المواجهة الجنائية للابتزاز الإلكتروني

م. د. محمد موسى جابر

مستشار قانوني/وزارة التربية

مقدمـــــة

إنَّ الاستخدام الهائل والمتسارع لأجهزة الحاسوب والهواتف الذكية ولشبكة المعلومات الدولية(الإنترنت) ولما بات يُعرف أيضا بوسائل التواصل الاجتماعي، فهو إضافة إلى سهولة الولوج إلى هذه التقنيات، أدى وبشكل متتابع تارة إلى كثرة وتنوع المستخدمين وبالتالي اختلاف ثقافاتهم وقيمهم، وهو ما يؤدي حتما إلى احتمال ظهور أنواع متعددة من سوء الاستخدام بحسب هذا الاختلاف والتنوع تارة أخرى؛ ومنها ما صار يعرف بجرائم تقنية المعلومات أو الجرائم الإلكترونية أو المعلوماتية أو السيبرانية نسبة إلى الوسائل المستخدمة في هذه الجرائم كونها تتخذ الطابع الإلكتروني أو المعلوماتي بحسب طبيعة المجال الذي تتخذ من تقنياته وسائلا لسلوكها الإجرامي، فهي بذلك تشكل نشاطا إجراميا تستخدم فيه تقنية متطورة تكنولوجيا بطريقة مباشرة أو غير مباشرة كوسيلة أو كهدف لتنفيذ الفعل الإجرامي العمدي في البيئة المعلوماتية. ونظرا للتعقيد الذي يكتنف هذه البيئة وتنوع التقنيات فيها وبالتالي تنوع الوسائل التي تتخذها إساءة استخدامها ما جعل من التساؤل يثار عن ضرورة سن تشريعات عقابية خاصة بهذا النوع من الجرائم ، وهو الأمر الذي سارت عليه الكثير من الدول ، أو القول بقدرة التشريعات الجنائية العادية المتمثلة بقوانين العقوبات على مجاراة هذا النوع من الجرائم كونها لا تعدو في اغلبها إلا أن تكون تغيرا بوسائل الإجرام، وهو ما يمكن أن تحتويه النصوص الحالية، والاكتفاء بسن تشريعات ببعض الجرائم المستحدثة. وأي يكن من أمر فان خطورة هذه الجرائم وتنوعها إضافة إلى كثرة مرتكبيها يستدعي أن يقف المجتمع الدولي والمشرع الجزائي بنظرة فاحصة ومتعاونة لمكافحتها وإيجاد الأساليب الناجعة لمعاقبة مرتكبيها خاصة ما يتعلق بوسائل الإثبات التي أضافت لها تقنيات المعلومات الحديثة تعقيدات جمة تختلف بطبيعتها عن أساليب الإثبات التقليدية؛

ويشكل الابتزاز الإلكتروني أحد صور هذه الجرائم والتي يحاول هذا البحث الوقوف على تحديد مفهومه وبيان صيغ مواجهته من الناحية الجزائية.

أولا: أهمية البحث

تكمن أهمية هذا البحث من تلمس الآثار الخطيرة في المجتمع العراقي التي ترتبت على انتشار جرائم الابتزاز الإلكتروني ما يجعل من تسليط الضوء عليها جديرا بالبحث لاصطدامها بالعادات والأعراف الاجتماعية خاصةً وان هذه الجريمة غالباً ما تكون ضحاياها من النساء جوهر بناء المجتمعات ومدارس أجيال المستقبل، مستهدفا بذلك الوصول إلى وسائل جزائية ناجعة لمكافحتها من خلال عرض مختلف التجارب التشريعية بغية حث المشرع العراقي للأخذ بها.

ثانياً : مشكلة البحث

تتحدد مشكلة البحث في معرفة مدى كفاية نصوص قانون العقوبات العراقي التقليدية في مواجهة هذه الجريمة لردع مرتكبيها ومدى توفير الحماية الجنائية للمجني عليهم.

ثالثاً : منهجية البحث

إنَّ طبيعة الموضوع تقتضي معالجته ، بحسب رؤية الباحث، على وفق المنهجين الوصفي والمقارن بغية الوصول إلى معالجة مشكلة البحث.

