزاز الالكتروني حين يكون المبتز رجلاً. خاصة في العلاقات عبر الوسائط الالكترونية والغرف الافتراضية والتي تبدأ بالثقة الوهمية والأساليب الخداعة والملتوية لإقناع الأنثى ومن ثم وقوعها ضحية لهذا الرجل المبتز، فيهددها ويخوفها بنشر صورها أو التشهير بسمعتها وسمعة أسرتها فتقع ضحية للذعر والخوف وتنفذ له ما يطلبه بغية سكوته وعدم فضحها[٣]. وقد تستهدف الشخصيات الاعتبارية وذلك عن طريق الحصول على معلومات سرية تخص الشخص الاعتباري ويتم تهديده بنشر وإعلان هذه المعلومات للعامة مقابل مبالغ مالية يوقن الجاني أن الشخص الاعتباري وحماية لسمعته لن يتوانى في دفعها[٤].

---

[١]- انظر، خليفة علي محمد، ابتزاز الأحداث وعقوبته في النظام السعودي، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٥م، ص ٧٢ وما بعدها.

[٢]- انظر، داليا عبد العزيز، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي "دراسة مقارنة"، مجلة جيل الأبحاث القانونية المعمقة، المملكة العربية السعودية، العدد ٢٥، مايو ٢٠١٨م، ص ٣٥ و٣٦.

[٣]- انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مرجع سابق، ص ٤٩٧.

[٤]- انظر، ماجد سعد مرشد العتيبي، دور الأنظمة في الحد من جريمة الابتزاز الالكتروني "دراسة مقارنة في الأنظمة المنظمة للابتزاز الالكتروني في النظام السعودي والقانون الاماراتي"، مرجع سابق، ص ٤٤٤.

ويرى الباحث أنه وفي ظل انعدام الأخلاق وغياب دور الأسرة وانعدام الحياء فإن الأنثى أصبحت ضحية للرجل المبتز، لذلك ينبغي التوعية والتنبه وعدم استسهال هذه الأمور وأخذ العبرة بعواقب هذه الجريمة الخطيرة وما تؤدي اليه من مساس بسمعة الأسرة.

النوع الثاني: بالنظر إلى أهداف الجاني.

بالنظر إلى أهداف الجاني فإن جريمة الابتزاز الالكتروني تأخذ صوراً متعددة، فقد يكون هدف الجاني تحقيق كسب مادي وهنا يسعى الجاني للغنى والثراء بطرق غير مشروعة خاصة عندما يعتدي الجناة على المؤسسات المالية أو الأغنياء من الضحايا وابتزازهم بصور، أو تسجيلات صوتية، أو مقاطع مرئية أو أي معلومات شخصية وسرية بغرض الوصول إلى النفع المادي[١]. وقد يسعى الجاني إلى تحقيق منفعة معنوية أو عينية وذلك عن طريق تهديد المجني عليه بتلبية طلب الجاني وإلا يقوم بنشر الصور أو الفيديوهات التي يخشى المجني عليه من نشرها ويقع ضحية لهذا النوع من الابتزاز[٢]. والهدف النفعي يتمثل في قيام الجاني بتهديد المجني عليه بنشر اسراره أو صوره أو غيره من الأمور الشخصية مقابل مصلحة، أو ارتكاب جريمة السرقة، أو ترويج المخدرات، أو التوسط لدى شخص لإتمام عمل غير مشروع أو

[١]- انظر، سعد الحاج بكري، شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الأمنية والتدريب، الرياض، ١٩٩٠م، ص ٩٢.

[٢]- انظر، زهراء عادل عبد الحميد، جريمة الابتزاز الإلكتروني "دراسة مقارنة"، مرجع سابق، ص ٤٤.

مشروع[١]. وقد يكون الابتزاز الالكتروني بهدف تحقيق هدف جنسي، والدافع الجنسي هو السمة الغالبة في جرائم الابتزاز الالكتروني التي يتعرض لها النساء والاحداث كضحايا للمبتز حيث يتم استغلالهم جسدياً بالابتزاز والتهديد والاجبار على إقامة علاقة غير مشروعة مع الجاني وإلا ينفذ ما هدد به بالنشر أو الافتضاح وتشويه السمعة[٢]. ويكون ذلك بتهديد امرأة أو حدث بافتضاح سره أو ما يخصه من معلومات شخصية إذا لم يمارس معه الرذيلة، وقد يتكرر التهديد مرة وأخرى ويكون الاذعان والاستسلام من المجني عليه خوفاً وخشية من افتضاحه وتشويه سمعته[٣]. وقد يكون الابتزاز بهدف الانتقام وهو أخطر أنواع الابتزاز الالكتروني لأن شخصية الجاني توصف بأنها مضطربة وغير سوية فهو يستمتع بتهديد المجني عليه وخوفه والذعر من افتضاح أمره والراحة النفسية التي يحس بها عندما يستمع إلى توسلات المجني عليه بغض النظر عن الدافع وراء هذا الانتقام. فالانتقام قد يكون بسبب الانفصال في العلاقات الزوجية أو العلاقات المحرمة أو حتى المهنية، وهذه الأخيرة تكون عندما يقوم الجاني وهو صاحب العمل بتهديد المجني عليه بالقيام بالعمل لساعات طويلة

[١]- انظر، ماجد سعد مرشد العتيبي، دور الأنظمة في الحد من جريمة الابتزاز الالكتروني "دراسة مقارنة في الأنظمة المنظمة للابتزاز الالكتروني في النظام السعودي والقانون الاماراتي"، مرجع سابق، ص ٤٤٥.

[٢]- انظر، ممدوح رشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، مرجع سابق، ص ٢٠١.

[٣]- انظر، ماجد سعد مرشد العتيبي، دور الأنظمة في الحد من جريمة الابتزاز الالكتروني "دراسة مقارنة في الأنظمة المنظمة للابتزاز الالكتروني في النظام السعودي والقانون الاماراتي"، مرجع سابق، ص ٤٤٥.

وبدون اجر أو أن يجبره على التنازل عن المكافأة أو الحافز المالي نظير عدم كشف سره الخاص به أو بأحد أفراد اسرته[١].

النوع الثالث: الابتزاز بتركيب الصور أو المقاطع (خاصية التزييف العميق)

إن التطور التقني والذكاء الاصطناعي الذي يجتاح عالمنا اليوم له عظيم الأثر في ظهور جرائم معلوماتية حديثة ومنها جريمة الابتزاز الالكتروني، والتي تتم باستخدام التقنيات الحديثة بتركيب الصور أو مقاطع الفيديو المرئي وهو ما يعرف تقنياً بخاصية التزييف العميق (deep fake)

والتي يقصد بها: "المعالجة التي تتم لصورة أو صوت شخص ما ليبدو حقيقياً، أو هي تقنية لصق وجه شخص على جسد شخص آخر باستخدام خوارزميات معينة تتم من خلال هذا التركيب". وقد أصبحت هذه الظاهرة سلاحاً خطراً لتشويه سمعة وشرف الأبرياء[٢].

النوع الرابع: الابتزاز بتهكير التسجيلات الصوتي وسرقة المعلومات والبيانات

إن الدخول غير المشروع على المواقع الإلكترونية للأفراد أو المؤسسات وقرصنة المعلومات والحصول على الصور والفيديوهات والتسجيلات الصوتية هو أحد أخطر أنواع جريمة الابتزاز الالكتروني التي يقوم بها الجناة والاستيلاء عليه بدون علم أو

[١] – انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مرجع سابق، ص ٥٠١.

[٢] – انظر، أحمد مصطفى محرم، استخدامات الذكاء الاصطناعي "استخدام خاصية التزييف العميق" في قذف الغير أنموذجاً" "دراسة فقهية مقارنة معاصرة"، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بالقاهرة، العدد ٣٩، أكتوبر ٢٠٢٢م، ص ٢٥١٨.

اذن ذويها، ومن ثم التهديد بنشرها تلبية لما يطلبه الجناة اشباعاً لرغباتهم[١]. وقد عرف نظام مكافحة جرائم المعلوماتية السعودي مصطلح لدخول غير المشروع بأنه: "دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها". وأشار النظام السعودي إلى المقصود بالموقع الإلكتروني: "وهو مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد"[٢].

المبحث الثاني

أركان وعقوبة جريمة الابتزاز الالكتروني في النظام السعودي

تمهيد:

من المعلوم إن المملكة العربية السعودية قد اتخذت خطوات حازمة في مكافحة الابتزاز الإلكتروني، حيث أصدرت العديد من التشريعات للتصدي لها، كما فرضت أشد العقوبات على مرتكبي هذه الجرائم وذلك بهدف حماية أمن المواطنين واستقرار المجتمع وردع كل من تسول له نفسه ابتزاز الآخرين أو استغلال ضعفهم. وسنناقش في هذا المبحث أركان جريمة الابتزاز الإلكتروني في النظام السعودي وذلك في المطلب الأول منه، ونبين بالتحليل في المطلب الثاني لعقوبة جريمة الابتزاز الإلكتروني التي قررها النظام السعودي والأوضاع القانونية التي تتعلق بها.

[١]- انظر، المرجع نفسه، ص ٥٩.

[٢]- انظر، المادة رقم ١، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

المطلب الأول: أركان جريمة الابتزاز الالكتروني في النظام السعودي

جريمة الابتزاز الالكتروني هي جريمة تقوم على أسلوب الضغط والتهديد على المجني عليه، وفيها يلجأ المبتز لتهديد الضحية أو التشهير بها. وكأي جريمة الكترونية تقوم على مجموعة محددة من الأركان والتي تتمثل في الركن الشرعي والركن المادي والركن المعنوي.

