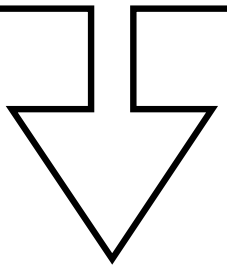
جريمة الابتزاز الالكتروني

The crime of electronic extortion



م.م. حسين عباس حميد

كلية الحقوق – جامعة ذي قار

Hussein Abbas Hameed

hussein.abbas1994@gmail.com

Summary

It goes without saying that the crimes vital information Mattei of the novel crimes ، emerged with the development of the use of the World Wide Web, with the emergence of a new type of crime in a new environment was needed on legislation to be the bulwark to stand against such illegal acts.

The world still day after day offers us new ideas and different worlds that take us to a new society, where it is called today the Information Society, for information is the hallmark of global development and the lifeline of countries in their progress and development, and it is very natural that this society has left behind many new crimes that we do not find. It has an analogue in previous crimes, and this development has allowed the perpetrators to commit traditional crimes in innovative ways such as electronic extortion, electronic theft, insult, slander and the like, and what makes the task of detecting these crimes difficult is that they are crimes that do not recognize borders, so that the perpetrator can commit a crime while he is in a state. And the victim in another country.

The problem of research is the novelty of the crime of electronic extortion, and this crime has also raised many questions about the extent to which traditional texts can be applied to this crime, and through that, we find there is also a prominent problem in the extent to which traditional procedures can adequately detect this crime.

And for that, we will adopt in the research the analytical and comparative approach, by analyzing the punitive texts as well as comparing the texts with other countries in order to reach a clear and integrated view of this crime..

key words:

Electronic extortion - information crime - electronic searches - social networking sites

الملخص

من نافلة القول إن الجرائم المعلوماتية من الجرائم المستحدثة، ظهرت مع تطور استخدام الشبكة العالمية، مع هذا البزوغ لنوعٍ جديد من الجرائم في بيئة جديدة كان من اللازم على التشريعات أن تكون هي حائط الصد للوقوف بوجه هكذا أفعال غير مشروعة.

ما زال العالم يومًا بعد يوم يقدم لنا أفكارًا جديدة وعوالم مختلفة تأخذنا لمجتمعٍ جديد إذ يطلق عليه اليوم مجتمع المعلومات، فالمعلومة هي سمت التطور العالمي وطوق نجاة الدول في تقدمها وتطورها، ومن الطبيعي جِدًّا أن هذا المجتمع قد خلف وراءه الكثير من الجرائم المستحدثة التي لا نجد لها مثيل في الجرائم السابقة، وهذا التطور قد أتاح للجناة ارتكاب جرائم تقليدية بطرق مستحدثة مثل الابتزاز الإلكتروني والسرقة الإلكترونية والسب والقذف وما يقع في شاكلتها، ومما يُصعب مهمة كشف هذه الجرائم هو أنها جرائم لا تعترف بالحدود، بحيث يمكن للجاني أن يرتكب جريمة وهو في دولة والمجني عليه في دولة أخرى.

تتمثل مشكلة البحث في حداثة جريمة الابتزاز الإلكتروني، وكذلك أثارت هذه الجريمة تساؤلات كثيرة في مدى إمكانية تطبيق النصوص التقليدية على هذه الجريمة، ومن خلال ذلك نجد هنالك مشكلة بارزة أيضًا في مدى إمكانية كفاية الإجراءات التقليدية في الكشف عن هذه الجريمة.

ولأجل ذلك سنعتمد في البحث المنهج التحليلي والمقارن، من خلال تحليل النصوص العقابية وكذلك المقارنة بين النصوص مع دول أخرى في سبيل الوصول لرؤية واضحة ومتكاملة لهذه الجريمة.

الكلمات المفتاحية:

الابتزاز الإلكتروني- الجريمة المعلوماتية- التفتيش الإلكتروني- مواقع التواصل الاجتماعية.

المقدمة

من بوادر القول إن الجرائم المعلوماتية من الجرائم المستحدثة والتي ظهرت مع تطور استخدام الشبكة العالمية -الإنترنت- في القطاع المدني، مع هذا البزوغ لنوعٍ جديد من الجرائم في بيئة جديدة كان من اللازم على التشريعات أن تكون هي حائط الصد للوقوف بوجه هكذا أفعال غير مشروعة.

فما زال العالم يومًا بعد يوم يقدم لنا أفكارًا جديدة وعوالم مختلفة تأخذنا لمجتمعٍ جديد حيث يطلق عليه اليوم مجتمع المعلومات، فالمعلومة هي سمت التطور العالمي وطوق نجاة الدول في تقدمها وتطورها، ومن الطبيعي جدًّا أن هذا المجتمع قد خلف وراءه الكثير من الجرائم المستحدثة التي لا نجد لها مثيل في الجرائم السابقة، وهذا التطور قد أتاح للجناة ارتكاب جرائم تقليدية بطرق مستحدثة مثل الابتزاز الإلكتروني والسرقة الإلكترونية والسب والقذف وما يقع في شاكلتها، ومما يُصعب مهمة كشف هذه الجرائم هو أنها جرائم لا تعترف بالحدود، بحيث يمكن للجاني أن يرتكب جريمة وهو في دولة والمجني عليه في دولة أخرى.

مما تجدر الإشارة اليه هو أن هذه الجرائم يقتضي لمواجهتها وجود بُنية أو مجموعة من المتطلبات في بدايتها وجود بيئة قانونية تشريعية لمكافحتها والحد منها، وكذلك وجود جهات تحقيق متخصصة للبحث والتحري وكذلك في التحقيق والمحاكمة، ولا ننكر الجهود الدولية المُضنية التي تحاول الحد من انتشار هكذا نوع من الجرائم، ولكن نجد الكثير من المعاناة التي يواجهما القضاء العراقي وخاصة مع عدم وجود قانون لمكافحة للجريمة المعلوماتية التي جعلت المحاكم تلجأ للقواعد الجنائية التقليدية.

ولكن مع هذا التطور السريع نجد أن هذه القواعد التقليدية تقف قاصرة ولربما عاجزة لمواجهة هكذا جرائم بسبب حداثتها وطريقة كشفها مما يسبب ضررًا كبيرًا للمجني عليه، فانتشار هذه الجرائم يستحق الكثير من الجهد في سبيل تحقيق الهدف الذي وجد لأجله القضاء ألا وهو تحقيق العدل وعدم التفريط بحقوق الأشخاص وحماية حقوق الإنسان أيضًا، وبهذا لا بُدَّ من وجود قانون يجرم ويحد من الانتهاكات التي تحصل في العالم الافتراضي مع كثرة الاستخدامات لهذا الواقع، وبُغية مواكبة التطور الذي يشهده الجانب المعلوماتي مما يتطلب وجود بيئة قانونية سليمة وداعمة لهذا التطور، فمن غير القانون تبقى الساحة مفتوحة لارتكاب الجرائم التي تؤثر بشكل كبير على النسيج الاجتماعي وتجعل منه بيئة للصراعات والأزمات وارتكاب الجرائم الكُبرى وانتهاكًا لحقوق الإنسان.