رابعاً : خطة البحث

وللوصول إلى ما يبتغيه البحث ، يرى الباحث من المفيد تقسيمه إلى مطلبين يحدد الأول التعريف بالابتزاز الإلكتروني من حيث المفهوم والصور التي يتخذها، ثم بيان أهم الجهود الدولية لمواجهته، ويتناول الثاني موقف التشريع الجنائي من ذلك وكما يلي:

المطلب الأول/ مفهوم الابتزاز الإلكتروني والجهود الدولية لمواجهته

سيتم بيان مفهوم الابتزاز الإلكتروني أولا ثم ما يتعلق بالجهود الدولية الساعية لمواجهته في ضوء معالجتها للجرائم الإلكترونية التي يمثل أحد صورها وذلك في فرعين وكما يلي:

الفرع الأول: مفهوم الابتزاز الإلكتروني: لتحديد مفهوم الابتزاز القانوني سيتم البحث في محاولة تحديد المقصود به والصور أو الأشكال التي يتخذها والخصائص التي يتميز بها وذلك تباعا فيما يلي:

أولا: معنى الابتزاز الإلكتروني: يمثل ما يعرف بالابتزاز الإلكتروني أحد أنواع الجرائم الإلكترونية، ويتكون من مفردتين تتعلق الأولى بطبيعة الفعل (ابتزاز) والثانية بصورته (الكتروني). أما الابتزاز كفعل فيأتي لغة من (بزَّ) وابتزه سلبه، والبزُّ يشير إلى الغلبة والسلب بها، والابتزاز مفرد مصدر ابتزَّ، وهو الحصول على منافع أو مال من شخص تحت التهديد بفضح بعض أسراره أو غير ذلك، والنزعة الابتزازية هي نزعة للحصول على أهداف معينة بطرق غير مشروعة [1].ولا شك في أن هذا التهديد ينافي الرضا، وهو ما يتحقق معه الإكراه ، والإكراه بصورة

عامة قد يكون ماديا أو معنويا، ويكون معنويا اذا اتخذ أسلوب الضغط النفسي للتأثير على إرادة المُكرَه لحمله على القيام بعمل أو الامتناع عنه، وقد ينصب على مال المُكرَه أو نفسه أو شرفه وسمعته أو نفس أو مال أو شرف وسمعة الغير ممن يهتم لأمرهم؛ [١] أما وصفه بالإلكتروني فهو بسبب اتخاذه من وسائل تقنية المعلومات أداة للتنفيذ من خلال فضح ما يريد الضحية ستره ، وبهذا يكون الابتزاز الإلكتروني–بحسب الباحث– هو الضغط الذي يباشره شخص ما بواسطة وسائل تقنية المعلومات على إرادة شخص آخر لحمله على القيام بعمل أو الامتناع عن عمل وذلك بتهديده بإسناد أو إفشاء أية بيانات أو معلومات سرية خادشة للشرف أو الاعتبار تتعلق به أو بغيره ممن يؤثر عليه، وقد عُرِّف الابتزاز الإلكتروني على أنه عملية تهديد وترهيب للضحية بنشر صور أو أفلام أو تسريب معلومات سرية، لحملها على دفع مبالغ مالية أو لاستغلالها للقيام بأعمال غير مشروعة لصالح المبتز أو غيره، كالإفصاح عن معلومات سرية خاصة سواء أكانت شخصية أو عامة أو لممارسة أفعال جنسية محرمة[٢].وتصل هذه البيانات الشخصية إلى الشخص المبتز إما عن طريق اختراق الحسابات الشخصية في الأجهزة الإلكترونية أو استعادة محتويات الهاتف النقال بعد بيعه، أو من خلال الضحايا أنفسهم، الذين قد يرسلون صورهم وفيديوهات خاصة بهم في أوضاع غير لائقة يمكن أن يستغلها الشخص المبتز [٣]. وتشكل مواقع التواصل الاجتماعي وبوابات التراسل، الساحة الرئيسية للابتزاز سواء من خلال انتحال شخص ما اسماً مستعاراً لفتاة أو رجل أو مؤسسة، ليبدأ باستدراج الضحايا عبر طلبات التعارف ليتطور الأمر إلى اختراق بيانات الضحية، أم كما غالبًا ما تبدأ عملية الابتزاز عن طريق إقامة علاقة تواصل مع الضحية، عن طريق برامج المحادثات المرئية أو المسموعة أو المكتوبة، وقد يتحقق الحصول على محل الابتزاز عن طريق ما يعرف بالقرصنة التي تُخترق فيها الحسابات الشخصية وتُسحب البيانات والصور والمعلومات الموجودة في حساب الضحية[٤].

ثانيا: صور الابتزاز الإلكتروني تتعدد صور الابتزاز الإلكتروني بحسب الغاية منه أو بحسب الضحية المراد ابتزازها ، وهو ما سنتولاه بالبيان الوجيز تباعا:

١– بحسب الغاية.