الركن الأول: الركن الشرعي

تخضع جريمة الابتزاز الالكتروني لمبدأ الشرعية الجزائية وسيادة حكم القانون في مجال التجريم والعقاب. وقد نص النظام الجزائي السعودي على هذا المبدأ وقد خصص نظاماً كاملاً تحت مسمى نظام مكافحة الجرائم المعلوماتية للنص على جريمة الابتزاز الالكتروني وما يتعلق بها من أحكام، وجاء النص في المادة الثالثة منه بتجريم هذه الجريمة ووضع العقاب المقرر لها. وجاء النص بقوله: " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.

٢. الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا.

٣. الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

٤. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

٥. التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة."[١].

يتضح للباحث من نص الفقرة الثانية من المادة الثالثة أن المنظم السعودي جرم فعل الابتزاز الالكتروني وعاقب على فعل الابتزاز الالكتروني بالتعبير عنه بفعل الدخول غير المشروع عبر شبكة المعلوماتية لتهديد شخص أو ابتزازه؛ وذلك لحمله على القيام بفعل أو الامتناع عن فعل، حتى ولو كان القيام بهذا الفعل أو الامتناع عن هذا الفعل مشروعًا.

الركن الثاني: الركن المادي

يعرف بأنه: "مظهر الجريمة الخارجي أو كيانها المادي، ويعد من الماديات المحسوسة والتي تظهر في العالم الخارجي، ويعد جوهر وأساس الجريمة فلا تقوم الجريمة بدونه"[٢].

[١]- انظر، المادة رقم ٣، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

[٢]- انظر، سامح السيد جاد، شرح قانون العقوبات- القسم العام، الدار الهندسية الحديثة للطباعة والنشر، القاهرة، ٢٠٠٥م، ص ٢٠٤.

ويتمثل في النشاط المادي الذي يظهر في شكل خارجي، ولا تقوم الجريمة مكتملة الأركان ومستحقة للعقاب إلا إذا توفر ركنها المادي فلا جريمة ولا عقوبة بدون الركن المادي. ويشترط لقيام الركن المادي توفر عناصره الأساسية وهي السلوك الاجرامي والنتيجة الاجرامية وعلاقة السببية. ونتناول هذه العناصر الثلاثة بالدراسة التحليلية وفقاً لما نص عليه نظام مكافحة جرائم المعلوماتية السعودي.

أولا: السلوك الاجرامي

ويتمثل السلوك الاجرامي في جريمة الابتزاز الالكتروني في فعل التهديد للمصلحة أو الحق الذي يحميه القانون ويتخذ هذا السلوك التهديد المقترن بأي شكل كتابة أو شفاهه، بنشر الصور، أو المقاطع المرئية، أو التسجيلات الصوتية، أو أي اسرار شخصية تخص المجني عليه أو من يهمه أمره مما يزرع الذعر والخوف في نفس المجني عليه بتنفيذ الجاني لما هدد به إذا لم ينفذ المجني عليه طلبه[١]. ويقع فعل التهديد من الجاني على المجني عليه بالضغط عليه لإرغامه على القيام بعمل أو الامتناع عن عمل حتى ولو كان مشروعاً، وبغض النظر عن الوسيلة التي حصل أو استولى بها الجاني على الصور أو الفيديوهات أو المعلومات الشخصية. ولا يشترط التهديد بطريقة معينة إذ يمكن أن يتم عبر غرفة الدردشة، أو البريد الالكتروني، أو التسجيل الصوتي، أو الاتصال[٢].

---

[١]- انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، مرجع سابق، ص ٨٩٩.

[٢]- انظر، مريم غراب، جريمة التهديد والابتزاز الالكتروني، مجلة الدراسات القانونية المقارنة، المجلد ٧، العدد ١، الجزائر، ٢٠٢١م، ص ١٢٠٨.

ثانياً: النتيجة الاجرامية

النتيجة الاجرامية في الجريمة هي الأثر الجنائي الذي يرتبه السلوك الاجرام وتربطه بالسلوك الاجرامي علاقة السببية. وفي جريمة الابتزاز الالكتروني فإن خصوصية الأفراد في حفظ المعلومات داخل أجهزة الحواسيب الشخصية أو الهواتف المحمولة دون اعتداء عليها أو انتهاكاً لخصوصياتهم وحقوقهم التي يحميها القانون. وفعل التهديد يحدث أثراً بالخوف والذعر في نفس المجني عليه يحمله للقيام بعمل أو الامتناع عن عمل يطلبه الجاني المبتز خوفاً من تنفيذ ما هدد به بنشر ما استولى عليه من صور أو مقاطع فيديو تمس سمعته. وهذا الأثر هو الاعتداء أو إيقاع الضرر الجسدي أو المعنوي الذي يقع على المجني عليه جراء فعل التهديد والاجبار من خلال وسائل التقنية الالكترونية[١]. إن القاء الخوف في نفس المجني عليه وحمله على إجابة طلب الجاني المبتز هو النتيجة الاجرامية التي تترتب على سلوك الجاني بالتهديد قولاً أو فعلاً يتم عبر وسيلة الكترونية وعادة ما يكون المبتز ملماً بهذه الوسيلة[٢].

[١]- انظر، ممدوح رشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، مرجع سابق، ص ١٩٣.

[٢]- انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، مرجع سابق، ص ٩٠٥. وانظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مرجع سابق، ص ٥١٤-٥١٥.

ثالثا: علاقة السببية

يقصد بعلاقة السببية تلك العلاقة التي تربط بين الفعل الاجرامي ونتيجته الاجرامية، ولا يكفي لقيام السلوك الاجرامي تحقق نتيجته الاجرامية وإنما يجب أن ترتبط النتيجة بالسلوك واثبات هذه العلاقة في فعل الجاني ونتيجته المترتبة عليه. وتتمثل علاقة السببية في جريمة الابتزاز الالكتروني بأن خوف المجني عليه من نشر ما هدد به الجاني وتشويه سمعته يدفعه لتنفيذ ما طلبه الجاني منه، وإن لم تقم هذه العلاقة بين السلوك ونتيجته فلا يقوم الركن المادي لجريمة الابتزاز الالكتروني، حيث إنه وبانقطاع علاقة السببية لا يكتمل الركن المادي. ولا يشترط لقيام علاقة السببية أن يكون الابتزاز الالكتروني سابقاً على قيام المجني عليه بتنفيذ طلبات الجاني، بل يصح أن يكون سابقاً عليه بزمنٍ متى كان له أثر في ذلك[١].

بناء على ما سبق يرى الباحث، إن الركن المادي يقع صحيحاً إذا توفرت عناصره الثلاثة، وذلك عندما يبث المبتز الخوف في نفس الضحية بالتهديد والوعيد بإفشاء اسراره أو تشويه سمعته مقابل ما يحصل عليه من منفعة مادية أو معنوية أو جنسية. ويترتب على ذلك قيام المسؤولية الجنائية على الجاني بوقوع الركن المادي للجريمة حتى وإن لم ينفذ الجاني ما وعد به بنشر أو افتضاح تلك الأسرار أمام العلن، المهم هو حصول فعل التهديد والوعيد بما يكفي ليزرع الخوف والرعب في نفس المجني

[١] - انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، المرجع السابق، ص ٩٠٦.

عليه ويذعن بتنفيذ ما طلبه الجاني[١]. ونجد أن المنظم السعودي في المادة الثالثة من نظام مكافحة جرائم المعلوماتية السعودي لعام ١٤٢٩هـ تتطلب لقيام جريمة الابتزاز الالكتروني وجود الركن المادي والذي عبر عنه بقوله: " الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا"، ويتضح من نص المادة أن فعل السلوك الاجرامي عبر المنظم عنه بلفظ "تهديد شخص أو ابتزازه" وهو الفعل الاجرامي الصادر عن الجاني تعدياً على حق المجني عليه بغير وجه حق. ومن ناحية أخرى عبر عن نتيجته الاجرامية بلفظ "حمله على القيام بعمل أو الامتناع عنه" وهو بث الخوف والذعر في نفس المجني عليه لتنفيذ ما يطلبه الجاني حتى ولو كان فعلاً مشروعاً.

الركن الثالث: الركن المعنوي

يتطلب قيام جريمة الابتزاز الالكتروني ركناً معنوياً إلى جانب الركن المادي والركن الشرعي. ويعرف الركن المعنوي بأن: "علم وإرادة الجاني التي تتمثل في القصد الجنائي في ارتكاب الجريمة"، فهي تعبير عن موقف الجاني النفسي بعلمه بأن بما يقوم به من فعل يمثل اعتداءً على حق يحميه القانون وأن تتجه إرادته إلى هذا السلوك الاجرامي فيكتمل القصد الجنائي. وفي جريمة الابتزاز الالكتروني يجب أن يكون التهديد الصادر من الجاني جدياً بحيث يقع في نفس المجني عليه، ويجب أن تتجه إرادة الجاني لارتكاب الفعل المادي لكي يتحقق القصد الجنائي العام للجريمة. ويتوفر القصد الجنائي إذا كان الجاني يريد إلحاق الضرر بالمجني عليه أو نتج عن فعله

[١]- انظر، ديب أرم بن بو عبد الله نورة، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مرجع سابق، ص ٤٠٧.

