https://doi.org/10.26682/chjuod.2023.26.1.5
مجلة جامعة دهوك، المجلد: 26، العدد: 1 (العلوم الانسانية والاجتماعية)، ص 44-56، 2023 (عدد خاص)
المؤتمر العلمي الرابع الموسوم "دور القانون والعلوم الإنسانية في حماية المرأة وتمكينها 1444 هـ - 2023م "، جامعة دهوك 6 اذار 2023

الحماية الجنائية للمرأة من ظاهرة الابتزاز الالكتروني

سلام عبد شعيبث * و نور علي السعدي**
*وزارة الداخلية ، مكتب الوزير التدريسي في كلية الفارابي الجامعة -العراق
**الامانة العامة لمجلس الوزراء -العراق

(تاريخ القبول بالنشر:*27* تموز، *2003*)

الخلاصة

يتلخص هذا البحث في تسليط الضوء على ظاهرة إجرامية خطيرة على المستوى الوطني والدولي على حد سواء، الامر الذي يتطلب اهتمام الباحثين القانونيين والاجتماعيين وغير القانونيين المهتمين بالجانب الفني والتقني لتلك الأفعال التي زاد انتشارها بشكل كبير مع زيادة استعمال الكومبيوتر وأجهزة الاتصال المختلفة وهي الحماية الجنائية للمرأة من ظاهرة الابتزاز الالكتروني، وتمثلت اهداف الدراسة في بيان المعوقات والصعوبات التي تواجه الجهود التشريعية والأمنية الموجهة للقضاء على ظاهرة الابتزاز الإلكتروني في القانون العراقي وتوضيح تلك الصعوبات التي تعرقل مواجهة تلك الظاهرة الاجرامية وايجاد الحلول القانونية لإزاحة تلك العراقيل مع تفعيل التشريعات المكافحة والواقية من أثار جريمة الابتزاز الإلكتروني وتنفيذها حتى تؤتي ثمَّارها، ولوجود فراغ تشريعي في القوانين محل الدراسة من ناحية الابتزاز الالكتروني بصورة خاصة والجرائم المعلوماتية بصورة عامة، وتوصلت الدراسة إلى بعض الاستنتاجات المتمثلة في إن جريمة الابتزاز الإلكتروني هي إحدى أنواع الجرائم المعلوماتية التي تتم عبر التقنية الحديثة، وهي من أكثر أنواع الجرائم المعلوماتية انتشاراً في الوقت الحالي، والتي تُمثل عملية ترهيب وتهديد للمرأة وأن مواقع التواصل الاجتماعي أصبحت بيئة خصبة للمجرمين المبتزين والذين يرون في هذه المواقع وسيلة ملائمة للتعبير عن سلوكهم الإجرامي، ويمكن اعتبار الابتزاز الإلكتروني من الجرائم الدولية لأنها جريمة عابرة للحدود وأن المجني عليه في جرائم الابتزاز الإلكتروني في أغلب الأحيان يكون هو السبب في تعرضه للابتزاز وذلك بسبب قلة وعيه أو عدم المعرفة الجيدة في استخدام التقنية الحديثة أو الثقة الزائدة بالجاني المبتز. واقترح الباحث على المشرع العراقي إلى ضرورة الإسراع في تشريع قانون مكافحة الجرائم الإلكترونية فضلاً عن تعديل البنود والفقرات الخاصة بالابتزاز الإلكتروني في القانون العراقي بما يتلائم مع الخطورة الإجرامية الكامنة فيه.

كلمات الدالة: ابتزاز الكتروني ، ظاهرة ، مسؤولية جنائية ،جريمة ابتزاز ، امرأة

المقدمة الدراسة

تعد جريمة الابتزاز الالكتروني أحد صور الابتزاز الالكتروني التي تخترق المجتمع وتهدد دعائمه، من خلال اخلال شعورهم بالأمان في حياتهم، ولعل جوهر وسبب تجريم جريمة الابتزاز الالكتروني هو التهديد والابتزاز، عن الضغط الذي يمارسه الجاني على المجنى عليه، عن طريق تهديده بإفشاء سرٍ يرى في كشفه معرة له وتعييب، مما يضطر معه إلى الانصياع والاذعان لرغبة الجاني، وتحقيق مطالبه تحت اكراه الخوف من الفضيحة، ومن هنا تنبع المصلحة المعتبرة في تجريم السلوك الاجرامي المكون للابتزاز الالكتروني، كما واهتم شُراح القانون بتفسيره وشرحه، وبيان أركان الجريمة التي تقوم عليها، وكذلك طرق التحقيق وإثبات الجريمة، حى أن خصوصية هذه الجريمة ألقت بآثارها على طرق الإثبات فيها، حتى أن لدليل الجريمة الرقمي، أسس وقواعد مختلفة، للتعامل معه، في التحقيق والإثبت، وسنتناول المسؤلية الجزائية المترتبة على جريمة الابتزاز الالكتروني، إذ ان المسؤولية الجزائية في جريمة الابتزاز الالكتروني للشخص

الطبيعي لا تثير مشاكل تذكر، من حيث بنيان هذه المسؤولية على افعاله التي يجرمها القانون، وذلك بافتراض توافر مقومات الإثبات التي تسمح بالتعرّف عليه، بالنظر إلى السعي المتواصل لعلماء التقنية في تطوير آليات التعامل مع مكافحة جريمة الابتزاز الالكتروني، فان هذه المسؤولية محاطة بكثير من الغموض، في معرض طرحها، على النحو الذي يحقق الغرض الذي من اجله جرّم القانون هذا أو ذاك الفعل.

مشكلة الدراسة

تكمن إشكالية الدراسة في انتشار ظاهرة الابتزاز الالكتروني واستغلال جانب من الجناة للتطور التكنولوجي في مجال الاتصالات الالكترونية لارتكاب هذه الجريمة ضد النساء، خصوصا أن معظم مستخدمي الاتصالات الالكترونية يجهلون التعامل السليم مع هذه التقنية فيقعون فريسة للمبتزين، فضلا عن سهولة ارتكاب هذه الجريمة، لأنها ترتكب عن بعد كونها متخطية الحدود الجغرافية.

واستنادا لما تقدم تتلخص الإشكالية في بيان الحماية الجنائية للمرأة من ظاهرة الابتزاز الالكتروني.

المطلب الاول

التعريف بجريمة الابتزاز الالكتروني

ان لجريمة الابتزاز الالكتروني خصوصية واختلاف عن جريمة الابتزاز التقليدية، وهذه الخصوصية وذاك الاختلاف انما مرجعه الى الطبيعة المميزة لتلك الجريمة، حيث انها تتم في مسرح جريمة افتراضي، يكتنفه الغموض والتخفي، وتختلف ادلته عن تلك الادلة الملموسة من بصمات اصابع تركت بإهمال وتعجل او قطرات دماء لجاني جرح مع الضحية، او مني مغتصب في مسرح جريمة مادي، فجريمة الابتزاز الالكتروني كأحد صور الجريمة الالكترونية – ترتكب في مسرح جريمة تحده نقاط الاتصال والتكنولوجيا الرقمية، وهذا الاختلاف بين الجريمتين التقليدية والالكترونية يجعل طرق ارتكاب الاخيرة تعتمد على وسائل التكنولوجيا الحديثة بشكل اساسي[1]، إذ ادى التطور السريع في أنظمة الحاسب الآلي وتكنولوجيا المعلومات والأجهزة المستخدمة فيها إلى أن أصبح كل انسان يحمل في جيبه كاميرا داخل جهاز النقال الجوال أو المحمول وليست كاميرا تصوير فقط بل هي كاميرا متعددة الاستخدامات تستخدم في التصوير العادي والفيديو وتحمل أدق المواصفات العالمية في كاميرا التصوير عبر قدرتها على التقاط المشاهد عن بعد أو قرب وبرؤية واضحة، فضلاً عن قدرتها – هذه الأجهزة – في المراسلة للابتزاز بمختلف انواعه واغراضه وغاياته، فضلاً عن ذلك فان جميع الفيديوهات والصور والمعلومات المخزونة بهذه الاجهزة المتطورة يمكن نقلها أو إرسالها للأصدقاء أو نشرها على مواقع التواصل الاجتماعي في أقل من ثوان معدودة[2]، أذ ان التطور الكبير في مجال الاقمار الصناعية ساهم بسهولة نقل المعلومات على جوالات وهواتف الاصدقاء وكذلك آلاف الجوالات وإلى شبكة المعلومات الدولية مما يجعل هذه المعلومات تنتشر انتشار النار في الهشيم بسرعة البرق وتصل إلى آلاف وملايين المتصفحين للشبكة المعلوماتية[3].