يختلف الهدف الذي يسعى المبتز إلى تحقيقه من جريمته باختلاف كل جريمة، فقد يكون الهدف لتحقيق منفعة مادية، وذلك بطلب مبالغ مالية أو عينية كي لا يقوم المبتز بنشر الأسرار التي لا يريد الضحية نشرها علنا ، وقد يكون الهدف من الابتزاز جنسيا وهو ما يبدو شائعا إن كانت الضحية امرأة أو حدث، ويتحقق هدف المبتز الجنسي حينما يكون المقابل الذي يطلبه لعدم إفشاء أسرار الضحية هو إما ممارسة الجنس بأشكاله مع الضحية والمبتز مباشرة ، أو للقيام بهذه الممارسات مع شخص آخر غيره ولمرة واحدة أو لمرات متعددة؛ كما قد يكون هذا الهدف نفعيا بقيامه بتهديد الضحية بإفشاء أسراره ونشرها إذا لم يقم بتحقيق طلب أو مصلحة للمبتز أو غيره، كطلب تنفيذ سرقة لصالح المبتز ، أو ترويج مخدرات، أو التوسط لدى شخص لإتمام عمل سواء كان هذا العمل مشروعاً أم غير مشروع [١].

٢– بحسب شخص الضحية.

ويكون للابتزاز أيضا صورا تبعاً لشخصية المجني عليه ، فهناك نوع من جرائم الابتزاز الإلكتروني تكون فيها الضحية **شخصية اعتبارية** من الحكومات والشركات والمؤسسات، وتتم عن طريق الحصول على معلومات سرية خاصة بالمؤسسة أو الشركة أو الوزارة عن طريق السطو على موقع الشخص المعنوي أو احد العاملين فيه ، والتهديد بالإعلان عن هذه المعلومات ونشرها ، أو قد تكون هذه الشخصية من **الأحداث** وهم الفئة من غير بالغي سن الرشد بحسب القانون، إذ يقوم المبتز بالضغط على الحدث بتهديده بنشر صور أو تسجيل مرئي أو محادثات على مواقع الدردشة، أو أية مادة، عن واقعة أو وقائع لا يريد الحدث اطلاع احد عليها؛ كما قد تكون الضحية من **النساء** وهي الصورة الأكثر شيوعا، سيما إذا كان المبتز رجلاً، فغالباً ما يكون تهديد المبتز للمرأة بنشر صور فاضحة أو محادثات خادشه للحياء، أو عرضاً مرئياً لعلاقة غير شرعية جمعت ما بين المبتز وضحيته، وقد بفضح أسرار عملها التجاري بسبب كونها سيدة أعمال أو بفضح محادثات سرية أو اتفاقات معينة كونها من المشتغلين بالسياسة مثلا، كما يكون **الرجل** عرضة لجرائم الابتزاز بسبب وجود أسرار في مجال عمله، أو عائلته أو مركزه الاجتماعي أو السياسي، ويكون الإفصاح عنها ونشرها ماساً بشرفه وسمعته أو يثير احتقاره في مجتمعه أو يؤثر سلبا في مركزه المالي [١].

ثالثا: خصائص جريمة الابتزاز الإلكتروني

جريمة الابتزاز الإلكتروني بعدّها أحد صور الجرائم الإلكترونية فإنها تتميز بما تتميز به هذه الجرائم من الخصائص التي تمنحها طابعا مختلفا عن غيرها من الجرائم التقليدية والتي يمكن إجمالها بإيجاز فيما يلي:

١– إنها ترتكب بواسطة شبكة الإنترنت وبوسائل تقنية المعلومات بمختلف أنواعها

٢- إنَّ مرتكب الجريمة غالبا ما يكون مجرم ذو خبرة في استخدام وسائل التقنية والشبكة المعلوماتية.

٣- إنها لا تحدّها حدود جغرافية ولا يحدها زمان معين، ما يجعلها من الجرائم العابرة للحدود التي تكتنفها الكثير من التحديات خاصة من حيث الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

٤- تتسم بالخطورة البالغة لما توفره الوسائل التقنية من سهولة في الاستخدام وسرعة في الانتشار إضافة إلى صعوبة معرفة الفاعل وصعوبة التحري والتحقيق والملاحقة ، فضلا عن سهولة إتلاف الأدلة من قبل الجناة.[٢]