خطر أكثر جسامة وهي حالة تجاوز القصد، ويكون القصد الجنائي قائماً افتراضياً إذا كان الفعل الاجرامي صحيحاً لإحداث النتيجة الجرمية المتوقعة[١].

وتعد جريمة الابتزاز الالكتروني من الجرائم العمدية التي تأخذ صورة القصد الجنائي والذي يجب لقيامه توفر عنصرين هما العلم والإرادة. ويتمثل العلم في معرفة الجاني المبتز بنتيجة السلوك الاجرامي الذي اقترفه وأن تهديده للمجني عليه أو الضحية بهذه الصور أو الفيديوهات أو الأسرار الشخصية يعد جريمة يعاقب عليها النظام السعودي. كما ويتطلب لقيام القصد الجنائي أن تنصرف إرادة الجاني إلى السلوك الاجرامي والنتيجة الاجرامية التي تترتب عليه وأن هذا الجرم من شأنه أن يضر بالمجني عليه ضرراً يمس سمعته أو شرفه[٢]. وقد اكتفى المنظم السعودي بالقصد العام المكون من العلم والإرادة لقيام جريمة الابتزاز الالكتروني ولم يتطلب توفر القصد الخاص.

في تقدير الباحث، ولقيام مسؤولية الجاني الجنائية يجب اثبات انه كان عالماً بإن الفعل يعد جريمة وان تتجه ارادته نحو تحقيق النتيجة الجرمية مثل الحصول على منفعة مادية أو معنوية أو إقامة علاقة غير مشروعة مع المجني عليه.

---

[١]- انظر، منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، مرجع سابق، ص ٩٠٧.

[٢]- انظر، مريم غراب، جريمة التهديد والابتزاز الالكتروني، مرجع سابق، ص ١٢٠٨. وانظر، جاسم ناصر السلماني، التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري، مرجع سابق، ص ٢٦.

المطلب الثاني

عقوبة جريمة الابتزاز الالكتروني في النظام السعودي

إن سياسة العقاب في المملكة العربية السعودية وضعت بناء على أحكام الشريعة الإسلامية، لذلك فإن العقوبة التي قررها المنظم السعودي هي عقوبة تقديرية لجريمة تعزيرية نصت عليها المادة الثالثة من نظام مكافحة جرائم المعلوماتية. وجاء نص النظام كالتالي: " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

٢. الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا"[١].

نص المنظم على العقوبة الاصلية لجريمة الابتزاز الالكتروني وهي السجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين. ومن الملاحظ أن العقوبة وجوبية وفقاً لتقدير القاضي بتفريد العقوبة المناسبة في حدود ما نص عليه النظام. وعند استخدام الصور أو الفيديو كوسيلة ابتزاز؛ تُطبَّق عقوبات جريمة المساس بالحياة الخاصة المنصوص عليها في المادة الثالثة، البند الثاني والرابع من النظام نفسه حيث نص المنظم على أن المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، يعرض

[١]– انظر، المادة رقم ٣، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.

مرتكب هذه الجريمة لعقوبة السجن الذي يصل إلى سنة والغرامة التي تبلغ خمسمائة ألف ريال. وفي حال اتبع الفعل بإتلاف أو نشر المواد، قد تُشدد العقوبة بموجب المادة الثامنة التي ترفع الحد الأدنى للعقاب إلى نصف الحد الأعلى إذا اقترنت الجريمة بظروف مشددة. كما نص المنظم السعودي على عقوبة تكميلية تتمثل في المصادرة للأجهزة، أو البرامج، أو الوسائل الالكترونية، أو أي وسيلة مستخدمة لارتكاب الجريمة أو أي أموال متحصل عليها من الجريمة وأيلولتها إلى ملكية الدولة. كما نص المنظم على إمكانية تنفيذ عقوبة أخرى وهي اغلاق الموقع الالكتروني أو المكان الخدمي الذي يقدم الخدمة الالكترونية سواء كان الإغلاق نهائياً أو مؤقتاً وفق الحال والظرف الذي يتوفر في الواقعة المعروضة أما القاضي للحكم فيها ووفقاً لظروف المالك ومدى علمه بالجريمة من عدمه. وفي جميع الأحوال، مع عدم الاخلال بحق الأشخاص حسني النية في كل تلك الحالات النظامية[١].

ايضاً نص المنظم السعودي على عقوبة التحريض أو المساعد أو الاتفاق وهو ما يعرف بالمساهمة الجنائية. فكل من يساهم في جريمة الابتزاز الالكتروني بالتحريض أو المساعدة أو الاتفاق يعاقب بما لا يتجاوز الحد الأعلى للعقوبة المقررة للجريمة، وفي حال لم تقع الجريمة الأصلية يعاقب المساهم أياً كان نوع مساهمته الجنائية في

[١] – انظر، المادة رقم ١٣، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨.والتي تنص على أنه: "مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقًا نهائيًا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه".

الجريمة بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة للجريمة[١]. وعاقب المنظم السعودي على الشروع في جريمة الابتزاز الالكتروني بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة للجريمة[٢]. وقد نص المنظم السعودي كذلك على سلطة المحكمة الجنائية المختصة في الإعفاء من العقوبة عن كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة وذلك قبل العلم بالجريمة وقبل وقوع الضرر المترتب عنها، ولكن إن كان الإبلاغ من الجناة بعد العلم بالجريمة يشترط ولكي يطبق أن يكون البلاغ ذو فائدة وجدي ومن شأنه أن يسهل ضبط بقية الجناة وضبط الأدوات المستخدمة في الجريمة[٣].

ويسعى المنظم إلى إضفاء الحماية الجنائية على حقوق وخصوصيات الأفراد داخل المجتمع ووضع العقوبة على قدر الاعتداء على هذا الحق الأساسي، ومقدار الايذاء

[١]– انظر، نص المادة رقم ٩، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨. "يعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية".

[٢]– انظر، نص المادة رقم ١٠، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢. "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة".

[٣]– انظر، نص المادة رقم ١١، نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢." للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة".

أو الضرر الذي يلحق بالمجني عليه من جراء هذا الاعتداء. وللقاضي السلطة التقديرية في تقدير العقوبة أو الجزاء الجنائي الواجب توقيعه في ضوء الاعتبارات والدوافع والظروف والملابسات التي تطرأ على كل واقعة على حدة[١].

خاتمة القول، أن قضايا الابتزاز الالكتروني أصبحت تمثل تحديًا كبيراً، حيث يستغل المجرمون التكنولوجيا لتهديد الضحايا واستغلالهم. وفي سبيل مواجهة الجريمة يفرض القانون السعودي عقوبات صارمة على المبتزين لحماية الأفراد والمجتمع من هذه الجريمة والحد من انتشارها.

[١]- انظر، ممدوح رشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، مرجع سابق، ص ٢٠٨.

المبحث الثالث

اثبات جريمة الابتزاز الالكتروني في النظام السعوي والتطبيق القضائي لمواجهتها

تمهيد

الابتزاز الإلكتروني يُعدّ من أخطر الجرائم الإلكترونية التي تهدد الأفراد والمجتمعات في العصر الرقمي، ويشهد انتشارًا متزايدًا مع التطور السريع في استخدام التكنولوجيا ووسائل الاتصال الحديثة. وفي المملكة العربية السعودية، باتت هذه الجريمة تمثل تحديًا كبيرًا للأمن الاجتماعي والاقتصادي، حيث يُستغل ضعاف النفوس الثغرات الرقمية لتهديد الآخرين والحصول على مكاسب غير مشروعة سواء كانت مادية أو معنوية. وانطلاقًا من اهتمام المملكة بحماية أمن المجتمع وضمان سلامة أفراده، أصدرت الدولة تشريعات صارمة لمكافحة جرائم الابتزاز الإلكتروني مسخرةً التكنولوجيا الحديثة لتقديم حلول فعّالة لهذه الظاهرة. ويظهر هذا الاهتمام الجاد من قبل السلطات السعودية حرصًا على بناء مجتمع رقمي آمن ومزدهر، يتناغم مع الرؤية الوطنية الطموحة للمملكة في مجال التحول الرقمي. وتتميز جريمة الابتزاز الالكتروني بصعوبة اثباتها، ونناقش في المطلب الأول كيفية اثبات جريمة الابتزاز الالكتروني في النظام السعودي وذلك عبر دراسة وتحليل موضوع الدليل الجنائي الرقمي ودور الجهات المختصة بالإثبات. ونتناول في المطلب الثاني بدراسة تحليلية للتطبيق العملي للتعامل مع جريمة الابتزاز الالكتروني وسبل موجهتها في النظام السعودي.

المطلب الأول

كيفية اثبات جريمة الابتزاز الالكتروني في النظام السعودي

الإنسان كائن اجتماعي يحتاج إلى التواصل مع بقية أفراد المجتمع ليعيش معهم ويعبر عن أفكاره ونفسه واحتياجاته. ووسائل التواصل الاجتماعي عبر شبكة الانترنت مثل الفيس بوك وهي شبكة اجتماعية تمكن مستخدميها من الانضمام والتفاعل مع الآخرين وتكوين صداقات، ويعد أبرز وسائل التواصل التي تجد ردود الفعل الفورية تجاه أي حدث اجتماعي أو اقتصادي أو غيره وبالتي ينعكس على تعليقات المستخدمين. ومن أمثلتها أيضاً تطبيق الإنستغرام وهو تطبيق مجاني لتبادل الصور عبر الانترنت وهو يتيح مشاركة الصور ومقاطع الفيديو بشكلٍ عام أو خاص. ومثال ثالث لهذه القنوات الاجتماعية وهو واتساب والذي يتيح ارسال الرسائل النصية والصور والفيديوهات من خلال تحميله على أجهزة الهواتف الذكية وهو آمن مقارنة بالأخريات[١].