المطلب الاول

تعريف الابتزاز الالكتروني

يُحيط مفهوم الابتزاز الالكتروني الكثير من الغموض منذ بدايتهِ، ولغاية تنفيذ هذه الجريمة وحتى تمامها، الأمر الذي يمثل تحدياً كبيراً أمام جهات الضبط القضائي، وقد اختلفت التعريفات لهذه الجريمة، وان كان جمعها في خط أساسي واحد وهو استخدام التكنولوجيا والواقع الافتراضي كمسرح جريمة، وكذلك مرتكبها ذو المهارات والصفات المتمايزة عن المجرم التقليدي، كما انه كان من الأهمية الوقوف على أسباب ودوافع هذه الجريمة الخطيرة وآثارها السلبية على المجتمع، ولدرء هذه الجريمة لزاماً التعرف على مفهوم هذه الجريمة، [4].

الفرع الاول

تعريف الابتزاز الالكتروني

عرّف الابتزاز بانه فعل يقوم به شخص بتهديد شخص اخر كتابة او شفاها ولا عبرة بنوع عبارة التهديد ما دام من شأنها

التأثير في نفس المجني عليه كتخويفه أو مجرد ازعاجه من خطر لم يتحقق بعد قد يلحق بماله او نفسه أو بمال أو نفس اي شخص اخر لهُ صلة بالمجني عليه.[5]

كما عُرّف الابتزاز بأنهُ الحصول على وثائق وصور ومعلومات عن الضحية من خلال الرسائل الالكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة عنه عن طريق استخدام الوسائل الالكترونية لتحقيق أهداف سعى إلى تحقيقها المبتز، كما يعرف الابتزاز بأنه حصول شخص على ما يستحق بالتهديد أو باستغلال نقاط الضعف في الشخص الأخر[6]

ويُمكن تعريف الابتزاز ايضاً: بأنه القيام بالتهديد بكشف معلومات معينة على شخص سواء كان ذكراً او انثى وغالباً من اجل ان يطلب منه القيام بأفعال مشروعة أو غير مشروعة والاستجابة لطلبات الجاني وهذه المعلومات غالبا ما تكون محرجة أو ذات طبيعة مدمرة اجتماعياً[7].

اما على الصعيد التشريعي، فنجد ان المشرع العراقي لم يعرّف جريمة الابتزاز الالكتروني كما لم ترد كلمة الابتزاز في قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل سيما وان القانون العراقي قد تم تشريعه منذ فترة طويلة في عام 1969، ولكن الابتزاز هو صورة من صور التهديد المجرم في المواد 430 او التي نصت على ان (1-يعاقب بالسجن مدة لا تزيد على سبع سنوات او بالحبس كل من هدد اخر بارتكاب جناية ضد نفسه او ماله او ضد نفس او مال غيره او بإسناد امور مخدشة بالشرف او افشائها وكان ذلك مصحوبا بطلب او بتكليف بأمر او الامتناع عن فعل او مقصودا به ذلك. 2 – ويعاقب بالعقوبة ذاتها التهديد اذا كان التهديد في خطاب خال من اسم مرسله او كان منسوبا صدوره إلى جماعة سرية موجودة او مزعومة، وأيضا المادة 452 تنطبق على الابتزاز الالكتروني).

كما نصت المادة 452 من القانون اعلاه على ان(1 – يعاقب بالسجن مدة لا تزيد على سبع سنين أو بالحبس من حمل آخر بطريق التهديد على تسليم نقود أو اشياء اخرى غير ما ذكر في المادة السابقة.

2 – وتكون العقوبة مدة لا تزيد على عشر سنين اذا ارتكبت الجريمة بالقوة أو الاكراه[8].

الفرع الثاني

خصائص جريمة الابتزاز الالكتروني

تُعد جريمة الابتزاز الالكتروني إفرازاً ونتاجاً لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما أكسبها لوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجموعة من الصفات قد يتطابق بعضها مع صفات أشكال أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإن اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية اكسبها خصوصية غير عادية، واستناداً لما سبق سيتم تقسيم هذا المطلب إلى الفرعين التاليين :

المقصد الاول: الخصائص التي تتعلق بكيفية ارتكاب جريمة الابتزاز الالكتروني

اولا– خطورة جريمة الابتزاز الالكتروني

تتعاظم خطورة جريمة الابتزاز الالكتروني يوماً بعد يوم كونها تمس الانسان في سمعته وفكره وحياته الخاصة وماله، كما تمس المؤسسات في اقتصادها وسمعتها ايضاً، ناهيك عن خطورتها على البلدان من النواحي الامنية والسياسية والاقتصادية، كما إن ما يبرز خطورة جريمة الابتزاز الالكتروني هو طبيعة الجاني في جرائم المعلومات، إذ قد يكون الجاني في جرائم الابتزاز الالكتروني شخصاً طبيعيا يعمل لحسابه، ويسعى إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها عن طريق الاستعانة بأحد نظم المعالجة الآلية للبيانات والمعلومات، أو ضد احد نظم المعالجة الآلية للبيانات والمعلومات، غير أنه غالباً ما يرتكب الشخص الطبيعي السلوك الإجرامي ليس لحسابه الخاص وإنما لحساب أحد الأشخاص كشركةٍ عامة أو خاصة تعمل في ميدان المعلوماتية أو

في ميدان آخر، لذا فأن تنوع اغراض وغايات جرائم الابتزاز الالكتروني يبرز من خطورتها(9).

ثانيا– ضرورة استخدام الحاسب لارتكاب الجريمة

كما تقدم فإن جريمة الابتزاز الالكتروني هي جريمة تقع عن طريق الحاسب الالكتروني "الحاسب الآلي" الذي يعد الأداة أو الوسيلة التي تُميز هذه الجريمة من غيرها، ومن ثمَّ فإن الخاصية الأوضح لهذه الجرائم هي استخدام هذا الحاسب أو أي جهاز يقوم مقامه وتكون له ذات الخصائص والاستخدامات، ومنها اليوم مثلاً العديد من أجهزة الهاتف النقال "المحمول" التي باتت مزودة بالخدمات الالكترونية والمعلوماتية والتي تتيح لمستخدميها التمتع بالمزايا ذاتها الموجودة في الحاسوب ومنها الاتصال بشبكة الانترنيت وما يرافقها من خدمات ومن ثمَّ فمن الممكن ارتكاب جريمة الابتزاز الالكتروني عن طريق هذا الجهاز.

