

عنوان الرسالة

الإبتهاز الإلكتروني: دراسة مقارنة بين التشريعين السعودي والإماراتي

رسالة ماجستير مقدمة في تخصص القانون الرقمي

إعداد الطالب/

سعيد سالم الزهراني

الرقم الجامعي/

243000600

إشراف/

د

العام الدراسي:

2025

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الإهداء

إلى من كان لهم الفضل بعد الله في وصولي إلى هذه المرحلة...

إلى من غمروني بحبهم، وصبرهم، ودعائهم الصادق...

إلى والديَّ العزيزين، اللذين زرعاً فيَّ حب العلم، وكانا دائماً الداعمين الأوائل لي في كل خطوة.

إلى إخوتي وأخواتي، سندي في الحياة، ومصدر سعادتي في لحظات التعب.

إلى أصدقائي الذين شاركوني رحلة البحث، ووقفوا بجاني في أوقات التحديات.

إلى كل من ساندني ولو بكلمة طيبة...

أهدي ثمرة هذا الجهد المتواضع، راجي من الله أن يكتب لي القبول والتوفيق.

الشكر والتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبفضله تيسر الصعوبات، وبه نستعين على إتمام الأعمال وتحقيق الغايات.

أتقدم بجزيل الشكر والعرفان لمشرفي الكريم على دعمه المستمر، وتوجيهاته السديدة، وصبره الكبير خلال إعداد هذه الرسالة، فله مني كل الاحترام والتقدير.

كما أود أن أعبر عن بالغ امتناني لكل أعضاء هيئة التدريس بقسم القانون الرقعي في جامعة ميدأوشن لما قدموه من علم ومعرفة كانت نبراساً في طريقي.

مستخلص الدراسة

هدفت هذه الدراسة إلى التعرف على الإبتزاز الإلكتروني في التشريعين السعودي والإماراتي، وتقييم مدى فاعلية القوانين الحالية في مواجهة الإبتزاز الإلكتروني، واقتراح توصيات قانونية علمية لتطوير التشريعات الحالية في ضوء ما تصل إليه من نتائج، واعتمدت هذه الدراسة علي المنهج الاستقرائي والمنهج التحليلي والمنهج المقارن، وأظهرت نتائج الدراسة أن كلاً من التشريعين السعودي والإماراتي تُدمجا الإبتزاز الإلكتروني في تشريعاتهما لمكافحة الجرائم الإلكترونية سعياً منهما لتسليط الضوء على هذه الجريمة. وفي ظل الثورة الرقمية، يُشير هذا إلى إدراك المشرعين لأهمية هذا الوضع، واتفق التشريعين على تجريم الإبتزاز الإلكتروني ومعاينة محاولاته والتورط فيه. كما اعتمدا مبدأ تمتع القضاة بسلطة تقديرية في تحديد العقوبة المناسبة، مع مراعاة خصوصيات كل حالة، وأوصت الدراسة بمعالجة هذه القضايا بفعالية وسرعة، ينبغي على الأجهزة الأمنية تفعيل فرق مكافحة الإبتزاز الإلكتروني وتزويدها بأحدث التقنيات والكوادر القانونية المؤهلة، ومن خلال الجهود المتواصلة التي تشارك فيها وزارات التعليم والإعلام والشؤون الاجتماعية، تعزيز فهم المجتمع للقانون والتكنولوجيا الرقمية لمكافحة هذه الجريمة، وخاصة بين الشباب.

قائمة المحتويات

الإهداء	3
الشكر والتقدير	4
مستخلص الدراسة	5
الفصل الأول	8
مقدمة:.....	9
مشكلة الدراسة:.....	11
تساؤلات الدراسة:.....	11
أهمية الدراسة:.....	12
أهداف الدراسة:.....	13
الدراسات السابقة:.....	13
- مبررات الدراسة:.....	17
المنهجية وطرق البحث:.....	18
خطة البحث:.....	19
الفصل الثاني	20
المبحث الأول: ماهو الابتزاز الإلكتروني وأركان جريمة الابتزاز الإلكتروني.....	21
1- ماهو الابتزاز الإلكتروني :	21
2- أركان جريمة الابتزاز الإلكتروني	24
المبحث الثاني خصائص الابتزاز الإلكتروني وأثاره.....	27
1- خصائص الابتزاز الإلكتروني	27
2- اثار جريمة الابتزاز الإلكتروني	29
المبحث الثالث أنواع جرائم الابتزاز الإلكتروني وصورها.....	32
1- أنواع جرائم الابتزاز الإلكتروني	32

34	2- صور جرائم الإبتزاز الإلكتروني
37	الفصل الثالث
37	المبحث الأول: الإبتزاز الإلكتروني في التشريع السعودي
37	1- عقوبة الإبتزاز في التشريع السعودي
40	2- تشديد عقوبة الإبتزاز الإلكتروني في النظام السعودي
41	3- عقوبة الشروع في جريمة الإبتزاز الإلكتروني
41	4- عقوبة المساهمة في جريمة الإبتزاز الإلكتروني
42	المبحث الثاني: الإبتزاز الإلكتروني في التشريع الإماراتي
42	1- عقوبة الإبتزاز في التشريع الإماراتي
44	2- عقوبة الشروع في جريمة الإبتزاز الإلكتروني
44	3- تشديد عقوبة الإبتزاز الإلكتروني في التشريع الإماراتي
44	المبحث الثالث: تقييم التشريعين السعودي والإماراتي والحلول المقترحة لمواجهة هذا الإبتزاز
44	1- تقييم التشريعين السعودي والإماراتي
46	2- الحلول المقترحة لمواجهة هذا الإبتزاز
47	الفصل الرابع
48	الخاتمة
49	نتائج الدراسة:
50	توصيات الدراسة:
51	المراجع:

الفصل الأول

تخطيط البحث

مقدمة:

الأمن والطمأنينة من أعظم النعم، والخوف والاضطراب من أسوء النقم؛ لذا كان الابتزاز من أبشع الجرائم، لكونه يؤثر في شعور الإنسان بالأمن، فيثر الرعب والفرع لديه، ويترك أثراً في نفسه أشد من إصابة جسده، فيدفعه لإتيان فعل أو الامتناع عنه، سواء أكان مشروع، أم غير مشروع دون إرادته، مما يشكل عدواناً على حقه في الرفاه الاجتماعي والنفسي كأحد حقوق الإنسان، فالتشريعات جليها لا تقيم وزناً للتصرفات التي ترتكب دون إرادة حرة مستنيرة¹

الجريمة ظاهرة إنسانية قديمة قدم الوجود البشري ومع التطور العلمي والتقني في ظل النهضة التكنولوجية التي نشهدها الآن ظهرت أنماط غير تقليدية من الجريمة، على نحو يدفع الأنظمة القانونية نحو التطور التشريعي لتصبح مواكبة لحركة التطور والتعقيد ولكي يمكن مواجهة مثل تلك الظواهر ولعل ظهور الإنترنت وانتشار تقنياته كان لها عظيم الأثر في نشر عدد من تلك الصور المستحدثة من الجريمة، في ظل ما يشهده العالم من تقدم ملحوظ في مجال التكنولوجيا وتقنية المعلومات والاتصالات أصبح العالم بفضلها قرية صغيرة، إذ إن من أبرز مميزاتها أنها سهلت عملية تواصل الأشخاص بعضهم ببعض بكل يسر وسهولة، كما أنها أصبحت ركيزة أساسية يعتمد عليها الكثير من الجهات الحكومية في تعاملاتها اليومية، وعلى الرغم من هذه الإيجابيات التي تشهدها تلك التكنولوجيا الحديثة، إلا أنها سرعان ما أصبحت نقمة على البشرية، حيث يستخدمها بعض الأشخاص الخارجين عن القانون بشكل غير مشروع، فأصبحت مسرحاً سهلاً لارتكاب جرائمهم التي تُهدّد أمن واستقرار الأفراد والدولة²

¹ صالح، تامر. (2018)، الابتزاز الإلكتروني: دراسة تحليلية مقارنة، مجلة كلية الحقوق للبحوث القانونية

والاقتصادية، (1)، ص 576

² محمد، محمد. (2024)، جريمة الابتزاز الإلكتروني: دراسة مقارنة، مجلة قطاع الشريعة والقانون، (16)، ص 1656

من بين هذه الجرائم ظهر الإبتزاز عبر الوسائط الإلكترونية أو ما نطلق عليه الإبتزاز الإلكتروني الذي يتخذ فيه الجاني من الوسائط الإلكترونية وسيلة لخرق خصوصية ضحيته والحصول على أسرارته ومعلوماته الخاصة التي يخشي نشرها ثم يهدده بنشرها وفضحها كي توصل من ذلك الى الحصول منه على منفعة مادية كانت أو غير مادية أو ليدفعه الى القيام بعمل أو الامتناع عن عمل ما كان ليقوم به لولا خشيته من التهديد لموجه اليه من الجاني بفضح أسرارته³

ومن بين تلك الدول التي ساهمت في تجريم هذه الجريمة المملكة العربية السعودية، حيث قام المنظم السعودي بوضع نظام خاص يعالج الجرائم الإلكترونية التي تُرتكب بواسطة التكنولوجيا الحديثة، ومن بينها الإبتزاز الإلكتروني بنظام مكافحة الجرائم المعلوماتية فوضع عقوبات سواء كانت أصلية أو غير أصلية وغيرها من العقوبات التي تسهم بردع الجناة، وأيضاً قامت دولة الإمارات العربية بتجريم ذات الجريمة، فقد قام المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية بمكافحة هذه الجريمة حيث وضع المشرع نصاً يجرمها، وسنَّ لها عقوبات توقع على مرتكبيها، فهدَفُ كُلُّ من المشرع الإماراتي وكذلك المنظم السعودي هو مكافحة الإبتزاز الإلكتروني، وحماية مصالح الأفراد من أن يقع عليها أي ضرر يهدد استقرارهم وأمنهم.

إن الانتشار المتزايد للإبتزاز الإلكتروني في الثقافة المعاصرة، وخاصة بين الشباب، هو ما دفعني لاختيار هذا الموضوع. إذ يتأثر الاستقرار النفسي والاجتماعي للضحيا سلباً عند استغلالهم مالياً أو أخلاقياً. كما أن حساسية هذه الجريمة تستلزم وجود هيكل قانوني دقيق يحقق التوازن بين ردع المجرمين وحماية الحريات والحقوق الفردية.

³ صالح، تامر. (2018)، الإبتزاز الإلكتروني : دراسة تحليلية مقارنة، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، (1)، ص 546

من الناحية القانونية، من المهم أن المملكة العربية السعودية والإمارات العربية المتحدة دولتان أولتا اهتمامًا بالغًا للجرائم الإلكترونية، وأصدرتا قوانين وأنظمةً مُحدثة لمواكبة التقنيات الناشئة. لذلك، من الضروري مقارنة الأنظمة القانونية في الدولتين لتحديد أوجه التشابه والاختلاف، وتقييم مدى فعالية هذه القوانين في الحد من وقوعها.