ويرى الباحث أن الممارسات الخاطئة للوسائل التقنية والذي تعرف بالأمية الرقمية تؤدي إلى انتشار جريمة الابتزاز الرقمي، والتي يصعب اثباتها نسبة لوقوعها عبر استخدام وسائل الكترونية مما يستوجب مناقشة تحليلية لماهية الدليل الجنائي الرقمي وقيمته القانونية. وكذلك بيان وسائل اثبات جريمة الابتزاز الالكتروني وما تقدمه

[١]- انظر، وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مرجع سابق، ص ٤٩٢-٤٩٥.

الجهات المختصة حماية لخصوصية الأفراد اثناء استخدامهم للمواقع الالكترونية والبرمجيات المختلفة ومكافحة للجريمة، وذلك من خلال النقاط التالية:

أولاً: مفهوم الدليل الرقمي الجنائي في جريمة الابتزاز الالكتروني

تعد مسألة اثبات جريمة الابتزاز الالكتروني من المسائل التي تشغل التحقيقات الجنائية نظراَ لطبيعة التقنية التي تحيط بالأدلة الجنائية المتحصل عليها من شبكة الانترنت أو الحواسيب الآلية أو الهواتف الذكية، والتي تحتاج إلى معرفة تقنية كافية، حيث إن اثبات جريمة الابتزاز الالكتروني تكون عن طريق الدليل الجنائي الرقمي الذي يرتبط بالفضاء الالكتروني. وما يتميز به هذا الدليل من خصوصية تقنية وقانونية في اثبات الجريمة؛ لذلك تعد عملية الاثبات من المعضلات القانونية ومدى حجية هذا الدليل أما القضاء الجنائي المختص.

والأدلة الجنائية في جريمة الابتزاز الالكتروني هي وسيلة الاثبات للجريمة المعلوماتية نسبة لوقوعها في مسرح جريمة افتراضي وليس عادي. ويقصد بالدليل الجنائي في مدلوله العام: "البينة أو الدليل الذي يؤدي إلى استقرار الحق لصاحبه"[١]. ويعرف أيضاً بأنه: "الواقعة التي يستمد منها القاضي البرهان على اثبات قناعته بالحكم النهائي، أو هو الوسيلة في التحقيق بغرض اثبات صحة واقعة الجريمة ونسبها إلى المتهم كظرفٍ مادي" [٢]. أما الدليل الجنائي الرقمي فيقصد به: "مجموعة المعلومات القيمة التي

[١]– انظر، عبد الرحمن خلفي، الإجراءات الجزائية في القانون الجزائري المقارن، الطبعة ٦، دار بلقيس، الجزائر، ٢٠٢٢م، ص ٤٩٢.

[٢]– انظر، عمر نروده، الاثبات في المواد الجنائية، بدون طبعة، دار هوقه، الجزائر، ٢٠٢١م، ص ١٢.

تخزن أو ترسل في شكل رقمي". ويعرف بأنه: "الدليل المأخوذ من الحاسب الآلي والذي يمكن تجميعه وتحليله في شكل دليل يمكن تقديمه أمام القضاء". وبهذا المعنى فإن الدليل الجنائي الرقمي يدخل ضمن الأدلة الجنائية التي يأخذ بها في الاثبات الجنائي ويعتد بحجيتها القضائية[١].

ثانياً: مميزات الدليل الجنائي الرقمي

يتميز الدليل الجنائي الرقمي بخصوصيته التي تميزه عن بقية الأدلة الجنائية الأخرى، فإذا نظرنا اليه من حيث الخصائص المتعلقة بطبيعته فنجده دليل علمي وتقني وتحليلي ومتنوع وقابل للنسخ ويمكن استرجاعه.

أ- دليل علمي: وهو دليل علمي لأنه يمثل الحقيقة وأنه مبني على أسس علمية وقانونية تتماشى مع أحكام القانون، وذلك بأساليب علمية حديثة ووسائل الكترونية وبرامج نظم معلوماتية خاصة.

ب- دليل تقني: ويتميز بأنه دليل فني وتقوم قيمته على طبيعته التقنية، حيث يتم عبر أجهزة الحاسب الآلي أو أي وسيلة تقنية أخرى.

ج- دليل تحليلي: أي أنه يمكن تعقبه ورصده عبر تحركات الجاني المعلوماتية والأماكن التي يتواجد فيها.

[١]- انظر، مروة صلاح الدين محمد، الدليل الالكتروني ومدى حجيته في الاثبات الجنائي، دار العربي للمعارف، القاهرة، ٢٠٢١م، ص ٦١.

د- دليل متنوع: أي أن الأدلة الجنائية الرقمية المستخدمة في اثبات جريمة الابتزاز الالكتروني تتسم بأنها تظهر في اشكال متعددة ومتطورة في بيئة افتراضية متجددة من الصعب احتوائها، وأنها ذات طبيعة ديناميكية حركية فائقة السرعة تنتقل من مكان لآخر في حدود زمانية محددة.

هـ- دليل قابل للنسخ: أي أنه يمكن نسخ صورة طبق الأصل من هذا الدليل، على عكس الأدلة الجنائية العادية التي لا يمكن نسخ صورة طبق الأصل منها[١].

و- دليل يمكن استرجاعه: أي أنه دليل ذو قيمة علمية عالية وتقنية تمكن من استرجاعه بسهولة في حال ما تم تعديل أو حذف محتواها، وذلك الاسترجاع يتم باستخدام برامج تقنية حديثة من خلال قرص التخزين حيث تظل محتفظة بشفرات رقمية خاصة بها تمكنها من استعادة الملفات[٢].

نستطيع القول، بأن كل هذه المميزات تساعد جهة التحقيق في الوصول إلى الجاني وضبطه وتحليل المعلومات والأدلة المتحصل عليها كدليل جنائي رقمي لإثبات جريمة الابتزاز الالكتروني وتوقيع العقوبة عليه.

[١]- انظر، انظر، مروة صلاح الدين محمد، الدليل الالكتروني ومدى حجيته في الاثبات الجنائي، مرجع سابق، ص ٦٤ وما بعدها.

[٢]- انظر، بن طالب ليندا، الدليل الإلكتروني ودوره في الاثبات الجنائي "دراسة مقارنة"، أطروحة دكتوراة، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٩م، ص ٤٣.

ثالثاً: القيمة القانونية للدليل الرقمي في جريمة الابتزاز الالكتروني

نشير في البداية إلى أن هناك صعوبة عملية تعتري الدليل الجنائي الرقمي في اثبات جريمة الابتزاز الالكتروني، تتمثل في امتناع المجني عليه عن الإبلاغ عن الجريمة وذلك خشية من تشويه سمعته سواء كان شخص طبيعي أم غير طبيعي. وبالتالي يصعب الحصول على الدليل الرقمي خاصة إذا مضى عليه زمن قبل أن يتم اكتشاف الجريمة أو التبليغ عنها، مما يهدد قيمة الدليل المادي ويضعف حجيته وبالتالي عد اثبات الجريمة وافلات الجاني المبتز من العقاب[١]. أيضاً هناك برامج إخفاء الهوية التي توفرها تكنولوجيا المعلومات الحديثة للمستخدمين أبرزها برنامج "تور" الأمريكي والذي يعتمد على تقنية التشفير، والتي تعني حظر الوصول وحركة المرور واخفاء عنوان بروتكول الانترنت أي أنه يسمح بتبادل البيانات والمعلومات دون أن يؤدي ذلك إلى كشف هوية ونشاط الجاني[٢].

تتمثل القيمة القانونية للدليل الجنائي الرقمي في أنه جوهر وأساس الحكم القضائي، ولا يمكن توفره إلا بتوفر عناصره والشروط والإجراءات التي يتطلبها نظام الاثبات السعودي. وبالتالي يمكن للقاضي ممارسة سلطته التقديرية في اصدار الحكم الجنائي بناء على هذا الدليل الإلكتروني الصحيح ذو الحجة القضائية. وسلطة القاضي الجنائي في تقدير الدليل الالكتروني تستند لمبدأ قناعة القاضي في تقدير الأدلة والتي

---

[١]- انظر، ديب أرم بن بو عبد الله نورة، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مرجع سابق، ص ٤١٣.

[2]- Obstacles to cyber crime investigations, united office on drugs and crime. Published by; www.unodc.org.

يبني عليها الحكم القضائي. كما أن طبيعة الدليل الرقمي تفرض على القاضي الاستعانة بأهل الخبرة للتأكد من أصالة الدليل الرقمي والحكم وفقاً للملابسات والظروف التي تحيط بالقضية الجنائية[١].

رابعاً: وسائل اثبات جريمة الابتزاز الالكتروني

ولإثبات جريمة الابتزاز الالكتروني على الجاني؛ لابد من اثبات الأدلة الجنائية اللازمة التي تؤكد قيامه بجريمته غير الأخلاقية، سواء كانت الأدلة مكتوبة أم شفهية. أما الأدلة الكتابية فهي تعد أقوى أنواع الأدلة التي يؤخذ بها كأدلة قوية لدى جهات التحقيق والمحاكم الجنائية، وأما الأدلة الصوتية او الشفاهية فهي تعتبر ضعيفة إلى حد ما في الإثبات، ولكنها تعتبر دليل ضد المبتز كفيل بأن يشتبه به في ارتكاب الجريمة تحتاج للتعضيد بأدلة أخرى. وهناك أدلة الكترونية حديثة مثل الرسائل النصية أو رسائل البريد الالكتروني أو الفيديوهات المرئية وحتى الصور التي قد تكون كفيلة بأن تكون دليل اثبات على المبتز[٢].