ثالثا– جريمة الابتزاز الالكتروني عابرة للحدود

لعل من ابرز الخصائص التي تميز جريمة الابتزاز الالكتروني انها جريمة متعدية الحدود، أي انها عابرة لحدود الدول، ومن ثمَّ فهي تكتسب صفة الجريمة الدولية، فمجتمع التقنية المعلوماتية "الالكترونية" لا يعترف بالحدود الجغرافية ولا يتقيد بها فهو مجتمع منفتح عبر الزمان والمكان دون ان يخضع للجانب التقليدي في الحراسة الدولية "حرس الحدود"، فهذه التقنية تسمح لمستخدميها بالتنقل المعنوي أو الافتراضي بين الدول والقارات دون أي تعقيد أو صعوبات أو عوائق، انطلاقاً من سهولة حركة المعلومات وتبادلها، وهو ما جعل من اليسير ارتكاب السلوك الاجرامي في دولة ما وتحقيق نتيجته في دوله أخرى، مما جعل من اليسير القول انها جريمة لا تعترف بالمكان والزمان، فهي من هذه الزاوية وان اشتركت في "دوليتها" و"عبورها" للحدود مع جرائم أخرى تقليدية كجرائم تجارة المخدرات بين الدول أو غسيل الأموال وما شابه، الا ان الفاعل في جريمة الابتزاز الالكتروني لا يغادر مكانه ومقعده من أمام شاشة الحاسوب على خلاف تلك الجرائم التي تتطلب مثل هذا التحرك والنشاط الحركي(10).

رابعا– جريمة الابتزاز الالكتروني، جريمة هادئة

يمكن القول أن جريمة الابتزاز الالكتروني، جريمة هادئة "ناعمة"، كونها لا تتطلب العنف أو السلاح أو الاصطدام مع رجال الأمن، كما انها جريمة لا تتطلب لوقعها سفكٌ للدماء أو آثار اقتحام لسرقة الأموال، وإنما هي ارقام وبيانات تتغير أو تمحى من السجلات المخزونة في ذاكرة الحاسب(11).

خامسا– صعوبة اكتشاف جريمة الابتزاز الالكتروني

حيث ان جريمة الابتزاز الالكتروني، جريمة عابرةٌ للحدود، وحيث انها جريمة تختلف عن الجريمة التقليدية في كثير من النواحي وحيث انها جريمة هادئة، لذا من غير اليسير اكتشاف وقوع هذه الجريمة، وان تم اكتشافها فإن ذلك يكون من قبيل الصدفة في غالب الاحيان. ولعل ابرز الاسباب التي تؤدي إلى الصعوبة المتقدمة في اكتشاف هذه الجريمة تتجلى في عدد من الأسباب، أبرزها:

1. سبب فني: فهذه الجرائم لا تترك وراءها أثراً مادياً كما هو الحال في الجرائم التقليدية.

2. سبب يتعلق بالمجنى عليه ذاته.

سادسا – صعوبة إثبات جريمة الابتزاز الالكتروني

يترتب على الخصائص المتقدمة المتعلقة بدولية هذه الجريمة وصعوبة اكتشافها وهدوئها، ان هذه الجريمة يصعب إثباتها، وهذه الصعوبة راجعة إلى عدد من الأسباب منها أنها جريمة لا تترك أثراً مادياً ملموساً فضلاً عن وقوعها في الأغلب من قبل مجرمين محترفين ولعل مما يزيد في صعوبة إثبات هذه الجرائم، نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء العام والقضاء، إذ أن هذا النوع من الجرائم يتطلب تدريباً وتأهيلاً لأفراد هذه الجهات في مجال التقنية الحديثة من حيث كيفية جمع الأدلة وإجراء التفتيش والملاحقة في بيئة النظام المعلوماتي، مما يجعل من الجهود المبذولة في هذا المجال غير متناسقة وحجم وخطورة هذه الجرائم، يضاف إلى ذلك إنها جرائم لا تخلف وراءها آثاراً مادية.

المقصد الثاني: سمات المجرم الالكتروني

يُعرف المجرم الالكتروني على انه الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الالكتروني والقادر على ارتكاب مختلف الجرائم عن طريق استخدام الحاسوب نفسه .[12]

اذ يتميز المجرم الالكتروني عن غيره من طائفة المجرمين التقليديين بعدد من السمات، فضلاً عن كون الدوافع التي تدفعه إلى ارتكاب الجريمة، متعددة ومتنوعة.

ولعل ابرز هذه السمات والتي درج معظم الفقه الجنائي على ذكرها، تتجلى في كونه مجرم ذكي، وغير عنيف ومتخصص وعائد إلى الاجرام، ومحترف ومتكيف اجتماعياً، والتي نتناولها في الاتي:

1- المجرم الالكتروني مجرم ذكي: الاجرام الالكتروني هو إجرام الاذكياء ولا يمكن ان يقال ان المجرم هنا ينتمي إلى طائفة المجرمين الاغبياء، فاذا كان من يسرق سيارة أو منزل يعد مجرماً منخفض الذكاء في كثير من الاحيان، فإن من يستعين بالكومبيوتر من اجل ابتزاز شخص او مصرف أو شركة فهو مجرم على درجة كبيرة من الذكاء بحيث يمكنهُ التغلب على كثير من المشكلات والعقبات الفنية التي تواجههُ[13].

2- المجرم الالكتروني مجرم غير عنيف: يقال في العادة ان الاجرام الالكتروني هو إجرام غير عنيف مقارنة بالإجرام التقليدي الذي يميل فيه المجرم إلى العنف، فاذا كان من الممكن تصور قيام العنف في جرائم الاعتداء على الحاسب "ماديات الحاسوب" الا ان الاجرام المعلوماتي كالابتزاز الالكتروني لا يتطلب عنفاً كونه من تقنيات التدمير الناعمة، التي تتمثل في التلاعب بالمعلومات أو الكيانات المنطقية أو البيانات[14]، ومثال ذلك يقال ايضاً بالنسبة لسرقة البيانات والابتزاز الالكتروني وما شابه ذلك من جرائم اخرى التي يتمثل فيها سلوك الجاني بشكل معالجة فنية هادئة للمعطيات الالكترونية التي تتم بهدوء ومن دون اي عنف.

3- المجرم الالكتروني مجرمٌ متخصص: حيث أثبتت العديد من الدراسات في هذا المجال ان المجرمين في مجال الابتزاز الالكتروني هم في الغالب لا يرتكبون سوى هذا النوع من الجرائم لتخصصهم فيها[15] .

4- المجرم الالكتروني مجرمٌ عائد إلى الاجرام: إذ يعمد مجرمو المعلوماتية في الغالب إلى العودة إلى ارتكاب جرائمهم انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم ومن ثمَّ كشفهم وتقديمهم للمحاكمة[16].

5- المجرم الالكتروني مجرمٌ محترف: يتطلب هذا النوع من الاجرام مهارةً فنية عالية لا يستطيع الشخص المبتدأ القيام بها، إذ تتطلب هذه الجريمة قدراً من الدقة والتخصص لتجاوز العقبات الالكترونية التي وضعها المتخصصون لحماية أنظمة الكومبيوتر كما يحدث في البنوك والشركات مثلاً، وهذا الاحتراف أو المهارة يكتسبها المبتز الكترونياً اما من الدراسة في مجال تكنولوجيا المعلومات أو عن طريق الخبرة العلمية في هذا المجال أو عن طريق التفاعل الاجتماعي مع الآخرين[17] .

6- المجرم الالكتروني مكيفٌ اجتماعياً: يوصف المجرم الالكتروني بانه انسانٌ اجتماعي، فهو لا يضع نفسهُ في حالة عداء سافر مع المجتمع الذي يحيط به، بل هو متكيف اجتماعياً انطلاقاً من كونه انسانٌ ذكي، وتطبيقاً لذلك فان الكثير من جرائم الابتزاز الالكتروني ترتكب بقصد الحصول على المال أو الاحتيال أو لإظهار مدى ما يتمتع به المبتز من تفوق في مواجهة أنظمة المعلوماتية[18].