مشكلة الدراسة:

تبرز جريمة الابتزاز الإلكتروني كإحدى الجرائم المستحدثة التي ظهرت مؤخرًا، والتي أثرت على عدد كبير من أفراد المجتمع، وخاصة النساء اللواتي تعرضن ولا زلن يتعرضن للابتزاز الإلكتروني من قبل بعض الشباب، وذلك من خلال التهديد بعرض صورهن في مواقع التواصل الاجتماعي، فمن الممكن أن يقوم الجاني بعد إطلاعه على بعض المعلومات باستغلال معرفته بهذه المعلومات لابتزاز أو تهديد صاحب هذه المعلومات أو من تمسكه هذه المعلومات؛ مما يؤدي إلى المس بحرمة الحياة الخاصة بالأفراد، أو الجهات التي ترتبط بها هذه المعلومة في حال عدم حصول المجرم الإلكتروني على مبتغاه من المجني عليه وهذا الأمر يستدعي دراسة الموضوع من الناحية القانونية لذلك جاءت الدراسة الحالية للتعرف على الابتزاز الإلكتروني: دراسة مقارنة بين التشريعين السعودي والإماراتي

تساؤلات الدراسة:

ويتمثل سؤال الدراسة الحالي في ماهو الابتزاز الإلكتروني في التشريعين السعودي والإماراتي؟ ويتفرع منه الأسئلة الفرعية التالية:

1. ماهو الابتزاز الإلكتروني؟ وماهو خصائصه؟
2. ماهو وسائل الابتزاز الإلكتروني وصوره؟
3. ماالأركان القانونية المكونة لجريمة الابتزاز الإلكتروني في النظامين السعودي والإماراتي ؟
4. مأوجه القصور والتحديات في التشريعين فيما يتعلق بمكافحة الابتزاز الإلكتروني؟

أهمية الدراسة:

- الأهمية العلمية:

1. وفقاً للهيئة التنظيمية السعودية والمشرّع الإماراتي، تُسهم هذه الدراسة في تعريف جريمة الابتزاز الإلكتروني وتُحقق ذلك من خلال توضيح تعريف الابتزاز الإلكتروني، وأشكاله المختلفة، ودوافعه. كما تُوضح مراحل، وأسس جريمة الابتزاز الإلكتروني، وعواقبه على المُبتز، وكيفية إيقافه.

2. إن تحليل الفروقات التشريعية وأوجه التشابه بين النظامين القانونيين في المملكة العربية السعودية والإمارات العربية المتحدة فيما يتعلق بجريمة الابتزاز الإلكتروني هو ما يُضفي على هذا العمل أهميته العلمية، إذ يُوسّع نطاق مقارنة القوانين العربية، ويُعزز الفهم القانوني في مجال الجرائم الإلكترونية.

3. تضيف الدراسة إلى مجموعة المعرفة حول كيفية تعامل التشريعات الوطنية مع هذه الجريمة، وهو ما قد يساعد الباحثين والخبراء الجنائيين والقانونيين على إنشاء دراسات مستقبلية أكثر تخصصاً.

- الأهمية العملية

1. إن المساهمة في توسيع نطاق البحث القانوني حول هذا الموضوع في المكتبات القانونية أمرٌ بالغ الأهمية لمساعدة القراء والباحثين القانونيين وغيرهم من المهتمين بهذا الموضوع. فإلى جانب لفت انتباه الدولة إلى خطورة هذه الجريمة التي تُهدد أمن واستقرار مواطنيها، يسعى المشروع أيضاً إلى زيادة الوعي العام.

2. في ظل الاستخدام المتزايد للتكنولوجيا ووسائل التواصل الاجتماعي، تتجلى الأهمية العملية للدراسة في مساهمتها في إرساء أنظمة قانونية وطنية وتعزيز إجراءات الوقاية من الابتزاز ومعاقبته.

3. كما تُشدد الدراسة على مخاطر الابتزاز الإلكتروني وضرورة زيادة الوعي العام به، مما يُعزز الأمن السيبراني ويحمي الأفراد من الوقوع ضحايا لهذه الجريمة، مما يُعزز السلامة والاستقرار في المجتمع.

أهداف الدراسة:

1. التعرف على الإبتزاز الإلكتروني في التشريعين السعودي والإماراتي.
2. التعرف على خصائص الابتزاز الإلكتروني
3. التعرف على وسائل الإبتزاز الإلكتروني وصوره
4. التعرف على موقف القانونين السعودي والإماراتي من الإبتزاز الإلكتروني.
5. تقييم مدى فاعلية القوانين الحالية في مواجهة الإبتزاز الإلكتروني، واقتراح توصيات قانونية علمية لتطوير التشريعات الحالية في ضوء ما تصل إليه من نتائج

الدراسات السابقة:

دراسة (غازي، 2024) بعنوان موظفو الأجهزة الأمنية والابتزاز الإلكتروني: دراسة في وزارة الداخلية هدفت الدراسة إلى الكشف عن الأسباب التي تقف وراء تعرض رجال الشرطة للابتزاز الإلكتروني ومعرفة الأهداف والأسباب الكامنة وراء ابتزاز رجال الشرطة، فضلاً عن معرفة الأسباب التي تدفع رجال الشرطة إلى اللجوء إلى مواقع التواصل الاجتماعي كبديل للجهات الرقابية الرسمية ومعالجة تلك الأسباب. ولتحقيق أهداف الدراسة تم تصميم وبناء استبانة في ضوء الأدبيات المتعلقة بموضوع البحث وآراء المختصين والخبراء. تم استخدام المنهج الوصفي التحليلي، إذ تكون مجتمع البحث من الضباط

والمنتسبين والموظفين المدنيين في مقر وزارة الداخلية في العاصمة بغداد، وتكونت عينة البحث من (٣٠٠) فرداً إجمالاً، وأظهرت نتائج الدراسة أن فئة ضباط الشرطة هي الفئة الأكثر عرضة للابتزاز نظراً لامتلاكهم الإمكانيات لتحقيق أهداف المبتز، وعدم إلمام معظم رجال الشرطة بالأدوات القانونية التي تجرم الابتزاز نظراً لعدم توفرها بشكل كافٍ. التدريب على مواجهة هذا التهديد. وبشكل عام فإن الدافع المالي وراء ارتكاب هذا النوع من الجرائم كان بالرغم من وجود دوافع وظيفية وشخصية أخرى منها خوف الشرطي من اتهامه بالابتزاز وضعف الإجراءات الرسمية قد يدفع عدداً من رجال الشرطة إلى الامتناع عن الإبلاغ عن حالات الابتزاز إلى التي يتعرضون لها. كما كشفت الدراسة عن وجود آثار نفسية واجتماعية ووظيفية يتعرض لها ضحايا رجال الشرطة. وأوصى البحث بضرورة اعتماد ما توصل إليه من نتائج بشأن أسباب تعرض ضباط الشرطة للابتزاز الإلكتروني، وحث وكيل الوزارة للشؤون الإدارية والمالية على توجيه كافة أقسام وإدارات الوزارة بإجراء تحقيق في أسباب الاستقالة أو الفصل من الوظيفة أو المسؤولية التي يوفرها ضابط الشرطة، بالإضافة إلى توجيه الدوائر القانونية في الوزارة بضرورة التحقق من هوية المشتكي قبل البدء في التحقيق، وتوفير الحماية القانونية للشرطي للتأكد من أنه مطلع على حالات ابتزاز.

دراسة (البياتي، 2022) بعنوان الابتزاز الإلكتروني

يتضمن البحث تعريف مشكلة البحث والتي تشمل توضيح طبيعة الابتزاز الإلكتروني كجريمة جديدة انتشرت في المجتمع وآثارها واضحة وتوضيح طبيعة مرتكبيها وضحاياها وأسبابها وأنواعها ودوافعها، والأحكام الشرعية والقانونية لمرتكبي جريمة الابتزاز الإلكتروني، ومن ثم تقديم المقترحات التي تعتبر نوعاً من المعالجات لمنع "الابتزاز الإلكتروني الذي يتعرض له أفراد المجتمع، رجالاً ونساء" ولذلك جاء البحث كمحاولة بسيطة لتسليط الضوء على هذه الظاهرة.

دراسة (حنون، 2021) بعنوان جريمة الابتزاز الإلكتروني: دراسة مقارنة

يستعرض هذا البحث جريمة الابتزاز الإلكتروني، التي أصبحت صورة من صور الجرائم الإلكترونية، التي تخترق المجتمع وتهدد دعائمه، كما تضرب في مقتل أهم أهدافه التي يسعى إليها في تحقيق الأمن لأفراده، والمحافظة على الأسرة والمجتمع بشكل عام. ولعل جوهر تجريم الابتزاز الإلكتروني وأساسه يكمن فيما يتضمنه من تهديد وضغط على إرادة المجني عليه، للقيام بأعمال ما كان ليقوم بها لو كانت إرادته حرة، سواء أكانت تلك الأعمال مشروعة أم غير مشروعة، وهو ما دعا بعض الدول الأجنبية والعربية إلى الإسراع بتجريم هذه الظاهرة، سواء بالنص عليها في قوانين خاصة بالجرائم الإلكترونية، أو بتعديل نصوصها التقليدية وتضمينها تجريم الابتزاز الإلكتروني.

دراسة (عبد الحميد، 2019) بعنوان جريمة الابتزاز الإلكتروني: دراسة مقارنة

تناولت هذه الدراسة إلى التعريف بجريمة الابتزاز الإلكتروني، والتعريف بطبيعتها القانونية، ودوافعها، وصورها، وخصائصها التي تميزها عن الجرائم المشبهة بها، إضافة إلى تحديد أركانها، وآلية التحقيق في هذه الجريمة، والعقوبات المقررة لها، وسمات ضحاياها، وذلك من خلال مقدمة وفصلين وباستخدام المنهج الوصفي والمنهج القانوني المقارن، وتأتي أهمية هذه الدراسة من أن الابتزاز يشكل خطراً اجتماعياً والحصول على المنافع المادية مقابل الضغط المعنوي على الضحية وأهمية التحرز من الوقوع في شرك فئة تلجأ لمثل هذا الأسلوب للكسب والحصول على المنافع، وتكمن مشكلة الدراسة في بيان عدم كفاية النصوص القانونية في قانون الجرائم الإلكترونية لمواجهة ومكافحة الابتزاز الإلكتروني، وغياب التعريف لهذه الجريمة في قانون الجرائم الإلكترونية الأردني رقم (27) لعام 2015 حيث أنه لم يعرف جريمة الابتزاز الإلكتروني ولم يقرر لها العقوبة المناسبة، وقد توصلت الدراسة إلى مجموعة من النتائج والتوصيات التي كان من أهمها غياب النص الصريح على هذا النوع من الجرائم إذا ما اقتربت بوسائل إلكترونية والاعتماد على النصوص العامة في قانون العقوبات الأردني، وتوصلت الدراسة إلى توصيات

تتعلق بضرورة تعديل قانون الجرائم الإلكترونية، والتوعية بكل الطرق من أخطار هذه الجريمة خاصة وأن ضحاياها عادة من صغار السن أو النساء، وما زالت هذه الجريمة تحدث على أرض الواقع رغم الجهود المبذولة للتنبيه من عدم الوقوع فيها، لغياب النص الصريح على تجريمها في القانون الأردني.

