

المواجهة الجنائية للإبزاز الإلكتروني بالتجريم والعقاب (في ضوء أحكام التشريع الإماراتي)

Criminal confrontation of electronic extortion with criminalization and punishment (in light of the provisions of UAE legislation)

إعداد: الباحث الرئيسي/ عائشة محمد هزيم السويدي

جامعة الشارقة - كلية القانون

Email: a.m.alsuwaidi@hotmail.com

الباحث المشارك/ الدكتور أحمد موسى هياجنه

جامعة الشارقة - كلية القانون

ملخص

يشهد العالم ارتفاعاً كبيراً في عدد الجرائم الإلكترونية وذلك لأسباب عديدة أهمها الإنترنت والهواتف المحمولة وتطبيقات التواصل الاجتماعي التي أصبحت في متناول الجميع، الأمر الذي أفرز جرائم ابتزاز إلكتروني تحدث يومياً ويقع بسببها مئات الضحايا الذين يتعرضون لتهديد وترهيب بنشر معلومات خاصة عنهم أو بنشر صور ومقاطع فيديو خاصة بهم مقابل دفع مبالغ طائلة من الأموال.

يتناول هذا البحث ظاهرة مستحدثة وهي ظاهرة جريمة الابتزاز الإلكتروني، ويكتسب هذا البحث أهميته من الطبيعة الخاصة لتلك الجريمة التي أصبحت تختلف باختلاف الوسيلة الإلكترونية التي يمكن من خلالها الوصول إلى معلومات سرية أو حساسة عن الضحايا، وهو الأمر الذي يكشف عن مدى الحاجة لوجود تشريع يواكب التطور الملحوظ لصور وأنماط الجرائم الإلكترونية سواء فيما يتعلق بمرتكبيها، وأدواتها أو أساليبها وطرق ارتكابها.

واعتمد هذا البحث على الأسلوب الوصفي التحليلي في جمع وتحليل الحقائق المتعلقة، وستتم معالجته من خلال ثلاثة مباحث سبّين لنا طبيعة الابتزاز الإلكتروني، وتُكشف لنا موقف المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث التجريم والعقاب.

وتمثلت أهم نتائج هذا البحث إلى أن جريمة الابتزاز الإلكتروني تُعتبر من الجرائم المستحدثة، ويطلق عليها الجرائم الناعمة التي تخلو من العنف، وهي جريمة يصعب إثباتها حيث من السهل أن تمحى آثارها بسهولة، كما أنها قد تتسبب في حدوث جرائم بعدها كالقتل أو السرقة.

وأخيراً أوصينا من خلال هذا البحث على مجموعة من التوصيات منها ضرورة استمرار نشر الوعي بين أفراد المجتمع، وتشجيع من يتعرض للابتزاز بالإبلاغ عن الجريمة وسط تأمين سرية للمجني عليه حتى لا يحجم عن الإبلاغ.

كلمات دالة: جريمة الكترونية، ابتزاز، تهديد، عقوبة، تكنولوجيا، قانون، ضحية، مجرم.

Criminal confrontation of electronic extortion with criminalization and punishment (in light of the provisions of UAE legislation)

Summary

The globe is witnessing a large volume of electronic crimes for so many reasons amongst which is the internet, mobiles and different applications of social media which is now can be in the reach of all, that led to electronic blackmailing crimes every day, hundreds of victims are subject to threats and terrorise by publishing their private formations or by publishing their personal pictures or videos and compelled to pay huge amount of money.

This research addresses recent phenomena which is the electronic blackmailing, this research gains its importance from the specific nature of that crime, which either according to the electronic mean through which one can have access to sensitive confidential information about the victims, therefore raised a need for legislation that catch up with the development in types and kinds of electronic crimes whether related to the criminals, tools, types, and its means of act.

This research depends on the analytical descriptive manner in gathering and analyzing the facts related, which shall be treated through 3 chapters which shall explain the nature of the electronical blackmailing and discover the Emirati legislator's point of view towards the electronical blackmailing from both sides of criminalization and punishment.

The most important results of this research conclude that, the crime of electronical blackmailing is one of the most recent crime which refers to it as soft crimes without violence and which is hard to prove and easy to hide its trucks thus it might consequently lead to other crimes like murder or theft.

At last we recommends through this research a bundle of recommendations amongst which is the necessity to raise continues awareness between society members and to encourage, those subject to blackmailing to report the crime in a confidential manner, so they will not hesitate to report the afore-said crime.

Keywords: Electronical crime, blackmailing, threat, punishment, technology, law, victim, criminal.

المقدمة

إن بناء الحضارة وتشبيدها يعتمد على جملة من الضرورات للبناء والتطوير، وعلى رأسها الأمن باعتباره حاجة أساسية، ومرتكز لبناء مجتمع سليم، ويمتلك حضارة قادرة على التأثير في الإنسان والبشرية. فالشعور بعدم الأمان والاطمئنان من محبطات العمل البناء لأي مجتمع (الجميل، 2001، ص:35).

عرفت المجتمعات القديمة ظاهرة الإجرام، وقد شرّعت الجزاءات لمحاربتها والقضاء عليها، كما شرّعت الجزاءات المترتبة على مخالفة بعض الأعراف المحلية والقواعد التي تراها الجماعة لازمة لوجودها واستمرارها، وليس من اليسير تحديد تلك الفترة التي ظهرت فيها الجريمة، ولكن من المتفق عليه أن هذه الظاهرة قديمة قدم المجتمع البشري نفسه منذ أن شرع الإنسان يعيش في نطاق العشيرة أو القبيلة رغم عدم وجود سلطات ومؤسسات رسمية في بادئ الأمر كالبوليس والمحاكم والسجون، وإن كانت قد تطورت تلك المؤسسات بأشكال وصور مختلفة انعكاساً للتغيرات التي أصابت ذلك المجتمع في علاقاته الاقتصادية والفكرية والدينية (د: جعفر، 2000، ص:5).

وقد أصبح الإنترنت أهم وسيلة إعلام متعددة المهام، بينما تراجع الدور الذي تلعبه وسائل الإعلام التقليدية؛ الأمر الذي يبرر القوة الكامنة وراء التأثير العميق لتكنولوجيا الاعلام الإلكتروني الحديث (احصائيات اعلام الكتروني، متوافرة على الموقع : <http://www.internetworldstats.com/stats5.htm>).

والذي أظهر لنا أنماط جرمية جديدة أفرزتها الجريمة الإلكترونية في مجال الاتصالات وتكنولوجيا المعلومات، وأصبحت هذه الجرائم خطراً مؤرقاً للمجتمع الدولي والمحلي على السواء. ولعل الابتزاز الإلكتروني كان من الأنماط الجرمية المستحدثة والتي قد توصف بأنها ذات طبيعة معقدة في طرق ارتكابها وفي وسائل كشفها، وعليه كان لابد من المزيد من الدراسات التي تهدف إلى كشف مدى الملائمة القانونية لمواجهة جريمة الابتزاز الإلكتروني.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في تناولها لظاهرة مستحدثة وهي ظاهرة الجرائم الإلكترونية وخاصة جريمة الابتزاز الإلكتروني، فالتطورات التكنولوجية على الرغم من آثارها الإيجابية إلا أن لها العديد من السلبيات التي تهدد أمن واستقرار المجتمع ليس على المستوى الفردي بل على المستوى الاجتماعي كذلك، فرغم التغييرات الاجتماعية التي تشهدها المجتمعات القديمة والحديثة منها، إلا أن هذه الظاهرة بقيت محل اهتمام المشرع لما تثيره من اضطراب في العلاقات الإنسانية والاجتماعية، ولما تشكله من تهديد يقع على سلطة الدولة والقانون.

ويُضاف لذلك أن العالم يشهد ارتفاعاً كبيراً في عدد الجرائم الإلكترونية وذلك لأسباب عديدة أهمها الإنترنت والهواتف المحمولة وتطبيقات التواصل الاجتماعي التي أصبحت في متناول الجميع، إضافةً إلى تطور البرمجيات الهائل والتي تساعد على قرصنة البيانات والاحتفاظ بها أو حتى استرجاعها، الأمر الذي أفرز جرائم ابتزاز إلكتروني تحدث يومياً ويقع بسببها مئات الضحايا الذين يتعرضون لتهديد وترهيب بنشر معلومات خاصة عنهم أو بنشر صور ومقاطع فيديو خاصة بهم مقابل دفع مبالغ طائلة من الأموال.

وتكتسب هذه الدراسة أهميتها من الطبيعة الخاصة لجريمة الابتزاز الإلكتروني، والتي أصبحت تختلف باختلاف الوسيلة الإلكترونية التي يمكن من خلالها الوصول إلى معلومات سرية أو حساسة عن الضحايا، ولعل هذه الوسائل تنتج يومياً وبشكل مضطرب جداً، فتطبيقات التواصل الاجتماعي والإلكتروني تعددت بشكل كبير ومخيف. ومن هنا جاءت أهمية وجود دراسة تستقصي ملاءمة التشريعات الحالية واستيعابها للتغييرات والتجديدات على مستوى التجريم والعقوبة لتلك الجريمة.

إشكالية الدراسة:

أفرزت وسائل الإعلام الإلكتروني العديد من الجرائم المستحدثة التي تستخدم وسائل وأساليب تكنولوجية مبتكرة لم تكن مألوفاً في المجتمع الإماراتي، الأمر الذي يكشف عن مدى الحاجة لوجود تشريع يواكب التطور الملحوظ لصور وأنماط

الجرائم الإلكترونية سواء فيما يتعلق بمرتكبيها، وأدواتها أو أساليبها وطرق ارتكابها، وهو ما يُبرر إلغاء القانون الاتحادي الإماراتي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، واستحداث قانون جديد في سنة 2012م في شأن مكافحة جرائم تقنية المعلومات والذي تم تعديله بموجب القانون الاتحادي رقم (12) لسنة 2016، وبعضاً من التعديلات التي اشتملها القانون الاتحادي لعام 2018 بشأن الجرائم الإلكترونية. وتتمثل إشكالية هذه الدراسة في محاولتها لإثارة تساؤلٍ حول مدى فعالية المواجهة التشريعية في الحد من جرائم الابتزاز الإلكتروني، وما إذا كان المشرع الإماراتي قد أفرد قواعد خاصة في مكافحتها سواء في التجريم ذاته، أو في فرض الجزاءات على مرتكبيها، أم أنه سار في فلك القواعد العامة.