المطلب الثاني

وسائل ارتكاب الابتزاز الالكتروني

وتتعدد وسائل الابتزاز بتعدد وسائل التقنية الحديثة، اذ ليس هناك وسيلة محددة يلجأ اليها المبتز لاستغلال ضحيته، باعتبار ان تلك الوسائل تعد مجالا خصبا لممارسة المبتز مبتغاه وتحقيق اهدافه، وبناءً على ما سبق تتنوع وسائل الابتزاز التي يلجأ اليها الجاني ومنها:

الفرع الاول

انشاء مواقع على الشبكة المعلوماتية

يلجأ الجاني المبتز احيانا الى انشاء مواقع الكترونية على الشبكة المعلوماتية بهدف حصوله على اكبر قدر ممكن من المعلومات التي تخص المجني عليه، امثال: المواقع الخاصة بالزواج، او الخاصة بالبحث عن الوظائف، اذ يقوم الجاني بعمل ملف يحتوي على معلومات تخص المجني عليه بدون علمه، او دون الحصول على موافقته، وقد يحدث ان يقوم الجاني بعمل مثل ذلك وبعلم المجني عليه بعد ايهامه بأن جميع المعلومات المرسلة سيتم التعامل معها بكل سرية، ولكي تكون تلك المواقع اكثر مصداقية، فإن الامر يتطلب احيانا للاشتراك بها واستخدامها من قبل المجني عليه تحويل مبالغ مالية، ومنها المواقع التي تهتم بالبحث عن الوظائف للعاطلين عن العمل، اذ تتطلب تلك المواقع للاشتراك بها التسجيل اولا، ومن ثم تعبئة البيانات الخاصة بالضحية كأرقام التواصل، او الاسم الثلاثي، او البريد الالكتروني[19].

ومن الطرق ايضا التي يلجأ اليها الجناة بهدف ابتزاز ضحاياهم انشاء مواقع للزواج بهدف اصطياد الفتيات الراغبات في البحث عن الزواج، ووضع شروط او طلبات للموافقة على الاشتراك بمثل تلك المواقع، ومن تلك الشروط ارسال صورهن الشخصية عبر البريد الالكتروني، وبياناتهن، ووسائل الاتصال التي تخصهن، وبعد ان تقوم الضحية بتقديم ما يصخها من معلومات كافية، تبدأ عملية الابتزاز من قبل الجاني والضغط على الضحية، ما يترتب عليه ان تعيش صراعا داخليا من ناحية الخوف من افتضاح امرها، ومن ثم الرضوخ لمتطلبات الجاني[20].

وايضا من ضمن مواقع التواصل الاجتماعي او ما يسمى بالشبكات الاجتماعية التي ظهرت نتيجة للتطور الهائل في وسائل الاتصالات ونتيجة للاعتماد على التكنولوجيا الحديثة في مجال الانترنيت، والتي عن طريقها اصبحت لغة التخاطب بين الجنسين اسهل من ذي قبل، نتيجة لاستخدام البلاك بيري وبرامج الماسنجر والفيس بوك و Skype ما ادى الى تطور وسهولة الابتزاز نتيجة للعلاقات التي تنشأ عبر هذه الشبكات، ويحدث ذلك بعد ان يكسب المجني عليه ثقة المبتز والاطمئنان له، ويقوم بارسال صوره او ان يقوم الجاني بعمل تسجيلات صوتية والاحتفاظ بها.

ويعرف الحاسب الالي بأنه: "تشتق كلمة الحاسب من الفعل يحسب وهو عبارة عن جهاز او آلة مركبة تتكون من مجموعة الاجهزة الالكترونية، التي تتضافر اعمالها في حل مشكلة معينة او معالجة بيانات مطلوبة وفق برنامج هو مجموعة من ارشادات واوامر تعطي للحاسب ليقوم بعمليات المعالجة للمعلومات المدخلة فيه، ثم الحصول على النتائج المطلوبة"[21] .

وكمثال على استخدام الحاسب كأداة في ارتكاب الابتزاز الالكتروني حيث يقوم احد الموظفين بالدخول على الحاسب الآلي التابع للشركة. ثم يقوم بالدخول الى المستند الخاص بمعلومات وبيانات الموظفين، فيقوم بالحصول على بيانات ومعلومات سرية عن الموظفين ويبتزهم[22].

الفرع الثاني

غرفة المحادثة والبريد الالكتروني والهواتف النقالة

اولا- غرف المحادثة

عندما تحدث لغة التخاطب عبر الانترنيت فإن ما يحدث هو كتابة رسالة باستخدام لوحة المفاتيح، حيث يمكن للآخرين رؤية ما تكتسب وبعدها تأتي ردودهم، ويمكن التخاطب مع فرد، او مجموعة، ولذلك بإمكان الشخص ان يختار موضوع التخاطب الذي يريده ونوعه الذي توفره تقنيات الانترنيت[23].

وتحصل جريمة الابتزاز عن طريق غرف المحادثات مثل: غرف البالتوك، ومواقع الدردشات الصوتية، والكتابية، التي تعد من اشهر طرق الابتزاز، ويكون ذلك بدخول بعض الاشخاص باسماء فتيات مستعارة بهدف ابتزاز الطرف الاخر وهم الشباب، او الفتيات، ونظرا لما تتمتع به مثل تلك الغرف من خصوصية تسمح لكلا الطرفين من تبادل الاحاديث بينهم والتعارف، دون اطلاع الاخرين عليهم، ماينتج عن تلك الاحاديث من كسب ثقة الطرفين وتساهل الطرف الاخر مع الجاني المبتز، حيث تعد فرصة

له لتحقيق ما يهدف اليه من ناحية حصوله على مطامعه المادية او المعنوية[24].

ثانيا- ارتكاب الجريمة عن طريق البريد الالكتروني

يعرف البريد الالكتروني بأنه عبارة عن وسيلة لتبادل الرسائل ما بين الطرفين، ويستطيع الفرد من خلاله ارسال واستقبال كل ما يريده من رسائل، سواء أكانت كتابية، ام صوتية ام ارسال واستقبال الصور، ويعد البريد الالكتروني الاكثر استعمالا من قبل مستخدمي شبكة الانترنيت، اذ يسمح بتبادل الرسائل وتوجيهها الى اكبر عدد ممكن من مستخدمي البريد الالكتروني، وتتحقق جريمة الابتزاز عن طريق دخول الجاني الى بريد المجني عليه الالكتروني وقراءة ما يحتويه من رسائل مرسلة دون علمه، او رضاه، او الاطلاع على الصور الخاصة به، وهذه الحالة تحدث كثيرا عن طريق سرقة الرمز السري الخاص بالبريد الالكتروني والاطلاع على محتواه من رسائل، وصور تخص المجني عليه، وبعد ان يحصل الجاني على تلك المعلومات والبيانات، يقوم بارسال رسالة عبر البريد الالكتروني متضمنة تلك الرسالة تهديدا للمجني عليه اما بنشر ما يخصه من صور، او رسائل تهدف الى تحقيق ما يسعى اليه كأن يهدده بارتكاب جريمة ضد نفسه، او ماله، او ضد نفس، او مال غيره، او تهديده بإفشاء امور تمس شرفه، وسمعته، سواء أكان ذلك مصحوبا بطلب، او بتكليف بأمر، او الامتناع عن فعل[25].