دراسة (صالح، 2018) بعنوان الإبتزاز الإلكتروني : دراسة تحليلية مقارنة

هدفت الدراسة إلى التعرف على الابتزاز الإلكتروني، دراسة تحليلية مقارنة. واعتمدت الدراسة على المنهج التأصيلي التحليلي المقارن لتحقيق هدفها. وقد انتظمت خطة الدراسة في فصلين، الأول تناول ماهية الابتزاز الإلكتروني موضحاً، مفهومه، والفرق بين الابتزاز الإلكتروني واستغلال النفوذ، والفرق بينه وبين انتهاز احتياج أو ضعف هوى النفس، ومدى ملائمة تجريم الابتزاز الإلكتروني. والثاني ناقش التهديد بإيذاء المقترن بطلب، مشيراً إلى مفهومه في جريمة الابتزاز الإلكتروني، والتهديد بالإيذاء المادي والتهديد بالإيذاء المعنوي، واقتراح التهديد بإيذاء في جريمة الابتزاز الإلكتروني بغاية معينة. أما الثالث فقد جاء بعنوان قيام المجني عليه بتنفيذ طلب الجاني من خلال، صور مقابل الطلب، والعقوبة المقررة عند أداء مقابل مشروع، والعقوبة المقررة عند أداء مقابل غير مشروع. وخلصت الدراسة بمجموعة من النتائج منها، أن الابتزاز الإلكتروني يعد أحد نتائج التقدم التكنولوجي، والاستخدام المذهل لوسائل التواصل الاجتماعي، بلغت خطورته على الأفراد، والمجتمعات حدًا كبيراً؛ لذا عاقبت عليه العديد من التشريعات الخاصة، وكذلك النصوص العامة في قانون العقوبات، وعلى الرغم من ذلك لم يكن التشريع المصري كافياً للعقاب على مثل هذه الجرائم.

- مبررات الدراسة:

سيتم تناول هذه الدراسة لكثير من الأسباب أهمها:

خطورة جريمة الابتزاز الالكتروني

مكنت الوسائل التكنولوجية الحديثة الأشخاص ضعاف النفوس من استغلالها لارتكاب الجرائم، والتخفى خلف أسماء ودلالات وهمية؛ لتحقيق منافع مادية، أو معنوية من خلال تهديد بعض الأفراد بالتهشير بهم عبر هذه الوسائل التي تنتشر بها الأخبار والمعلومات أسرع من البرق، وأشد من الرعد، فتحدث في المجتمع أثرا يفوق حرارة شمس الصيف. وتعد الجرائم الالكترونية - الابتزاز الالكتروني - واحدة من أهم التهديدات التي تواجه العالم اليوم، إضافة إلى تكلفتها من الناحية الاقتصادية، وخطورتها من الناحية السياسية والأمنية

تزايد حالات الابتزاز الالكتروني:

في الوقت الحالي، لكثرة وسهولة عمليات الاختراق - القرصنة - والاتصالات السلكية واللاسلكية في ظل الثورة التكنولوجية، والمعلوماتية، ففي عام ٢٠١١ م، كان عدد مستخدمي الإنترنت لا يقل عن ٢,٣ بليون نسمة، أي ما يعادل أكثر من ثلث سكان العالم، ويعيش أكثر من ٦٠ في المائة من جميع مستخدمي الإنترنت في البلدان النامية، ولا يتجاوز عمر ٤٥ في المائة من مجموع مستخدمي الإنترنت الـ ٢٥ عاما، وفي عام ٢٠١٧ م، كانت نسبة المشتركين في خدمة الإنترنت ٧٠ في المائة من مجموع سكان العالم، وبحلول عام ٢٠٢٠ م، من المتوقع أنه سيفوق عدد الأجهزة المتصلة بالشبكة عدد الناس بنسبة ستة إلى

واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت، ففي عالم الغد المتسم بالتطور البالغ، سيصعب تصور وقوع جريمة لا تنطوي على استعمال الوسائل الإلكترونية⁴

المنهجية وطرق البحث:

سوف يتم الاعتماد في هذه الدراسة على :

أولاً: المنهج الاستقرائي والذي ساعدني في استقراء مفهوم الابتزاز الإلكتروني وأنواعه العديدة والأسباب المؤدية لهذه الجريمة، ومراحلها المختلفة التي تقع قد يقع فيها الأفراد، وكذلك توضح أركان هذه الجريمة وأبرز العقوبات المقررة على مرتكبيها، وأيضاً بيان سبل مكافحتها.

ثانياً: المنهج التحليلي فمن خلاله تمكنت من تحليل النصوص النظامية بين كل من المنظم السعودي في نظام مكافحة الجرائم المعلوماتية، وكذلك المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية.

ثالثاً: المنهج المقارن الذي ساعدني في المقارنة بين كل من المنظم السعودي وكذلك المشرع الإماراتي وبين أوجه الشبه وأوجه الاختلاف بينهما.

⁴ صالح، تامر. (2018)، الابتزاز الإلكتروني : دراسة تحليلية مقارنة، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، (1)، ص 552

خطة البحث:

الفصل الأول/ تخطيط البحث

الفصل الثاني/ ماهية الابتزاز الإلكتروني

- المبحث الأول ماهو الابتزاز الإلكتروني وأركان جريمة الابتزاز الإلكتروني
- المبحث الثاني خصائص الابتزاز الإلكتروني واثاره
- المبحث الثالث أنواع جرائم الابتزاز الإلكتروني وصورها

الفصل الثالث/ الابتزاز الإلكتروني في التشريعين السعودي والإماراتي

- المبحث الأول الابتزاز الإلكتروني في التشريع السعودي
- المبحث الثاني الابتزاز الإلكتروني في التشريع الإماراتي
- المبحث الثالث: تقييم التشريعين السعودي والإماراتي والحلول المقترحة لمواجهة هذا الابتزاز

الفصل الرابع/ النتائج والخاتمة والتوصيات

المراجع

الفصل الثاني

- المبحث الأول ماهو الابتزاز الإلكتروني وأركان جريمة الابتزاز الإلكتروني
- المبحث الثاني خصائص الابتزاز الإلكتروني و آثاره
- المبحث الثالث أنواع جرائم الابتزاز الإلكتروني وصورها

المبحث الأول: ماهو الابتزاز الإلكتروني وأركان جريمة الابتزاز الإلكتروني

1- ماهو الابتزاز الإلكتروني :

وبالرغم مما تقدمه برامج شبكات التواصل الاجتماعي من خدمات إلكترونية هامة، فإن الواقع العملي أثبت أنه أيضاً بمثابة مصيدة إلكترونية للعديد من مستخدمي الشبكة من مختلف الأعمار، وخاصة الشباب من الجنسين؛ للإيقاع بهم من خلال الأساليب الاحتيالية والغش والخداع الذي تمارسه فئة ضالة عبر هذا الموقع، وتعيثُ فساداً في الفضاء الإلكتروني؛ للإيقاع بضحاياهم وابتزازهم والاستيلاء على معلوماتهم الخاصة، وانتهاك حرمتهم وخصوصياتهم؛ لتسهيل عمليات النصب والاحتيال على الضحايا ممن يجهلون أساليب الحماية والتأمين حال تعاملهم مع هذا الموقع، أو يفرطون في الثقة، ويسجلون عليه كافة معلوماتهم وصورهم الخاصة، غير مدركين لما يمكن أن يحدث لها من اختراقات وسطو إلكتروني، يتسبب في الإضرار بهم مادياً، ومعنوياً.

أولاً: تعريف الابتزاز في اللغة

الابتزاز في اللغة يأتي من الفعل (بز) بزه يبزه بزا أي سلبه وجاء في المثل أن " من عز بز " ومعناه " من غلب سلب " ، ويقال إبتزت الشيء أي إنتزعتَه، وبزه يبزه بزا بمعنى غلبه⁵

ثانياً: تعريف الابتزاز في الاصطلاح

⁵ أبو النصر الفارابي، الصحاح تاج اللغة وصحاح العربية، ط ٤: تحقيق أحمد عبد الغفور عطار ، دار العلم للملايين، بيروت، ١٤٠٧ هـ - ١٩٨٧ م ص ٣/٨٦٥ - ابن منظور، لسان العرب، ط ٣ ، دار صادر - بيروت ١٤١٤ هـ - ١٩٩٤ م ، ص ٥

يعرف الابتزاز على أنه حالة السعي للحصول على مكتسبات مادية، أو غير مادية من شخص المبتز، أو الأشخاص المبتزون، سواء أكانوا أشخاص اعتباريين أو أشخاص عاديين بالإكراه وباستخدام التهديد بالقوة، أو التهديد، بفضح أمر معين يكتمه من وقع عليه فعل الابتزاز⁶

ثالثاً/ الابتزاز الإلكتروني

تعتبر جريمة الابتزاز الإلكتروني من الجرائم الحديثة التي ظهرت مع دخول التكنولوجيا بشكل موسع الى جميع أفراد العائلة عن طريق استخدامهم الأجهزة الذكية.

ويعرف الابتزاز الإلكتروني على أنه محاولة الحصول على مكاسب مادية أو معنوية من شخص معين من خلال التهديد بإيقاع أذى سواء بكشف أسرار أو معلومات خاصة، أو إلحاق أذى بنفس أو مال الضحية، أو شخص عزيز لديه، معتمداً في ذلك على قوته ونفوذه لاستخراج ما يرغب من ضحيته عبر وسائل تقنية⁷

عرف على أنه كل تهديد يرتكبه الجاني بنفسه أو من خلال وسيط عبر إحدى الوسائل الإلكترونية ضد المجني عليه علي نحو يؤثر في نفسيته أو شخص عزيز لديه مما يحمله على القيام بما يكلفه به الجاني من أفعال مشروعة أو غير مشروعة⁸ كما يعرف أيضاً في ذات الاتجاه بأنه محاولة الجاني تحقيق مكاسب

6 آل رباح، عبد الكريم وآخرون (1430هـ): الابتزاز تعريفه، أنواعه، أسبابه، علاجه، ر م غ، جامعة أم القرى، السعودية

7 الكعبي، محمد عبيد، (2009): الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، ط1.

8 ممدوح رشيد مشرف، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الأمنية، مجلد 33 العدد 70، الرياض سنة 2017، ص 199

سواء كانت مادية أو معنوية عن طريق تهديد المجني عليه بإلحاق الأذى بنفسه أو بماله أو بشخص عزيز لديه، من خلال نشر معلوماته وأسراره الخاصة⁹

فرق المشرع الإماراتي بين الابتزاز وتهديد الشخص بعمل معين أو تهديد بفعل يُعد من الجنايات، حيث نص على أنه: "يعاقب بالحبس مدة لا تزيد عن سنتين والغرامة التي لا تقل مائتين وخمسون ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بأحدي هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات، وتكون العقوبة السجن مدة لا تزيد عن عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور مخلة للشرف أو الاعتبار"¹⁰

وسار على ذات النهج المشرع السعودي حيث نص بقانون مكافحة جرائم المعلوماتية السعودي والذي نص على أنه: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية : الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً"¹¹

ووفقا للنصوص السابقة فإن جريمة الابتزاز الإلكتروني تتمثل في تهديد شخص طبيعيا كان أو اعتباريا من خلال إحدى الوسائل الإلكترونية وإجباره على القيام بعمل أو الامتناع ولو كان هذا العمل أو الامتناع مشروع، فالعبرة في الجريمة في إجبار الشخص والتحكم في إرادته دون النظر إلى الشيء المجبر عليه، بالنظر لجميع التعريفات الاصطلاحية السابقة يتبين أن الابتزاز عبارة عن فعل منظم وقصدي، فلا يتم

⁹ مرجع سابق، ص 22

¹⁰ المادة (١٦) من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢

¹¹ مادة (٢ / ٣) من نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ٨ / ٣ /

١٤٢٨ م

بصورة عرضية أو عن طريق الصدفة المحضة، بل يتطلب من الجاني جمع المعلومات والوثائق والإثباتات سواء كانت مادية أو عينية، وتنظيمها بأسلوب يسهل عليه توظيفها واستثمارها لإحداث الضغط المطلوب على الضحية.