وعليه، فإن إثبات جريمة الابتزاز يعد أمرًا جوهريًا في أي دعوى جنائية تخص جريمة الابتزاز الالكتروني، والتي يتوجب لإثباتها أن يقدم المجني عليه الأدلة الكافية والقوية. وتتمثل هذه الوسائل في التالي:

---

[١]- انظر، ديب أرم بن بو عبد الله نورة، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مرجع سابق، ص ٤١٠-٤١١.

[٢]- انظر، مقال منشور على موقع سايبر وان، بتاريخ ١٩ فراير ٢٠٢٥م، على الرابط الالكتروني //https://cyberone.com

١.توثيق المحادثات الإلكترونية:

نشهد عصراً رقمياً أفرز لنا عدداً من الجرائم الالكترونية، وتعتبر جريمة الابتزاز الإلكتروني من أكثر جرائم المعلوماتية شيوعًا. ومن المفيد جداً في مسألة إثبات الجريمة توثيق المحادثات التي جرت بين المجني علية والجاني المبتز. وعلى المجني عليه أن يقوم الضحية بتصوير هذه المحادثات مع التركيز على إخفاء اسم الشخص المبتز، مع ضرورة إظهار الرقم أو الوسيلة التي تم من خلالها الاتصال أو ارسال الرسالة الالكترونية. وبهذه الضوابط يعد توثيق المحادثات أو الرسائل بمثابة دليل قوي ذو حجية قضائية ويمكن للمحكمة الاستناد إليه لإثبات تهديد وابتزاز الجاني الذي وقع على المجني عليه.

٢. شهادة الشهود

قد يكون هناك شهود على الابتزاز أو التهديد الصادر من الجاني في بعض حالات جريمة الابتزاز الالكتروني، قد يكون هناك شهود على الابتزاز أو التهديد. يكون لهؤلاء الشهود دور كبير في اثبات جريمة الابتزاز الالكتروني بتقديم شهادتهم أمام القضاء واثبات الجريمة على مرتكبها متى كانت شهادتهم صحيحة. ويجب أيضاً أن تتوفر الشروط القانونية في الشهود حتى يكونوا موثوقين، وأن تكون شهادتهم متفقة مع أحكام النظام السعودي الخاصة بالإثبات بشهادة الشهود أمام المحكمة المختصة.

٣. وسائل اثبات أخرى خاصة

يظهر من خلال الواقع العملي في إثبات قضايا الابتزاز الالكتروني؛ أن هناك وسائل اثبات أخرى إضافة إلى جانب توثيق المحادثات الالكترونية وشهادة الشهود. وذلك

مثل الرسائل النصية الإلكترونية أو العادية التي تحتوي على تهديدات صريحة أو ضمنية من المبتز. أيضا لقطات من كاميرات المراقبة تبين تصرفات مشبوهة من المبتز تجاه الضحية خاصة إذا تم الابتزاز في مكان عام. وكذلك الروابط الإلكترونية التي قد تحوي معلومات تخص الجريمة أو تستخدم كأداة للابتزاز[١].

إن اثبات الابتزاز الالكتروني في المملكة العربية السعودية يقوم على تضافر الجهود بين الجهات التشريعية والتقنية والأمنية، إلى جانب تعزيز الوعي المجتمعي. وتهدف الإجراءات المتبعة عملياً لإثبات جريمة الابتزاز الالكتروني إلى كشف المبتزين وتوقيع العقوبات الرادعة وحماية الأفراد من الانتهاكات الرقمية. وذلك يتم من خلال مراجعة نظام مكافحة جرائم المعلوماتية وتعديله ليتناسب مع المستجدات التقنية وأساليب الجريمة الجديدة، والتعاون بين جهات الدعم الفني من هيئة الاتصالات وتقنية المعلومات والتي توفير خبراء تقنية لتتبع الأدلة الرقمية وتحليلها واثبات الجريمة. أيضاً جهات التحقيق القضائي بهيئة التحقيق والادعاء العام والتي تتولى على عاتقها استلام البلاغات وتحريك الدعوى الجنائية وإحالة الجناة للمحاكم المختصة. إضافة إلى الدور الذي تلعبه حملات التوعية والتثقيف وذلك عبر نشر إرشادات لحماية الخصوصية وتوعية المستخدمين بسبل التعامل مع تهديدات الابتزاز الالكتروني[٢].

---

[١]- انظر، مقال على موقع شورى، بتاريخ ٢٤/ ٤/ ٢٠٢٥م، على الرابط الالكتروني https://www.shwra.sa/ar/blogs

[٢]- انظر، موقع مكتب محاماة الصفوة على الربط الالكتروني https://hd-lawfirm.com.sa/blog

وفي حال التعرض للابتزاز الالكتروني على الضحية حفظ كل ما يمكن أن يكون دليلاً في القضية من محادثات أو رسائل أو تسجيلات والتأكد من صحة المواد التي يهدد المبتز بنشرها وليس مجرد تخويف الضحية، والتي تساعد في إثبات قضية الابتزاز ومن المهم جداً عدم الخوف أو الاستجابة والاستسلام لمطالب المبتز[١].

كما تجدر الإشارة إلى أن مكافحة الابتزاز هي خدمة تقدمها هيئة الأمر بالمعروف والنهي عن المنكر في المملكة العربية السعودية تمكن من مكافحة ابتزاز وتهديد أي شخص سواء عن طريق الرسائل أو الصور لحمله على القيام بفعل الفاحشة أو إعطاء المال. حيث يتم التعامل مع جريمة الابتزاز بسرية تامة مع الحفاظ على خصوصية المجني عليه، حيث يتم فصلها عن أي قضايا أخرى قد تكون مرتبطة بها، ولا يحاسب المجني عليه ولو كان مخطئا ويعاقب المبتز وفقا للجريمة التي ارتكبها، دون التأثير على الضحية بأي شكل. وقد خصصت الهيئة العامة للأمر بالمعروف والنهي عن المنكر رقما موحدا لاستقبال بلاغات الابتزاز الإلكتروني وتقديم الدعم للأفراد المتعرضين لهذه الجرائم وهو (١٩٠٩). وإذا تم التأكد من ارتكاب جريمة الابتزاز الإلكتروني؛ تحال القضية إلى المحاكم الجزائية المختصة وتتم محاكمة الجاني وفقا للأدلة المقدمة[٢].

وللهيئة دور توجيهي بتثقيف جميع شرائح المجتمع من السلوكيات المنحرفة من خلال ‘دارة متخصصة تسمى بإدارة التوعية والتوجيه، ولها دور توعوي وتوجيهي في مكافحة

[١]- انظر، موقع بينة على الرابط الالكتروني //https://bynh.sa .

[٢]- انظر، موقع الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر على الرابط الالكتروني https://www.pv.gov.sa/Pages/PVHome.aspx

جريمة الابتزاز بأنواعه. ولها أيضا دور وقائي في محاربة جريمة الابتزاز قبل وقوعها من خلال متابعة تصرفات الأفراد وحماية الأماكن العامة مثل الأسواق والمدارس والكليات وأماكن تجمع العمالة الوافدة، وكذلك متابعة المواقع الإباحية باتخاذ التدابير اللازمة والنظامية لحفظ المجتمع من هذه الجريمة. وللهيئة دور رجل السلطة العامة بالضبط الجنائي وهو دور تقوم به الهيئة بعد وقوع الجريمة، وتسمى في دول أخرى بالشرطة المجتمعية. وتقوم الهيئة بتلقي البلاغات والشكاوى والإخباريات وجمع المعلومات والتحري الذي يدين الجاني والقبض عليه، مع المحافظة على أدلة الإدانة واثباتها في محضر خاص يسلم لهيئة التحقيق والادعاء العام. كما وللهيئة سلطة التفتيش والبحث بعد القبض على الجاني وضبط أدلة الجريمة وكشف الحقيقة، كما وتقوم الهيئة بإحالة الجاني للجهات المختصة بالتحقيق وهي هيئة التحقيق والادعاء العام[١].

وقد بينت الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر احصائيات تتعلق بجريمة الابتزاز في المملكة العربية السعودية، حيث بلغ عدد حالات الابتزاز بين العام ١٤٢١هـ حتى العام ١٤٢٨هـ بعدد (٢٠٤) حالة في المملكة العربية السعودية منها (١١٦) حالة في الرياض. وبزيادة ملاحظة وصلت الحالات (٣٧٣) حالة في المملكة العربية السعودية، مما يستوجب الوقوف على مسببات الجريمة والعمل على علاجها ومساندة الجهات الأمنية للهيئة. وباستفتاء قامت به الهيئة عن أسباب جريمة الابتزاز شارك فيه (١٠٨٦) فقد أجاب ٤٩,٨% من الأفراد أن سبب الجريمة يرجع إلى

[١]- انظر، علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، مرجع سابق، ص ٦٧-٦٩.