ثالثا- استخدام الهواتف النقالة المزودة بكاميرا

تتمثل سلبية الهواتف النقالة في سوء استخدامها، والتعامل معها كوسيلة من وسائل الاتصال، كما ساعدت تلك الهواتف بطريقة مباشرة، او غير مباشرة في ازدياد جريمة الابتزاز، ويتحقق ذلك عن طريق استخدامه الاستخدام غير المشروع من ناحية المساس بالحياة الخاصة بالأفراد بالتقاط الصور لهم عبر كاميرا الهاتف النقال، او عبر تقنية الفيديو الملحق به[26]، او نشر اخبار او تسجيلات صوتية، او مرئية ليبدأ الجاني بعد ذلك بتهديد المجني عليه بنشر تلك الصور او التسجيلات الصوتية اذا لم يرضخ لمطالبه. -الهواتف النقالة وملحقاتها وبرامجها يستخدم الهاتف النقال بواسطة المجرم الالكتروني باعتباره اداة لارتكاب الجريمة. وذلك عندما يستخدم الانترنت في برامج التواصل. كأن يقوم بالتجسس على الاخرين[27] .

ويعرف الاستخدام غير المشروع **للهواتف النقالة** بانه "كل سلوك ينشأ من الاستعمال غير المشروع لتكنولوجيا الاتصالات والمعلومات الخاصة بالهاتف النقال من شأنه الاضرار بمصلحة الغير او تعريضها للخطر، اما ملحقات الهاتف فهي الكاميرا والبلوتوث وآلات التسجيل[28].

ونرى خلو نظام مكافحة جرائم المعلومات من تعريف الهاتف النقال بالرغم من اعتباره من احد اهم الوسائل التي تستخدم في الابتزاز الالكتروني. لانه اصبح متاحا بايدي الجميع مما يسيء استخدامه كصغار السن لجهلهم بالانظمة. ولكن يلاحظ انه استدرك بعدم ذكره للتعريف اكتفاء بذكر العقوبة المقررة على الجاني عندما يسيء استخدام الهاتف، فقد ذكر في الفقرة الرابعة من المادة الثالثة: "يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة الف ريال، او باحدى هاتين العقوبتين: كل شخص يرتكب ايا من الجرائم المعلوماتية الاتية:... 4- المساس بالحياة الخاصة عن طريق اساءة استخدام الهواتف النقالة المزودة بالكاميرا، او ما في حكمها"[29] . كما خلا ايضا القانون الاماراتي من تعريف للهاتف النقال في نصوص مواده الافتتاحية، ولعل هذا النقص يرجع الى الشعور ببداهة التعريف الخاص بالهاتف النقال[30] .

المطلب الثالث

اركان جريمة الابتزاز الالكتروني

اولا- الركن المادي لجريمة الابتزاز الالكتروني

الركن المادي هو كل ما يدخل في كيان الجريمة وله طبيعة مادية تدركه الحواس ويتحقق ذلك بسلوكٍ إجرامي ايجابي أو سلبي جرمهُ القانون[31]، حيث يقصد بالركن المادي للجريمة السلوك المادي الخارجي الذي ينص القانون على كونه جريمة، وهو ما تدركه الحواس، الأمر الذي يترتب عليه أنْ لا تُعدُ من قبيل الركن المادي

ما يدور في الأذهان من أفكار ورغبات طالما لم تظهر في عالم الحواس[32].

ويتكون الركن المادي من ثلاث عناصر، وهى كما يأتي:

1- السلوك الإجرامي:

إن السلوك الإجرامي كعنصر من عناصر الركن المادي في الجريمة التقليدية غالباً ما يتم رؤيته رأي العين والتأكد منه كفعلِ القتل أو السرقة أو التزوير أو الابتزاز ، ولكن صعوبة جريمة الابتزاز الالكتروني والركن المادي فيها خاصةً أنها تُرتَكَب عن طريق معلومات تتدفق عبر نظم الحاسوب الآلي التي لا يمكن الإمساك بها مادياً، تماماً مثل التيار الكهربائي الذي يسري في توصيله دون أنْ نراه[33].

لذا فالسلوك الاجرامي في جريمة الابتزاز الالكتروني غالباً ما يكون ايجابيا فهي تتطلب صدور فعل إيجابي غير قانوني من قبل المتهم يتمثل في تلقي احد الأشخاص تهديد من افراد او جماعات او مؤسسات لاستغلال الضحية بطريقة أو بأخرى، وعادةً ما تكون الأهداف مادية وبعضها يكون جنسياً والآخر نفعياً بحسب الغرض الاساسي من عملية الابتزاز، فالابتزاز يكون فعل لغاية الحصول على مقابل مالي أو جنسي والاخير يعد خطير جداً على النسيج الاجتماعي ويتسبب في التفكك الاسري بسبب خطورته الكبيرة، والابتزاز النفعي الذي يكون لأصحاب المناصب العليا عادةً ويكون هدفه الحصول على منصب او إدارة شركة او غيرها من الأغراض الأخرى. ولكن السؤال الهام هل يتصور ان تقترف هذه الجريمة بالسلوك السلبي أي عن طريق الامتناع ؟ قد تقع هذه الجريمة بطريق الامتناع في حالة إذا كان يتطلب من المتهم القيام بعمل معين لصالح الضحية، فيأخذ المتهم موقفا سلبيا تجاه ذلك بهدف الضغط على الضحية وتهديده للقيام بعمل معين، وقد يكون محل التهديد معلومات او بيانات خاصة بالضحية أو بأسرته ويتخذها كوسيلة للتهديد، ويستوي لدى المشرع نوع هذه البيانات او المعلومات، كما يستوي لدى المشرع ان يكون المجني عليه شخص طبيعي او شخص معنوي[34].

2- النتيجة الجرمية:

للنتيجة مدلولان مدلول مادي باعتبارها مجرد ظاهرة مادية، ومدلول قانوني باعتبارها فكرة قانونية، وعلى الرغم من الاختلاف بين المدلولين ولكن بينهما صلة وثيقة تجعل ماهية النتيجة والأحكام التي تخضع لها مقتضية الرجوع معاً[35].

تُعدُ جرائم الابتزاز الالكتروني من الجرائم ذات الخطر التي لا يشترط فيها المشرع عنصري النتيجة والرابطة السببية، بل يكتفى فيها بعنصر السلوك فقط ، فالمشرع الجنائي يفترض فيها الخطر المتمثل في قيام السلوك الخارجي المحدد بنصوصِ القانون فتقوم الجريمة ويتمُّ العقاب عليها[36].

3- علاقة السببية:

ان الاتجاه العام في تجريم جرائم الضرر انه لا يكفي لقيام الركن المادي للجريمة أنْ يقع سلوك إجرامي من الفاعل وأنْ تحصل نتيجة، بل يلزم فضلاً عن ذلك أنْ تُنسب هذه النتيجة إلى ذلك السلوك، وتثبتُ أنَّ ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، فمثلاً يجب لتحقيق جريمة انتهاك الحق في الخصوصية عبر الإنترنت، أنْ يكون هناك دخول على الإنترنت باستخدام حاسوب عام أو نقال والقيام باختراق الخوادم المختلفة في مسارها، ثمَّ بعد ذلك التعدي على خصوصية موقعٍ ما، وكذلك يمكن اعتبار علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد البث، وكذلك التعدي على نشاط وأسرار الحكومات فيعتبر هذا التعدي ابتزاز إلكتروني[37].