2- أركان جريمة الابتزاز الإلكتروني

مثل أي جريمة ينبغي لتحقيق جريمة الابتزاز الإلكتروني توفر الأركان الرئيسية التالية:

- الركن التشريعي (القانوني):

ينطلق الركن التشريعي من القاعدة القانونية التي تنص على أنه لا عقوبة دون نص، فتجريم الابتزاز الإلكتروني يتطلب توفر نصاً قانونياً صريحاً يمكن اعتماده للتجريم، أو توفر نصاً مرناً يمكن تطويعه لهذا الغرض، يعتبر الركن الشرعي أو الركن القانوني هو نقطة الانطلاق للبحث في قيام جريمة ما، ويقصد به تكييف قانوني يسبغه المشرع على فعل ما ليوسم بعدم المشروعية، فالفعل يبقى مشروعاً من الناحية الجنائية حتى يقوم المشرع بالتدخل لجعل من هذا الفعل جرماً، ولما كان الركن الشرعي هو الصفة غير المشروعة للنشاط أو الفعل؛ فلا وجود للجريمة إلا بوجود الركن التشريعي أو القانوني لها وفي حال انتفاء هذا الركن فلا ضرورة للبحث في أركان الجريمة الأخرى، فالصلة قائمة بشكل واضح بين الركن الشرعي من جهة والركن المادي والمعنوي من جهة أخرى، وتفسير ذلك أن الركن المادي هو الذي يحدد ماديات الجريمة التي يسبغ عليها الشارع الصفة غير المشروعة و الفعل هو جوهر الركن المادي، كما إن الركن الشرعي هو الذي يوضح نطاق الصلة التي يتعين تحقيقها بين شخصية الجاني وماديات الجريمة (وهو الركن المعنوي)، وفي إطار هذه العلاقة يتم تحديد درجة المسؤولية وجسامتها، وليس هناك أدنى شك في أن مرجع ذلك هو نصوص قانون العقوبات والقوانين المكملة له¹² فوجود جريمة ما يجب

¹² المجالي، نظام توفيق (2017) شرح قانون العقوبات القسم العام دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، ل6 عمان: دار الثقافة للنشر والتوزيع، ص: 102

أن يكون هناك نص في قانون العقوبات يبين الفعل المكون لهذه الجريمة والعقاب الواجب فرضه على مرتكب جريمة الإبتزاز الإلكتروني، وهذا المبدأ هو المبدأ الذي يعبر عنه بمبدأ الشرعية.

- الركن المعنوي

يضم الركن المعنوي العناصر النفسية للجريمة، وذلك ان الجريمة ليست كيانا ماديا قوامه الفعل واثاره (النتيجة) ولكنها ايضا كيان نفسي، لذا فالركن المعنوي يمثل الحالة النفسية لماديات الجريمة والسيطرة عليها¹³.

فالركن المعنوي ارادة جرمية وتستمد الارادة هذه الصفة من اتجاهها إلى ماديات الجريمة وهي الافعال غير المشروعة ايجابية كانت ام سلبية، ولاتجاه الارادة الاجرامية صورتان هما

الأولى: القصد الجنائي وتقوم به الجرائم القصدية

الثانية: الخطأ وتقوم به الجرائم غير العمدية

- الركن المادي

يقصد بالركن المادي ارتكاب فعل مخالف نص قانوني أو فعل جرمه القانون العراقي، او الامتناع عن القيام بفعل امر به القانون، فالركن المادي يستوجب إما قيام فعل، أو توفر امتناع، ودون توفر إحداهما لا يتاح الحكم بوجود فعل جرمي.

¹³ مرجع سابق، ص 103

ويتطلب توفر الركن المادي لجريمة الابتزاز الإلكتروني توفر معلومات أو بيانات أو صور أو مقاطع فيديو، وغيرها من الموارد التي من الممكن ان تستخدم لأغراض التهديد أو الضغط أو الابتزاز، وهنا لا يتطلب في معظم التشريعات حالة عدم الرضا¹⁴

أي أن مجرد توفر هذه الموارد لدى الجاني يمثل حالة توفر الركن المادي، سواء تم أخذ هذه الموارد برضا الضحية او تم الحصول عليها دون علمه او قبوله، أو حتى في حال تصوير مقاطع الفيديو بعلم الضحية.

¹⁴ الكعبي، محمد عبيد، (2009): الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، ط1 .

المبحث الثاني خصائص الابتزاز الإلكتروني وأثاره

1 - خصائص الابتزاز الإلكتروني

أسلفنا أن جريمة الابتزاز الإلكتروني في غالب الأمر تقع بتهديد الجاني لضحيته بفضح أو نشر أموره الخاصة أو صوره أو غير ذلك من أمور تمس حياته الخاصة للتوصل من ذلك إلى دفعه لأداء مبالغ مالية له أو بالقيام بعمل أو الإمتناع عن عمل ونستخلص من ذلك الخصائص التي تتعلق بجريمة الابتزاز الإلكتروني ونعرضها فيما يلي كل خصيصة على حدة:

1- الابتزاز الإلكتروني جريمة تمس حرمة الحياة الخاصة

تتسم جريمة الابتزاز الإلكتروني بارتباطها بالإعتداء على حرمة الحياة الخاصة للمجني عليه، فالجاني لن يتمكن في غالب الأمر من تهديد المجني عليه وإلقاء الخوف في نفسه على نحو يدفعه نحو الإنصياع وتلبية رغبات الجاني الا إذا كان الأخير يحوز بين يديه معلومات شخصية وأمور يخشي المجني عليه فضحها ونشرها

٢ - الوسائط الإلكترونية الحديثة وسيلة الجاني في الابتزاز الإلكتروني

يتسم الابتزاز الإلكتروني عن الابتزاز في صورته التقليدية في كونه يتم عبر الوسائط الإلكترونية من خلال الهواتف الذكية أو أجهزة الحاسوب أو غيرها من الوسائل الإلكترونية الحديثة، ويستخدم في ذلك شبكة الإنترنت بحيث يتمكن الجاني من خلالها الوصول والتحصل على المعلومات الشخصية للمجني عليه تمهيدا لتهديده بفضحها ونشرها ، أي انه يلزم لإتمام هذه الصورة من الجريمة أن يتوفر لدى الجاني

تقنيات إلكترونية حديثة¹⁵، فهي لا تتم الا بواسطة تقنية المعلومات مستعينا في ذلك بأجهزة الحاسب الآلي والهواتف الذكية المتصلة بشبكة الانترنت.

3- جريمة بالغة الخطورة

وتبدو خطورة جريمة الابتزاز الإلكتروني جلية فيما يمكن أن تتسبب فيه من إلحاق الضرر بمصالح الفرد والدولة على السواء، فالتهديد الذي قد تتعرض له المؤسسات والشركات الكبرى من جراء هذه الجريمة وما يستتبع ذلك من أداء مبالغ مالية ضخمة للمبتز ترتب ضررا إقتصاديا بالغاً قد لا يمكن حصره لعدم إبلاغ تلك المؤسسات عن تعرضها لهذا النوع من الجريمة خشية افتضاح أسرارها، وذات الأمر في حالة المجني عليه الفرد الذي يكن قد لحقه الضرر بالاعتداء على حرمة حياته من ناحية وتهديده وسلبه أمواله أو دفعه وإكراهه على القيام بعمل أو الإمتناع عن عمل¹⁶، وبالتالي فإن هذه الجريمة تمس الفرد و الدول في أمنها القومي مما يظهر خطورة هذه الجريمة على نحو يتعين معه مكافحتها والحد من إنتشارها

4- الابتزاز الإلكتروني عابر للحدود الخاصة

إذا كانت السرقة أو النصب أو الضرب أو غيرها من الجرائم التقليدية الأخرى تتم داخل إقليم الدولة، فإن الابتزاز الإلكتروني عابر للحدود، فهو لا يحترم الحدود السياسية ومن الممكن ارتكابه عن بعد، مما قد يجعل العالم بأسره مسرحاً للجريمة لمرتكبها، فيمكن أن يكون الجاني في قارة والمجني عليه في قارة أخرى، فهي تعد شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية فهذه الخاصية تسبغ على الابتزاز الإلكتروني الصبغة العالمية، حيث يمكن أن يكون المجرم في الابتزاز الإلكتروني موجوداً

¹⁵ عبد العزيز بن حنين بن احمد الحميد الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، ندوة الابتزاز (المفهوم - الأسباب - العلاج) مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية بجامعة الملك سعود ، الرياض ، ١٤٣٢ هـ ، ص ٦٣

¹⁶ د/ زينب محمود حسين، المواجهة الجنائية للإبزاز الإلكتروني، جامعة كركوك ، كلية القانون والعلوم السياسية ، قسم القانون ، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد ١٠ العدد ٣٧ سنة ٢٠٢١ ، ص ٨٧٥

في الصين ويكون المجني عليه في مصر، وهو ما يتطلب وجود تعاون دولي في مكافحة هذه الجرائم حول العالم

5 - صعوبة إثبات الإبتزاز الإلكتروني:

تسهم طبيعة جريمة الإبتزاز الإلكتروني من حيث انها جريمة ليس لها آثار مادية وتعتمد بالأساس على استخدام التقنيات الدقيقة والحديثة في تمكين مرتكبها من طمس أفعالهم الإجرامية وإخفاء هوياتهم مما يصعب مهمة جهات التحقيق والمحاكمة في إثبات الجريمة خاصة وأنها من الجرائم التي ترتكب في الغالب من جاني يقطن في دولة مغايرة للتي يعيش بها المجني عليه، كما انه تصعب ادانة الجاني لغياب الدليل المادي الكافي كما هو حاصل في الجرائم التقليدية والأكثر من ذلك يستطيع الجاني أن يصل الي الأدلة ويتلفها .

6- جريمة جاذبة للجنة

تعتبر جريمة الإبتزاز الإلكتروني جريمة جاذبة للجنة فهي لا تحتاج من الجاني الي مجهود عضلي كما في أغلب الجرائم التقليدية لأن مسرح الجريمة فيها مختلف فهو عالم افتراضي لا يحتاج الجاني فيه الي استخدام عضلاته وكل ما يحتاجه هو حاسب الي او جهاز موبايل متصل بشبكة الانترنت فضلا عن قلة مخاطرها وعائدها المالي الكبير.

2- اثار جريمة الإبتزاز الإلكتروني

أولا: الآثار الشرعية :

إن من أعظم الآثار السيئة لجريمة الابتزاز الالكتروني هي الوقوع في معصية الله تعالى وانتهاك محارمه الامر الذي يعرض الفرد والمجتمع للعقاب الاخرى ويعرضه لسخط الله تعالى لا سيما عندما يتم الجهر بالمعصية واعلانها ذلك لان الله تعالى يغضب اذا انتهكت محارمه

ثانيا: الآثار النفسية

يترتب على ارتكاب جريمة الإبتزاز الإلكتروني آثارا نفسية سلبية بالغة على الضحية كالقلق والتوتر والشعور الدائم بالذنب وصعوبة النوم وعدم التركيز والخوف وكثرة الشك في الآخرين المحيطين حوله ويكون حساس تجاه سلوك المحيطين به خاصة من لهم خبرة في التكنولوجيا والحاسب الآلي بالإضافة الي التفكير الدائم في التخلص من ظلم الجاني بأي طريقة كانت وخاصة اذا تمادى الجاني في ايقاع ظلمه على الضحية فذلك قد يؤدي الى ان يفكر الضحية بايذاء نفسه كالإنتحار (١) خاصة . عدم قدرة الضحية على طلب المساعدة من المقربين منها بسبب الاحرج والخوف ناهيك عما تسببه مثل تلك الجرائم من تدمير نفسي لبعض الضحايا خاصة إذا كانوا من الأطفال الذين غالبا ما يقعون فريسة للابتزاز الجنسي الذي يعد أكثر صور الإبتزاز شيوعا¹⁷.