تساؤلات الدراسة:

تحاول هذه الدراسة الحالية الإجابة عن التساؤلات الآتية:

- 1- ما هي طبيعة الابتزاز الإلكتروني وما هي جريمة الابتزاز الإلكتروني؟
- 2- ما هو دور التشريع الإماراتي في مواجهة جرائم الابتزاز الإلكتروني من حيث التجريم؟
- 3- ما دور التشريع الإماراتي في مواجهة جرائم الابتزاز الإلكتروني من حيث العقاب؟

منهج الدراسة:

تعد هذه الدراسة نمطاً من الدراسات الكشافية الاستطلاعية، حيث لم يجد الباحث في حدود علمه أية دراسة قانونية تناولت هذا الموضوع على مستوى دولة الإمارات العربية المتحدة من قبل، وتعتمد هذه الدراسة على الأسلوب الوصفي التحليلي في جمع وتحليل الحقائق المتعلقة بموضوع الدراسة.

خطة البحث:

ستتم معالجة هذا الموضوع من خلال تقسيمه إلى ثلاثة مباحث، حيث سيتطرق المبحث الأول إلى بيان طبيعة الابتزاز الإلكتروني، والثاني إلى مواجهة المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث التجريم، والأخير إلى مواجهة المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث العقاب.

المبحث الأول

طبيعة وماهية الابتزاز الإلكتروني

تمهيد:

مع التطور التكنولوجي السريع الذي وصلت إليه غالبية بلدان العالم، أصبح بإمكان أي شخص وهو في مكانه الحصول على غايته وما يسعى إليه، وذلك من خلال تصفح مئات المواقع الإخبارية وآلاف من المتاجر الإلكترونية، وغيرها العديد من وسائل التواصل الاجتماعي التي اجتاحت القلوب قبل العقول، ومن هنا ظهرت بعض الممارسات أو المشكلات المرتبطة باستخدام الإنترنت والتي غدت تزداد يوماً بعد يوم وذلك بسبب استغلال بعض الجماعات الإلكترونية لهذه الوسائل وحساباتها وابتزاز أصحابها بهدف جمع الأموال.

ويعتبر الابتزاز الإلكتروني أحد أكبر المخاطر التي تواجه مستخدمي شبكة الإنترنت والأجهزة الذكية، فقد يؤدي الابتزاز الإلكتروني إلى حدوث مشاكل مؤثرة على الفرد بمستوياتها النفسية والاجتماعية وخصوصاً في مجتمعاتنا العربية المتمسكة بعاداتها وتقاليدها (عبدالمجيد، 2018).

كما وتمتاز جريمة الابتزاز الإلكتروني بخصوصية واختلاف كبيرين عن جريمة الابتزاز التقليدية، وهذه الخصوصية وذلك الاختلاف إنما مرجعه إلى الطبيعة المميزة لتلك الجريمة، حيث أنها تتم في مسرح جريمة افتراضي، يكتنفه الغموض والتخفي، وتختلف أدلته عن تلك الأدلة الملموسة في مسرح جريمة مادي، حيث تعتبر جريمة الابتزاز الإلكتروني صورة من صور الجرائم الإلكترونية التي تُرتكب في مسرح جريمة تحده نقاط الاتصال والتكنولوجيا الرقمية، وهذا الاختلاف بين الجريمتين التقليدية والإلكترونية يجعل طرق ارتكاب جريمة الابتزاز الإلكتروني تعتمد على وسائل التكنولوجيا الحديثة بشكل أساسي.

وكذلك فالغموض الذي يحيط بجريمة الابتزاز الإلكتروني منذ بداية تنفيذ هذه الجريمة وحتى تمامها، يمثل تحدياً صارخاً ومقلقاً في ذات الوقت أمام جهات الضبط الجنائي والقضائي، ويُطال هذا الغموض تعريف وأركان الجريمة، مما أظهر اختلافات في تعريفات هذه الجريمة، وإن تلاقت جميعها في استخدام التكنولوجيا والواقع الافتراضي كمسرح جريمة، وامتلاك مرتكبها لمهارات وصفات متميزة عن المجرم بشكله التقليدي.

المطلب الأول

مفهوم الابتزاز الإلكتروني وأنواعه

يشهد العالم ثورة معرفية وتكنولوجية هائلة أسفرت عن ظهور وسائل التقنيات الحديثة التي كان لها الدور في تسهيل حياة البشر وطورتها بشكل وفرّ عليهم الكثير من الوقت والجهد، وعلى الرغم من إيجابيات تلك الوسائل التي لا تعد ولا تحصى إلا أنها أوجدت بعض السلوكيات والأنماط السلبية منها "الجرائم الإلكترونية" وهو أكثر أنواع الجرائم انتشاراً في وقتنا الحالي.

ومن المتفق عليه أن الابتزاز الإلكتروني كفعل جرمي يرجع إلى أصله اللغوي، وتأسيساً على هذا المنطلق فإننا لا بد لنا من التعرّيج على مفهوم الابتزاز لغةً واصطلاحاً وصولاً إلى المفهوم القانوني للابتزاز الإلكتروني.

فالاقتزاز في اللغة: مشتق من كلمة (بزز)، والبزز بفتح الباء هو السلب، ومنه قولهم في المثل: من عزَّ بززاً؛ معناه من غلب سلباً، وبزَّه يبزُّه بززاً: غلبه وغصبه، وبزَّ الشيء يبزُّه بززاً: انتزعه. وبزَّه ثيابه بززاً. وبزَّه: حبسه، وحكي عن الكسائي: لن يأخذه أبداً بززةً مني أي قسراً. وابتزَّه ثيابه: سلبه إياها (ابن منظور، 1999، ص398).

وبالنسبة لتعريف الابتزاز في الاصطلاح الفقهي: فيُقصد به أخذ الشيء بجفاء من غير رضی صاحبه (أ.د. قلعة جي، 1997، ص38)، وقد عرّفه بعض الفقهاء المعاصرين بالآتي:

1- محاولة تحصيل مكاسب مادية، أو معنوية من شخص، أو أشخاص: طبيعي أو اعتباري بالإكراه، أو التهديد بفضح سر من وقع عليه الابتزاز.

2- فرض أسلوب التهديد بالفعل، أو التترك للحصول على مكاسب من شخص، أو جهة ممنوعة شرعاً وعقلاً. ويؤخذ على هذا التعريف ذكر الغرض الغالب من الابتزاز، وهو الحصول على مكاسب؛ سواء كانت هذه المكاسب مادية أو مالية، لأنه قد يكون غرضه مجرد الأذى كتشويه سمعته، أو من يسوؤه فعل ذلك به (ابن منظور، 1999، ص398).

ومن الناحية القانونية: فقد تعددت وتنوعت التعريفات القانونية للابتزاز لكنها تدور حول معنى واحد ومما عُرّف به الابتزاز، هو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيء لتدمير الشخص المُهدد إن لم يقيم بالاستجابة إلى بعض الطلبات، وهذه المعلومات تكون عادة محرّجة أو ذات طبيعة مدمرة اجتماعياً (محسن، 2015، ص: 52). ويُعرف الابتزاز كذلك بأنه نمط جرمي يرتكز إلى تخويف الأفراد وتهديدهم لإرغامهم على دفع مبالغ نقدية أو تقديم الأشياء العينية، في مقابل عدم تعرضهم للإيذاء الجسدي أو النفسي. وينطوي الابتزاز على استخدام التهديد بالإيذاء الجسدي والنفسي والإضرار بالسمعة والمكانة الاجتماعية من خلال تفتيق الفضائح وإصاق التهم بهم ونشر أسرارهم؛ مما يجبر الشخص المبتزّ على الدفع مجبراً وكارهاً لمن يبتزُّه، وهذا النمط الجرمي يُعد أحد شكلاً خطيراً من أشكال الفساد الإداري (لطي، 2019، ص: 54).

وقد يكون دوافع ارتكاب تلك الجريمة الإلكترونية نفسية متمثلة في نية المبتز لارتكاب هذه الجريمة، أو مادية بطلبه مقابل مادي نقدي، أو جنسية لا أخلاقية، وكما هو معلوم بأن لجريمة الابتزاز الإلكتروني أضراراً نفسية واجتماعية، وأن غالبية من يتعرضون للابتزاز أو التهديد يعانون من أعراض قلق حاد وأحياناً تصل إلى مرحلة الهلع والخوف الشديد واضطرابات في النوم والأكل وقلة التركيز، وقد يصل الأمر أحياناً إلى الشعور بالإحباط الشديد ونوبات البكاء وقد يحصل لدى الضحية أفكار انتحارية ربما تصل إلى الانتحار حسب شخصية الضحية وثقافته، أما بالنسب للضرر الاجتماعي فهذا يعتمد على مدى ثقافة المجتمع الذي يعيش فيه وحسب جنس الضحية، فمثلاً عندما تكون الضحية امرأة وفي مجتمع محافظ أو متشدد ربما يصل الأمر إلى النبذ أو التحقير أو الطرد وأحياناً يصل إلى القتل والضرر أحياناً يتعدى إلى عائلة الضحية وقد يستمر إلى سنوات طويلة (أحمد، 2011).