ولذا من الضروري تهيئة الأجواء المناسبة في سبيل الحد من هذه الجرائم، من خلال وجود بيئة قضائية وأمنية تساهم في مواجهة هكذا أفعال غير مشروعة، فالعالم الافتراضي هو

عالم واقعي بصورة أخرى ذلك أن السرقة تحولت من سرقة تقليدية إلى سرقة تقع على العملة الإلكترونية وكذلك السب والقذف والابتزاز الإلكتروني وغيرها الكثير من الجرائم إذ تحولت من جرائم تقليدية لجرائم تقع في واقع افتراضي، فهذه الأفعال تحتاج لقدرة وإمكانية دولية في مواجهتها والحد منها.

وبهذا فإن مشكلة البحث:

تتمثل مشكلة البحث في حداثة جريمة الابتزاز الإلكتروني، وكذلك أثارت هذه الجريمة تساؤلات كثيرة في مدى إمكانية تطبيق النصوص التقليدية على هذه الجريمة، ومن خلال ذلك نجد هنالك مشكلة بارزة أيضًا في مدى إمكانية كفاية الإجراءات التقليدية في الكشف عن هذه الجريمة.

أهمية البحث:

تبرز أهمية البحث من خلال إن القانون هو حائط الصد الأول في مواجهة إساءة استخدام وسائل التِقنية والاعتداء على الأشخاص، حيث يُعد القانون الطريق الذي اتخذ من قبل المجتمع الدولي وتبنته الاتفاقيات الدولية والإقليمية في سبيل مكافحة هذا النوع من الجرائم.

تساؤلات البحث:

١- مدى إمكانية تطبيق النصوص التقليدية في مواجهة جريمة الابتزاز الإلكتروني.

٢- نجاعة الإجراءات التقليدية في الكشف عن الجريمة.

٣- أهمية وجود قانون خاص يعالج هكذا نوع من الجرائم .

منهجية البحث :

اعتمدنا في البحث المنهج التحليلي والمقارن، من خلال تحليل النصوص العقابية وكذلك المقارنة بين النصوص مع دول أخرى في سبيل الوصول لرؤية واضحة ومتكاملة لهذه الجريمة.

خطة البحث :

المبحث الأول: ماهية جريمة الابتزاز الإلكتروني

المطلب الأول: تعريف جريمة الابتزاز الإلكتروني

المطلب الثاني: خصائص جريمة الابتزاز الإلكتروني

المبحث الثاني: صعوبات مكافحة جريمة الابتزاز الإلكتروني

المطلب الأول: الصعوبات التشريعية.

المطلب الثاني: الصعوبات الإجرائية.

المبحث الأول: ماهية جريمة الابتزاز الإلكتروني

مما لا شك فيه أن التطور الحديث في اَلتِّقْنِيَّة نتج عنه ممارسات غير مشروعة، وأفكار جديدة في ارتكاب الجريمة، فالمجرم في الجريمة المعلوماتية لا يرتكب الجريمة بصورة تقليدية بل يرتكب جرائم تتصف بأنها أكثر خطورة وعدوانية، ومع هذا التطور في ارتكاب الجريمة سعت الدول بسلطتها التشريعية في رفد المؤسسة القضائية بقوانين تحد وتكافح هذه الجرائم لمساسها بالمؤسسات العامة والخاصة والأفراد.

فجريمة الابتزاز الإلكتروني هي صورة من صور الجريمة المعلوماتية التي بانت ملامحها واضحة في ظل انتشار مواقع التواصل الاجتماعي ودخول التِقنية مناحي الحياة كافة.

ومع التطور المستمر للشبكة العالمية وتوفر السرية التامة جعلا من الشبكة العالمية جهازًا مثاليًا لارتكاب الكثير من الجرائم بعيدًا عن أنظار الجهات الأمنية، حيث مكنت هذه الشبكة مافيا الجرائم المعلوماتية من نقل المعلومات الخطرة والمحظورة سواء معلومات مخابراتية أو خطط تجريبية أو صور سرية بمجرد الضغط على زر لوحة المفاتيح دون أدنى جهدٍ ودون الخوف من العقاب(١)

ترتبط الجريمة المعلوماتية ارتباطًا وثيقًا لا يقبل التجزئة بتقدم تقدم الدول والشعوب في استخدام تقنية الحاسوب والشبكة العالمية فبنهما علاقة طردية حيث كلما زادت كان مؤشرًا رئيسا على زيادة معدل الجريمة المعلوماتية، حيث من المعلوم إن الجريمة المعلوماتية لها طابع تِقني، كما أنه من السهل اخفاء معالم الجريمة وصعوبات تتبع مرتكبيها، كما وانه

يصعب على المحقق التقليدي التعامل مع هذه الجرائم، وذلك يصعب عليه متابعة جرائم الشبكة العالمية والكشف عنها وإقامة الدليل عليها فهي بطبيعة الحال جرائم تتسم بالغموض، والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.[٢]

المطلب الأول: تعريف جريمة الابتزاز الإلكتروني

تُعد الشبكة العالمية المصدر الرئيس التي تتشكل منها المجتمعات المعلوماتية، فقد حدثت طفرة في الاتصالات حولت العالم إلى حجرة صغيرة فأصبح المستخدم باستطاعته أن يرصد ما يحصل في الجانب الآخر من العالم بالصوت والصورة وكذلك الكتابة، وأصبحت عملية تبادل المعلومات والمعارف سهلة وميسورة، وأدى الانتشار السريع للمعلومات عبر وسائل الاتصال المختلفة إلى تدفقٍ هائل من المعلومات والأخبار والمعرفة والأبحاث التي يصعب على الإنسان الإلمام بها ومتابعتها بصورة دقيقة لولا وجود الشبكة العالمية، وإن كانت شبكة المعلومات مصدر وخزائن المعرفة وبحر المعلومات إلّا أنها أيضا تُعد ركيزة في ارتكاب الجريمة حيث في هذه البيئة الكبيرة الممتلئة تضيق قبضة الأمن والمراقبة والتحكم وتنمو عمليات التجسس على المعلومات المعالجة إلكترونيًا وسرقتها حتى باتت تشكل تهديدًا كبيرًا لأغلب المنظمات الحكومية والخاصة التي يكون مصدر عملها الحاسوب والشبكة العالمية [٣].

إن الجريمة المعلوماتية نوع من الجرائم المستحدثة والتي لم تحظَ بالكثير من التطبيقات القضائية من حيث الاختصاص القضائي بمنازعاتها والقانون واجب التطبيق عليها، كذلك فالدول ما زالت تعاني من الفراغ التشريعي الذي يعالج هذه الإشكاليات والتي تعددت محاولات الفقه لتحديد أنواع الجرائم المعلوماتية وذلك لصعوبة حصر هذه الأنواع بصفة دقيقة ويرجع ذلك التطور التقني المستمر في كل يوم في جديد [٤] .

يُعد الابتزاز الالكتروني من الجرائم التقليدية في أساليبها التي من الممكن أن يرتكبها المُبتز من خلال النظام المعلوماتي عامة، بهدف حمل شخص آخر على القيام بفعل أو الامتناع عنه، سواء أكان هذا الفعل مشروعًا، أو غير مشروع، بواسطة الدخول بطريقة متعمدة إلى الحاسوب بواسطة شخص، أو موقع إلكتروني، أو بريد إلكتروني، مستخدمًا وسائل تقنيات

المعلومات المختلفة، ومنها الهواتف النقالة المزودة بالكاميرا، حيث إن الابتزاز هو ممارسة المبتز، الضحية مستخدمًا أسلوبًا من أساليب الضغط والإكراه بهدف التعدي على حياته الخاصة والمساس بها عن طريق التشهير فيما يخصه من معلومات، كصورة شخصية، أو بياناته، وبيانات عائلته [٥].