ثالثا: الآثار الإجتماعية

أثرت مواقع التواصل الإجتماعي بشكل واضح على الأسرة والمجتمع, حيث فتحت اكثر ابواب التعارف والتواصل بكافة اشكاله صوت وصورة مما ادى ذلك إلى زيادة سهولة وقوع جريمة الإبتزاز الإلكتروني وهذا النوع من الجرائم له أثر أكبر عن بقية الجرائم الإلكترونية في المساس بسلامة المجتمع والعائلة ، حيث يترتب عليها إرهاب المجني عليه ووضعه تحت تأثير الخوف بالإضافة إلى قهر إرادته، ودفعه نحو القيام بأعمال لم يكن ليقوم بها لولا التهديد الواقع عليه حيث ان اغلب ضحايا هذه الجريمة من النساء وتسببت هذه الظاهرة في انفصالهم عن ازواجهم ، كما ان اغلب الفتيات اللاتي يتعرضن للإبتزاز يخشون من تقديم شكوي في الجاني خوفا من الفضيحة وتأثيرها على فرصتهم في الزواج حيث يحجم الشباب عن التقدم للزواج ن ، كما قد ترفض الفتاة نفسها خوفا من ان يفتضح أمرها امام الزوج في المستقبل.

¹⁷ Cezarita Cordeiro, La prevalence et l'impact de la cyber- sextorsion sur les adolescents, Article a Droit des enfants, Droit Humains, nov 21, 2023 Available at: [www. Humanium.org/fr](http://www.Humanium.org/fr)

رابعاً: الآثار الاقتصادية

أسلفنا أن جريمة الابتزاز الإلكتروني إحدي صور الجرائم السيبرانية التي يترتب على إنتشارها المساس بالإقتصاد الوطني نتيجة فقدان الثقة في التعاملات ولا شك أن الثقة في التعاملات هي أساس المعاملات التجارية فالهجمات السيبرانية المتكررة تؤدي إلي شل حركة التبادل التجاري الذي أصبح معتمد في الغالب على الوسائط الإلكترونية ويؤدي الخوف من الوقوع فريسة للهجمات السيبرانية وإختراق الحسابات البنكية إلي التراجع عن إتمام العديد من العمليات التجارية التي تعد بالأساس عماد الاقتصاد الوطني ناهيك عما يترتب على ذلك من إضرار بالأمن القومي¹⁸.

خامساً : الآثار الأمنية

جريمة الابتزاز وغيرها من الجرائم الجنسية تؤثر بالسلب على امن الفرد وشعوره بالخوف على سمعته وعرضه وشرفه وتؤثر على امن المجتمع لاقتنائها بجرائم اخري قد ترتكب بسببها مثل الاغتصاب والزنا والدعارة والتسلط على أموال الناس والسطو عليها، فهي تؤدي الي تفشي الفساد وانهايار الاخلاق والقيم في المجتمع فلا يأمن الافراد على شرفهم واعراضهم وأموالهم كما قد تؤدي جريمة الابتزاز الالكتروني الي جرائم عنف مثل جريمة القتل التي تحدث انتقاما من المبتز الذي دمر مستقبل ضحيته بنشر ما يسئ الي سمعتها وشرفها بين الناس.

¹⁸ إبتسام كريم ، وآخرون، انتشار ظاهرة الابتزاز الالكتروني في المجتمع العراقي، استطلاع اراء عينة من المجتمع لعراقي حول التعامل مع هذه الظاهرة، المؤتمر العلمي الدولي الأول النقابة الاكاديميين العراقيين، مركز التطور الاستراتيجي الاكاديمي جامعة داهوك ، العراق ، ١١ ، ١٢ فبراير ٢٠١٩ ص ١٦٥

المبحث الثالث أنواع جرائم الإبتزاز الإلكتروني وصورها

1- أنواع جرائم الإبتزاز الإلكتروني

- جرائم القرصنة الإلكترونية

يشير مفهوم القرصنة الإلكترونية إلى أي ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونياً، وذلك من خلال قرصنة الكتابة أو استخدام برامج الحاسب الجاهزة، ويختلف سبب القرصنة من واقعة إلى أخرى، فبعضها يكون بهدف مهاجمة جهاز الحاسب لابتزاز مالكة أو لتحقيق مكاسب مالية شخصية مثل ابتزاز معلومات بطاقات الائتمان، وتحويل الأموال من حسابات مصرفية مختلفة إلى حساب المقرض الخاص أو أي حسابات أخرى.

وبالإضافة إلى ذلك يعتمد بعض القراصنة على ابتزاز الشركات العالمية وتهديدها بنشر المعلومات الخاصة بها والسرية في حال عدم قيامهم بدفع أو تحويل المبلغ المالي المطلوب. يضاف إلى ذلك، أن هناك من يقوم بإستهداف المواقع الحكومية الهامة للحصول على الشهرة من خلال التغطية الصحفية الاعلامية.

- جرائم استغلال الأطفال في المواد الإباحية:

والمقصود من هذا المصطلح هو ظهور الأطفال والقصر الذين تقل أعمارهم عن 18 عاماً في صور أو أفلام أو مشاهد ذات طبيعة إباحية أو مضمون جنسي، بما فيها مشاهد أو صور للاعتداء الجنسي على الأطفال وهي جريمة منفردة قائمة بذاتها، يعاقب عليها قانوننا في أغلب دول العالم، وتتعامل أغلب دول العالم بحسم وجدية مع هذا النوع من الجرائم على كل من تثبت عليه تهمة الاتجار أو تداول صور أو أفلام إباحية للأطفال، وكذلك المنظمات الدولية بشدة مثل اليونسيف والشرطة الدولية الإنتربول¹⁹

¹⁹ عبد الجواد الرائي التكوين المستمر للقضاة: عرض حول جرائم الأموال المنعقدة بتاريخ 15/03/2008، المملكة المغربية وزارة العدل المعهد العالي للقضاء، مديرية تكوين المحققين القضائيين والقضاة. قسم التكوين المستمر، ص:3

وتوجد تجارة عبر شبكة الإنترنت تختص بهذا النوع من الاستغلال الجنسي للأطفال تشمل صوراً وأفلام تظهر أطفالاً أو قصر يجرى استغلالهم جنسياً.

- جرائم المطاردة الإلكترونية

ويقصد بها استخدام الإنترنت لتعقب أو مطاردة أي فرد لغرض الإحراج العام، أو المضايقات الشخصية، أو الابتزاز المالي وغيرها من الأمور بسلوك تهديدي، ويقوم المضايقون بجمع المعلومات الشخصية عن الضحية مثل إسمه، ومعلومات عن عائلته، وأرقام هواتفه، ومكان الإقامة ومكان العمل وما إلى ذلك عن طريق مواقع الشبكات الاجتماعية والمدونات وغرف المحادثة وغيرها من المواقع.

- جرائم الفيروسات وطريقة نشرها :

ذلك أن الفيروسات بصفة عامة، هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بمواقع أو أجهزة أخرى، أو السيطرة عليها أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة، ويتصف فيروس الحاسب بأنه برنامج قادر على التناسخ والانتشار، حيث يربط الفيروس نفسه ببرنامج آخر يسمى الحاضن، ولا يمكن أن تنشأ الفيروسات من ذاتها ولكن يمكنها أن تنتقل من حاسب مصاب الآخر سليم. وأهم طرق الانتقال الآن هي الشبكة العنكبوتية (الإنترنت) لكونها وسيلة سهلة لانتقال الفيروسات من جهاز لآخر، ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات، وكذلك عن طريق وسائط التخزين مثل ذاكرة الفلاش والأقراص الضوئية والمرنة سابقاً ويأتي أيضاً ضمن رسائل البريد الإلكتروني²⁰.

- برامج القرصنة:

²⁰ د/ زينب محمود حسين، المواجهة الجنائية للإبتيار الإلكتروني، جامعة كركوك، كلية القانون والعلوم السياسية، قسم القانون، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد ١٠ العدد ٣٧ سنة ٢٠٢١، ص 866

ويقصد بالقرصنة هنا الاستخدام أو / و النسخ غير المشروع لنظم التشغيل أو / ولبرامج الحاسب الآلي المختلفة، وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنة واتسعت وأصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجاناً أو بمقابل مادي، ومن هنا وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها ووجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز بمرتبات عالية لتكون مهمتهم منع محاولة اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبل للوقاية اللازمة من الأضرار التي يتسبب فيها قرصنة الحاسب، ففي هذه الحالة بدأت صورة الهاكر في كسب الكثير من الإيجابيات إلا أن المسمى الأساسي يظل واحداً²¹.

- جرائم الإحتيال باستخدام بطاقات الإئتمان عبر الإنترنت:

حيث يهدف احتمال الإنترنت في العادة إلى الاحتيال على المستخدمين عن طريق سلب أموالهم، إما بابتزاز أرقام بطاقات ائتمانهم أو يجعلهم يرسلون حوالات مالية أو شبكات، ويهدف بذلك لغرض شخصي كالشراء عبر الإنترنت أو دفعهم إلى الكشف عن معلومات شخصية بغرض التجسس أو انتحال الشخصية أو الحصول على معلومات حساسهم في مركز حساس، ويمكن تعريف احتمال بطاقات الإئتمان بشكل عام على أنه خداع الشخص وسرقة معلوماته عن طريق الاستخدام غير المصرح وغير المشروع به لبيانات البطاقة الائتمانية

2- صور جرائم الإبتزاز الإلكتروني

(1) جرائم الإضرار بالبيانات

²¹ مرجع سابق، ص 5

يعتبر هذا الصنف من جرائم الابتزاز الالكتروني من أشدها خطورة وتأثيراً وأكثرها حدوثاً وتحقيقاً للخسائر للإفراد والمؤسسات، ويشمل هذا المطلب كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة الكترونية (Digital Form) على الحواسيب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها، وصولاً إلى التحصل على مطالب ابتزازية.

وأبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها، ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوى القبعات البيضاء (White Hat Hackers) الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت مستغلين بعض الثغرات في تلك النظم، ومخترقين بذلك كل سياسات وإجراءات امن المعلومات التي يقوم بها مديري تلك الأنظمة²².

(2) جرائم الاعتداء والتشهير والأضرار بالمصالح الخاصة والعامة:

من بين هذه الممارسات الهجوم على الأنظمة السياسية والدينية والتشهير بها؛ ومن أشهرها قيام هواة بنسخ بعض المعلومات على شكل آيات قرآنية ونشرها على أحد مواقع البث المجانية المعروفة، موقع ياهو، وعنوانه <http://www.yahoo.com>. ونتيجةً لذلك، خاطب المجلس الأعلى للشؤون الإسلامية والأزهر الشريف والعديد من المنظمات الإسلامية حول العالم القائمين على الموقع. وبالفعل أُغلقت هذه الصفحات واعتذر القائمون عليها.

أما فيما يتعلق بما يشكل جريمة كمبيوترية، فهي تشبه التشهير بالأشخاص الاعتباريين أو الفعليين من خلال نشر الأفكار والمعلومات، فضلاً عن اختلاق الأخبار والفضائح في بعض الأحيان من خلال بناء

²² المجالي، نظام توفيق (2017) شرح قانون العقوبات القسم العام دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، ل6 عمان: دار الثقافة للنشر والتوزيع، ص: 150

مواقع على الإنترنت تحتوي على كافة المعلومات والبيانات الشخصية، فضلاً عن مجموعة متنوعة من الأخبار والموضوعات التي قد تسبب للشخص أو الكيان المستهدف ضرراً معنوياً وأخلاقياً ومادياً.