ثانيا– الركن المعنوي لجريمة الابتزاز الالكتروني: يظهر الركن المعنوي للجريمة بشكل عام بإحدى صورتين، الأولى صورة القصد الجرمي فنكون أمام جريمة مقصودة تتطلب قصداً جرمياً عاماً، أو إضافة للقصد العام تتطلب قصداً جرمياً خاصاً . والثانية هي صورة الخطأ فنكون أمام جريمة غير مقصودة.

وجريمة الابتزاز الالكتروني هي من الجرائم التي لا تقع إلا مقصودة. ولا تقوم بصورة الخطأ مهما بلغت نسبة جسامته.

ان الابتزاز الالكتروني جريمة قصدية، لذا لا بد من توافر القصد الجرمي العام لتقوم الجريمة، فإذا انتفى القصد انتفت الجريمة ويتوافر القصد الجرمي بعلم الجاني بأن من شأن خطابه أو فعله أو قوله أو إشارته أن يدخل القلق في نفس المجني عليه؛ لما يتوقعه من ضرر يصيبه في نفسه أو ماله أو نفس من يرتبط به بصلة أو ماله، وأن يقصد الجاني مجرد التخويف أو حمل المجني عليه على القيام بفعل أو الامتناع عن فعل[38]

فالقانون العراقي يعاقب على مجرد التهديد، بغض النظر عما إذا كان الجاني قد عزم على تنفيذ تهديده أو عدم تنفيذه، وأن قصد الجاني يستخلص من ملابسات الواقعة، نظراً لتعكير أمن المجني عليه وليس بوصفه دليل تصميم أو تحضير لارتكاب جريمة، ومتى كانت عبارات التهديد جدية فإنها تكون قرينة على توافر القصد الجرمي، ولا عبرة بالباعث على التهديد، فالقصد الجرمي يتحقق ويعاقب الجاني على الفعل متى قصد إحداث الخوف لدى المجني عليه، سواء بدافع الانتقام أو الحصول على المال، أو حتى مجرد حب الاستطلاع ورغبته في اختبار شجاعة المجني عليه أو مجرد المداعبة أو المزاح. وتطبيقا لذلك قضت محكمة التمييز العراقية بأنه "إذا كان القصد من التهديد مجرد التخويف دون انصراف نية المتهم لارتكاب جريمة معينة فيكون الفعل منطبقا عليه أحكام المادة 431 من قانون العقوبات"[39].

ثالثا– عقوبة جريمة الابتزز الالكتروني

اما المشرع العراقي، وان لم تتطرق القوانين فيه إلى مفردة الابتزاز الالكتروني الا ان للقضاء العراقي الدور الحازم في معالجة هذا الخلل وفقا لأحكام المواد 430 و433 و437 و 452 من قانون العقوبات العراقي وهي جرائم التهديد والتشهير وانتهاك حرمة الحياة الخاصة وافشاء الاسرار والسب والشتم من ابتزاز النساء والاطفال والرجال، وان الدوافع وراء ارتكاب جريمة الابتزاز الالكتروني قد تكون دوافع جنسية او الابتزاز المالي او الانتقام ونجد من الضروري تشريع قانون لمكافحة جريمة الابتزاز الالكتروني وعدم الاكتفاء بما ورد في قانون العقوبات العراقي واعتبار جريمة الابتزاز الالكتروني من جرائم الحق العام وذلك لكونها من الجرائم الخطيرة على الاسرة والمجتمع .

حيث نصت الفقرة الأولى من المادة 430 من قانون العقوبات العراقي على أن " يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من هدد آخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره أو بإسناد أمور مخدشة بالشرف أو إفشائها وكان ذلك مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل مقصود به ذلك". ونصت الفقرة الثانية من المادة المذكورة على أن "يعاقب بالعقوبة ذاتها إذا كان التهديد في خطاب خال من اسم مرسله أو كان منسوبا صدوره إلى جماعة سرية موجودة أو مزعومة". أما المادة 431 فقد نصت على أنه "يعاقب بالحبس كل من هدد آخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره بإسناد أمور خادشة للشرف أو الاعتبار أو إفشائها بغير الحالات المبينة في المادة 430". وجاء نص المادة 432 على أنه "كل من هدد آخر بالقول أو بالفعل أو بالإشارة كتابةً أو شفاهاً أو بواسطة شخص آخر في غير الحالات المبينة في المادتين 430 و431، يعاقب بالحبس مدة لا تزيد على سنة واحدة أو بغرامة...."

الخاتمة

تعتبر جريمة الابتزاز الالكتروني من الجرائم المستحدثة، ويطلق عليها في علم الجريمة الجرائم الناعمة، التي تخلو من العنف، وهى أحد صور الابتزاز الالكتروني، حيث توصل الباحث الى مجموعة من الاستنتاجات والمقترحات وعلى النحو الآتي:

اولا– الاستنتاجات

توصلت الباحث من خلال ما تقدم إلى مجموعة الاستناجات نوردها فيما يلي:

1. لم ينص المشرع العراقي في القوانين النافذة على جريمة الابتزاز الالكتروني الا أننا نجد تطبيقاتها في أحكام المواد (430، 431، 432، 433، 434، 435، 436، 437، 438، 452) من قانون

العقوبات العراقي رقم 111 لسنة 1969 المعدل وهى جرائم التهديد بالقول أم الفعل والسب والشتم والقذف وإفشاء الاسرار وأنتهاك حرمة الحياة الخاصة

2. لجريمة الابتزاز الالكتروني طرق مختلفة في ارتكابها كما أن لها وسائل أيضا خاصة بها تختلف عن الابتزاز التقليدي، وهى قد تستهدف النساء والرجال والاطفال فضلاً عن الشخصيات المعنوية لتحقيق الكسب المادي، فهي جريمة عابرة للحدود، فقد يكون المبتز في دولة بالعالم، ويقوم بابتزاز ضحيته في أقصى العالم.

3. ابتزاز النساء هو من أكثر أنواع الابتزاز الإلكتروني شهرة وانتشارا من حيث شخص المجني، حيث أن الابتزاز الإلكتروني للنساء يعد الأنموذج الأمثل للجريمة، خاصة ما إذا كان الجاني رجلا، ففي الغالب تبدأ العلاقة بين الطرفين بالثقة الوهمية والتحايل عليها بفكرة الحب والحنان والعاطفة والأساليب الملتوية المخادعة، بحيث يقوم الجاني بالتعرف على الفتاة والتواصل معها عن طريق الاتصال العشوائي أو المواقع والمنتديات الإلكترونية أو القنوات الفضائية أو غير ذلك من الوسائل الأخرى، ثم يستدرجها للحصول على صور أو مقاطع شخصية فاضحة لها أو بيانات أو غير ذلك مما قد يسيء للفتاة عند نشره ويهددها بالنشر مالم تقم بدفع أموال أو يطلب منها أعمال جنسية غير مشروعة.

4. ففي ظل الفساد الخلقي والديني وغياب دور الأسرة يدخل الشباب والفتيات في المحادثات الصوتية والمرئية عبر الإنترنت ووسائل التواصل الإلكترونية، والتي تشتمل في كثير من الأحيان على الحديث حول الأمور الجنسية و الخادشة للحياء أو يتم إرسال الصور والفيديوهات العارية للفتيات والنساء والتي يتم استخدامها من قبل الجناة فيما بعد للابتزاز الإلكتروني، والذي قد يسبب إما الوقوع في شرك المبتز والرضوخ لطلباته او اللجوء في بعض الأحيان للانتحار تلافيا للفضيحة التي ستطالهن إن نفذ المبتز تهديده بنشر ما لديه من صور وفيديوهات.

5. انعدام النّصوص الصّريحة التي تشير الى معالجة حالات ابتزاز النساء الكترونيًّا، واضطرار القضاء العراقيّ الى اللجوء للقواعد العامة، وتطويعها بما يناسب كل فعل وطبيعة الضرر الواقع على القاصرات.