نَجد هنالك من عرف الابتزاز الإلكتروني بأنه الوعيد بالنشر أو زرع الخوف في النفس وذلك بالضغط على إرادة الإنسان من أنّ ضررًا ما سيلقاه أو سيلحق أشخاصًا أو أشياء له به صلة، أو هو ذلك الفعل الذي يقوم به شخص بإنذار آخر بخطر يريد إيقاعه بشخصيه أو ماله أو بشخص أو مال غيره وهذا الإنذار سواء كان شفاهية أو كتابة لا فرق بينهما وكذلك بأي عبارة من شأنها إلقاء الرعب في نفس المجني عليه أو مجرد إزعاجه أو تخويفه من خطرٍ قد يلحق بنفسه أو ماله [٦].

في الحقيقة تختلف وسائل الابتزاز الإلكتروني باختلاف الوضع العام لكل مبتز وضحية، حيث تعددت هذي الوسائل بتعدد طرق وأساليب الاتصالات الحديثة، حيث تعد الطرق والوسائل مجالًا خصبًا حتى يمارس الجناة مبتغاهم ويحققوا أهدافهم، وقد حدد المشرع الاماراتي على سبيل الحصر حيث نجد المادة ٩ من قانون مكافحة جرائم تقنية المعلومات، تحدد هذي الوسائل وذلك عن طريق أستعمال مواقع الإنترنت أو احدى وسائل تقنيات المعلومات، وهو الحال عند المشرع السعودي .[٧]

كذلك عُرف الابتزاز الالكتروني بأنه الحصول على وثائق وصور ومعلومات عن الضحية من خلال الوسائل الإلكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة بالضحية باستخدام الوسائل الإلكترونية لتحقيق أغراض يستهدفها المُبتز [٨].

من الواضح إن من بين الجرائم المعلوماتية التي تفاقم خطرها بشكل ملحوظ في الوقت القريب، جريمة الابتزاز الذي يتعرض له أحد الأشخاص من قبل شخص آخر أو فئة معينة، إذ تتعدد أنماط الابتزاز وصوره فمنها ما يكون ابتزاز الرجال للنساء أو العكس ولو كان قليلًا، ومنها ابتزاز بعض الأشخاص الذين يقومون باختراق أجهزة الحاسوب العائدة لأشخاص آخرين، وقد يكون بشكل ابتزاز بعض الموظفين للمراجعين لإرغامهم على دفع مبالغ مالية

مقابل تسهيل معاملاتهم وغيرها الكثير، فجريمة الابتزاز الإلكتروني أصبحت من الجرائم المصنفة عَالَمِيًا ضمن الجرائم الجنائية وقد تصل أقصى عقوبة لها في القوانين الدولية إلى ٢٠ عامًا حسب وجهة نظر مشرع كُلِّ دولة، وأصبح ضحايا الابتزاز الإلكتروني في العالم ١٥٠ مليون حالة ابتزاز للنساء، فجريمة الابتزاز الإلكتروني هي –كما أسلفنا– أحد صور الجريمة المعلوماتية، وغالبًا ما تقع النساء ضحية لمثل هذا النوع من الجرائم[٩] .

من الجدير بالذكر إن المشرع الإماراتي قد تناول موضوع الابتزاز الإلكتروني "يعاقب بالحبس مدة لا تزيد عن سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كُلّ من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.[١٠] "

فمن خلال ذلك يمكن لنا تعريف الابتزاز الإلكتروني بأنه عملية استغلال الأشخاص بواسطة الشبكة المعلوماتية أو الوسائل الإلكترونية، لإجبارهم على القيام بعمل أو الامتناع عنه.

المطلب الثاني: خصائص جريمة الابتزاز الإلكتروني

الطبيعة الخاصة التي اتصفت بها جريمة الابتزاز الإلكتروني جعلتها تتميز عن الجرائم التقليدية بعدد من السمات فمنها ما هو متعلق بالجريمة والآخر متعلق بشخصية مرتكبها.

في البدء من أبرز السمات التي تتصف بها الجريمة المعلوماتية هي أنها تُعد جرائم صعبة الاثبات، حيث يصعب في الكثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية؛ يعود السبب في ذلك إلى استخدام الجاني وسائل فنية وتِقنية معقدة في كثيرٍ من الاوقاتِ كما يتصف السلوك المكون للركنِ المادي فيها بعمل سريع قد لا يستغرق أكثر من بضعِ ثوان علاوة على سُهولةِ محو الدليل والتلاعب به في الوقتِ الذي تفتقر فيه هذه الجرائم إلى الدليلِ المادي التقليدي، لذا فهذه الجرائم في طبيعة الحال لا تترك اثرًا لها بَعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها أن وجدت [١١].

والجدير بالذكر أن من السمات التي تتصف بها الجريمة المعلوماتية بأنها جريمة عابرة للحدود وعابرة للدول والقارات، حيث تكون غير خاضعة لنطاق إقليمي محدد، حيث إن عالم المعلومات تختفي فيه الحدود الجغرافية بين الدول؛ لارتباط العالم بشبكة معلوماتية واحدة، حيث أن اغلب الجرائم المرتكبة من خلال الشبكة العالمية يكون فيها الجاني في دولة ما والمجني عليه في دولة أو مكان اخر، وقد يكون الضرر المترتب عن الجريمة غير واقعًا داخل إقليم دولة الجاني(١٢).

ولعل من المناسب أن نشير للتساؤل الذي يثار، ما مكانة الجريمة المعلوماتية من الجريمة الدولية والجريمة العالمية؟

وفي مجال الإجابة عن هذا التساؤل نجد من المناسب توضيح لمفهوم الجريمة الداخلية والدولية والعالمية، ثم بعد ذلك بيان إلى أي منهم تنسب الجريمة المعلوماتية، في بداية القول يخضع تعريف الجريمة الداخلية للمفهوم المجرد للجريمة بصفة عامة وهو الفكرة العامة الأساس التي يقوم عليها بغض النظر عن أيَ وصفٍ يلحق بها، وهذه الفكرة العامة الأساس هي أن الجريمة فعل معاقب عليه في القانون لما لهذا الفعل من اعتداء على مصلحة مشمولة بالحماية القانونية، ويتكفل بالنص عليها بالقانون الداخلي أو القوانين المكملة له، كما أنها ترتكب باسم المتهم ولحسابه الخاص، ولا يقبل من المتهم الدفع بالجهل بالقانون وأن جاز له الدفع بالغلط في الوقائع، في حين الجريمة الدولية نجد من يعرفها بأنها عدوان على مصلحة يحميها القانون الدولي الجنائي وذلك باتفاق المجتمع الدولي على كونِ مجموعة من الأفعال تشكل جرائم، ويُعد مصدر النص على صفتها غير المشروعة هو العُرف الدولي، في حين أن الجريمة العالمية فهي تلك التي ينظمها ما يمكن أن يسمى بقانون العقوبات العالمي وتتمثل في التصرفات المنافية للأخلاق والمنطوية على عدوان للقيم البشرية الأساس في العالم المتمدين، ويشترك في النص عليه القوانين الجنائية الداخلية كافة، ولبيان مكانة الجريمة المعلوماتية من الجريمة الدولية والجريمة العالمية هو أنها مزيج من كل منهما، إلّا أنه يغلب عليها الطابع العالمي العابر للحدود ويترتب على هذا الطابع العلمي عدة نتائج أهمها ضعف فرص اكتشاف الجريمة المعلوماتية ومحاكمة مرتكبها، وصعوبة

إقامة الدعوى على تلك الجرائم في ظل القوانين الحالية إذ تصطدم بمبدأ سيادة الدولة على إقليمها [١٣].