(3) جرائم الاعتداء على الأموال:

حيث ترتب على التجاء المؤسسات المصرفية والمالية الى تكنولوجيا المعلومات والاتصالات والتحول التدريجي في كافة أنحاء العالم نحو ما يطلق عليه البنوك والمصارف والمؤسسات المالية الالكترونية، فقد شهد هذا التطور ظهور عدد كبير من جرائم الابتزاز الالكتروني.

لضمان بساطة وسهولة إدارة العمليات المالية داخل البنوك والمؤسسات المالية الأخرى، أتمت أنظمة الإدارة والمحاسبة، وربطت الاحتياجات المختلفة لهذه المؤسسات ببعضها البعض عبر شبكات المعلومات. وفي تعاملاتها عن بُعد مع عملائها، واستخدمت هذه المؤسسات الإنترنت لتوفير واجهة لهذه المعاملات، أو تواصلت مباشرة عبر شبكات معلومات خاصة لا يستطيع مستخدمو الإنترنت الوصول إليها (شبكات خاصة)، والتي تفرض قيوداً مكانية على التواصل. (Web Interface)²³

في إطار التحول إلى مجتمع بلا نقد، طُرحت أنواع أخرى من بطاقات الائتمان لتسهيل المعاملات وتقليل التعاملات النقدية المباشرة. لهذا النوع من المعاملات المالية آثار سلبية كبيرة على جرائم الابتزاز الإلكتروني، رغم مزاياه وأهميته، وآثاره الإيجابية على الاقتصاد ككل، وعلى فعالية البنوك في أداء أدوارها.

²³ مرجع سابق ، ص 155

الفصل الثالث

الابتزاز الإلكتروني في التشريع السعودي والإماراتي

- المبحث الأول الابتزاز الإلكتروني في التشريع السعودي
- المبحث الثاني الابتزاز الإلكتروني في التشريع الإماراتي
- المبحث الثالث: تقييم التشريع السعودي والإماراتي والحلول المقترحة لمواجهة هذا الابتزاز

المبحث الأول: الابتزاز الإلكتروني في التشريع السعودي

1- عقوبة الإبتزاز في التشريع السعودي

حددت الهيئة السعودية للمواصفات والمقاييس والجودة عقوبات جريمة الابتزاز الإلكتروني في نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8 هـ وقرار مجلس الوزراء رقم 17 بتاريخ 1428/3/7 هـ. وجاء في المادة الثالثة من نظام مكافحة الجرائم المعلوماتية: "يُعاقب

بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب أيًا من الجرائم المعلوماتية الآتية:²⁴

١. التنصت على بيانات منقولة عبر جهاز حاسوب أو شبكة معلومات أو اعتراضها دون سبب مشروع أو قانوني.

٢. الدخول غير المشروع لإجبار شخص على القيام بعمل ما أو الامتناع عنه، حتى لو كان ذلك العمل أو الامتناع عن القيام به قانونيًا، وذلك عن طريق التهديد أو الابتزاز.

٣. الدخول غير المصرح به إلى موقع إلكتروني، بما في ذلك الدخول إليه لتغيير عنوانه أو إتلافه أو تغييره أو احتلاله.

٤. انتهاك الخصوصية بإساءة استخدام الهواتف المحمولة المزودة بكاميرات أو ما شابهها.

٥. استخدام أدوات تقنية المعلومات المتنوعة لإيذاء الأفراد والتشهير بهم. ووفقًا لهذه المادة، يُعاقب القانون السعودي على الدخول غير المصرح به بقصد تهديد الضحية والحصول على منافع - سواء كانت مالية أو معنوية أو جنسية - من خلال التأثير على نفسية المجني عليه وتخويفه وسلب إرادته بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، كما عاقب المنظم قيام الجاني بالمساس بالحياة الخاصة للضحية من خلال استخدامه وسائل التقنية الحديثة بنفس العقوبة، وقد جمع المنظم السعودي بين السجن والغرامة وحرص على ترك السلطة التقديرية للقاضي في اختيار العقوبة الأصلية بقوله أو بإحدى هاتين العقوبتين حسب مجريات الدعوى. حيث ترك له التقدير للعقاب بالسجن والغرامة إن رأى بدأً من التشديد جمع بين العقوبتين، وهو ما يؤكد أن الأصل في العقوبة الجمع بين السجن والغرامة (١٤٣) و وحدد نص المادة الثالثة من نظام مكافحة جرائم المعلوماتية الحد الأقصى

²⁴ د. داليا عبد العزيز أحمد المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي، دراسة مقارنة، العدد ٢٥ مركز جيل البحث العلمي، ٢٠١٨ م، ص ٣٧.

للعقوبة وهي السجن لمدة لا تزيد على سنه والغرامة التي لا تزيد على نصف مليون ريال، وترك تحديد الحد الأدنى للمحكمة حسب جسامة الجريمة والظروف التي ارتكبت فيها، وبالإضافة للعقوبة الأصلية الجريمة الابتزاز الالكتروني، فقد نص المنظم السعودي على عقوبات تكميلية. حيث أكد على أنه يجوز مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، كما يجوز مصادرة الأموال المحصلة منها، بالإضافة إلى جواز الحكم بإغلاق الموقع الالكتروني أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدر لارتكاب أي من هذه الجرائم أو كانت الجريمة قد ارتكبت بعلم مالكة²⁵ وهو ما أخذ به القضاء السعودي في القضية التي يحمل قرارها الرقم (٣٢٨٨٥٩٩) الصادر بتاريخ ١٤٣٢/٥/١هـ، وتتلخص وقائعها في توجيه المدعى العام السعودي إلى المتهم بعد إقراره بتهمة ابتزاز فتاة تعرف إليها عن طريق موقع الانترنت، وقام بإرسال رسائل تهديد وابتزاز للمجني عليها إن لم تستجب لطلبه فإنه سوف يقوم بفضحها. وذلك لكونه يحتفظ بصور للفتاة، كما وجه إلى المدعى عليه تهمة مقاومته للفرقة القابضة عليه، والاعتداء على رجل الأمن، وتمزيق جزء من الزي الرسمي لرجل الأمن، وطالب المدعى العام بمعاقبته وفقاً للمادة السادسة من نظام مكافحة الجرائم المعلوماتية، ومصادرة الجوال المضبوط وفقاً لذات النظام، وتوجيه الدعوى للمدعى عليه أقر بصحة ما وجه إليه من اتهام، وأنه قام فعلاً بالاختلاء المحرم مع الفتاة، ومارس معها مقدمات الفاحشة من تقبيل وضم، كما أقر بوجود صور الفتاة لديه، وأن الفتاة هي التي قامت بإرسال صورها إليه، ولكون ما أقدم عليه المتهم من الخلوة غير الشرعية مع الفتاة وابتزازها يعد أمراً محرماً شرعاً يستحق التعزيز، فقد تم الحكم عليه تعزيراً بالعقوبات التالية:

1- عقوبة السجن لمدة عشرة أشهر ابتداء من تاريخ دخوله التوقيف بسبب هذه القضية، وجلده خمسة وتسعين جلدة دفعة واحدة بمكان عام لاختلائه المحرم بالفتاة.

²⁵ المادة الثالثة عشر من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ، وقرار مجلس الوزراء رقم ١٧ بتاريخ ١٤٢٨/٧/٣هـ

2- عقوبة السجن سنة ونصف، وبغرامة مالية قدرها عشرون ألف ريال تودع في خزانة الدولة، وذلك لقاء الابتزاز وفقاً لنظام مكافحة الجرائم المعلوماتية، مع التوصية بترحيل المتهم خارج البلاد (كون المتهم أجنبياً)، وعدم السماح له بالعودة للبلاد مرة أخرى اتقاء لشره²⁶

واستثنى المنظم السعودي من جواز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، في حال كونها مملوكة للغير وكان حسن النية²⁷ فالأشياء المضبوطة لم تكن مملوكة للمبتز حال تنفيذ جريمته، وبالتالي ينبغي مراعاة الحقوق الثابت ملكيتها للغير وقت ارتكاب جريمة الابتزاز الإلكتروني، وقبل مباشرة إجراءات الدعوى الجزائية

2- تشديد عقوبة الابتزاز الإلكتروني في النظام السعودي

شدد المنظم السعودي العقوبة على مرتكبي جرائم الابتزاز الإلكتروني، إذا ارتكبت الجريمة في إحدى الحالات التالية

- الحالة الأولى: ارتكاب الجاني جريمته من خلال عصابة منظمة.
 - الحالة الثانية: إذا كان الجاني قد ارتكب جريمته بسبب شغل وظيفته العامة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.
 - الحالة الثالثة: تغيير الجاني بالقصر ومن في حكمهم واستغلالهم.
 - الحالة الرابعة: صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.
- فيعاقب المبتز إذا ارتكب جريمته وتوافرت حالة من الحالات سالفه الذكر بعقوبة السجن أو الغرامة التي لا تقل عن نصف حدها الأقصى. فلا تقل عقوبة السجن عن ستة أشهر، ولا نقل الغرامة عن مائتين

²⁶ نصت المادة الثالثة عشر من نظام مكافحة جرائم المعلوماتية السعودي على أنه مع عدم الإخلال بحقوق حسنى النية.

²⁷ رقم القرار (٣٢٨٨٥٩٩) الصادر بتاريخ ١٠ / ٥ / ١٤٣٢هـ، المجلد رقم (٨٦)، ملحق رقم (٣)، ص ٢.

وخمسين ألف ريال، ويرجع التشديد هنا إلى أن الجريمة في هذه الحالات تكون أكثر جسامة وخطورة على المجتمع، ويرى البعض أن الجريمة تنتقل من كونها جريمة تعزيرية إلى جريمة حدية وهي جريمة الحراقة، وذلك للتشابه بين الجريمتين بجامع التهديد والتخويف، وأخذ مال الغير بالقوة من خلال تشكيل عصاني في كلتا الجريمتين، ولهذا ارتأى المنظم السعودي أن تشدد العقوبة على الجاني في هذه الحالات، بحيث لا تقل العقوبة عن نصف الحد الأقصى.

3- عقوبة الشروع في جريمة الابتزاز الالكتروني

عاقب المنظم السعودي على جريمة الشروع في جريمة الابتزاز الالكتروني بقوله يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأقصى للعقوبة المقررة²⁸، فالمنظم السعودي يعاقب على الشروع في الجريمة في حال إذا بدأ الجاني في الجريمة ولكن لم تكتمل الأسباب خارجة عن إرادته، وتكون العقوبة بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها، ويجب علينا أن نفرق بين الأعمال التحضيرية والأعمال التي تعد شروعا في الجريمة، فمرحلة التفكير في الجريمة والتحضير لها، لا يعاقب الجاني عليها حتى ينتقل إلى التنفيذ وعلى ذلك فإن المنظم السعودي قد عاقب على الشروع في جريمة الابتزاز الالكتروني بالسجن الذي لا تزيد مدته على ستة أشهر وبالغرامة التي لا تزيد على مائتين وخمسون ألف ريال أو بإحدى هاتين العقوبتين.

4- عقوبة المساهمة في جريمة الابتزاز الالكتروني

بحسب المادة التاسعة من نظام مكافحة جرائم المعلوماتية، فرضت الهيئة السعودية للمحاكم السعودية على من ساعد في جريمة الابتزاز الإلكتروني العقوبة نفسها التي فرضت على الجاني الأصلي. على أن "إذا ارتكبت جريمة نتيجة التحريض أو المساعدة أو الاتفاق مع شخص آخر على ارتكاب أي من الجرائم المذكورة في هذا النظام، فإن العقوبة المفروضة على هذا الشخص لن تكون أكبر من الحد

²⁸ المادة العاشرة من نظام مكافحة جرائم المعلوماتية السعودي.