6. الابتزاز في غالبيّة صورهُ يشكل جريمة من جرائم الاعتداء على حرمة الحياة الخاصة و انتفاء، ووجود التنظيم القانوني للابتزاز الالكترونيّ تجعل لكل من تسول له نفسه الاعتداء على خصوصيّة الآخرين من دون معرفته بالعواقب واستهانته بانعدام الجزاء، الأمر الذي يدعو لتفشي الظاهرة في المجتمع وهذا ما لا تحمد عقباه.

ثانيا– المقترحات:– لخصوصية الموضوع وما لهُ من ترابط تقني قانوني، ستقسم الباحث المقترحات إلى فنية وقانونية وعلى النحو الآتي:

1. دعوة المشرع العراقي إلى ضرورة التدخل بإصدار قانون مكافحة الجرائم المعلوماتية، بما لا يتعارض مع الحقوق والحريات المكفولة دستورياً في العراق، مع تضمينه نص يجرم الابتزاز الالكتروني بصراحة ويجيز للجهات المعنية حظر المواقع الإباحية، وتوفير ضمانات لضحايا الابتزاز الالكتروني.

2. نرى بأن المسؤولية الجزائية الانسب في جريمة الابتزاز الالكتروني في جرائم الابتزاز يجب أن تكون وفق المسؤولية التضامنية التي تحقق غاية المشرع في الموازنة في الحفاظ على امن المجتمع من جرائم الابتزاز الالكترونية المنظمة، وعدم الاقتصار عند التجريم والعقاب على انماط السلوك المحظور المرتكبة حالياً بل يجب مراعاة الابعاد المستقبلية لان تكنلوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل.

3. سن القوانين والأنظمة الخاصة التي تسد كافة ثغرات جريمة الابتزاز الالكتروني، مثل القوانين المتعلقة بكيفية اكتشاف الأدلة الالكترونية، وحفظها، والنص على طرق ثبوتها.

4. التنسيق وتوحيد الجهود بين الجهات المختلفة: التشريعية، والقضائية، والضبطية، والفنية، وذلك من اجل سد منافذ الابتزاز الالكتروني قدر المستطاع، والعمل على ضبطها وإثباتها بالطرق القانونية والفنية.

5. ابتداءً نشد على يدّ المشرّع العراقيّ في ضرورة إقرار قانون الجرائم المعلوماتيّة، وعدم تركه يراوح مكانة على طاولة البرلمان، لما له من الأثر البالغ في زيادة الثقافة القانونيّة الالكترونيّة، وتحديد الأطر القانونيّة لهذه الجرائم والمفاهيم الموضحة لها، والجهات المختصة بالنّظر في الدّعاوى التي تقام والآليات المعتمدة في إثباتها والوصول اليها.

6. بالإضافة الى ضرورة تفعيل تنظيم شرطة الكترونيّة أو شعب لمكافحة الجرائم المعلوماتيّة في المحافظات العراقيّة بمعيّة جهاز وزارة الدّاخليّة ومديرية الأمن، لتلقي الشكاوى بكل سرية ومهنية، مع تدريب كوادرها بصورة حرفيّة عالية المستوى لمساعدة ضحايا الجرائم الالكترونيّة عامة، والتّعامل مع النساء على وجه التّخصيص.

7. نوصي الأسرة العراقيّة بوجوب متابعة ومراقبة الفتيات حرصًا وحبًا بهن، مع ضرورة زرع الثّقة بهن، والتأكيد على مخافة الله في كل تصرف، والتّحذير من الأغيار على مواقع التّواصل الاجتماعيّ وعدم الدّخول على روابط مجهولة المصدر، الأمر الّذي من شأنه أن يحجّم هذه الظاهرة ويجعل منها حالات نادرة.

الهوامش

(1) د. ماجد عمار: المسئولية القانونية الناشئة عن استخدام فيروس برنامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989، ص156.

(2) د. محمد المرسي زهرة: الحاسب الالكتروني والقانون، دراسة حول حجية مخرجات الحاسوب الالكتروني في الاثبات في المسائل المدنية والتجارية، دراسة مقارنة، مكتبة سعيد عبد الله وهبة، القاهرة، 1992، ص211.

(3) د. داليا عبد العزيز: المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة، السعودية، 2017، ص27.

(4) زهرة، محمد المرسي،(1992)، الحاسب الإلكتروني والقانون، دراسة حول حجية مخرجات الحاسوب الإلكتروني في الإثبات في المسائل المدنية والتجارية، دراسة مقارنة، متكبة سعيد عبدالله وهبة، القاهرة، ص211.

(5) شهلوب، محمد عبدالمحسن (2012)، جريمة الابتزاز، رسالة ماجستير، الرياض، ص 102.

(6) زهرة، محمد المرسي، (1992)، مرجع سابق، ص211.

(7) د. داليا عبد العزيز: المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة، السعودية، 2017، ص27.

(8) ان التشريع الاردني لم يعرف جريمة الابتزاز الالكتروني في القانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012، وانما عاقب على بعض الأفعال التي تُشكل اعتداءً على النظام المعلوماتي، أو اعتداء على آخرين في معظم نصوصه، فيما عرّفها قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية السوري رقم 17 لسنة 2012 بانها (جريمة ترتكب باستخدام الأجهزة الحاسوبية، أو الشبكة، أو تقع على المنظومات المعلوماتية، أو الشبكة)، اما التشريع السعودي، والتشريع العماني، والتشريع الاماراتي من ناحية تعريفهم للابتزاز الالكتروني إذ نجد اتفاقهم على ان الابتزاز هو تهديد شخص بهدف ابتزازه باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات لحمله على القيام بفعل او الامتناع عنه، ولو كان القيام بهذا الفعل او الامتناع عنه مشروعا وهذا ما نصت عليه المادة 2/3 من نظام مكافحة الجرائم المعلوماتية السعودي، المادة 18 من قانون مكافحة جرائم تقنية المعلومات العماني، المادة (9) من قانون مكافحة جرائم تقنية المعلومات الاماراتي.

(9) حمزة، عبدالرحمن جلهم، بلا سنة نشر، جرائم الإنترنت من منظور شرعي وقانوني، ظافر للتصميم، والطباعة، بغداد، ص 22.

(10) القاضي، رامي متولي، (2011)، مكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، ص22.

(11) رشدي، محمد علي ، مرجع سابق، ص33.

(12) قشقوش، هادي حامد (1992)، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، ص32.

(13) حجازي، عبدالفتاح بيومي، مرجع سابق، ص28.

(14) قشقوش، حامد، مرجع سا بق، ص32.

(15) المناعسة، أحمد، مرجع سابق، ص12.

(16) طه، احمد حسام (2000)، الجرائم الناشئة عن استخدام الحاسب الآلي، "الحماية الجنائية للحاسب الآلي"، دراسة مقارنة، القاهرة، ص33.

(17) قايد، اسامة (1998)، الحماية الجنائية وبنوك المعلومات، دار النهضة العربية، القاهرة. ص10.

(18) العريان ، محمد علي (2004)، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، ص62.

(19) عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، مصر: دار الكتب القانونية، 2007، ص134.