ونجد في ذلك أن الجريمة المعلوماتية لا تَعترف بالحدود المكانية ولا الزمانية حيث إنها جريمة غير محدد ولا تلتزم بموقع جغرافي محدد؛ وهو ما يميزها عن الجرائم التقليدية، وفي ذلك تُعد الجريمة المعلوماتية نوعًا جديدًا من الجرائمِ التي ظهرت مع المواكبة العالمية للتطور الحديث للتقدم العلمي في مجال التِقنية، وهذه السمة التي تتصف بها الجريمة المعلوماتية ما هي إلا دليلًا على أهمية هذه الجريمة ويجب رفد المشرع لها مجموعة من القوانين التي تحد من استخدامها في سبيل الإضرار بالغير.

ومن بين السمات التي لا بُد من التطرق إليها والتي تتميز بها هذه الجريمة هو انها جريمة ناعمة، إذ إن هذه الجريمة لا وجود للعنف فيها على عكسِ الجرائم التقليدية مثل جريمة الإرهاب والسرقة والسطو المسلح وغيرها من الجرائمِ، لكن الجريمة المعلوماتية هي جريمة ناعمة لا تتطلب عنفًا في الأساسِ، فإن نقل البيانات من حاسوب لآخر أو السطو الإلكتروني على أرصدةِ بنك مُعين لا يتطلب من الجاني استخدام العنف ولا تبادل لإطلاق النار مع رجال الأمن [١٤].

وفي ضوء ذلك نجد أن الجريمة المعلوماتية جريمة ناعمة وهادئة في ذات الوقت، فعدم وجود العنف فيها من السمات التي تتصف بها هذه الجريمة، ومن خلال ذلك فلا نجد السلاح في حالة السرقة ولا وجود له في أي استعمال أخر، فاستخدام المعلومات هو المرتكز الأساس الذي تستند عليه هذه الجريمة.

ولعل من المناسب أن ذكر الخصيصة الثالثة التي تتصف بها الجريمة المعلوماتية هو صعوبة إثباتها، حيث تتميز الجرائم المعلوماتية عن الجرائم التقليدية بأنها صعبة الإثبات؛ وهذا راجع إلى الافتقار لوجود الآثار التقليدية للجريمة، وعدم وجود الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل، أو تدميره في زمن قصير جدًا، وفي ذات السياق نضيف لذلك نقص الخبرة لدى الشرطة والنظام العدلي وعدم كفاية القوانين النافذة [١٥].

الجدير بالذكر أن ومن السمات التي تتميز بها الجريمة المعلوماتية هو أن ارتكابها يتم في بيئة الحاسوب والشبكة العالمية، ومحلها يكون المعلومات المخزنة على الحاسوب وشبكاته، كما أنها قد ترتكب في إحدى مراحل تشغيل نظام المعالجة الآلية للمعلومات سواء في مرحلة الإدخال أو المعالجة أو الإخراج [١٦].

ونستنتج من بعد ذلك كله ومن بين أسطر البحث أن الجريمة المعلوماتية لا يمكن أن تكتمل ولا نتصور وجودها دون وجود بيئة معلوماتية خاصة في ارتكابها، كجهاز الحاسوب والشبكة الدولية، وتستهدف من خلالها البيانات المعالجة آليًا في الحاسوب.

المبحث الثاني: صعوبات مكافحة جريمة الابتزاز الإلكتروني

أن الجريمة بصورة عامة وجريمة الابتزاز الإلكتروني خاصة تعاني الكثير من الصعوبات فمنها تشريعي وصعوبات أخرى إجرائية، فمن خلال ذلك سنقسم هذا المبحث لمبحثين نذكر في الأول الصعوبات التشريعية لهذه الجريمة في حين سنخص المطلب الثاني بالصعوبات الإجرائية التي تواكب هذه الجريمة.

المطلب الأول: الصعوبات التشريعية

إن من أبرز الصعوبات التي ظهرت مع تطور هذا النوع من الجرائم هو عدم وجود تشريعات تكافح هذا النوع من الجرائم من خلال نصوصٍ عقابيةٍ، ومما يتأسف له ولغاية هذه اللحظة عدم وجود قانون خاص يكافح هذه الجريمة في التشريع العراقي، مما جعل هنالك صعوبة كبيرة في مواجهة هذه الجريمة.

في ظل تلك المؤشرات كان من الضروري أن تعنى الدول بإصدار تشريعات تهدف إلى حماية الحياة الخاصة ضد أي انتهاكات محتملة، ومن بينها إساءة استخدام تقنية المعلومات والاتصالات.[١٧]

يُعد الابتزاز الإلكتروني أحد المخاطر الكبيرة التي تواجه مستخدمي الشبكة العالمية والأجهزة الذكية ممن لا يملكون أي معرفة عن أمن المعلومات، فقد يؤدي الابتزاز الإلكتروني إلى حدوث مشاكل توثر على الوضع النفسي للشخص الذي يُبتز، ومع التطور التِقني المتسارع لغالبية الدول أصبح بإمكان أي شخصٍ وهو جالس في منزليه الحصول على ما يريد، فبضغطة

الزر الواحدة يمكننا تصفح مئات المواقع وآلاف المتاجر الإلكترونية وغيرها العديد من مواقع التواصل الاجتماعي الذي بات يستخدمها الصغير والكبير، ومن هنا بدأت مشاكل الشبكة العالمية تزداد وذلك بسبب استغلال بعض العصابات الإلكترونية هذه الحسابات وابتزاز أصحابها بهدف جمع الأموال [١٨]، بالإضافة إلى ضعف الوعي والاستغلال الذي تتولد منه هذه الجريمة نجد الضعف الحقيقي في مواجهتها هو عدم وجود قوانين عقابية رادعة لفاعليها.

وحسنًا فعلت التشريعات المقارنة في رفد القضاء بنصوص عقابية لمكافحة والحد من هذا النوع من الجرائم، فمثلا نجد أن المرسوم السلطاني لعام ٢٠١١ في عمان والخاص بمكافحة جرائم تقنية المعلومات قد عالج هذا النوع فعاقب عليها بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات بالإضافة للغرامة [١٩].

وكما نجد عقوبة هذه الجريمة في القانون الاماراتي الخاص بمكافحة جرائم تقنية المعلومات، بأنها الحبس لمدة لا تزيد على سنتين والغرامة أو بإحدى هاتين العقوبتين، وقد شدد المشرع الاماراتي العقوبة في حالة كون التهديد بإسناد أمور خادشة للشرف أو الاعتبار .[٢٠]

في حين إن التشريع العراقي يخلو من قانونٍ يكافح الجريمة المعلوماتية بصورة عامة وجريمة الابتزاز الإلكتروني بصورة خاصة، إلّا إننا نجد أن نص المادة ٤٥٢ من قانون العقوبات العراقي رقم ١١١ لعام ١٩٦٩ قد عالج جريمة الابتزاز المالي [٢١].