ضعف الإيمان وقلة الوازع الديني، وبنسبة ٢٥,٧% من الأفراد عزى سبب جريمة الابتزاز إلى الإعلام والفضائيات الهابطة. وبنسبة ١٣,٣% من المشاركين في الاستفتاء أكدوا على أن غياب دور الأسرة هو السبب الرئيسي لوقوع جريمة الابتزاز، وبنسبة ١,٢% اجابوا أن السبب هو رفقاء السوء والصحبة السيئة[١]. وبلغت عد الحالات (٢٨٦) حالة ابتزاز في منطقة القصيم شملت النساء والأحداث في الفترة بين (١٤٢٦هـ- ١٤٢٨هـ)، وفي منطقة مكة المكرمة رصدت الهيئة (٦٥) حالة بين الشباب والفتيات بصورهن خلال العام ١٤٢٩هـ، ورصدت (٣٠) حالة في محافظة بريدة و(١٢) حالة في محافظة ينبع[٢].

وأكدت الإدارة العامة للقضايا في الرئاسة العامة لهيئة الأمر بالعروف والنهي عن المنكر أنه قد سجلت (١٨,٨٠٨) قضية في عام ١٤٣١هـ في مختلف مدن المملكة تتنوع بين قضايا ابتزاز أخلاقي وابتزاز مادي وأخرى. وأثبتت الدراسات أن دور ضحايا الابتزاز بسبب ضعف الوازع الديني، وأثبتت دراسة علمية أن أكثر من ٦٥% من الحالات كانت فيها علاقات سابقة وكان للمرأة دور إغراء ضعاف النفوس والتلاعب بمشاعرهم[٣].

إذن، فإن سبل المواجهة لجريمة الابتزاز الالكتروني تتركز في الدور الوقائي والذي هو خير من العلاج. ويتمثل في اصلاح اعوجاج الشباب الأخلاقي وتعلم آداب الشرع

---

[١]- انظر، المرجع نفسه، ص ٢٥-٢٦.

[٢]- انظر، علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، مرجع سابق، ص ٦٦.

[٣]- انظر، المرجع نفسه، ص٤٦.

واحترام خصوصيات وحريات الافراد والتثقيف بمخاطر وسائل التواصل الاجتماعي وضرورة رقابة الأسر بالتوجيه والإرشاد. ويأتي الدور العلاجي عند وقوع الجريمة؛ فنصوص التشريع الملائمة والعقوبات الصارمة ودور الجهات الأمنية المختصة في ملاحقة وضبط الجناة بناء على ما يقدم من شكاوى وبلاغات من الضحايا لدى اللجان المعنية جميعها تصب في سبل المواجهة لجريمة الابتزاز الالكتروني. وان الأدلة الجنائية الرقمية تلعب دورًا حاسمًا ومهماً في اثبات جريمة الابتزاز الالكتروني أمام القضاء الجنائي وضبط الجاني. كما أن الهدف من هذه الإجراءات القانونية في الاثبات هو حماية الأفراد من الاستغلال وضمان تحقيق العدالة بتطبيق العقوبات المناسبة على المبتزين وفقاً لقوانين المملكة العربية السعودية. وإذا كنت ضحية لأي نوع من أنواع الابتزاز الإلكتروني، فلا تتردد في الإبلاغ عنه، وتذكر أن الجهات المختصة قادرة على حمايتك ومعاقبة الجاني ووثق للأدلة التي تساعدك في اثبات الجريمة. وخذ الحيطة والحذر وتأكد دائمًا من تأمين بياناتك وحساباتك الإلكترونية لتفادي الوقوع ضحية لمثل هذه الجريمة.

المطلب الثاني

التطبيقات القضائية لمواجهة جريمة الابتزاز الالكتروني

الابتزاز الإلكتروني هو أحد أنماط الجرائم الالكترونية الاكثر انتشارًا في الفترة الأخيرة ولاسيما في المجتمعات العربية، حيث إن جريمة الابتزاز الإلكتروني اليوم هي جريمة تطال كافة المجتمعات ومختلف الفئات فليس بغريب أن تتفشى أيضاً في المملكة العربية السعودية. لذلك فإن قضايا الابتزاز الإلكتروني تتباين وتتنوع فمنها ما يسهل

حله بطرق ودية ومنها ما يصعب، لذا يضطر البعض للجوء إلى الحلول التقنية والتي قد لا تكون مفيدة أو مجدية في كثير من الأحيان وذلك بسبب الثغرات التقنية. وتعتبر قضايا الابتزاز في المملكة العربية السعودية من أخطر الجرائم التي تواجه المجتمع الحديث، وتتعدد أشكال الابتزاز من ابتزاز إلكتروني إلى ابتزاز عادي استغلال نقاط الضعف في الأفراد بهدف تحقيق مكاسب مادية أو شخصية. وبسبب التطور التكنولوجي السريع، أصبح من الضروري توعية المجتمع حول أخطار الابتزاز وأهمية معرفة العقوبات التي تُفرض على مرتكبي هذه الجرائم وفقًا للقانون السعودي. ومفهوم قضايا الابتزاز يشير إلى الجرائم التي يُجبر فيها شخص أو مجموعة أشخاص على تقديم خدمات أو أموال لجهة معينة تحت التهديد أو التخويف بالكشف عن معلومات خاصة أو إلحاق الأذى بهم، تشمل هذه الجرائم الابتزاز الإلكتروني والذي يُعد من أكثر الأنواع انتشارًا في عصرنا الحالي حيث يستخدم المبتزون التكنولوجيا للسيطرة على الضحايا وتهديدهم.

تجدر الإشارة الهامة إلى أننا سنتناول بالدراسة التحليلية لمجموعة بارزة من قضاء المحاكم الجزائية السعودي، تم عنونة موضوعها الرئيسي بالابتزاز بالتهديد بنشر صور أو مقاطع فديو تحقيقاً لرغبات جنسية أو انتقاماً وتشويه لسمعة الضحايا وما يرتبط به من جرائم اخرى ارتكبها المجرمون ذات صلة بجريمة الابتزاز الإلكتروني. وقد تمت محاكمتهم بناء على نصوص الشريعة الإسلامية أو نظام مكافحة جرائم المعلوماتية السعودي أو نظم جنائية أخرى، وجاءت العقوبات بين العقوبات العادية والعقوبات المشددة وفقاً لظروف كل قضية على حدة. لذلك سنورد الأحكام كما أصدرها القضاء

بما يخص جريمة الابتزاز وما اتصل بها من جريمة أخرى ذات علاقة لا نستطيع تجزأت الحكم فيها أو العقوبات المقررة للأفعال في مجملها احتراماً لهذه الأحكام.

القضية الأولى:

أقام المدعي العام دعواه ضد المدعى عليه بإثبات إدانة المدعي عليه بالخلوة بامرأة أجنبية وفعل الفاحشة وتصويرها بهاتفه الجوال، وبالاستيلاء على أموالها عبر ارتكاب جريمة الابتزاز الالكتروني بنشر صورها مع التخطيط المسبق للجريمة. عرضت الدعوى على المدعى عليه، فأقر بالخلوة المحرمة ودفع بأنها بقصد خطبة الفتاة وأنكر بقية التهم المنسوبة إليه. وجه إليه القاضي التهم وفق ما تم الإقرار به وثبوت صحة نسبته للمتهم من جريمة وحكم عليه بالسجن لمدة عشر سنوات وجلده ألف جلدة متفرقة وبغرامة خمسين ألف ريال، وصُدق الحكم من محكمة الاستئناف[١].

القضية الثانية:

في قضية ثانية عرضت أمام القضاء السعودي وجه المدعي العام الدعوى الجنائية ضد المدعي عليهما وطالب إدانتهما بابتزاز عدد من الفتيات وابتزازهن وذلك بعد مراودتهن عن أنفسهن وتهديدهن والتلفظ عليهن بألفاظ كفر، إضافة لقيامهما بعلاقات محرمة مع بعضهن وممارسة الفاحشة معهن. وجاء الابتزاز بنشر صورهن وأرقامهن عبر الانترنت لتشويه سمعتهن وتخزين مواد اباحية في جوال المتهم الأول، وطلب فعل اللواط مع شخص. وإدانة المتهم الثاني بتخزين مواد إباحية في جواله واتهامه

[١]- انظر، قرار رقم (٣٥٢٥٧٣٤٢) وتاريخ صدوره ٢٦/ ٥/ ١٤٣٥هـ، مجلة الأحكام القضائية لعام ١٤٣٥هـ، ص ١٣٣-١٤١.

بالهروب من أعضاء الهيئة القابضة. عرضت الدعوى على المدعي عليهما فأنكر الأول الدعوى وما نسب إليه من تهم وأن العلاقة كانت بدافع الزواج، أما المتهم الثاني فقد أقر بصحة ما نسب إليه من اتهام.

وبناء على ما ورد في محاضر القبض والتفتيش وشهادة أعضاء الهيئة القابضة يقوي التهمة في حق المتهم الأول وبصحة ما أنكره. قررت المحكمة رد طلب المدعي العام بإقامة حد الردة على المتهم الأول لعدم ثبوتها، إلا أنها أثبتت الإدانة عليه بتهمة إقامته علاقة محرمة مع امرأة والتهديد وابتزازها وحيازة صور ومقاطع فاضحة لهن. وجاء حكم المحكمة على المتهم الأول بالسجن مدة سبع سنوات وبجلده ثمانمائة جلدة مفرقة ومصادرة جواله المستخدم في الجريمة واتلافه مع التوصية بإبعاد المتهم، وحكمت على المتهم الثاني بستين جلدة متفرقة وأوصت بإبعاده عن البلاد، وصدقت محكمة الاستئناف على الحكم[١].