وتتعدد أنواع الابتزاز الإلكتروني؛ وينقسم إلى (المطيري، 2014):

1. **ابتزاز مادي:** ويرتكب هذا النوع من الابتزاز من خلال طلب مبالغ مالية من الضحية مقابل عدم فضحه وإفشاء أسراره، وبرأينا فإن هذا النوع عادة ما يرتكبه مجموعة من العصابات المتخصصة في جرائم الابتزاز الإلكتروني والمتواجدين خارج بلاد المبتزين من أجل الحصول على الأموال التي يطلبونها بموجب عملية الابتزاز هذه، مما يجعل عملية اكتشاف الجريمة والقبض على المجرم ومقاضاته جنائياً شبه مستحيلة.
2. **ابتزاز جنسي:** ويرتكب من خلال إجبار الضحية على تقديم خدمات جنسية أو ارتكاب أفعال جنسية مقابل عدم كشف أسراره أو نشر صور ومقاطع فيديو خاصة فيه، وبرأينا فإن هذا النوع يُعتبر من أخطر وأشهر أنواع الابتزاز لاسيما عند النساء اللواتي ينجرفون بسهولة إلى طلبات المبتز، تقادياً للفضيحة التي قد تواجههم في ظل مجتمعاتنا العربية الإسلامية المحافظة.
3. **ابتزاز منفعة:** ويرتكب هذا النوع الأخير من خلال إرغام الضحية على القيام بخدمات أخرى غير مشروعة أو قد تكون مشروعة إلى حد ما مقابل عدم بث صور أو بيانات سرية، وأكثر الفئات عرضة لهذا النوع من الابتزاز هم الأشخاص ذوي المناصب الحساسة وصانعي القرار في المجتمع. وهذا لا يقتصر على تهديد الأشخاص وابتزازهم إلكترونياً، بل أصبحت هناك كيانات منظمة للقرصنة وابتزاز الشركات والمؤسسات في شتى وأكبر دول العالم، ففي عام 2015م تعرضت 40 شركة أمريكية لسرقة بياناتها والتهديد بنشر هذه البيانات ما لم تدفع ملايين الدولارات بالمقابل (الزعاوي، 2014، ص: 68)، وقد توالى الجرائم المشابهة واستمرت إلى أن انتشرت بشكل كبير في مختلف دول العالم.

المطلب الثاني

الآثار الخطيرة للابتزاز الإلكتروني وكيفية مواجهته

مخاطر جريمة الابتزاز الإلكتروني قد تدمر الأفراد ونظام المجتمع بصفة كلية أو جزئية، عندما يكون الغرض من استهداف الضحية هو تدميرها أو استغلالها أو تشويه سمعتها لتحقيق مصالح وغايات المبتز الشخصية والتي تكون على حساب الضحية، وهذه الجريمة لا شك في أنها عمدية تؤدي إلى حدوث الكثير من الأضرار التي قد تؤثر بشكل سلبي على الفرد أو الحكومة، وهو ما يُبرر برأينا تدخل المشرع بسن قوانين وأحكام خاصة لهذا النوع من الجرائم. ونظراً لكل الميزات الخاصة بالشبكة العنكبوتية فقد أصبحت الكثير من المعاملات تُبرم عبر الإنترنت، ذلك ما جعل هذه المعاملات عرضة لأن تكون محل اختراق وسرقة وقرصنة (وابتزاز كذلك)، فالإعلام الآلي الذي يستخدمه الأفراد في مجال المعلوماتية هو نفسه الذي يستخدمه المجرمون لتحقيق مآربهم الشخصية (أمين، 2015، ص: 5)، وفيها قد يستخدم المبتز ضحيته كأداة للجريمة، بتحريضه على ارتكاب جريمة لصالح المبتز كالسرقة أو خلافه.

وقد تمتد مخاطر هذه الجريمة لتمس الضحية وأسرته، فلا يُخفى علينا مدى التأثير الذي تحدثه مواقع التواصل الاجتماعي مثل "الفيس بوك، تويتر، انستجرام" وغيرها من المواقع، التي تجذب العديد من الفئات العمرية في المجتمعات المختلفة، وخاصة فئة المراهقين وهم الأكثر متابعة والأقل إدراكاً لمجريات الأمور، وبالتالي يقعون فريسة سهلة لتلك المواقع الإلكترونية، خاصة أن جريمة الابتزاز الإلكتروني سخرت الإنترنت والمواقع الإلكترونية ليُصباح وسيلة للتخفي والتمويه وممارسة سلوكيات جرمية بهدف الإيقاع بالآخرين وابتزازهم، وهذا برأينا ما يُميّز الإجرام الإلكتروني عن الفعل الإجرامي العادي.

وعلى الصعيد الاقتصادي الوطني، فإن جريمة الابتزاز الإلكتروني قد تؤثر بشكل كبير على اقتصاد الدول، فما لم نستطع تأمين بُنيّتنا التحتية الإلكترونية فإن كل ما يحتاجه المجرم لتعطيل اقتصادنا ووضع حياتنا موضع الخطر هو نقرات بسيطة على جهاز الحاسوب والاتصال عن طريق الإنترنت، فالفأرة يمكن أن تكون الآن أكثر خطورة من الرصاص والقنبلة، وهذا ما أدلى به (لامار سميث) رئيس اللجنة الفرعية المسؤولة عن الجريمة في الكونغرس الأمريكي للتدليل على الخسائر الاقتصادية التي قد تلحق بالولايات المتحدة الأمريكية جراء هذه الجريمة وغيرها من الجرائم المعلوماتية. (أمين، 2015، ص34-ص35).

أما على المستوى الاجتماعي، فقد تؤثر جريمة الابتزاز الإلكتروني سلبيًا على الطبقات الاجتماعية فتزيد الهوة بينها بمقدار ما تملك من معلومات فيجد المبتز الفضاء الإلكتروني مناخاً مناسباً له، وخير وسيلة للوصول إلى مبتغاه. وعلى المستوى السياسي، فإن العابثين في شبكة الإنترنت يجدون ضالتهم في ممارسة أساليب الضغط السياسي واستغلال هذه الشبكة في لتحقيق مآربهم الإجرامية والتي تتناسب مع مصالحهم الخاصة.

وخلاصة القول أن لجريمة الابتزاز الإلكتروني آثار خطيرة، فهذه الجريمة أصبحت تساهم في انهيار القدوة والتفكك الأسري الذي يصل حد الطلاق، مما أصبح إحجام الشباب والفتيات عن الزواج وتأخرهم أمراً سببته فقد الثقة بسبب ما يطفو على سطح المجتمع من أسرار مفضوحة بسبب الإبتزاز، وتتمثل الآثار النفسية في حالة الاضطراب النفسي، والقلق، والخوف، والاكنتاب الذي يتولد لدى المجني عليه، وتنتج عنه الشخصية العدوانية أو المضادة للمجتمع، كما قد تصل الأمور إلى حد اقدام الضحية على الانتحار. (العنبي، 2016).

ونظراً لتلك الآثار والمخاطر التي خلقتها جريمة الابتزاز الإلكتروني أصبح من الضروري أن تتم مواجهة تلك الظاهرة التي اجتاحت مجتمعاتنا، وشكّلت خطراً على حياة أفرادها، حيث أصبحت مسؤولية مواجهة هذا النوع من الابتزاز من وجهة نظر الباحث تقع على عاتق كل من الفرد والدولة مجتمعين، خاصة أنه في الآونة الأخيرة ظهرت محاولات الابتزاز الإلكتروني لتكون أكثر شراسة وقوة عن قبل، فتكمن مسؤولية الفرد الشخصية في أن يحرص على عدم وضع بياناته أو معلوماته الشخصية وصوره في مواقع التواصل الاجتماعي دون إدراج خاصية الخصوصية، التي تتيح المجال لأصدقائه والأشخاص الذين يثق بهم لرؤية ومشاركته تلك الصور والمعلومات، بالإضافة إلى الامتناع عن التواصل أو مراسلة أي شخص غريب،

وتجنب تصفح المواقع الإلكترونية مجهولة المصدر أو الغير معروفة لاحتمالية تضمّنها روابط قد تخترق الحاسوب الخاص بالمتصفح دون علمه، وتبرز مسؤولية الوالدين في المراقبة والإشراف على أبنائهم المراهقين أثناء تصفحهم للمواقع الإلكترونية تقادياً لوقوعهم ضحايا جرائم الابتزاز الإلكتروني.

وتكمن مسؤولية الدولة لمكافحة هذه الجريمة من خلال نشر الوعي حول مخاطر جريمة الابتزاز الإلكتروني بشتى الطرق والوسائل، والتنسيق مع الجهات المعنية لتتقيد أفراد المجتمع وتزويدهم بالمعرفة اللازمة حول التعامل مع تلك الجريمة. ومن هنا يأتي دور المشرع من خلال سن القوانين والأنظمة والإجراءات القانونية اللازمة مع الأخذ بعين الاعتبار مدى تفشي هذه الجريمة، وإقرار نصوص تشريعية مشددة للحد من جريمة الابتزاز الإلكتروني وإغلاق جميع الثغرات القانونية التي قد يستغلها مرتكبي هذه الجريمة.

المبحث الثاني

مواجهة المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث التجريم

تمهيد:

تعد دولة الإمارات العربية المتحدة من الدول المتقدمة في المجال المعلوماتي وكانت من أوائل الدول التي تنبّهت إلى خطر الجريمة الإلكترونية وفرضت قوانين ملزمة تُعاقب من يتسبب في جرائم الابتزاز، حيث أن دولة الإمارات توفر كافة التقنيات والجهود للتبليغ عن هذا النوع من الجرائم ضمن سرية معقدة وضمن آلية متطورة، ولما كانت دولة الإمارات من أكثر الدول التي تهتم بعالم التكنولوجيا وتتسابق في توفير كافة الوسائل التي تساعد المواطن على مواكبة التطور فهي أيضاً تنبّهت إلى خطر الاستخدام السيء لتلك الوسائل التكنولوجية، و فرضت أنظمة وقوانين تساعد على حماية المواطن بالدرجة الأولى، وتُعاقب المجرمين بعقوبات قاسية تبعاً لنوع الجريمة الإلكترونية المقترفة، فهي تعاقب مجرمي الابتزاز الإلكتروني بعقوبات قاسية جداً دون النظر إلى نوع الابتزاز سواء كان ابتزاز جنسي أو مالي أو غيرها من أنواع الابتزاز. (العتيبي، 2016)

المطلب الأول

الركن المادي في جريمة الابتزاز الإلكتروني

على المستوى القانوني في دولة الإمارات العربية المتحدة فقد تطرّق المرسوم بقانون اتحادي رقم (5) لسنة 2012م بشأن مكافحة تقنية المعلومات وتعديلاته إلى فعل الابتزاز والتهديد باستخدام وسيلة من وسائل تقنية المعلومات، حيث نصّت المادة رقم (16) من القانون المذكور على أنه: "يُعاقب بالحبس مدة لا تزيد على عامين والغرامة التي لا تقل عن 25 ألف درهم ولا تتجاوز 500 ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخصاً آخر لحمله على القيام بفعل أو الامتناع

عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات، وتكون العقوبة السجن مدة لا تزيد على 10 سنوات إذا كان التهديد بارتكاب جنابة أو بإسناد أمور خادشة للشرف أو الاعتبار".