واستخلاصًا لما سلف خلو التشريع العراقي من نصٍ صريح يعالج جريمة الابتزاز الإلكتروني، وانما تُرك الموضوع ليعالج حسب القواعد العامة.

وفي هذا المقام نجد حادثة من الحوادث الغريبة والدخيلة على المجتمع حيث حكم على شخص قام بابتزاز زوجته مهددًا بنشر صورها عبر الفيسبوك، حيث عُقب وفق المادة ٣٤٠ من قانون العقوبات العراقي .

تُعد جريمة الابتزاز الإلكتروني من الجرائم ذات الأنواع والصور المختلفة بالنسبة للمجني عليه والهدف والدافع من الجريمة فقد يستهدف الأشخاص المعنوية كالشركات أو المؤسسات وقد يستهدف الأحداث من الأطفال وذلك عن طريق استغلالهم وتهديدهم بنشر

صور أو تسجيل مرئي أو محادثات على مواقع الدردشة أو أي مادة أخرى حيث يستغل الجاني صغر السن وقلة الخبرة لدى الأحداث وقد يكون المستهدف من النساء حيث يُعد أكثر أنواع الابتزاز الإلكتروني شهرة وانتشارًا عن طريق الابتزاز بنشر صور فاضحة أو محادثات خادشة للحياء كما قد يكون المستهدف من الرجال عن طريق استغلال وسائل الاتصال في الحصول على صور أو مقاطع فيديو ومن ثم التهديد بنشرها إذا ما كان نشرها يؤدي إلى تشويه سمعه أو المساس بالشرف حيث تكون دوافع الابتزاز إما دوافع مادية أو دوافع أخلاقية أو دوافع عاطفية وجريمة الابتزاز الإلكتروني تُعد من الجرائم الخطيرة التي تشكل تهديد على أمن المجتمع بالإضافة إلى تأثيرها على الجوانب الاجتماعية، حيث تؤدي إلى التفكك الأسري وحدوث المشكلات التي تؤدي إلى وقوع الطلاق وفقدان الثقة بالإضافة إلى الآثار النفسية (القلق، الخوف، الاكتئاب)، كما تتميز هذه الجريمة بصعوبة إثباتها لأنها من الجرائم الحديثة وإن الفاعل فيها يستخدم التِقنية الحديثة في ارتكاب جريمته ولا بُدِّ أن يصار إلى تشديد العقوبة على هذه الجرائم وإصدار تشريع خاص بها وعدم الاكتفاء بالعقوبة المنصوص عليها في قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ والتأكيد على تطوير أساليب البحث عن الجناة لخطورة هذه الجريمة على عموم المجتمع[٢٢] .

ولتوضيح ذلك نشير في هذا الخصوص لحكم محكمة جنايات واسط الهيئة الأولى حيث حكمت بالسجن ٢١ عام بواقع السجن سبع سنوات عن ثلاث قضايا بحق مُدان عن جريمة الابتزاز الإلكتروني، وهذه الاحكام استنادًا لأحكام المادة ٤٣٠ من قانون العقوبات العراقي رقم ١١١ لعام ١٩٦٩ [٢٣].

في حالة أخرى، كان من الحري بنا ذكر الطعن الخاص بجريمة الابتزاز الإلكتروني والصادر من محكمة النقض المصرية في أحد الطعون المقدمة لها، بخصوص شخص قام بابتزاز مجموعة من النساء في سبيل الحصول على ما يريده من أموال أو ممارسات جنسية عبر الشبكة العالمية، وقد استخدم في فعله الجرمي هذا موقعين على الشبكة العالمية أحدهما باسم مستعار وهمي وآخر باسمه الحقيقي.[٢٤]

المطلب الثاني: الصعوبات الإجرائية

حين التطرق لموضوع الجرائم المعلوماتية نجد إن هنالك صعوبة تكمن في خصائصها ألا وهي الصعوبات التي ترافق الكشف عنها والتفتيش والتحقيق.

لقد اثارت الجرائم المعلوماتية عمومًا، مسألة كفاية قواعد الإجراءات الجزائية الخاصة بملاحقة الجريمة ومحاكمة مرتكبيها واثبات ارتكابهم للجريمة، حيث عكست طبيعة الجرائم المعلوماتية ووسائل ارتكابها الحاجة إلى قواعد إجرائية خاصة، في مجال هذه المسائل المرتبطة بذلك في نطاق الإجراءات والاثبات مثل الأساليب الفنية لارتكاب الجرائم المعلوماتية، وارتكابها من قبل جناة من خارج الحدود الوطنية غالبًا، ووجود مرتكب الجريمة في نطاق الشبكة المعلوماتية تحت اسم مستعار أو وهمي، وبصورة غير صورته الحقيقية، ووقوع الجريمة على معطيات الحاسوب التي ليس لها طبيعة مادية ملموسة، ومشكلات الاختصاص القضائي وتنازع القوانين بالنظر لتعدد امكنة وجود أنظمة المعلومات سواء المستخدمة في ارتكاب الجريمة، أو تلك التي يستهدف محتواها في النشاط الجرمي [٢٥] .

في واقع الأمر إن تجريم الجرائم المعلوماتية وحده لا يكفي، يصدمنا بعقبات منها كيفية إثبات تلك الجرائم ومسائل قضائية مثل كيفية البحث عن الأدلة ذات الصلة وضبطها، وسيطعن على هذا النوع من الأدلة في المحكمة وأي خطأ أو خلل فني قد ينتج عنه تدمير قوة هذه الأدلة، بالإضافة إلى ذلك هنالك مسألة ما إذا كان ينبغي تمكين القائمين على تنفيذ القانون من اختراق أنظمة الحاسوب من أجل ملاحقة أحد المجرمين، حيث يشاهد المتتبع لأحوال الجريمة والطريقة التي ترتكب بها يجدها أنها تسير جنبًا إلى جنبٍ مع التطور الحضارة الإنسانية وارتقائها، حيث إنه مع مرور الوقت تقدمت طرق ارتكاب الجريمة، وأصبح المجرمون يرتكبون الجرائم باحترافية كبيرة، وهذا ما يساعدهم على إخفاء كُلّ الدلائل والآثار التي توصل إليهم، وكذلك الإفلات من العقاب، وعليه من اللازم على الأجهزة الأمنية إيجاد جهاز فني متخصص تسند له هذه المهمة ورفده بمختلف الإمكانيات والوسائل الحديثة التي تمكن من القيام بالعمل على أكمل وجه، وأيضًا لمواكبة التطور الكبير الحاصل في طرق ارتكاب الجرائم [٢٦]، ومن

الممكن للمجرم الحديث أن يسرق بواسطة الحاسوب أكثر مما عليه حين استخدامه للسلاح (٢٧).