القضية الثالثة:

تتلخص وقائعها في توجيه المدعي العام السعودي إلى المتهم تهمة ابتزاز فتاة تعرف إليها عن طريق موقع الانترنت، وقام بإرسال رسائل تهديد وابتزاز للمجني عليها إن لم تستجب لطلبه فسوف يفضحها بالصور التي يحتفظ بها. ووجه إلى المدعى عليه تهمة مقاومة الفرقة القابضة عليه والاعتداء على رجل الأمن وتمزيق جزء من الزي الرسمي له، وتمت مصادرة الجوال المضبوط وفقاً لأحكام النظام. عرضت الدعوى

[١]- انظر، قرار رقم (٣٥٢٩٢٤٠٣) وتاريخ صدوره ٢٤/ ٦/ ١٤٣٥هـ، مجلة الأحكام القضائية لعام ١٤٣٥هـ، ص ١١٠-١٢٦.

على المدعى عليه وأقر بصحة الاتهام الموجه له. كما أقر بأنه قام بالاختلاء المحرم بالفتاة ومارس معها مقدمات الفحشاء، وأقر بوجود صور للفتاة بحوزته حيث قامت بإرسال الصور اليه وقد قام بابتزازها. وهو أمر محرم شرعاً يستحق التعزير، وقد حكم عليه تعزيراً بالعقوبات التالية:

اولاً: عقوبة السجن لمدة عشرة أشهر ابتداءٍ من تاريخ دخوله التوقيف بسبب هذه القضية وجلده خمسة وتسعون جلدة دفعة واحدة بمكان عام لاختلائه المحرم بفتاة.

ثانياً: عقوبة السجن سنة ونصف، وبغرامة مالية قدره عشرون ألف ريال تودع في خزنة الدولة؛ وذلك وفقاً لنظام مكافحة جرائم المعلوماتية. مع التوصية بترحيل المتهم خارج البلاد –كون المتهم اجنبياً– وعدم السماح له بالعودة للبلاد مرة أخرى اتقاءٍ لشره[١].

القضية الرابعة:

القضية التي بين أيدينا وضوعها جريمة ابتزاز الكتروني بالتهديد والنشر لصور فتاة وقعت ضحية للابتزاز وتم التشهير بسمعتها. حيث أقام المدعي العام دعواه الجزائية لدى المحكمة المختصة ضد المدعي عليه بطلب ادانته بتهديد فتاة ونشر صورها والتشهير بها عبر مواقع التواصل الاجتماعي، والحكم عليه بناءً على نص المادة الثالثة من نظام مكافحة جرائم المعلوماتية السعودي لعام ١٤٢٩هـ وبتطبيق العقوبة المقررة بنص المادة. وعرضت الدعوى على المدعي عليه وأقر بصحة الدعوى

[١]- انظر، قرار رقم (٣٢٨٨٥٩٩) بتاريخ ١/ ٥/ ١٤٣٢هـ، المجلد رقم (٦/ ٨)، ملحق رقم (٣)، مجلة الأحكام القضائية لعام ١٤٣٢هـ، ص ٢.

الموجهة ضده، وبعد ثبوت الإدانة من القاضي المختص بنظر الدعوى الجنائية تم الحكم على المتهم بالسجن مدة وقدرها سنتين وجلده ثلاثمائة جلة مفرقة وبالغرامة عشرة آلاف ريال مع التوصية بإبعاده عن البلاد بعد قضاء عقوبته ومحكوميته، وصدق الحكم لدى محكمة الاستئناف[١].

القضية الخامسة:

أقام المدعي العام تهمة تهديد فتاة ونشر صورها وابتزازها عبر شبكة الانترنت وحيازة مواد اباحية بجواله وأفعال اخرى لإدانة المدعي عليه؛ وذلك في الدعوى الجنائية المعروضة أمام المحكمة الجنائية المختصة. عرضت الدعوى على المدعي عليه وأقر بعلاقته المحرمة مع الفتاة وحيازته للمواد الإباحية وأنكر بقية التهم المنسوبة اليه بالابتزاز الالكتروني. وبالاطلاع على محاضر التفتيش والاستجواب والمعاينة والأدلة المقدمة بالدعوى التي تتضمن صحة الاتهام الموجه للمدعي عليه فيما اقره؛ حكمت المحكمة عليه بالسجن لمدة ستة أشهر وبجلده مئة وخمسين جلدة مفرقة وصرف النظر عن العقوبة الواردة في المادة الثالثة من النظام والتي طالب بتطبيقها المدعي العام ومصادرة المضبوطات، وصدق الحكم من محكمة الاستئناف[٢].

---

[١]- انظر، قرار رقم (٣٥١٠٢٤٠٨) بتاريخ ٢/ ١/ ١٤٣٥هـ، مجلة الأحكام القضائية لعام ١٤٣٥هـ، ص ١٠٦.

[٢]- انظر، قرار رقم (٣٥١٨٥٢٤٢) بتاريخ ٢٢/ ٣/ ١٤٣٥هـ، مجلة الأحكام القضائية لعام ١٤٣٥هـ، ص ١٢٧-١٣٢.

خاتمة:

اتسعت استخدامات شبكة المعلوماتية والانترنت في مختلف المجالات ورغم مزاياها التي لا ينكرها أحد؛ إلا أن لها أضرار أيضاً منها جريمة الابتزاز الالكتروني والتي تتمثل في السلوك الاجرامي الذي يمس خصوصيات وحرمات الأفراد في المجتمع ويشيع الجرائم غير الأخلاقية بينهم. فكان لابد من الوقوف على موضوعات جريمة الابتزاز الالكتروني بالدراسة التحليلية وفقاً لأحكام النظام السعودي ودور لجنة هيئة الأمر بالمعروف والنهي عن المنكر وتطبيقات القضاء؛ لمكافحة هذه الجريمة والحد منها وحماية لحرية الأفراد ومنع الاعتداء على سمعتهم وأموالهم دون وجه حق. وتوصل البحث إلى أبرز النتائج والتوصيات، وهي كالآتي:

أولا: النتائج

١. جريمة الابتزاز الالكتروني هي الدخول غير المشروع بتهديد أو ابتزاز المجني عليه للقيام بعمل أو الامتناع عن العمل ولو كان مشروعاً إلا إذا نفذ ما هدد به من نشر الصور أو الفيديوهات أو المعلومات السرية.

٢. حداثة جريمة الابتزاز الالكتروني وعالمية الجريمة وقيام السلوك الاجرامي عبر وسائل الكتروني جعل من الصعب اكتشاف الجريمة ومعاقبة الجاني.

٣. الدليل الجنائي الرقمي له أثر كبير في اثبات جريمة الابتزاز الالكتروني، ولكن احجام المجني عليه عن التبليغ يهدد حجية هذا الدليل وبالتالي عدم إثبات الجريمة وإفلات الجاني أو المبتز.

٤. تتمثل جهات مكافحة جريمة الابتزاز الالكتروني في المملكة العربية السعودية، في التشريعات وهيئة الأمر بالمعروف والنهي عن المنكر وهيئة التحقيق والادعاء العام والمحاكم المختصة.

ثانياً: التوصيات

١. تشديد العقوبات المقررة لجريمة الابتزاز الالكتروني للحد من الجريمة وتخويف المجرمين بالجزاء الجنائي الصارم الذي ينتظرهم.

٢. على الجهات المعنية بالمكافحة تقديم البرامج التثقيفية والتوعوية بخطورة جريمة الابتزاز الالكتروني والتي تستهدف فئة الشباب ودورهم الفعال في الوقاية من الجريمة.

٣. تشجيع الضحايا بتقديم الشكاوٍ السرية عبر رقمٍ موحد ضد المبتزين لملاحقتهم وضبطهم، ومساعدة وتأهيل الضحايا وفقاً لبرامج علاجية معينة تقدمها الجهات المختصة في الدولة.

٤. تكامل التعاون الدولي لمواجهة جريمة الابتزاز الالكتروني والاستفادة من خبرات الدول في التعامل مع الدليل الرقمي لإثبات الجريمة وكشف الجناة ومعاقبتهم.

قائمة المراجع والمصادر

اولاً: كتب اللغة

١. أحمد رضا، معجم متن اللغة العربية، مكتبة الشروق الدولية، ٢٠١٧م.
٢. محمد بن مكرم بن علي أبو الفضل جمال الدين ابن منظور الأنصاري الرويفعي (المتوفي عام ٧١١هـ)، لسان العرب، (٥/ ٣١٢)، دار صادر بيروت، الطبعة الثالثة، ١٤١٤هـ.

ثانياً: الكتب القانونية

١. أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣م.
٢. أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم العام، ج ١، دار النهضة العربية، القاهرة، ١٩٨١م.
٣. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني، دار النهضة العربية للطباعة والنشر، مصر، ٢٠٠٦م.
٤. أنغام سالم سعيد بن غانم، جرائم الابتزاز الالكتروني (دراسة مقارنة)، دار النهضة العلمية للنشر والتوزيع، الامارات، ٢٠٢٤م.
٥. جميل عبد الباقي الصقر، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ١٩٩٢م.
٦. حسن صادق المرصفاوي، شرح قانون العقوبات –القسم الخاص، منشأة المعاف، الإسكندرية، ١٩٩٠م.

٧. زهراء عادل سلبي، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، ط١، دار الأكاديميون للنشر والتوزيع، عمان – الأردن، ٢٠٢٠م.

٨. رمسيس بهنام، قانون العقوبات– القسم الخاص، ط١، منشأة المعارف، الإسكندرية، ١٩٩٩م.