واستناداً إلى ذلك النص، يتّضح لنا أن المشرع الإماراتي تطلّب لقيام فعل الابتزاز الإلكتروني المجرّم توافر كل من: السلوك الإجرامي والنتيجة الإجرامية وقيام العلاقة السببية بينهما، وهو ما يُطلق عليه الركن المادي للجريمة أي السلوك المادي بالفعل المجرّم الذي يكون ظاهراً ويبرز هذه الجريمة فيجعلها تخرج إلى العالم الخارجي، حيث يُشترط لوقوع جريمة الابتزاز أن يكون هناك سلوك إجرامي صادر من المبتز المتمثل في طلبه لأمر رغماً عن إرادة المجني عليه، كأن يطلب المبتز من ضحيته مالاً ليس من حقه، وأن يكون المبتز جاداً فيما يُهدد به، بغض النظر عن الطريقة التي تم فيها التهديد، وفي المقابل أن يكون الضحية عالماً أن هذا الطلب هو نوع من أنواع الابتزاز يُمارسه المبتز لتحقيق مبعثه.

إضافةً إلى السلوك الإجرامي المشار إليه فالمشرع الإماراتي تطلب كذلك تحقق نتيجة إجرامية من ذلك السلوك، ويُقصد بالنتيجة الإجرامية: الأثر الذي ترتب على السلوك الاجرامي للمبتز ضد المجني عليه، كما أنه بلغة أعم تعتبر النتيجة الاجرامية هي الاعتداء الواقع على المصلحة المعتبرة والمحمية بنص القانون، سواء أضر هذا الاعتداء بالمصلحة المعتبرة نظاماً أو شكل تهديداً لها بأي صورة من صور الابتزاز، سواء كان ذلك تهديداً بالصور أو ملفات أو فيديوهات أو أي وسيلة أخرى.

وفي جريمة الابتزاز الإلكتروني تقع النتيجة الجرمية بمجرد قيام الجاني بتهديد المجني عليه بإفشاء سر من أسرارها بأن يقوم بنشره على الملأ أو نشره على مواقع التواصل الاجتماعي أو غير ذلك والتي يعتبرها أمراً لا يجب الاطلاع عليه أمام الملأ وكان التهديد بأمر غير مشروع، طالما سبب ذلك الخوف والهلع والتأثير على إرادة نفسية المجني عليه بأن ألقى في نفسه قلقاً من قيام المبتز بتنفيذ تهديده. (أحمد، 2011، ص 132)

والعنصر الأخير الذي اشترطه المشرع لقيام الركن المادي لجريمة الابتزاز الإلكتروني هو قيام علاقة سببية بين السلوك الإجرامي والنتيجة الإجرامية، وبدون هذه العلاقة لا يمكن نسبة الجريمة إلى الفاعل، وتطبيقاً لذلك لو أن النتيجة الجرمية في جريمة الابتزاز الإلكتروني تحققت بإفشاء أسرار المجني عليه ولكن بفعل شخص آخر لم يكن هو المبتز، أو بسبب ضياع هذه المستندات وانتشارها بمحض الصدفة، فلا مسؤولية على الفاعل للانتفاء العلاقة السببية، ولربما يسأل عن جريمة أخرى بحسب التكييف القانوني للفعل مثل قيام الفاعل بالابتزاز والتهديد ولكن الإفشاء تم لسبب آخر لا دخل للفاعل فيه، وهنا برأينا أيضاً تقع جريمة الابتزاز نتيجة الضرر الذي ترتب على ذلك الإفشاء حتى وإن كان دون قصد مباشر.

المطلب الثاني

الاشتراك الجرمي والشروع في جريمة الابتزاز الإلكتروني

جريمة الابتزاز الإلكتروني قد يرتكبها فاعل وحيد، وقد يشترك في الركن المادي لها أكثر من فاعل، وهذا هو الاشتراك المباشر كما يعرفه الفقه الجنائي الإسلامي والقوانين الوضعية، إلا أن هناك صورة أخرى للاشتراك وهي حالة الاشتراك غير المباشر والتي تسمى بالمساهمة المعنوية في الجريمة سواء كانت المساهمة قبل ارتكاب الجريمة أو أثناءها أو بعد تنفيذها، فقد تُرتكب جريمة الابتزاز الإلكتروني بناءً على تحريض المبتز على ارتكابها، أو الاتفاق معه على ارتكابها، أو مساعدته في ارتكاب تلك الجريمة، ومما لا شك فيه أنه وبالنظر إلى نص تجريم فعل الابتزاز الإلكتروني الوارد في المادة (16) من المرسوم بقانون اتحادي بشأن مكافحة جرائم تقنية المعلومات الإماراتي والذي سبق وأن تمت الإشارة إليها، فإن نص المادة لم يتطرق إلى صور الاشتراك غير المباشر السالفة الذكر بنص خاص، وبالتالي فإن المشرع قد لجأ إلى تطبيق القواعد العامة في هذا النوع من المشاركة الجنائية، باعتبار الشريك المتسبب مرتكباً للجريمة كما لو كان هو الفاعل الأصلي ومستحقاً للعقاب مثله، فإن تشددت العقوبة على الفاعل الأصلي فيتمد أثرها إلى الشريك بالتسبب.

وفيما يتعلق بالشروع: فإن جريمة الابتزاز الإلكتروني كغيرها من الجرائم الجنائية الأخرى إما أنها تتم فتكون جريمة تامة، أو لا تكتمل فتكون جريمة ناقصة أو تقف عند مرحلة الشروع، ويُقصد بالشروع استناداً إلى القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي الذي عرّف الشروع بأنه: " البدء في تنفيذ فعل بقصد ارتكاب جريمة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الجاني فيها. وبعد بدء في التنفيذ ارتكاب فعل يعتبر في ذاته جزءاً من الأجزاء المكونة للركن المادي للجريمة أو يؤدي إليه حالاً ومباشرة.

ولا يعتبر شروعا في الجريمة مجرد العزم على ارتكابها ولا الأعمال التحضيرية لها ما لم ينص القانون على خلاف ذلك"، وبهذا يتضح لنا بأن الشروع هو البدء في التنفيذ في الجريمة التي يعقد الجاني العزم على ارتكابها، ولكنه لا يصل إلى النتيجة التي يريد تحقيقها، فهي جريمة ناقصة لعدم اكتمال النتيجة الاجرامية المرجوة.

وبرجوع الباحث إلى المرسوم بقانون اتحادي رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات وتعديلاته يجد أن المشرع الإماراتي لم يغفل عن الشروع في الابتزاز الإلكتروني لمجرد اعتبار أن الجريمة لم تتم، بل إنه اعتبر مجرد الشروع في عملية الابتزاز الإلكتروني هو فعل مجرم وقرر له عقوبة سيتم التطرق لها لاحقاً، وذلك بموجب نص المادة رقم (40) من المرسوم بقانون اتحادي المشار إليه والتي نصّت على أنه: "يُعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة" فطالما عاقب المشرع الاماراتي على الشروع فهذا برهان على أن المشرع قد توسّع في نطاق التجريم ليشمل الشروع في الابتزاز الإلكتروني ضمن ذلك النطاق.

المطلب الثالث

الركن المعنوي في جريمة الابتزاز الإلكتروني

الركن المعنوي هو القصد الجنائي للجريمة، وهذا القصد ينهض على عنصرين هما:

العلم:

ويقصد به علم الجاني بنتيجة السلوك الذي يرتكبه، والوقائع التي تتصل بها، والتي تعد من عناصر الجريمة والعلم بموضوع الجريمة، فيجب أن ينصب علمه على أن ما يقوم به من الحصول على صور فاضحة لحد الأشخاص وتهديده بهذه الصور مقابل الحصول على منفعة جريمة يعاقب عليها المشرع فهنا يتحقق العلم وتكتمل أركان الجريمة، كما ينبغي أن يكون عالماً بماهية الفعل أو الامتناع المجرم، ويعلم بأن فعله يلحق ضرراً بالمجني عليه، ولا عبرة في قيام القصد إن انصرفت الإرادة إلى هذه النتيجة إذ يكفي توقعها العلم المسبق بها. (عودة، بدون سنة نشر، ص 228)

والأصل أن الجاني في الابتزاز الإلكتروني يحيط بكل العناصر المكونة للجريمة وبجميع أركانها، ولكن المسؤولية الجنائية تقوم في جرائم العمد فقط، فهذه الجريمة لا تكون إلا عمدية.