وفي ظل تلك الظروف فأنه يتطلب لمواجهة الجرائم المعلوماتية وجريمة الابتزاز بصورة خاصة، التحقيق الفعال وكذلك القدرة على جمع الأدلة والإثبات الجنائي، هذا النهج يتطلب بداية تحديد نموذج حقيقي أمثل، وكذلك الاستجابة للتحديات القانونية التي تعيق تنفيذ القانون وصولًا للتحقيق في الجريمة وإثباتها، يعود تاريخ التحقيق الإلكتروني إلى منتصف الثمانينيات من القرن الماضي كردِ فعلٍ على تسارع انتشار الجرائم المعلوماتية، وقد شهد التحقيق الإلكتروني تطورًا لافتًا في الآونة الأخيرة، حيث يمر التحقيق الجنائي الإلكتروني بمرحلتين أساسيتين فالمرحلة الأولى تتمثل بالإجراءات التي يتم تنفيذها في مسرح الجريمة وتشمل إغلاق أو تجميد مسرح الجريمة لمنع فقدان أو تلف أو تلوث الأدلة، والحفاظ على مسرح الجريمة وتأمينه ومنع العبث به، والمرحلة الثانية تتمثل في الإجراءات التالية التي ينبغي على فريق مسرح الجريمة من مأموري الضبط القضائي (٢٨).

وتأسيسًا لذلك فإن التفتيش الإلكتروني يُعد من أهم وأخطر إجراءات التحقيق المقررة في الجرائم المعلوماتية بصورة عامة وجريمة الابتزاز بشكل خاص، وذلك لمساسه بالحريات الخاصة المكفولة دُستوريًا، وكذا خطورة ما قد يسفر عنه من أدلة تؤدي لكشف الحقيقة عن الجريمة التي وقعت باستخدام إحدى أنظمة المعلوماتية، والتفتيش الإلكتروني كما عُرف بأنه الاطلاع على محلٍ منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون المحل جهاز الحاسوب أو أنظمة أو الشبكة العالمية، وكذلك عرف من جانب المجلس الأوربي بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بصورة إلكترونية.(٢٩)

ونؤيد الرأي أعلاه بإمكانية التفتيش الإلكتروني المساس بالحريات العامة التي كفلها الدستور لهذا لا بُدَ من ان يرفد المشرع نصوصًا خاصة لحمياتها وعدم المساس بها، وبهذا فإنه لا يمكن التجاوز على هذه الحريات لو أُصدر قانون لتنظيم هذا التفتيش بشكل يتلاءم مع القواعد الدستورية.

ونجد هنالك من عرف هذا التفتيش بأنه البحث عن الأدلة الجُرمية في أجهزة الحاسوب التي استخدمت في ارتكاب الجريمة أو من خلال شبكات الاتصال مثل الشبكة العالمية، ويُنفذ هذا التفتيش بقيام السلطات بالدخول إلى النظام الحاسوبي الذي ارتكبت فيه أو من خلاله الجريمة، وذلك لبحث وفحص البيانات الموجودة فيه [٣٠].

ولعل من المناسب ان نشير إلى مضامين القواعد الشكلية لتفتيش الحاسوب، حيث تتضمن هذه القواعد مجموعة من الشروط: [٣١]

١- إن يتم التفتيش بأسلوب إلكتروني من قِبل الأجهزة القائمة بالتفتيش، وبصورة سريعة.

٢- مراعاة إبعاد المشتبه فيهم والعاملين على أجهزة الحاسوب عن المكان ومن ثم تفتيش الأجهزة والمعطيات المخزنة فيه.

٣- معرفة رقم الاتصال الذي تم منه مسرح الجريمة ونقل المعطيات والمعلومات على نسخ احتياطية.

٤- إن التفتيش عن الأدلة في الجرائم المعلوماتية يتطلب مهارة فنية معينة يجب أن تتوفر في المحقق وأيضًا يجب أن يمتاز بها حتى يتمكن من العمل بسرعة من أجل الحفاظ على الأدلة من الإتلاف أو الشطب أو التعديل وذلك لسرعة تغيير الأدلة الرقمية.

لا شك إن الحث في المكونات المادية للحاسوب بحثًا عن شيءٍ ما يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية متوقف على طبيعة المكان الموجودة فيها تلك المكونات وهل هي من الأماكن العامة أو الخاصة [٣٢].

وعلى خلاف المكونات المادية تجدر الإشارة إلى الخلاف الفقهي في مدى صلاحية المكونات المعنوية لان تكون مَحَلًا للتفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها تفتقر إلى المظهر المادي المحسوس في المحيط الخارجي مما يجعلها تتعارض مع الهدف الذي يصبو إليه التفتيش وهو البحث عن الأدلة المادية، فبهذا الخصوص ذهب اتجاه فقهي لصلاحية هذه المكونات لأن تكون مَحَلًا للتفتيش كونها تتناسب مع الهدف من التفتيش وهو ضبط الأدلة

المادية التي تفيد في الكشف عن الحقيقة في الجرائم المعلوماتية، وحجتهم في ذلك هو أنه إن كانت نظم برامج الحاسوب عبارة عن بصمات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية إلّا أنها قابلة للتسجيل والتخزين والتحميل على وسائط ودعائم مادية معينة، ولها سلوك مادي محسوس، وبالتالي يمكن إخضاعها لقواعد التفتيش التقليدي(٣٣) .

وعلى النقيض من الرأي السابق يذهب رأي آخر إلى أن المفهوم المادي لا ينطبق على بيانات الحاسوب غير المحسوسة أو الملموسة، ويقترح أصحاب هذا الاتجاه مواجهة هذا القصور التشريعي بإضافة عبارة إلى القوانين ذات العلاقة إلى مذكرات التفتيش، مثل المواد المعالجة عن طريق الحاسوب أو البيانات الحاسوب، لذلك تُعد البيانات والمعلومات المخزنة في الحاسوب تصلح لأن تكون محلًا للتفيش، ويمكن ضبطها أو استنساخها على الورق أو على أي دعامة أخرى كالفلاش ميموري؛ بحيث يمكن الاستناد إليها كالدليل على ارتكاب المتهم للجريمة في مرحلة المحاكمة، لذلك ينبغي الإشارة في قوانين الإجراءات الجنائية على حرية تفتيش المكونات المادية والمعنوية لأجهزة الحاسوب (٣٤).

من خلال ذلك لست مترددًا من الانحياز للرأي الثاني مع الاضافة في صلاحية المكونات المعنوية للتفتيش كونها تمثل محالّ جديدة غير موجودة سابقًا وغير متعارف عليها في التفتيش المادي، وهذه المحالّ تحتاج لخبرة في آلية التعامل معها، خوفًا من تدميرها أو إتلافها عن طريق الخطأ أو سوء التعامل.

ولعل من المناسب أن نشير إلى أنه من المتصور وبشكل كبير أن يقوم مرتكبو الجريمة بتخزين بياناتهم في أنظمة تقنية المعلومات وتكون هذه الأنظمة في الغالب خارج الدولة عن طريق شبكات الاتصالات بهدف عرقلة سلطات الادعاء من جمع الأدلة، ولمواجهة هذا الاحتمال نص قانون جريمة الحاسوب في هولندا أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأماكن وبما ينطوي عليه تفتيش نظم الحاسوب المرتبطة حتى إذا كانت موجودة في دولة أخرى شريطة أن يكون هذا التدخل مؤقتًا وأن تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة، ووفقًا لما جاء بتقرير المجلس الأوربي فإن هذا الاختراق المباشر يُعد انتهاكًا لسيادة الدولة ما لم تجد اتفاقية دولية في هذا الشأن ويؤيد الفقه الألماني ما جاء بهذا التقرير، حيث إن

السماح باسترجاع البيانات التي تم تخزينها بالخارج يُعد انتهاكًا لحقوق السيادة وخرقًا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائية، فلا مناص من التعاون الدولي في المجال بمقتضى اتفاقية ثنائية أو متعددة الأطراف، أو من خلال الحصول على إذن الدولة التي يتم التفتيش في مجال اقليمها [٣٥].