٩. سامح السيد جاد، شرح قانون العقوبات– القسم العام، الدار الهندسية الحديثة للطباعة والنشر، القاهرة، ٢٠٠٥م.

١٠. سعد معن إبراهيم الموسوي، الابتزاز الالكتروني: طرقه والوقاية منه، دار الهالة للنشر والتوزيع، مصر، ٢٠٢٢م.

١١. سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم التواصل الاجتماعي "دراسة مقارنة"، دور المعرفة للنشر والتوزيع، الإسكندرية، ٢٠٢٢م.

١٢. عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات – شرح الاحكام الموضوعية في قانون الجرائم الإلكترونية، ط١، دار وائل للنشر والتوزيع، عمان، الأردن، ٢٠١٧م.

١٣. عبد الرحمن خلفي، الإجراءات الجزائية في القانون الجزائري المقارن، الطبعة ٦، دار بلقيس، الجزائر، ٢٠٢٢م.

١٤. عبد العزيز بن حمين، الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، بحوث ندوة الابتزاز المفهوم الأسباب العلاج، فهرسة مكتبة الملك فهد الوطنية، الرياض، ١٤٣٢هـ.

١٥. على حسن الطوالبة، الجرائم الإلكترونية، مطبعة جامعة العلوم التطبيقية، البحرين، ٢٠٠٨م.

١٦. عمار عباس الحسيني، جريمة الابتزاز الالكتروني، منشورات زين الحقوقية، بيروت، لبنان، ٢٠٢٢م.

١٧. عمر نروده، الاثبات في المواد الجنائية، بدون طبعة، دار هوقة، الجزائر، ٢٠٢١م.

١٨. محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الاردن ٢٠٠٩م .

١٩. محمد شلال العاني، علي حسن طوالبة، علم الإجرام والعقاب، ط١، دار المسيرة، عمان، ١٩٩٨م.

٢٠. محمد علي العريان، الجرائم المعلوماتية: انعكاسات دورة المعلومات على قانون العقوبات، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٤م.

٢١. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م.

٢٢. مروة صلاح الدين محمد، الدليل الالكتروني ومدى حجيته في الاثبات الجنائي، دار العربي للمعارف، القاهرة، ٢٠٢١م.

ثالثاً: المقالات والدوريات

١. أحمد مصطفى محرم، استخدامات الذكاء الاصطناعي "استخدام خاصية التزييف العميق" في قذف الغير أنموذجاً" "دراسة فقهية مقارنة معاصرة"،

مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بالقاهرة، العدد ٣٩، أكتوبر ٢٠٢٢م.

٢. أشرف عبد لسلام علي كيلاني، الابتزاز الالكتروني والآثار المترتبة عليه "دراسة فقهية مقارنة"، مجلة البحوث الفقهية والقانونية، العدد ٤٦، يوليو ٢٠٢٤م.

٣. افراح بن خميس بن عامر، مشكلة الابتزاز الالكتروني لدى طلبة مرحلة التعليم ما بعد الأساس ودور الخدمة الاجتماعية في المجال المدرسي في التعامل معه، رسالة ماجستير- كلية الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، سلطنة عمان، ٢٠١٨م.

٤. آمال قارة، الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، ٢٠٠٢م.

٥. ايمان بنت محمد علي عادل عزام، العقوبة في نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية "دراسة تأصيلية مقارنة"، مجلة العدل، العدد ٨٢، رجب ١٤٣٩هـ.

٦. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري – دراسة مقارنة، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٩م.

٧. بن طالب ليندا، الدليل الإلكتروني ودوره في الاثبات الجنائي "دراسة مقارنة"، أطروحة دكتوراة، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٩م.

٨. جاسم ناصر السلماني، التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري، رسالة ماجستير، جامعة قطر، ٢٠٢٣م.

٩. خالد حسن أحمد، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، ٢٠١٩م.

١٠. خليفة علي محمد، ابتزاز الأحداث وعقوبته في النظام السعودي، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٥م.

١١. داليا عبد العزيز، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي "دراسة مقارنة"، مجلة جيل الأبحاث القانونية المعمقة، المملكة العربية السعودية، العدد ٢٥، مايو ٢٠١٨م.

١٢. ديب أرم بن بو عبد الله نورة، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مجلة الحقوق والعلوم الإنسانية، المجلد ٦، العدد ١، ٢٠٢٣م.

١٣. ذياب موسى البداينة، الجرائم الإلكترونية المفهوم والأسباب"، ورقة علمية مقدمة خلال الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من ٢-٤ /٢٠١٤/٩ م، عمان – الأردن، ٢٠١٤م.

١٤. زهراء عادل عبد الحميد، جريمة الابتزاز الإلكتروني "دراسة مقارنة"، رسالة ماجستير، كلية الحقوق- جامعة عمان الأهلية، الأردن، ٢٠١٩م.

١٥. زينب محمود حسين، المواجهة الجنائية للابتزاز الالكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ١٠، العدد ٣٧، ٢٠٢١م.

١٦. سامي مرزوق نجا، المسؤولية الجنائية عن الابتزاز الالكتروني في النظام السعودي، رسالة ماجستير- جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٥م.

١٧. سعد الحاج بكري، شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الأمنية والتدريب، الرياض، ١٩٩٠م.

١٨. سليمان بن عبد الرازق القريات وآخرون، صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، العدد ٦٩، يناير ٢٠١٨م .

١٩. علي عبد الله شديد الصياح، بحوث ندوة الابتزاز (المفهوم- الأسباب- العلاج)، مركز باحثات لدراسات المرأة، مكتبة الملك فهد الوطنية للنشر، الرياض، ١٤٣٢هـ.

٢٠. ماجد سعد مرشد العتيبي، دور الأنظمة في الحد من جريمة الابتزاز الالكتروني "دراسة مقارنة في الأنظمة المنظمة للابتزاز الالكتروني في النظام السعودي والقانون الاماراتي"، المجلة العربية للنشر العلمي، العدد ٧٥، الإصدار الثامن، كانون الثاني ٢٠٢٥م.

٢١. محمد علي سالم، حسون عبيد، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد ١٤، العدد ٢، العراق، ٢٠٠٧.

٢٢. مريم غراب، جريمة التهديد والابتزاز الالكتروني، مجلة الدراسات القانونية المقارنة، المجلد ٧، العدد ١، الجزائر، ٢٠٢١م.

٢٣. ممدوح رشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الأمنية، المجلد٣٣، العدد٧٠، الرياض، ٢٠١٧م.

٢٤. منصور عبد السلام عبد الحميد حسان، جريمة الابتزاز الالكتروني "دراسة مقارنة بين القانون المصري والفرنسي والاماراتي والنظام السعودي"، المجلة القانونية، بدون سنة نشر.

٢٥. وفاء محمد صقر، جريمة الابتزاز الالكتروني "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق- جامعة بني سويف، المجلد ٣٦، العدد ٢، يوليو ٢٠٢٤م.

رابعاً: المراجع الالكترونية

١. طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الالكتروني عبر وسائل التواصل الاجتماعي،٢٠٢٢م، ص ٤٠-٤٦، مقال على موقع المرجع الالكتروني للمعلوماتية، https://almerja.com/reading.php?idm=187687

٢. مقال على موقع شورى، بتاريخ ٢٤/ ٤/ ٢٠٢٥م، على الرابط الالكتروني https://www.shwra.sa/ar/blogs

٣. مقال منشور على موقع سايبر وان، بتاريخ ١٩ فراير ٢٠٢٥م، على الرابط الالكتروني https://cyberone.com

٤. موقع الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر على الرابط الالكتروني https://www.pv.gov.sa/Pages/PVHome.aspx

٥. موقع بينة على الرابط الالكتروني //https://bynh.sa

٦. موقع مكتب محاماة الصفوة على الربط الالكتروني https://hd-lawfirm.com.sa/blog

خامساً: القوانين والقضايا

١. نظام مكافحة جرائم المعلوماتية، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ.

٢. قرار رقم (٣٢٨٨٥٩٩) بتاريخ ١/ ٥/ ١٤٣٢هـ، المجلد رقم (٦/ ٨)، ملحق رقم (٣)، مجلة الأحكام القضائية لعام ١٤٣٢هـ.

٣. قرار رقم (٣٥١٨٥٢٤٢) بتاريخ ٢٢/ ٣/ ١٤٣٥هـ، مجلة الأحكام القضائية لعام ١٤٣٥هـ.

٤. قرار رقم (٣٢٨٨٥٩٩) بتاريخ ١/ ٥/ ١٤٣٢هـ، المجلد رقم (٦/ ٨)، ملحق رقم (٣)، مجلة الأحكام القضائية لعام ١٤٣٢هـ.

٥. قرار رقم (٣٥٢٩٢٤٠٣) وتاريخ صدوره ٢٤/ ٦/ ١٤٣٥هـ، مجلة الأحكام القضائية لعام ١٤٣٥هـ.

سادساً: المراجع الأجنبية

1.John. Dr. Mercer, Cybersquatting: blackmail on the information superhighway, Hein onlin68. U. J. SCI& Tech L. 290,2000, P.11.

2.Omer Abdulsalam Hussein, prof, Dr. Nazura Abdul manap, prof, Dr. Mohammed Rizal, Cyber blackmail crime against women- A case study, journal of positive school psychology, 2022 Vol No3,6882- 6893, P3.

3. Obstacles to cybercrime investigations, united office on drugs and crime. Published by; www.unodc.org.