الإرادة:

تعتبر الإرادة هي الدافع الأساسي للسلوك الاجرامي، ويجب أن تكون هناك إرادة للسلوك والنتيجة في نفس الوقت، كمن يعقد عزمه بأن يقوم بابتزاز فتاة بمعلومات سرية تشينها، ففي هذه الحالة أراد المبتز أن يحقق نتيجة الحصول على المال (أحمد، 2011، ص 179)، وكما هو معلوم أن الإرادة تنقسم إلى قسمين، إرادة الفعل وإرادة النتيجة، ولكي تقوم المسؤولية يجب إثبات أن إرادة الفاعل اتجهت إلى القيام بهذا الفعل، وذلك دون أن تقع إرادته في عيب من عيوب الإرادة، كأن يكون مختاراً ومدركاً أنه يحصل على معلومات وصور سرية وخاصة بالضحية من مستودع أسرار الأخير فإن كان مكرهاً فلا يوجد قصد جنائي، ولا تقوم مسؤولية الفاعل المكره، كما أنه لقيام المسؤولية الجنائية لا بد أن يتحقق القسم الثاني من الإرادة وهو إرادة النتيجة فلا بد أن تتجه إرادة الجاني إلى تحقق النتيجة الاجرامية من فعله بالحصول على المنفعة المادية أو المعنوية غير المشروعة أو اللاأخلاقية.

وفي جميع الأحوال ينصّح لنا بأن المشرع الإماراتي في نصوصه التجريبية الخاصة بالابتزاز الإلكتروني اشترط القصد الجنائي العام الذي يتحقق بمجرد توافر لدى الجاني نية العمد لارتكاب الفعل، مع علمه بأنه يرتكب فعلاً محظوراً قانوناً (نصّت المادة (16) من المرسوم بقانون اتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات على أنه: "يعاقب بالحبس مدة لا تزيد على عامين والغرامة التي لا تقل عن 25 ألف درهم ولا تتجاوز 500 ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخصاً آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات،... الخ").

المبحث الثالث

مواجهة المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث العقاب

تمهيد:

الثابت هو أن العقوبات تعد من أهم الآثار التي تترتب على تجريم السلوك المعتدي، لذا نظم المشرع الإماراتي كل فعل أو ترك مخالفةً لنصوصه الموضوعية، وجعل مقابل هذا الفعل أو الترك المجرمين عقوبة، هذه العقوبة هي لضمان تحقيق الردع الخاص للمجرم، ولتحقيق الردع العام للمجتمع ككل، فللعقوبة وجهين، العلاجي والوقائي، وتختلف الأنظمة والقوانين المجرمة في كل دولة وذلك باختلاف كل سياسة جنائية يتخذها المشرع ما بين التخفيف أو التشديد في العقوبات (السلمي، 2010م، ص 68)

وتُعرّف العقوبة بأنها: الجزاء الذي يُقرره القانون الجنائي لمصلحة المجتمع تنفيذاً لحكم قضائي على من تثبتت مسؤوليته عن الجريمة لمنع ارتكاب الجريمة مرة أخرى من قبل المجرم نفسه أو غيره (<https://www.mohamah.net/law>)، والعقوبة كجزاء لا تُقرر إلا بنص استناداً لمبدأ قانونية العقوبات، وكون العقوبة جزاء يقتضي أن تنطوي على ألم يحيق بالمجرم نظير مخالفته نهى القانون أو أمره، وذلك بحرمانه من حقوقه التي يتمتع بها، سواء في شخصه أو حريته أو مباشرته لنشاطه السياسي، كما أن هذا الجزاء يتعين أن يكون مقابلاً لجريمة، فلا عقوبة ما لم ترتكب جريمة وتتوافر لها جميع أركانها وتنشأ المسؤولية عنها (د. ربيع، 1993، ص:15)، وتُقسّم العقوبات الجزائية بنظر المشرع الإماراتي إلى نوعين، هي: العقوبات الأصلية والعقوبات الفرعية وتشمل: (العقوبات التبعية والعقوبات التكميلية).

فالعقوبات بحسب أهميتها كجزاء قائم بذاته إلى عقوبات تكفي بذاتها لتحقيق معنى الجزاء المقابل للجريمة الذي ينطق به القاضي وتُسمى: العقوبات الأصلية، والقسم الآخر هو عقوبات ليست لها نفس أهمية العقوبات الأصلية وبالتالي لا تكون هي الجزاء الوحيد الذي ينطق به القاضي، وإنما توقع إلى جانب العقوبة الأصلية وتُسمى: العقوبات الفرعية، وقد ورد في قانون مكافحة جرائم تقنية المعلومات الإماراتي النص على العقوبات الأصلية والفرعية لجريمة الابتزاز الإلكتروني، وسنسلط الضوء على هذه العقوبات بالإضافة إلى عقوبة كل من الشروع والمشاركة الإجرامية في ثلاثة مطالب على النحو التالي:

المطلب الأول

العقوبات الأصلية

يُقصد بالعقوبات الأصلية تلك الجزاءات والعقوبات الذي ينص عليها المشرع ويقدرها للجريمة والتي تحكم بها المحكمة عند ثبوت إدانة المتهم، ولا تنفذ تلك العقوبة الأصلية على المحكوم عليه إلا في حال نصّت عليها المحكمة في حكمها وتشمل: عقوبات الحدود والقصاص والدية، والعقوبات التعزيرية وهي الإعدام، السجن المؤبد أو المؤقت، والحبس، والغرامة.

وفيما يتعلق بجريمة الابتزاز الإلكتروني محل هذه الدراسة فإنه وبالنظر إلى نص التجريم والعقاب الوارد في المادة (16) من المرسوم بقانون اتحادي رقم (5) لسنة 2012م نجد أن المشرع الإماراتي نصّ على أنه: "يُعاقب بالحبس مدة لا

تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز 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 أو الاعتبار".

فالعقوبة الحبس الواردة في النص المذكور تُعتبر إحدى العقوبات السالبة للحرية، متمثلة في وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة قانوناً لهذا الغرض وذلك للمدة المحكوم بها (انظر: المادة رقم (69) من القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي)، أما بالنسبة إلى الغرامة المنصوص عليها كعقوبة أصلية فتُعرف بأنها: إلزام المحكوم عليه أن يدفع للجزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى على مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح، وذلك كله ما لم ينص القانون على خلافه. (انظر: المادة (71) من النص المعدل سنة 2016م للقانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي)

ويتضح لنا من خلال نص المادة (16) أعلاه أن المشرع الإماراتي قد جعل العقوبة الأصلية لجريمة الابتزاز الإلكتروني هي الحبس والغرامة، وحدد الحبس في سقفه الأعلى بسنتين، وكذلك حدد الغرامة في حدها الأدنى والأعلى خمسمائة ألف درهم، ولم يضع حداً أدنى للحبس تاركاً الأمر للقواعد العامة في القانون الجنائي، واستناداً إلى تلك القواعد العامة فإن الفقرة الثانية من المادة رقم (69) من القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي نصت على القاعدة العامة بالنسبة للحد الأدنى والأعلى لعقوبة الحبس على أنه: "... ولا يجوز أن يقل الحد الأدنى للحبس عن شهر ولا أن يزيد حده الأقصى على ثلاث سنوات ما لم ينص القانون على خلاف ذلك". كما أن للقاضي حرية الاختيار في أن يحكم بعقوبتي الحبس والغرامة معاً أو اختيار أحدهما حسبما يترأى في تقديره مدى جسامة الجريمة ومقدار الأضرار الناتجة عنها بالإضافة إلى خطورة الجاني الإجرامية سواء فيما يتعلق بجرائمه السابقة أو بدوافعه لارتكاب تلك الجريمة.

بالإضافة إلى أن المشرع الإماراتي قد قرر كذلك عقوبة السجن لمرتكب جريمة الابتزاز الإلكتروني والتي تصل إلى عشر سنوات إذا كان التهديد بالابتزاز من أجل ارتكاب جنائية أو بإسناد أمور خادشه للشرف والاعتبار (نصت الفقرة الثانية من المادة رقم (16) من المرسوم بقانون اتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات على أنه: (...وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جنائية أو بإسناد أمور خادشه للشرف أو الاعتبار)، إلا أنه لم يتبين من ذلك إن كانت عقوبة السجن منفردة أم يمكن جمعها مع الغرامة كما كان واضحاً في عقوبة الحبس، وبرأينا فإن الغرامة كعقوبة أصلية لم ترد إطلاقاً في الجنايات وإن وردت فترد كعقوبة تكميلية وليست أصلية (انظر: المادة رقم (28) من القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي)، وبهذا يكون المشرع الإماراتي قد وضع رادعاً قوياً حين يتصل التهديد بارتكاب جنائية وهي الجريمة الكبيرة،

أو يكون التهديد له علاقة بإسناد أمور تمس الشرف والاعتبار. (انظر: المادة رقم (28) من القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الاماراتي)

كما نجد أن المشرع الاماراتي في قانون العقوبات الاتحادي المعدل سنة 2005م أورد نصاً عاماً في المادة رقم (378) فيما يتعلق بالاعتداء على حرمة الحياة الخاصة باستخدام إحدى طرق التكنولوجيا، حتى وإن لم يتضمن الاعتداء على حرمة الحياة الخاصة تهديداً، وهو ما نثمن للمشرع الاماراتي هذا الاتجاه لحماية الخصوصية، مغلقاً بذلك كل الثغرات أمام أصحاب النفوس الآثمة.

وليس هذا فقط بل إن المشرع الاماراتي استند إلى قاعدة التشديد في العقوبة بحق مرتكب جريمة الابتزاز الإلكتروني، وذلك عندما تتوافر أسباب التشديد التي تؤثر على حدود السلطة التقديرية للقاضي، فهي تستبدل بحدودها المادية حدوداً جديدة حينما تكون وجوبية فتُلزم القاضي أن يحكم بعقوبة من نوع أشد مما يقرره القانون للجريمة، أو أن يحكم بعقوبة الجريمة مجاوزاً في مقدارها حداً أقصى، أو هي توسع نطاق هذه السلطة -حينما تكون جوازية- بتمكينها القاضي، بالإضافة إلى الحكم بالعقوبة المادية للجريمة أن يحكم بعقوبة أشد منها نوعاً أو مقداراً، وعلّة هذه الأسباب هي تمكين القاضي من تحقيق ملاءمة كاملة بين العقوبة التي ينطق بها والظروف الواقعية للدعوى التي تقتضي مزيداً من التشديد يجاوز ما يسمح به القانون في النص الخاص بالجريمة.