الأقصى للعقوبة المسموح بها لتلك الجريمة، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية"، فالعقوبة المقررة للمساهم هي نفس العقوبة للفاعل الأصلي، بحيث لا تتجاوز السجن لمدة سنة والغرامة التي لا تتجاوز نصف مليون ريال أو بإحدى هاتين العقوبتين، وفي حال وقفت جريمة الابتزاز الإلكتروني عند حد الشروع، فإن المساهم يعاقب بالسجن لمدة لا تتجاوز ستة أشهر والغرامة التي لا تزيد على ربع مليون ريال سعودي.

المبحث الثاني: الابتزاز الإلكتروني في التشريع الإماراتي

1- عقوبة الابتزاز في التشريع الإماراتي

وبالاطلاع على قانون مكافحة جرائم تقنية المعلومات الإماراتي ، تبين أنه نص على تجريم الابتزاز الذي يتم عن طريق تقنية المعلومات حيث تنص المادة 16 منه على "يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام

شبكة معلوماتية أو وسيلة تقنية معلومات وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جنائية أو بإسناد أمور خادشه للشرف والاعتبار²⁹

وقد كان معيار المشرع الاماراتي في الجرائم التي توجب الحبس الاحتياطي معياراً، مرناً، فلم ينص صراحة على اعتبار الجرائم الإلكترونية ومنها جريمة الابتزاز الإلكتروني من الجرائم التي يجب فيها الحبس الاحتياطي، حيث لم يحدد قانون الإجراءات الجزائية الاتحادي مبررات الحبس الاحتياطي بل اكتفت المادة (106) على انه " يجوز لعضو النيابة العامة أن يصدر أمراً بحبسه احتياطياً إذا كانت الدلائل كافية.. " ³⁰، ومع عدم تصريح المشرع الاماراتي بالجرائم الواجبة الحبس الاحتياطي فيها ، إلا أننا نجد أن أكثر مسوغات الحبس الاحتياطي تكمن في منع المتهم من الهرب، ومنع المتهم من التأثير في سير التحقيق، كما أنه لا يجوز اصدار أمر

كما يجوز للمحكمة أن تقضى بمصادرة الأجهزة أو البرامج أو الوسائل التي استخدمها المبتز لتهديد الضحية، كما يجوز لها أن تقضى بمصادرة الأموال المتحصلة من الجريمة، والعقوبة التكميلية عقوبة عينية، وتقديرية للقاضي، وتتبع العقوبة الأصلية وجوداً وعدماً، واستثنى المشرع الإماراتي من جواز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، في حال كونها مملوكة للغير، وكان حسن النية³¹ فالأشياء المضبوطة لم تكن مملوكة للمبتز حال تنفيذ جريمته، وبالتالي ينبغي مراعاة الحقوق الثابتة ملكيتها للغير وقت ارتكاب.

²⁹ المادة 16 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الاماراتي رقم 5 لسنة 2012.

³⁰ قانون الإجراءات الجزائية الاماراتي رقم 35 لسنة 1992.

³¹ المادة 41 من قانون مكافحة جرائم تقنية المعلومات الإماراتي

2- عقوبة الشروع في جريمة الابتزاز الالكتروني

نص المشرع الإماراتي على عقوبة الشروع في جريمة الابتزاز الالكتروني بإعلانه أن الشروع في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون يُعاقب بنصف عقوبة الجريمة كاملةً، وبتخفيض عقوبة الشروع في الابتزاز الإلكتروني إلى نصف عقوبة الجريمة كاملةً، اتفق المشرع الإماراتي مع المشرع السعودي، وفقاً لهذا النص.

3- تشديد عقوبة الابتزاز الالكتروني في التشريع الإماراتي

شدد المشرع الإماراتي العقوبة في جريمة الابتزاز الالكتروني، إذا استلزم التهديد ارتكاب جناية أو فعل مخل بالشرف، فقد رفع المشرع الإماراتي عقوبة جريمة الابتزاز الإلكتروني إلى السجن لمدة أقصاها عشر سنوات.

بتهديد متصل بجناية أو يكون التهديد له علاقة بإسناد أمور تمس الشرف والاعتبار، كما أن المشرع الإماراتي نص على عقوبة أخرى على مرتكب جريمة الابتزاز الالكتروني، حيث أكد المشرع على أن للمحكمة أن تقضى بإبعاد الأجنبي الذي يحكم عليه بعقوبة، بعد تنفيذها.

المبحث الثالث: تقييم التشريعين السعودي والإماراتي والحلول المقترحة

لمواجهة هذا الابتزاز

1- تقييم التشريعين السعودي والإماراتي

بمقارنة موقف كل من المشرع السعودي والإماراتي من تشديد العقوبة نجد أن موقف المشرع السعودي من تحديد الحالات التي تؤدي إلى تشديد العقاب كان أفضل من المشرع الإماراتي، حيث حدد المشرع السعودي هذه الحالات بأربع حالات الأولى إذا تم ارتكاب الجريمة من خلال عصابة منظمة، فخطر الجريمة وضررها في هذه الحالة أكبر من أن ترتكب بواسطة شخص واحد، والحالة الثانية إذا كان

الجاني يشغل وظيفة موظف عام واتصلت الجريمة بهذه الوظيفة أو ارتكبها مستغلاً سلطانه ونفوذه وذلك لخيانته الثقة التي وضعها الدولة فيه بأن استغل منصبه ونفوذه لتهديد الأشخاص وابتزازهم والحالة الثالثة التغير بالقصر ومن في حكمهم من ناقصي الأهلية نتيجة مرض أو عاهة وخيراً فعل المشرع السعودي بالتشديد على الجاني في هذه الحالة لصفه خاصة في المجني عليه لأن القصر ومن في حكمهم أولى بالحماية من البالغين والحالة الرابعة إذا كان قد صدر ضد الجاني أحكام محلية أو أجنبية سابقة بالإدانة في جرائم مماثلة وذلك التشديد وفقاً للقواعد العامة في العود لمواجهة الخطورة الاجرامية التي تفصح عنها شخصية الجاني في هذه الحالة، بينما إذا نظرنا إلى التشديد في التشريع التشريعي الإماراتي يكون إذا كان الفعل يشكل جريمة جنائية أو إسناد أمور خادشه للشرف واعتبار يظهر من خلال دراسة النصوص القانونية في كلا النظامين أن هناك تبايناً واضحاً في عدة جوانب تتعلق بتجريم وعقوبة جريمة الابتزاز الإلكتروني، ويمكن توضيح هذه الفروقات كما يلي:

يُلاحظ أن المشرع الإماراتي قد انتهج سياسة عقابية أكثر صرامة وتشدداً، حيث نص في المادة (16) من قانون مكافحة جرائم تقنية المعلومات على أن العقوبة قد تصل إلى السجن عشر سنوات في حال كان التهديد بارتكاب جنائية أو بمواد خادشة للشرف. في المقابل، فإن النظام السعودي، بموجب المادة الثالثة من نظام مكافحة جرائم المعلوماتية، حدد العقوبة بالسجن لمدة لا تزيد عن سنة، والغرامة بما لا يتجاوز خمسمائة ألف ريال، مما يجعل سقف العقوبة أقل بكثير مقارنة بالنظام الإماراتي.

جاء النص الإماراتي أكثر تفصيلاً ودقة في وصف الجريمة، حيث استخدم تعبير "ابتزاز أو تهديد باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات" بشكل مباشر وواضح. أما النظام السعودي فقد صاغ الجريمة بشكل غير مباشر، من خلال عبارة "الدخول غير المشروع لتهديد شخص أو ابتزازه"، مما قد يؤدي إلى اختلاف في فهم النص وتطبيقه، ويقلل من وضوح التوصيف القانوني للجريمة.

في النظام الإماراتي، نص القانون صراحة على إمكانية إبعاد الأجنبي المحكوم عليه بعد تنفيذ العقوبة، كعقوبة تكميلية تقديرية. بينما في السعودية، لا يوجد نص صريح في النظام، ولكن القضاء قد يلجأ إلى ترحيل الأجنبي بموجب توصية قضائية، كما ورد في بعض الأحكام القضائية، مما يجعل الإبعاد في السعودية مسألة تقديرية وليست إلزامية.

التشريع الإماراتي تميّز بوضع حد أدنى للعقوبة، حيث نص على أن الغرامة لا تقل عن 250,000 درهم، مما يعكس رغبة واضحة في ردع الفعل الإجرامي بشدة. أما النظام السعودي فلم يُحدد حدًا أدنى للعقوبة، وترك الأمر للسلطة التقديرية للقاضي وفقًا لظروف الواقعة، وهو ما قد يؤدي أحيانًا إلى تفاوت في الأحكام القضائية لنفس نوع الجريمة.

قام المشرّع الإماراتي بتقسيم الجريمة إلى درجات خطورة (عادية ومشددة) وفقًا لنوعية التهديد أو الابتزاز، بينما اكتفى النظام السعودي بذكر الظروف المشددة دون تحديدها بنفس الوضوح القانوني، مثل الابتزاز ضمن عصابة منظمة أو استغلال المنصب، ولكنه لم يُفرق ذلك بتقسيم قانوني واضح للحالات كما فعل المشرّع الإماراتي.

2- الحلول المقترحة لمواجهة هذا الابتزاز

يري الباحث انه يمكن اقتراح عدة حلول لمواجهة مشكلة الابتزاز الإلكتروني تتمثل في:

1. لمواكبة أحدث التطورات التكنولوجية والاستراتيجيات التي يستخدمها المجرمون، ينبغي على المشرّعين في المملكة العربية السعودية والإمارات العربية المتحدة مراجعة تشريعاتهم المتعلقة بالجرائم الإلكترونية وتنقيحها باستمرار. ولتسهيل مقاضاة مرتكبيها يُفضّل أن تُعرّف التشريعات الابتزاز الإلكتروني تعريفًا دقيقًا، مع وصف مظاهره وأساليبه المعاصرة.
2. لمكافحة الجرائم الإلكترونية، وخاصةً الابتزاز، يُنصح بإنشاء أو دعم مجموعات أمنية متخصصة. كما يجب أن تتمتع هذه الوحدات بالخبرة القانونية والتقنية اللازمة لاستخدام

أحدث التقنيات للعثور على الجناة والقبض عليهم، مع حماية خصوصية الضحايا وسرية بلاغاتهم.

3. يُعدّ التثقيف المجتمعي من أهمّ استراتيجيات الوقاية. لذا، من الضروريّ تكثيف الحملات الإعلامية والتوعوية، لا سيّما للشباب، حول مخاطر الابتزاز الإلكتروني، وكيفية تجنّبه، وعواقب الانخراط فيه، وأهمية الإبلاغ عنه دون تردد أو خوف.

4. ينبغي إتاحة إمكانية تلقي البلاغات بسرية تامة من خلال تطوير منصات إلكترونية رسمية. بالإضافة إلى تلقي الدعم القانوني والنفسي طوال فترة التحقيق والمحاكمة، ينبغي تشجيع الضحايا على الإبلاغ عن حالات الابتزاز دون القلق بشأن الفضيحة أو الانتقام.

5. يُعدّ التعاون بين الدول من خلال الاتفاقيات الدولية وتبادل المعلومات أمرًا بالغ الأهمية لمكافحة الابتزاز الإلكتروني نظرًا لطبيعة الجرائم الإلكترونية العابرة للحدود الوطنية، لا سيما عندما يكون الجاني مقيمًا في الخارج.