في قبالة هذا التقدم المتسارع في التِقنية بات ارتكاب الجرائم من دولة لأخرى من السهولة بمكان، ولهذا أصبح من الضروري البحث عن مشروعية القيام بالتفتيش والضبط القضائي لمتهم في دولة أخرى . [٣٦]

فمن خلال ما تقدم نجد إن الصعوبات الإجرائية التي تواجه السلطات المختصة في الدولة تحتاج للكثير من الأدوات والإمكانيات التي تساعدهم في سبيل مكافحة هذه الجريمة، التي تمس بصورة كبيرة المجتمع بكل أركانه.

الخاتمة

في الختام وبعد هذا العرض، تبين لنا ما لهذه الجريمة من ضرر على المجتمع من خلال استخدام المجرم أساليب غير تقليدية في سبيل تهديد وارعاب المجني عليه، وكذلك القصور التشريع في معالجة هذه الجريمة جعلها أكثر صعوبة لما تتصف بها من خصوصية، ولهذا سيورد الباحث أهم النتائج التي توصل إليها خلال الدراسة، وأيضًا السعي في ذكر مجموعة من التوصيات التي تُكَوِّن إجابة لتساؤل الدراسة الرئيس.

النتائج:

١- عدم وجود نص صريح لمعالجة جريمة الابتزاز الإلكتروني في التشريع العراقي.

٢- قصور القواعد العامة في معالجة ظاهرة الابتزاز الإلكتروني.

٣- جريمة الابتزاز الإلكتروني تمتاز بأنها عابرة للحدود، وكذلك بأنها جرائم صعبة الإثبات.

التوصيات:

١- لا بد للمشرع العراقي في الإسراع بتشريع قانون لمكافحة الجريمة المعلوماتية.

٢- إنشاء محكمة متخصصة في دعاوى الجريمة المعلوماتية، ويكون التعامل فيها إلكترونيًا من رفع الدعوى لحين النطق بالحكم.

٣- إنشاء هيئة عامة مستقلة للحفاظ على الأمن السيبراني للدولة.

٤- تهيئة متخصصين للتفتيش والتحقيق الإلكتروني ونقترح أن يسمى بشرطة مكافحة جرائم الحاسوب

الهوامش

(١) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، الإسكندرية، ٢٠١٩، ص ٥.
(٢) د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مرجع سابق، ص ١١.
(٣) إبراهيم بن احمد زمزمي، الجرائم المعلوماتية دراسة وفق نظام مكافحة جرائم المعلوماتية السعودي، المنتدى السنوي للمحامين، مجموعة الابداع الاداري، السعودية، ٢٠١٩، ص ١٤٣.
(٤) د. شريف حسين محمد، الجريمة الإلكترونية معرفة وتقويض الجوانب الخطرة من التكنولوجيا، الاقتصاد والتجارة، العدد ٦٦٤، مصر، نادي التجارة، ٢٠١٧، ص ١٨.
(٥) د. ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الامنية، المجلد ٣٣، العدد ٧٠، الرياض، ص ١٩٤.
(٦) أفراح بنت خميس بن عامر اللويهية، مشكلة الابتزاز الإلكتروني لدى طلبة مرحلة التعليم ما بعد الأساسي ودور الخدمة الاجتماعية في المجال المدرسي في التعامل معها، رسالة ماجستير، كلية الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، عمان، ٢٠١٨، ص ٦.
(٧) د. اميل جبار عاشور، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في مواقع التواصل الاجتماعي دراسة مقارنة، مجلة أبحاث ميسان، المجلد ١٦، العدد ٣١، جامعة ميسان، ٢٠٢٠، ص ١١٨.
(٨) أفراح بنت خميس بن عامر اللويهية، مرجع سابق، ص ٢١.
(٩) هديل سعد احمد العبادي، جريمة الابتزاز الالكتروني للنساء، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد العاشر، العدد ٢، جامعة الانبار، كلية القانون والعلوم السياسية، ٢٠٢٠، ص ٥٣٥.
(١٠) المرسوم بقانون اتحادي الامارات رقم ٥ لسنة ٢٠١٢، مادة ١٦.
(١١) محمد بن احمد بن علي المقصودي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيًا: التكامل الدولي المطلوب لمكافحتها، المؤتمر الدولي لمكافحة الجرائم المعلوماتية- ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية، الرياض، ٢٠١٥، ص ٢٧.
(١٢) د. محمود فتوح سعدات، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية- ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية، الرياض، ٢٠١٥، ص ٤٢.
(١٣) د. محمود فتوح سعدات، مرجع سابق، ص ٤٢.
(١٤) د. كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة، مصر، الإسكندرية، ٢٠١٨، ص ٤٣.
(١٥) عبد الله ن محمد اليوسف، الجرائم المعلوماتية والدليل الجنائي مسميات وخصائص وابعاد اجتماعية وأمنية وصحية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية- ICACC، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية، الرياض، ٢٠١٥، ص ٩٧.
(١٦) د. كمال عبد السميع شاهين، مرجع سابق، ص ٤١.
(١٧) سارة محمد حنش، المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الاردن، ٢٠٢٠، ص ٤٥.

[١٨] عبير نجم عبد الله الخالدي، دور الوعي الاجتماعي في مواجهة الابتزاز الالكتروني للمرأة، المؤتمر العلمي الدولي الثاني، نقابة الأكاديميين العراقين/ مركز التطور الأكاديمي وجامعة صلاح الدين، كلية التربية الاساس، اربيل، ١٠-١١- شباط، ٢٠٢٠، ص ٢٠٥٣.

[١٩] المادة ١٨ من قانون مكافحة جرائم تقنية المعلومات العماني رقم ٢٠١١/١٢ "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثالثة آلاف ريال عماني أو بإحدى هاتني العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في تهديد شخص أو ابتزازه لحمله على القيام بفعل أو امتناع ولو كان هذا الفعل أو الامتناع عنه مشروعًا، وتكون العقوبة السجن المؤقت مدة ال تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثالثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا كان التهديد بارتكاب جناية أو بإسناد أمور خملة بالشرف أو الاعتبار" .

[٢٠] المادة ١٦ قانون ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات "يعاقب 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 جناية أو بإسناد أمور خادشة للشرف أو الاعتبار..

[٢١] المادة ٤٥٢ "١- يعاقب بالسجن مدة لا تزيد على سبع سنين أو بالحبس من حمل آخر بطريق التهديد على تسليم نقود أو أشياء أخرى غير ما ذكر في المادة السابقة.

٢- وتكون العقوبة مدة لا تزيد على عشر سنين إذا ارتكب الجريمة بالقوة والإكراه.

[٢٢] القاضي كاظم عبد جاسم الزيدي، جريمة الابتزاز الالكتروني، على الموقع الالكتروني https://www.hjc.iq/view.4915/، تاريخ النشر ٢٠١٨/١٢/١٨، تاريخ الزيارة ٢٠٢١/١/٢.

[٢٣] على موقع مجلس القضاء الاعلى، https://www.hjc.iq/view.5904/، تاريخ النشر ٢٠١٩/٩/٢، تاريخ الزيارة ٢٠٢١/١/٢.

[٢٤] جلسة ١٧ أكتوبر، ٢٠١١، الطعن رقم ٣٩٨١، سنة ٨٠ القضائية.