وتطبيقاً على ذلك، فإن جريمة الابتزاز الإلكتروني في التشريع الاماراتي تتضمن حالات تتشدد فيها العقوبة حال ارتكاب تلك الجريمة، والمقصود بالتشديد هنا أن يحكم القاضي بالحد الأعلى للعقوبة المقررة أو أن يحكم بكلا العقوبتين أي الحبس والغرامة معاً، فقد نصّت المادة (16) من المرسوم بقانون اتحادي رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات الاماراتي على أنه: "... وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جنائية أو بإسناد أمور خادشه للشرف والاعتبار".

كما ونصّت الفقرة الثانية من المادة رقم (46) من ذات المرسوم بقانون المشار إليه على أنه: "... كما يعد ظرفاً مشدداً ارتكاب أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة".

نستدل مما سبق أن المشرع الإماراتي قد خرج عن القواعد العامة بتقريره الظروف المشددة في نصوص خاصة قد غلظت من عقوبة جريمة الابتزاز الإلكتروني، حيث ارتفع مقدار العقوبة فيها مما أثر ذلك على نوع عقوبتها فلم تعد جنحة كما كانت في أصلها المقرر، وإنما تم استبدالها بعقوبة أخرى من نوع أشد، وبالتالي تحولت نوع العقوبة من جنحة إلى جنائية، وبهذا يكون المشرع الإماراتي قد وضع رادعاً قوياً حين يتصل التهديد بارتكاب جنائية وهي الجريمة الكبيرة، أو يكون التهديد له علاقة بإسناد أمور تمس الشرف والاعتبار أو في حال ارتكبت تلك الجريمة لحساب أو لمصلحة دولة أجنبية أو جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة.

وعلى الرغم من أن المشرع قد شدد في العقوبات المقررة لجريمة الابتزاز الالكتروني بنصوص خاصة تفرّد فيها عن تلك المنصوص عليها في القواعد العامة، إلا أنه جاء في المادة رقم (48) من المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات ونصّ على أنه: "لا يخل تطبيق العقوبات المنصوص عليها في هذا المرسوم بقانون بأي عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر" وبرأينا هذا نوع آخر من التشديد كذلك.

وبناءً على ما سبق ومن وجهة نظرنا فإن المشرع الإماراتي قد أحسن في تطبيق مبدأ التشديد في العقوبة بنصوص خاصة ضمن قانون خاص، إلا أنه كان لا بد له أن يُعالج حالة العود في جريمة الابتزاز الالكتروني التي تُعتبر ظرفاً من الظروف المشددة العامة عن طريق التشديد من العقاب بنص خاص بدلاً عن تطبيق القواعد العامة بشأن العود في هذه الجريمة، أملاً في أن تنتج العقوبة الشديدة من الأثر ما عجزت عن تحقيقه العقوبة الأقل شدة، وذلك لأن العود دليل على إصرار الجاني في إكمال سيره في طريق الإجرام لا سيما في هذه الجريمة محل دراستنا، وما ينطوي على ذلك من استهانة في الحكم بالعقاب المسبق مما سيُحقق الردع بنوعيه العام والخاص.

المطلب الثاني

العقوبات الفرعية

تُقسّم العقوبات الفرعية إلى عقوبات تبعية وعقوبات تكميلية، وتُعرّف العقوبات التبعية بأنها تلك العقوبات التي تلحق بعقوبة أصلية بقوة القانون دون حاجة إلى أن ينص القاضي عليها صراحة في الحكم، وقد بيّنت المادة رقم (73) من القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي العقوبات التبعية في قولها أن "العقوبات التبعية هي:

1- الحرمان من بعض الحقوق والمزايا.

2- مراقبة الشرطة.

وتلحق هذه العقوبات المحكوم عليه بقوة القانون دون حاجة إلى النص في الحكم وذلك على النحو المبين في هذا الفرع" (الفرع الأول من الفصل الثاني من الباب الخامس من الكتاب الأول من قانون العقوبات الاتحادي) (د. ربيع، 1993، ص:40).

أما بالنسبة إلى العقوبات التكميلية فهي تلك العقوبات التي تُصيب الجاني بناءً على الحكم بالعقوبة الأصلية بشرط أن يحكم القاضي بالعقوبة الأصلية (عودة، بدون سنة نشر، ص: 633)، وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناءً على الحكم بالعقوبة الأصلية دون الحاجة إلى إصدار حكم تباعي فهي مرتبطة ارتباطاً وثيقاً ومباشراً بالعقوبة الأصلية (عودة، بدون سنة نشر، ص: 641)،

وهذا النوع من العقوبات قد تكون وجوبية يلتزم القاضي بالنطق بها صراحة في حكمه المتضمن العقوبة الأصلية وإلا جاز الطعن على الحكم كالمصادرة، وقد تكون جوازية للقاضي سلطة تقديرية بالنطق بها في حكمه أو لا ينطق بها، وهنا يكون قد اكتفى بالنطق بالعقوبة الأصلية.

وبالإطلاع على المرسوم بقانون رقم (5) لسنة 2012 تبين أن المادة رقم (43) نصّت على أنه: "مع عدم الإخلال بالعقوبات المنصوص عليها في هذا المرسوم بقانون يجوز للمحكمة أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى، أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة"، كما ونصّت المادة رقم (41) على أنه: "مع عدم الإخلال بحقوق الغير حسني النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً أو للمدة التي تقدرها المحكمة."

ومن خلال استعراضنا لتلك النصوص فإنه يتضح لنا أن المشرع الإماراتي قد قرر عقوبة تكميلية لجريمة الابتزاز الإلكتروني متمثلة في المصادرة، مخاطباً بها القاضي الذي يتعين عليه أن يلتزم بالنطق بها في حكمه إلى جانب العقوبة الأصلية، فتكييفنا القانوني للمصادرة بأنها عقوبة وليست تدبير وقائي مبرره أن محل المصادرة في هذه الجريمة هي أشياء لا يعتبرها القانون بمجرد حيازتها أنها جريمة، بالإضافة إلى أن المشرع الإماراتي في الوقت نفسه قد راعى عند إقراره لتلك العقوبة التكميلية حقوق غير حسني النية (الشخص الأجنبي عن الجريمة) عندما يكون لهذا الشخص حق عيني على الأشياء محل المصادرة مثل: حق الملكية، وحق الرهن وغيرها من الحقوق العينية الأخرى، ومن المؤكد أن مراعاة حقوق الغير هنا لا يُقصد بها عدم جواز المصادرة مطلقاً، وإنما تنتقل ملكية الشيء محل المصادرة إلى الدولة محملة بحقوق هؤلاء الغير.

كما وقرر المشرع الإماراتي مجموعة من التدابير الجنائية المقيدة والسالبة للحرية المتمثلة في: حرمان المحكوم عليه من استخدام أي شبكة معلوماتية أو نظام المعلومات الإلكتروني أو أي وسيلة تقنية معلومات أخرى، وإغلاق المحل أو الموقع الذي ارتكبت فيه الجريمة وذلك للمدد التي تقدرها وتراها المحكمة مناسبة، وبهذا لم يُحدد المشرع مدد معينة للقاضي ليحكم بها، بل ترك تحديدها بالرجوع إلى القواعد العامة في قانون العقوبات الإماراتي السالف الذكر.

وأخيراً وجب علينا توضيح أن المشرع الإماراتي أجاز كذلك وضع المحكوم عليه تحت الإشراف والمراقبة كنوع من التدابير الجنائية المقيدة للحرية، والمراقبة هنا لا يمكن من وجهة نظرنا تكييفها كعقوبة تبعية لسببين: أحدهما أن المراقبة لتكون عقوبة تبعية يجب أن تُلحق بالمحكوم عليه بقوة القانون دون حاجة إلى النص عليها في الحكم،

والثانية استناداً إلى حكم المادة رقم (79) من قانون العقوبات الاتحادي الإماراتي (نصت الفقرة الأولى من المادة (79) من القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي على أنه: من حكم عليه بالسجن المؤبد أو المؤقت في جريمة ماسة بأمن الدولة الخارجي أو الداخلي أو في جريمة تزوير نقود أو تزويرها أو تقليدها أو تزوير طوابع أو مستندات مالية حكومية أو محررات رسمية أو في جريمة رشوة أو اختلاس أو سرقة أو قتل عمد، يوضع بحكم القانون بعد انقضاء مدة عقوبته تحت مراقبة الشرطة وفقاً للقواعد التي يحددها وزير الداخلية مدة مساوية لمدة العقوبة على أن لا تزيد على خمس سنوات)، فالمراقبة كعقوبة تبعية يُحكم بها لارتكاب جرائم مُحددة على سبيل الحصر، وأن يكون المتهم قد حكم عليه بعقوبة أصلية (السجن المؤبد والسجن المؤقت)، وبالتالي تُكَيّف المراقبة من الناحية القانونية على أنها تدبير من التدابير الجنائية التي تحكم بها المحكمة.

المطلب الثالث

عقوبة الشروع والمشاركة الإجرامية

يُقصد بالشروع كما ذكرناه سابقاً البدء بالتنفيذ في الجريمة التي يعقد الجاني العزم على ارتكابها، ولكنه لا يصل إلى النتيجة التي يريد تحقيقها، والشروع هو جريمة ناقصة تخلفت بعض عناصرها، أما في حال توافرت جميع عناصر الجريمة فالجريمة تصبح تامة ولا تعتبر شروعاً والعنصر المفقود فيها هو النتيجة الإجرامية، فالجاني قد يرتكب الفعل الذي أراد به تحقيق هذه النتيجة ولكن فعله لم يفض إلى ذلك، بمعنى أن الشروع يتوافر فيه عناصر الجريمة التامة باستثناء النتيجة الإجرامية.