(20) محمد شفيق، الجريمة والمجتمع محاضرات في الاجتماع الجنائي والدفاع الإجتماعي، ط1، مصر: المكتب الجامعي الحديث، 2001، ص76

[21]وعرفته الفقرة السادسة من المادة الاولى من نظام مكافحة جرائم المعلوماتية السعودي بانه: "... اي جهاز الكتروني ثابت او منقول سلكي او لا سلكي يحتوي على نظام معالجة البيانات، او تخزينها، او ارسالها، او استقبالها، او تصفحها، يؤدي وظائف والاوامر المعطاة له..." ، بينما نجد ان المشرع الاماراتي لم ينص على تعريف الحاسب الالي في القانون الاتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، الخليفة، محسن سليمان: جرائم الحاسب الالي وعقوبتها في الفقه والنظام – جريمة استنساخ الحاسب الآلي وبيعها وانتاج الفيروسات ونشره. رسالة ماجستير قسم العدالة الجنائية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية، المملكة العربية السعودية، 1424، ص21.

[22]البلوي، سالم حامد: التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة ماجستير قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية، المملكة العربية السعودية، 1430هـ، ص 168-169.

[23]أحمد عفيفي، الأحكام العامة للعلانية في قانون العقوبات، إطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 2001، 154.

[24]د. محمد الشناوي: جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المحلة الكبرى، 2008، ص22.

[25]د. حسن الغافري: السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهضة العربية، القاهرة، 2009، ص22.

[26]د. طارق الدسوقي عطية: الأمن المعلوماتي، " النظام القانوني للحماية المعلوماتية"، دار الجامعة الجديدة، الاسكندرية، 2010، ص11.

[27]احمد، طارق عفيفي: الجرائم الالكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والاماراتي والنظام السعودي المركز القومي للاصدارات القانونية، مصر 2014، ص41.

[28]عبد خشان، امل فاضل: حمد الله، احمد، الاثبات الجنائي في جرائم اساءة استعمال الهاتف النقال مجلة كلية القانون للعلوم القانونية والسياسية، العدد 12، المجلد 4، الجزء 1، جامعة كركوك، العراق، 2015، ص317.

[29]المادة رقم 3 فقرة 4 من نظام مكافحة الجرائم المعلوماتية السعودي الصادر من مجلس الوزراء برقم 79 في تاريخ 1428/3/7هـ.

[30]اما الخدمات التي يقدمها الانترنت:

أ-البريد الالكتروني: يعمل البريد الالكتروني على تبادل الرسائل الالكترونية بما فيها النصوص والمقاطع الصوتية والصور. وقد وفرت هذه الخدمة كثيرا من الوقت بحيث تصل الرسائل في نفس اللحظة الى اي مكان في العالم.

ب-خدمة الدردشة: هو برنامج يسمح بتجمع عدد من الاشخاص في جميع انحاء العالم للتواصل مع بعضهم اما كتابة او صوتا او عن طريق الفيديو. ينظر : يوسف صغير: الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، 2013، ص 2 حاشية رقم 2.

[31]ممدوح، عبد الحميد عبد المطلب، مرجع سابق، ص11.

[32]عتيق، السيد، مرجع سابقق، ص101.

[33]حجاز، عبد الفتاح بيومي، ص114.

[34]حجاز، عبد الفتاح بيومي، مرجع سابق، ص114.

[35]الحسيني، عمر الفاروق، (199)، المشكلات الهامة في الجرائم المتعلقة بالحاسب الآلي وابعادها الولية، دراسة تحليلية لنوص التشريع المصري مقارناً بالتشريع الفرنسي، ط2.

[36]الشناوي، محمد (2008)، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المحلة الكبرى، ص88

[37] حجازي، عبد الفتاح بيومي، مرجع سابق، ص114.

[38]الشناوي، محمد: (2008)، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المحلة الكبرى، ص88.

[39]حكم محكمة التمييز العراقية، رقم 2007/585، تاريخ 2007/8/11، مشار اليه في: صادق، ناهدة عمر (2015)، جريمة التهديد في قانون العقوبات العراقي، حكومة إقليم كوردستان، وزارة العدل، دهوك، ص23.

قائمة المراجع

محمد المرسي زهرة: الحاسب الالكتروني والقانون، دراسة حول حجية مخرجات الحاسوب الالكتروني في الاثبات في المسائل المدنية والتجارية، دراسة مقارنة، مكتبة سعيد عبد الله وهبة، القاهرة، 1992.

داليا عبد العزيز: المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة، السعودية، 2017.

ماجد عمار: المسئولية القانونية الناشئة عن استخدام فيروس برنامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989.

الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، مصر: دار الكتب القانونية، 2007.

محمد شفيق، الجريمة والمجتمع محاضرات في الاجتماع الجنائي والدفاع الإجتماعي، ط1، مصر: المكتب الجامعي الحديث، 2001.

البلوي، سالم حامد: التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة ماجستير قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الامنية، المملكة العربية السعودية، 1430هـ.

أحمد عفيفي، الأحكام العامة للعلانية في قانون العقوبات، إطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 2001.

محمد الشناوي: جرائم النصب المستحدثة، دار الكتب القانونية، مصر، المحلة الكبرى، 2008.

حسن الغافري: السياسة الجنائية في مواجهة جرائم الانترنيت، دار النهضة العربية، القاهرة، 2009.

طارق الدسوقي عطية: الأمن المعلوماتي، " النظام القانوني للحماية المعلوماتية"، دار الجامعة الجديدة، الاسكندرية، 2010.

احمد، طارق عفيفي: الجرائم الالكترونية، جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والاماراتي والنظام السعودي المركز القومي للاصدارات القانونية، مصر 2014.

عبد خشان، امل فاضل: حمد الله، احمد، الاثبات الجنائي في جرائم اساءة استعمال الهاتف النقال مجلة كلية القانون للعلوم القانونية والسياسية، العدد 12، المجلد 4، الجزء 1، جامعة كركوك، العراق، 2015.

WOMEN CRIMINAL PROTECTION FROM THE ELECTRONIC EXTORTION PHENOMENON

SALAM **A**BDSHEIBTH *and **N**OOR **A**LI **A**LSADI**
* Ministry of the Interior, the Office of the Teaching Minister at Al-Farabi College, University of Iraq-Iraq
**General Secretariat of the Cabinet - Iraq

ABSTRACT

This research is summed up in shedding light on a serious criminal phenomenon at the national and international levels alike, required the attention of legal, social and illegal researchers interested in the technical aspect of those acts, whose spread increased significantly with the increase in the use of computers and various communication devices, represented by "criminal protection of women from the phenomenon of electronic extortion", and the objectives of the study is to clarify the obstacles and difficulties facing the legislative and security efforts aimed at eliminating the phenomenon of electronic extortion in Iraqi law and to clarify those difficulties that impede the confrontation of this criminal phenomenon and to find legal solutions to remove these obstacles with anti- and protective legislation from the effects of the crime of electronic extortion and its implementation In order to bear fruit, and due to the none-existence of legislation of the laws under study in terms of electronic extortion in particular and information crimes in general, the study reached some conclusions represented in the fact that the crime of electronic extortion is one of the types of information crimes taking place through modern technology, and it is one of the most types of information crimes widespread at the present time, which represents a process of intimidation and threat to women, and that social networking sites have become a fertile environment for blackmail criminals who see these sites as an appropriate way to express their criminal behavior, and electronic extortion can be considered an international crime because it is a crime that crosses borders and that the victim in the crimes of electronic extortion in most cases, he is the reason he is exposed to blackmailing, due to his lack of awareness and good knowledge in the use of modern technology, or excessive confidence in the blackmailer. The researcher suggested to the Iraqi legislator, the need to expedite the enactment of the Anti-Cybercrime Law, as well as to amend the clauses and paragraphs related to electronic extortion in the Iraqi law in a way consistent with the criminal danger inherent in it.

***KEYWORDS*:** electronic blackmailing - phenomenon - criminal responsibility - blackmailing crime - woman