6. إن دمج مبادئ الأمن السيبراني والوعي الرقمي في المناهج الدراسية منذ الصغر يمكن أن يُسهم في منع هذا النوع من الجرائم من خلال تنشئة جيل واعي ومؤهل للتعامل مع المخاطر الرقمية.

الفصل الرابع

- الخاتمة
- النتائج
- التوصيات

الخاتمة

اتسعت في العصر الحديث دائرة استخدام شبكة المعلومات كوسيلة للاتصال في شتى مجالات الحياة لتحقيق ما تصبو إليه الإنسانية من اختصار المسافات، والوقت، والجهد ، وأصبحت هذه الشبكات تحوي معلومات في مختلف مجالات الحياة لا تقع تحت حصر وعلى الرغم من المزايا التي تقدمها هذه الشبكات للإنسانية إلا أنه في المقابل أدى الاستخدام المتزايد لها إلى كثير من المخاطر، إذ افرزت أنواع جديدة من الجرائم يطلق عليها الجرائم الإلكترونية ومن بينها جريمة الابتزاز الإلكتروني وهي تشبه جريمة الابتزاز التقليدية في استخدام التهديد بإيذاء المقترن بطلب المال أو أي منفعة أخرى ، ولكنها تختلف عنها

في الوسيلة التي تتم بها فهي تتم باستخدام الشبكة المعلوماتية وفي عالم افتراضي مما جعل انتشارها أسرع وخطرها وضررها أكبر من جرائم الابتزاز التقليدية، فالابتزاز الإلكتروني سلوك إجرامي يمس أعراض وحرمان الناس ويخالف الدين والشرع لما فيه من إشاعة الفاحشة بين الناس قال تعالى (إن الذين يحبون أن تشيع الفاحشة في الذين آمنوا لهم عذاب أليم في الدنيا والآخرة و الله يعلم وأنتم لا تعلمون) وقال رسول الله صلى الله عليه وسلم (يا معشر من أسلم بلسانه ولم يفض الإيمان إلى قلبه لا تؤذوا المسلمين ولا تعيروهم ولا تتبعوا عورتهم فإن من تتبع عورة أخيه المسلم تتبع الله عورته وإن من تتبع الله عورته يفضحه ولو في جوف رحله، وإذا كانت النصوص الجنائية التقليدية لا تسعف لمواجهة هذه الجرائم المستحدثة التي تعتمد في ارتكابها على وسائل تقنية المعلومات المتطورة، وحماية حرية الأشخاص وسمعتهم وشرفهم واعتبارهم ودرءاً للعدوان على الممتلكات والأموال حاولت الدول في البداية أن تطوع تشريعاتها لتواكب هذه الجرائم المستحدثة ثم تنهت غالبية الدول لضرورة أفراد نصوص تشريعية خاصة بهذه الجرائم الإلكترونية فالأثار والتحديات المتعلقة بظاهرة الابتزاز الإلكتروني تتطلب نهجاً أكثر استباقية كجزء من استراتيجيات الأمن السيبراني للسيطرة على هذه الظاهرة وباستعراض موقف المشرعين الإماراتي والسعودي من جريمة الابتزاز الإلكتروني توصلنا إلى عدد من النتائج والتوصيات نوردتها في ما يلي:

نتائج الدراسة:

1. أظهرت نتائج الدراسة أن كلاً من التشريعين السعودي والإماراتي تُدمجا الابتزاز الإلكتروني في تشريعاتهما لمكافحة الجرائم الإلكترونية سعياً منهما لتسليط الضوء على هذه الجريمة. وفي ظل الثورة الرقمية، يُشير هذا إلى إدراك المشرعين لأهمية هذا الوضع.

2. اتفق التشريعين على تجريم الابتزاز الإلكتروني ومعاقبة محاولاته والتورط فيه. كما اعتمدا مبدأ تمتع القضاة بسلطة تقديرية في تحديد العقوبة المناسبة، مع مراعاة خصوصيات كل حالة.
3. إن نظام الإمارات العربية المتحدة أكثر وضوحاً وقسوة في عقوباته، حيث ينص على ما يصل إلى عشر سنوات في السجن في الحالات المشددة، وعلى النقيض من النظام السعودي الذي يحدد الحد الأقصى للعقوبة بالسجن لمدة عام واحد، ما لم تكن هناك ظروف مشددة مثل إساءة استخدام المنصب أو ارتكاب الجريمة من خلال عصابة،
4. الحالات التي تستوجب تشديد العقوبة، مثل إساءة معاملة الأطفال أو ارتكاب جريمة أثناء أداء الواجب الرسمي، مُدرجة بالتفصيل في النظام السعودي. ويتجلى الفرق بين نهجي النظامين في العقاب في ربط المشرع الإماراتي بين التشديد وطبيعة التهديد (مثل التهديد بجناية أو تشهير).
5. أقرّ كلا النظامين القانونيين عقوبات إضافية، مثل مصادرة الأصول والمعدات. وهذا يشير إلى وجود مصلحة مشتركة في صون حقوق الملكية الخاصة وتحقيق العدالة.

توصيات الدراسة:

1. لمعالجة هذه القضايا بفعالية وسرعة، ينبغي على الأجهزة الأمنية تفعيل فرق مكافحة الابتزاز الإلكتروني وتزويدها بأحدث التقنيات والكوادر القانونية المؤهلة.
2. من خلال الجهود المتواصلة التي تشارك فيها وزارات التعليم والإعلام والشؤون الاجتماعية، تعزيز فهم المجتمع للقانون والتكنولوجيا الرقمية لمكافحة هذه الجريمة، وخاصة بين الشباب.

3. من خلال الاتفاقيات الثنائية التي تُسهّل تبادل المعلومات وتسليم المجرمين، وخاصة في قضايا الجرائم العابرة للحدود، يمكن للمملكة العربية السعودية والإمارات العربية المتحدة تعزيز تعاونهما القضائي والأمني في مكافحة الجرائم الإلكترونية.
4. لإنشاء جيل رقمي مُدرّك لإرشادات الاستخدام المسؤول للتكنولوجيا وكيفية حماية نفسه أخلاقياً وقانونياً، يجب تضمين مفاهيم الأمن السيبراني والابتزاز الإلكتروني في المناهج الدراسية.

المراجع:

المراجع العربية:

إبتسام كريم، وآخرون، انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العراقي، استطلاع اراء عينة من المجتمع لعراقي حول التعامل مع هذه الظاهرة، المؤتمر العلمي الدولي الأول النقابة الأكاديميين العراقيين، مركز التطور الاستراتيجي الأكاديمي جامعة داهوك، العراق، ١١،

١٢ فبراير ٢٠١٩ ص ١٦٥

أبو النصر الفارابي، الصحاح تاج اللغة وصحاح العربية، ط ٤ : تحقيق أحمد عبد الغفور عطار ، دار العلم للملايين، بيروت، ١٤٠٧ هـ - ١٩٨٧ م ص ٣/٨٦٥ - ابن منظور، لسان العرب، ط ٣ ، دار صادر - بيروت ١٤١٤ هـ - ١٩٩٤ م ، ص ٥

أحمد غازي، (2024)، موظفو الأجهزة الأمنية والابتزاز الإلكتروني: دراسة في وزارة الداخلية، مجلة الأدب، عدد خاص، 301 - 332

آل رباح، عبد الكريم وآخرون (1430هـ): الابتزاز تعريفه، أنواعه، أسبابه، علاجه، ر م غ، جامعة أم القرى، السعودية

باقر حنون.(2021)، جريمة الابتزاز الإلكتروني: دراسة مقارنة، مجلة دراسات البصرة، عدد خاص، 47 - 92

تامر صالح.(2018)، الابتزاز الإلكتروني : دراسة تحليلية مقارنة، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، (1)، 536 - 689

د. داليا عبد العزيز أحمد المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي، دراسة مقارنة، العدد ٢٥ مركز جيل البحث العلمي، ٢٠١٨ م، ص ٣٧.

د/ زينب محمود حسين، المواجهة الجنائية للإبتزاز الإلكتروني، جامعة كركوك ، كلية القانون والعلوم السياسية ، قسم القانون ، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد ١٠ العدد ٣٧ سنة ٢٠٢١ ، ص ٨٧٥

رنا البياتي.(2022)، الابتزاز الإلكتروني، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، (44)، 467 - 484

زهراء عبد الحميد.(2019)، جريمة الابتزاز الإلكتروني: دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة عمان الأهلية، الأردن.

عبد الجواد الرائي التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 15/07/2008، المملكة المغربية وزارة العدل المعهد العالي للقضاء، مديرية تكوين المحققين القضائيين والقضاة. قسم التكوين المستمر، ص:3

عبد اللطيف، عبد الرزاق المواني (2014)، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة، الكتاب الأول، دبي: سلسلة الدراسات والبحوث القانونية والقضائية العلمية المحكمة، معهد دبي القضائي، ص: 179-180

عودة، عبد القادر عودة ((د/سنة)، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي بيروت: دار الكاتب العربي، ص: 228.

الكعبي، محمد عبيد، (2009): الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، ط1 .

عبد العزيز بن حنين بن احمد الحميد الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، ندوة الابتزاز (المفهوم - الأسباب - العلاج) مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية بجامعة الملك سعود ، الرياض ، ١٤٣٢ هـ ، ص

٦٣

محمد محمد.(2024)، جريمة الابتزاز الإلكتروني: دراسة مقارنة، مجلة قطاع الشريعة والقانون، (16)،

1686 - 1621

ممدوح رشيد مشرف ، الحماية الجنائية للمجني عليه من الإبتزاز ، المجلة العربية للدراسات الأمنية،

مجلد ٣٣ العدد ٧٠ ، الرياض سنة ٢٠١٧ ، ص ١٩٩

المجالي، نظام توفيق (2017) شرح قانون العقوبات القسم العام دراسة تحليلية في النظرية العامة

للجريمة والمسؤولية الجزائية، ل6 عمان: دار الثقافة للنشر والتوزيع، ص: 102

وفاء صقر.(2024)، جريمة الابتزاز الإلكتروني: دراسة مقارنة، مجلة البحوث القانونية والاقتصادية،

584 – 452، (2)36

المراجع الأجنبية

Cezarita Cordeiro, La prevalence et l'impact de la cyber- sextorsion sur les adolescents,

Article a Droit des enfants, Droit Humains, nov 21, 2023 Available at: www.

Humanium.org/fr

النصوص القانونية:

○ المادة 16 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الاماراتي رقم 5 لسنة 2012.

○ قانون الإجراءات الجزائية الاماراتي رقم 35 لسنة 1992.

○ المادة (١٦) من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢

○ هكذا وردت في متن القانون (شخص) والصحيح لغة شخصا المادة (16) من القانون الاتحادي

رقم 5 لعام 2012 بشأن مكافحة جرائم تقنية المعلومات

○ مادة (٢ / ٣) من نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/

١٧) بتاريخ ١٤٢٨ / ٣ / ٨ م

○ المادة الثالثة عشر من نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم

م/١٧ بتاريخ ١٤٢٨/٣/٨هـ، وقرار مجلس الوزراء رقم ١٧ بتاريخ ١٤٢٨/٧/٣هـ

○ نصت المادة الثالثة عشر من نظام مكافحة جرائم المعلوماتية السعودي على أنه مع عدم

الإخلال بحقوق حسن النية.

○ رقم القرار (٣٢٨٨٥٩٩) الصادر بتاريخ ١٠ / ٥ / ١٤٣٢هـ، المجلد رقم (٨٦)، ملحق رقم (٣)،

ص ٢.

○ المادة العاشرة من نظام مكافحة جرائم المعلوماتية السعودي.