ويُشترط في الشروع شرطين: الأول، البدء في التنفيذ، أي ارتكاب فعل في حد ذاته يعتبر جزءاً من الأجزاء المكونة للركن المادي للجريمة أو يؤدي إليه مباشرة، ولا يعتبر شروعاً في الجريمة بمجرد العزم على ارتكابها أو التفكير فيها ولا حتى الأعمال التحضيرية لها طالما كان التحضير لا يشكّل جريمة بنفسه، وتسبق مرحلة التنفيذ المُعاقب عليها ما لم ينص القانون على خلاف ذلك، والشرط الثاني، هو عدم إتمام الجريمة لأسباب خارجة عن إرادة الفاعل، مثاله قيام المبتز بتهديد ضحيته وذلك بعد اختراق هاتفه المتنقل وإبلاغه بحصوله على صور فاضحة له، إلا أنه وقبل التهديد تعطل هاتفه المتنقل الذي كان سيرسل ابتزازه عن طريقه، فهنا الجريمة وقفت لسبب خارج عن إرادة الجاني، فتُصبح الجريمة ناقصة لعدم اكتمال النتيجة الإجرامية المرجوة.

وينقسم الشروع إلى قسمين: الشروع التام، ويُقصد به قيام الجاني بارتكاب جريمته كاملة، ولكن النتيجة الإجرامية لم تتحقق، كقيام شخص هدد آخر للحصول على أموال بعد حصوله على مقاطع مصورة له تشينه، وقبل أن تتحقق النتيجة الإجرامية قبض عليه (أحمد، 2011، ص: 159)، والشروع الناقص، ويُقصد به أن النشاط الاجرامي الذي يقوم به الجاني لم يتم بشكل كامل، مثال ذلك أن تتمكن السلطات من القبض على المبتز بعد حصوله على مستندات سرية لشركة تجارية،

وقبل أن يقوم بتنفيذ تهديد الشركة وابتزازها (أحمد، 2011، ص: 153) أي أنه فقط كانت عنده نية الابتزاز ولم ينفذ تلك الجريمة بالفعل.

وبعد دراستنا وإطلاعنا على النصوص التشريعية الإماراتية المتعلقة بالشروع، اتضح لنا بأن المشرع قد سار في فلك القواعد الخاصة حينما قرر أن يُعاقب الجاني على شروعه في ارتكاب الجرائم الجنحية (جريمة الابتزاز الإلكتروني) وجعلها نصف العقوبة المقررة للجريمة التامة، وهذه الصلاحية استمدّها المشرع من القواعد العامة الواردة في قانون العقوبات الاتحادي الذي لم يُحدد أنواع الجرائم الجنحية التي يُعاقب على الشروع فيها وكذلك مدة العقوبة تاركاً تحديدها للنصوص الخاصة (انظر: المادة رقم (36) + (37) من القانون الاتحادي رقم (3) لسنة 1987 بشأن إصدار قانون العقوبات الإماراتي)، فالجنايات برأينا هي جرائم جسيمة الأصل فيها أن يُعاقب على الشروع فيها لذلك جرّم المشرع الشروع فيها وحدد لها عقوبة،

أما بالنسبة إلى الجنح فخطورتها تعتبر أقل جسامة فهي غير جديرة بالعقاب إلا إذا كان المشرع يرى عكس هذا الأمر فإنه ينص على تجريم الشروع فيها بنصوص خاصة، وهذا ما ذهب إليه المشرع في المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات، تاركاً تطبيق القواعد العامة للشروع في الجنايات.

أما بالنسبة إلى عقوبة المشاركة الإجرامية: فقد يكون الاشتراك مباشراً أو بالتسبب، فبالنسبة إلى الاشتراك المباشر فكل من يُباشِر في ارتكاب الركن المادي للجريمة سواء أكان شخصاً واحداً فيُعاقب عقوبة الفاعل الأصلي أو عدة أشخاص فيعتبر كل منهم مباشر للجريمة ويُعاقب عقوبة الاشتراك المُباشِر، أي بمعنى يُعاقب هؤلاء نفس عقوبة الفاعل الأصلي، فعقوبة من اشترك مع آخرين في مباشرة الجريمة هي ذات العقوبة المقررة لمن يرتكب الجريمة وحده، وقد قرر المشرع الإماراتي في الفصل الثالث من الباب الثالث من قانون العقوبات الاتحادي قاعدة المشاركة الإجرامية (انظر: المواد رقم (44 إلى 52) من القانون الاتحادي رقم (3) لسنة 1987 بشأن إصدار قانون العقوبات الإماراتي).

أما بالنسبة إلى الاشتراك غير المباشر أو بالتسبب، فهو نشاط يرتبط بالفعل الإجرامي ونتيجة برابطة سببية دون أن يتضمن تنفيذاً للجريمة أو قياماً بدور رئيس في ارتكابها، أي أن تكون مساهمة الشريك بفعل من الأفعال "الممهدة أو المسهلة للفاعل" في تنفيذ جريمته دون أن يكون هذا الفعل داخلاً في نطاق الركن المادي للجريمة، والمشارك التبعي هو من يقوم بنشاط ثانوي في تنفيذ الجريمة وبذلك فلا يعتبر نشاطه رئيساً، ذلك أنه لا يقوم بدور رئيسي في الجريمة ويرتبط نشاطه بنشاط المساهم الأصلي ويستمد منه صفة الإجرامية (د. مصبح، 2015، ص: 258+259)، وقد بيّنت المادة رقم (45) من قانون العقوبات الاتحادي صور الاشتراك الغير مباشر أو بالتسبب المتمثل في التحريض، الاتفاق، والمساعدة (نصت المادة (45) من القانون الاتحادي رقم (3) لسنة 1987 بشأن إصدار قانون العقوبات الإماراتي على أنه: "يعد شريكاً بالتسبب في الجريمة: أولاً: من حرض على ارتكابها فوَقعت بناء على هذا التحريض، ثانياً: من اتفق مع غيره على ارتكابها فوَقعت بناء على هذا الاتفاق، ثالثاً: من أعطى الفاعل سلاحاً أو آلات أو أي شيء آخر استعمله في ارتكاب الجريمة مع علمه بها أو

ساعد الفاعل عمدا بأي طريقة أخرى في الأعمال المجهزة أو المسهلة أو المتممة لارتكاب الجريمة، وتتوفر مسؤولية الشريك سواء أكان اتصاله بالفاعل مباشرة أم بالواسطة).

وفيما يتعلق بجريمة الابتزاز الإلكتروني محل هذه الدراسة، فإنه وبالرجوع إلى المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات الإماراتي نجد أن المشرع الإماراتي لم ينص صراحة في المادة رقم (16) على عقاب الشريك، كما أنه لم يفرد نصاً خاصاً للعقاب على المساهمة أو المشاركة الجنائية لجريمة الابتزاز الإلكتروني، إلا أننا نرى أنه في هذه الحالة تُطبق القواعد العامة في المشاركة الجنائية، باعتبار الشريك المتسبب مساهماً في الجريمة ومستحقاً للعقاب مثله، والقانون قد سوى بين عقوبة الفاعل الأصلي وعقوبة الشريك بالتسبب، وهذه المساواة من وجهة نظرنا هي مساواة تشريعية حيث يُطبق نص تشريعي واحد على كل من الفاعل الأصلي والثانوي ويخضعون لذات النص المتعلق بالجريمة التي اقترفوها والعقوبة المقررة لها.

المطلب الرابع

مواجهة جريمة الابتزاز الإلكتروني بالإبعاد

الإبعاد كما هو معلوم أنه تدبير جنائي مقيد للحرية يتم فرضه من قبل السلطات المختصة في حالات معينة على بعض المقيمين في الدولة ويقتصر على الأجانب فقط، وهم هؤلاء الذين صدرت ضدهم أحكام إدانة بجرائم واقعة على العرض أو ارتكابهم لبعض الجرائم التي تضر أمن المجتمع كالإتجار والتعاطي بالمواد المخدرة والمؤثرات العقلية، فيفرض عليهم مغادرة الدولة وعدم العودة إليها مرة أخرى إما بصفة دائمة أو مؤقتة، كما ويتم فرض تدبير الإبعاد في بعض الحالات بشكل إداري وخصوصاً عندما تستدعي المصلحة العامة أو الأمن والنظام العام استبعاد أحد الأشخاص عن أراضي الدولة.

نصّ المرسوم بقانون رقم (5) لسنة 2012م بشأن مكافحة جرائم المعلومات في مادته رقم (41) على أنه: "مع مراعاة حكم الفقرة الثانية من المادة (121) من قانون العقوبات تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجنائية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها. "

ولعل هذا الحكم بالإبعاد للأجنبي بعد تنفيذه للعقوبة هو نوع من التدابير الجنائية المقيدة للحرية، وهو حكم متصور ومنطقي للأجنبي الذي يسئ إلى الوطن الذي يعيش فوق أرضيه، وبرأينا فإن المشرع الإماراتي أحسن بالنص على هذا النوع من التدبير، فثقافة احترام القانون تعتمد على إيجاد علاقة إيجابية بين الفرد والقانون لدورها في حماية الأرواح وحفظ الحقوق، لأن المجتمع لا يعتمد على فهم القانون من نصوصه، إنما على فهم طبيعة الحالات المجرمة التي تحدث في الواقع. (عابد، 2019)

واستناداً إلى جميع ما ذكر، فما توصل إليه الباحث من خلال هذه الدراسة يُثبت أن دولة الإمارات العربية المتحدة من أوائل الدول التي أصدرت تشريعها الخاص في شأن مكافحة جرائم تقنية المعلومات ضمن القوانين الملزمة والنافذة لديها،

في حين أن هناك دول عربية أخرى لم تتناول أي تشريعات تعاقب المجرّم على الجرائم الإلكترونية وجرائم الابتزاز بالدرجة الأولى، والتي للأسف تساعد المجرمين على اقتراف المزيد من هذا النوع من الجرائم، فعدم وجود تشريعات في بعض الدول الأخرى سواء على المستوى العربي أو العالمي تُعاقب على جريمة الابتزاز الإلكتروني فهذا يؤثر سلباً على دولة الإمارات وخصوصاً أن هذا النوع من الجريمة يُعتبر من الجرائم الدولية الممتدة، وبالتالي يجعل من جريمة الابتزاز جريمة معقدة وحلولها تواجه صعوبات منها في عدم وجود قوانين مساعدة ومشتركة كما أسلفنا ذكره من ناحية، وذكاء مجرم متمرس ومتخفي عبر الإنترنت من ناحية أخرى.