[٢٥] مصطفى خالد الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، رسالة ماجستير، عمادة الدراسات العليا، جامعة اهل البيت، الاردن، ٢٠١٩، ص ٣٢.

[٢٦] حسين عباس حميد، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2020، ص 83.

[27] John w. Rittinghouse and willam M. Hancocl, cybersecurity operation handbook,elsevier digital press, 2003, p. 309.

[٢٨] مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية اثباتها في فلسطين دراسة مقارنة، دراسات- علوم الشريعة والقانون، مجلد ٤٥ ملحق، الجامعة الأردنية، عمادة البحث العلمي، ٢٠١٨، ص ٢٨٦.

[٢٩] د. فاطمة الزهراء عربوز، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العدد ٣٤، ٢٠١٩، ص ١٠٥.

[٣٠] د. عبد الغني جاد المولى، دور الدليل الإلكتروني في الاثبات الجنائي، دار الفكر الجامعي، الإسكندرية، ٢٠١٩، ص ١١٧.

[٣١] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية، والاختصاص القضائي بها دراسة مقارنة للتشريعات العربية والأجنبية، مكتبة الوفاء القانونية، مكتبة الإسكندرية، ٢٠١٦، ص ٣٠٤.

[٣٢] د. أسامة فرج الله محمود الصباغ، الحماية الجنائية للمصنفات الالكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦، ص ٢٤٥.

[٣٣] د. فاطمة الزهراء عربوز، مرجع سابق، ص ١٠٧-١٠٨.

(٣٤) د. أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الامنية والتدريب، المجلد ٢٩، العدد ٥٨، جامعة نايف العربية للعلوم الأمنية، ٢٠١٣، ص ٩٠.
(٣٥) حسين عباس حميد، مرجع سابق، ٩١.
(٣٦) د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠١٨، ص٢٣٤.

المصادر والمراجع

القوانين والأحكام:

١- المرسوم بقانون اتحادي الامارات رقم ٥ لسنة ٢٠١٢.
٢- طعن رقم ٣٩٨١، سنة ٨٠ القضائية، محكمة النقض المصرية.
٣- قانون ٥ لسنة ٢٠١٢ الإماراتي بشأن مكافحة جرائم تقنية المعلومات.
٤- قانون العقوبات العراقي.
٥- قانون مكافحة جرائم تقنية المعلومات العماني رقم ٢٠١١/١٢.
٦- قانون مكافحة جرائم تقنية المعلومات العماني رقم ٢٠١١/١٢.

الكتب العربية:

١- إبراهيم بن احمد زمزمي، الجرائم المعلوماتية دراسة وفق نظام مكافحة جرائم المعلوماتية السعودي، المنتدى السنوي للمحامين، مجموعة الابداع الاداري، السعودية، ٢٠١٩ .
٢- أسامة فرج الله محمود الصباغ، الحماية الجنائية للمصنفات الالكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٦.
٣- أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية، والاختصاص القضائي بها دراسة مقارنة للتشريعات العربية والأجنبية، مكتبة الوفاء القانونية، مكتبة الإسكندرية، ٢٠١٦.
٤- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، الإسكندرية، ٢٠١٩.
٥- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠١٨.
٦- شريف حسين محمد، الجريمة الإلكترونية معرفة وتقويض الجوانب الخطرة من التكنولوجيا، الاقتصاد والتجارة، العدد ٦٦٤، مصر، نادي التجارة، ٢٠١٧ .
٧- عبد الغني جاد المولى، دور الدليل الإلكتروني في الاثبات الجنائي، دار الفكر الجامعي، الإسكندرية، ٢٠١٩.
٨- كمال عبد السميع شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة، مصر، الإسكندرية، ٢٠١٨.

٩- ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الامنية، المجلد ٣٣، العدد ٧٠، الرياض.

الرسائل:

١- أفراح بنت خميس بن عامر اللويهية، مشكلة الابتزاز الإلكتروني لدى طلبة مرحلة التعليم ما بعد الأساسي ودور الخدمة الاجتماعية في المجال المدرسي في التعامل معها، رسالة ماجستير، كلية الآداب والعلوم الاجتماعية، جامعة السلطان قابوس، عمان، ٢٠١٨.

٢- حسين عباس حميد، نحو اختصاص محكمة إلكترونية خاصة بالجرائم المعلوماتية دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، ٢٠٢٠.

٣- سارة محمد حنش، المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الاردن، ٢٠٢٠.

٤- مصطفى خالد الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، رسالة ماجستير، عمادة الدراسات العليا، جامعة اهل البيت، الاردن، ٢٠١٩.

بحوث ومقالات:

١- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الامنية والتدريب، المجلد ٢٩، العدد ٥٨، جامعة نايف العربية للعلوم الأمنية، ٢٠١٣.

٢- اميل جبار عاشور، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في مواقع التواصل الاجتماعي دراسة مقارنة، مجلة أبحاث ميسان، المجلد ١٦، العدد ٣١، جامعة ميسان، ٢٠٢٠،.

٣- فاطمة الزهراء عربوز، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العدد ٣٤، ٢٠١٩.

٤- مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية اثباتها في فلسطين دراسة مقارنة، دراسات- علوم الشريعة والقانون، مجلد ٤٥ ملحق، الجامعة الأردنية، عمادة البحث العلمي، ٢٠١٨.

٥- هديل سعد احمد العبادي، جريمة الابتزاز الالكتروني للنساء، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد العاشر، العدد ٢، جامعة الانبار، كلية القانون والعلوم السياسية، ٢٠٢٠.

مؤتمرات:

١- عبد الله بن محمد اليوسف، الجرائم المعلوماتية والدليل الجنائي مسميات وخصائص وابعاد اجتماعية وأمنية وصحية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية–ICACC ، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية، الرياض، ٢٠١٥.

٢- عبير نجم عبد الله الخالدي، دور الوعي الاجتماعي في مواجهة الابتزاز الالكتروني للمرأة، المؤتمر العلمي الدولي الثاني، نقابة الأكاديميين العراقين/ مركز التطور الأكاديمي وجامعة صلاح الدين، كلية التربية الاساس، اربيل، ١٠-١١- شباط، ٢٠٢٠.

٣- محمد بن احمد بن علي المقصودي، الجرائم المعلوماتية خصائصها وكيفية مواجهتها قانونيًا: التكامل الدولي المطلوب لمكافحتها، المؤتمر الدولي لمكافحة الجرائم المعلوماتية–ICACC ، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية، الرياض، ٢٠١٥.

٤- محمود فتوح سعدات، خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية–ICACC ، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات، المملكة العربية السعودية، الرياض، ٢٠١٥.

المراجع الاجنبية:

1- John w. Rittinghouse and willam M. Hancocl, cybersecurity operation handbook,elsevier digital press, 2003.

مواقع إلكترونية:

١- القاضي كاظم عبد جاسم الزيدي، جريمة الابتزاز الالكتروني، على الموقع الالكتروني https://www.hjc.iq/view.4915/، تاريخ النشر ٢٠١٨/١٢/١٨، تاريخ الزيارة ٢٠٢١/١/٢ .

٢- على موقع مجلس القضاء الاعلى، https://www.hjc.iq/view.5904/ ، تاريخ النشر ٢٠١٩/٩/٢، تاريخ الزيارة ٢٠٢١/١/٢ .