الخاتمة

تعتبر جريمة الابتزاز الإلكتروني من الجرائم المستحدثة، ويطلق عليها في علم الجريمة الجرائم الناعمة التي تخلو من العنف، وهي أحد صور الجريمة الإلكترونية، والابتزاز الإلكتروني هو الوجه الآخر لجريمة الابتزاز التقليدية التي تنشأ وترتكب في عالم مادي، وفي مسرح جريمة تقليدي، حيث يترك الجاني فيه بصمة، أو نقطة دم، أما الابتزاز الإلكتروني فيتم في عالم افتراضي مليء بالرموز والشفرات، ويتنامى التحدي حين نجد العقبات والصعوبات التي تواجه أجهزة التحقيق في التحقيق فيها وفي التعامل مع الدليل الرقمي، وهذه الجريمة أصبحت تمثل هوساً لدى مستخدمي التكنولوجيا الحديثة، وذلك بعد ثورة المعلومات والتكنولوجيا التي تفجرت بالقرن العشرين، وإزاء هذه الثورة حاولت الدول في البداية أن تطوع التشريعات لتواكب هذه الجرائم المستحدثة، ثم تنبّهت لضرورة إفراد نصوص تشريعية خاصة بهذه الجرائم الإلكترونية، وجريمة الابتزاز الإلكتروني على وجه الخصوص، وكل ما سلف ذكره هو نتيجة دراسات حاولنا من خلال خطة منطوية لا نزعم كمالها أن نتوصل إلى المخاطر التي أفرزتها تلك الجريمة وكيفية ومواجهتها من خلال التشريع، حيث اتضح لنا من خلال هذه الدراسة أن المشرع الإماراتي قد أفرد قواعد خاصة في تجريم الابتزاز الإلكتروني قيد فيها الأحكام العامة، وحسناً فعل المشرع لأن هذا النوع من الجريمة هو بمثابة جريمة العصر برأينا التي تُعتبر من أبشع الجرائم التي حدثت خلال السنوات الماضية، والتي وجدت لها سبيلاً سهلاً وسريعاً وفعالاً مع تقدم الوسائل التكنولوجية الحديثة والمتطورة، جعل من إفراد القواعد الخاصة لها لازماً للتمكن من التصدي لها ومواجهتها تشريعياً وقانونياً.

النتائج والتوصيات

أولاً: النتائج:

توصلنا في دراستنا هذه إلى عدد من النتائج نوردتها فيما يلي:

1. جريمة الابتزاز جريمة قد تتسبب في حدوث جرائم بعدها، كالزنا أو القتل أو جريمة عنف أو سرقة.
2. جريمة الابتزاز جريمة عابرة للحدود، فقد يكون المبتز في دولة بالعالم، ويقوم بابتزاز ضحيته في أقصى العالم.

3. جريمة الابتزاز الإلكتروني جريمة يصعب إثباتها، حيث من السهل أن تمحى آثارها بسهولة، وتحتاج لعمل شاق حتى يتم اثباتها.

ثانياً: التوصيات:

1. ضرورة استمرار نشر الوعي المجتمعي بأخطار جريمة الابتزاز الإلكتروني.
2. تشجيع من يتعرض للابتزاز بالإبلاغ عن الجريمة، وسط تأمين سرية للمجني عليه حتى لا يحجم عن الإبلاغ.
3. إنشاء قاعدة بيانات أمنية عن المبتزين الذين يتم القبض عليهم في جرائم الابتزاز الإلكتروني، لتكون متاحة على جميع المنافذ بالدولة لمنع هؤلاء المبتزين من العودة مرة أخرى بعد ابعادهم عن ربوع دولتنا الحبيبة.

قائمة المصادر والمراجع

أولاً: الكتب:

1. ابن منظور، لسان العرب، بيروت: دار إحياء التراث العربي، مؤسسة التاريخ العربي، ط:1، ج:1، سنة 711هـ / 630م.
2. د. حسن محمد ربيع، شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، دبي: كلية شرطة دبي، ج:2، سنة 1413هـ / 1993م.
3. خالد حسن لطفي، جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني-دراسة مقارنة- الاسكندرية: دار الفكر الجامعي، سنة 2019م.
4. نياض موسى البداينة، ورقة عمل علمية: الجرائم الإلكترونية، المفهوم والأسباب، الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحويلات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان: سنة 2014م.
5. طعباش أمين، الحماية الجنائية للمعاملات الالكترونية، الاسكندرية: دار الوفاء لدنيا الطباعة والنشر، مكتبة الوفاء القانونية، ط:1، سنة 2015م.
6. عبد الرحمن توفيق أحمد، شرح قانون العقوبات القسم العام، عمان: دار الثقافة للنشر والتوزيع، سنة 2011م.
7. عبد القادر عودة، الأحكام العامة للتشريع الجنائي الإسلامي، بيروت: دار الكتاب العربي، ط:1، بدون سنة نشر.
8. د: علي محمد جعفر، قانون العقوبات والجرائم، بيروت: المؤسسة الجامعية للدراسات والنشر والتوزيع، ط:1، سنة 1420هـ / 2000م.
9. د. عمر عبدالمجيد مصبح، شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، مصر: دار الكتب القانونية، سنة 2015م.

10. فتحية عبدالغني الجميلي، الجريمة والمجتمع ومرتكب الجريمة، عمان: دائرة المكتبة الوطنية، سنة 2001م.
11. محمد سالم الزعابي، الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكتروني، الرياض: مكتبات جامعة الملك سعود، سنة 2014م.
12. أ.د. محمد واس قلعة جي، معجم لغة الفقهاء، بيروت: دار النفائس للطباعة والنشر والتوزيع، ط:2، سنة 1997م.

ثانياً: الرسائل العلمية:

1. سليمان بن غازي العتيبي، دور البحث الجنائي في الكشف على الجرائم المعلوماتية، أطروحة دكتوراه، المملكة العربية السعودية جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الدراسات الأمنية، سنة 2016م.
2. مسلم بن شباب المطيري، التعويض عن إساءة السمعة عبر وسائل التواصل الاجتماعي الحديثة، أطروحة دكتوراه، المملكة العربية السعودية: جامعة نايف العربية للعلوم الأمنية، سنة 2014م.
3. منصور صالح السلمي، المسؤولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، سنة 2010م.

ثالثاً: التشريعات:

1. القانون الاتحادي رقم (3) لسنة 1987م بشأن إصدار قانون العقوبات الإماراتي وتعديلاته.
2. المرسوم بقانون رقم (5) لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات وتعديلاته.

رابعاً: مواقع ومنشورات إلكترونية:

1. <https://www.mohamah.net/law>
2. احصائيات اعلام الكتروني، متوفرة على الموقع:
<http://www.internetworldstats.com/stats5.htm>
3. أحمد عابد – العقوبات تشمل «المزاحين» والجهل بالعقوبة لا يعفي من المساءلة، منشور في الانترنت، الامارات العربية المتحدة: أبوظبي، صحيفة الاتحاد، التاريخ: 27 يناير 2019.
4. داليا عبدالعزيز، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة، المملكة العربية السعودية: كليات القصيم الأهلية، بحث نشر في مجلة جيل الأبحاث القانونية المعمقة، العدد 25، سنة 2017م.

5. سينا عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، أعمال الندوة الإقليمية حول: الجرائم المتصلة بالإنترنت، المملكة المغربية: إصدارات برنامج الأمم المتحدة لتعزيز حكم القانون في بعض الدول العربية، سنة 2015م، ص: 52.
6. عبد المحسن بدوي محمد أحمد، بحث منشور في الإنترنت بعنوان تشريعات الإعلام الجديد وجرائم الإنترنت، مجلة الأمن والحياة، العدد 347، مارس/إبريل 2011.
7. نبيه طارق عبد المجيد، الأمن الإلكتروني ضرورة ملحة لأمن المجتمعات، المجلة العربية الدولية للمعلوماتية، المجلد 06، العدد 11، سنة 2018م.

فهرس المحتويات

الصفحة	الموضوع
1	المقدمة
1	أهمية الدراسة
2	إشكالية الدراسة
2	تساؤلات الدراسة
2	منهج الدراسة
3	خطة البحث
المبحث الأول	
طبيعة وماهية الابتزاز الإلكتروني	
3	تمهيد
4	المطلب الأول: مفهوم الابتزاز الإلكتروني وأنواعه
6	المطلب الثاني: الآثار الخطيرة للابتزاز الإلكتروني وكيفية مواجهته
المبحث الثاني	
مواجهة المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث التجريم	
7	تمهيد
8	المطلب الأول: الركن المادي في جريمة الابتزاز الإلكتروني
9	المطلب الثاني: الإشتراك الجرمي والشروع في جريمة الابتزاز الإلكتروني
10	المطلب الثالث: الركن المعنوي في جريمة الابتزاز الإلكتروني

المبحث الثالث	
مواجهة المشرع الإماراتي لجريمة الابتزاز الإلكتروني من حيث العقاب	
11	تمهيد
12	المطلب الأول: العقوبات الأصلية
14	المطلب الثاني: العقوبات الفرعية
16	المطلب الثالث: عقوبة الشروع والمشاركة الإجرامية
18	المطلب الرابع: مواجهة جريمة الابتزاز الإلكتروني بالإبعاد
19	الخاتمة
19	النتائج والتوصيات

جميع الحقوق محفوظة © 2021، الأستاذ الدكتور/ أحمد موسى هياجنه، الباحثة/ عائشة محمد هزيم سيف السويدي،
المجلة الأكاديمية للأبحاث والنشر العلمي. (CC BY NC)