الفرع الثاني: الجهود الدولية لمواجهة الابتزاز الإلكتروني

نظرا لما تمثله الجرائم الإلكترونية بصورها كافة من خطر كبير على الجوانب الاجتماعية والأمنية بل وحتى الاقتصادية والسياسية للدولة، فقد تكاتفت الجهود سواء على صعيد المنظمات الدولية أو الإقليمية من أجل الوصول إلى رؤى مشتركة لوضع آليات تعاون دولي لتصل في نهايتها إلى تشريعات عالمية أو اتفاقيات دولية عامة أو ثنائية من شأنها مكافحة هذه الجرائم، وقد عملت العديد من هذه المنظمات لوضع استراتيجيات لمكافحة جرائم الإنترنت بصورة عامة ومنها جريمة الابتزاز الإلكتروني بوصفها أحد أنواع الجرائم الإلكترونية التي تنتهك حرمة الحياة الخاصة، و من أبرز هذه المجموعات والمنظمات التي عملت في موضوع جرائم شبكة الإنترنت هي:

أولا: الجمعية العامة للأمم المتحدة

طلبت الجمعية العامة في قرارها ٢٣٠/٦٥ إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقاً للفقرة (٤٢) من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية :نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، فريق خبراء حكوميًّا دوليًّا مفتوح العضوية ينعقد قبل دورة اللجنة العشرين من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية والممارسات الفضلى والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين وقد اعتمد فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عُقد في فيينا في الفترة من ٢٧الى ٢٩ آذار/مارس ٢٠١٩ تقريره في جلسته السادسة المعقودة في ٢٩ آذار/مارس ٢٠١٩ المنشور بالوثيقة /UNODC/CCPCJ/EG.4/2019) الذي جاء بالعديد من التوصيات باتجاه مواجهة جزائية للجريمة الإلكترونية سواء بالاستمرار نحو تشريع صك دولي بهذا الشأن أو حث الدول الأعضاء على التعاون الدولي بشان هذه الجرائم وإصدار التشريعات اللازمة لذلك[١]. والجدير بالذكر أن منظمة الأمم المتحدة أصدرت العديد من القرارات لمكافحة الجريمة الإلكترونية وتأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية وتشارك وكالاتها في مختلف المفاوضات لإيجاد توافق دولي لوضع معايير توفير الحماية لشبكات الإنترنت ومستخدميها، ومن ابرز قرارات الجمعية العامة للأمم المتحدة في هذا المجال، القرارات ١٢١/٤٥ العام ١٩٩٠، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام ١٩٩٤و٧٠/٥٣ في ٤ كانون الأول/ديسمبر ١٩٩٨، و٤٩/٥٤ في ١ كانون الأول/ديسمبر ١٩٩٩، ٢٨/٥٥ في ٢٠ تشرين الثاني/نوفمبر ٢٠٠٠ و١٩/٥٦ في ٢٩ تشرين الثاني/نوفمبر ٢٠٠١ و٥٣/٥٧ في ٢٢ تشرين الثاني/نوفمبر ٢٠٠٢ و٣٢/٥٨ في ١٨ كانون الأول/ديسمبر ٢٠٠٣ حول موضوع «التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي» و ٦٣/٥٥ في ٤ كانون الأول/ديسمبر ٢٠٠٠، و١٢١/٥٦ في ١٩ كانون الأول/ديسمبر ٢٠٠١ بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية، و٢٣٩/٥٧ في ٢٠ كانون الأول/ديسمبر ٢٠٠٢ بشأن «إنشاء ثقافة عالمية للأمن السيبراني»، و ٢٣٩/٥٧ في ٣١ كانون الثاني/يناير ٢٠٠٣ و١٩٩/٥٨ في ٣٠ كانون الثاني/يناير ٢٠٠٤ بشأن «إنشاء ثقافة عالمية للأمن السيبراني»، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني[١].

ثانيا: مجموعة الدول الثماني:

إذ اعتمد وزراء العدل والداخلية فيها سياسات مكافحة العديد من جرائم الإنترنت تعتمد عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، والتنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، وتدريب المكلفين بتنفيذ القوانين وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية، وقد أصدرت المجموعة العديد من الوثائق في هذا المجال من بينها مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (١٩٩٧) ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (١٩٩٩) وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات

الإرهابية والإجرامية (٢٠٠٢) ومبادئ توافر البيانات الأساسية لحماية السلامة العامة (٢٠٠٢) وإعلان بيان دول الثمانية على نظم حماية المعلومات (٢٠٠٢)، إضافة إلى تشريع قوانين جزائية خاصة بالجرائم الإلكترونية[٢].

ثالثا- المجلس الأوروبي[٣]

إدراكا لأهمية إعادة النظر في الإجراءات الجزائية في مجال تكنولوجيا الكمبيوتر والإنترنت أصدر المجلس الأوروبي التوصية رقم ٩٥/١٣ في ١٩٩٥/٩/١١ في شأن مشاكل الإجراءات الجزائية المتعلقة بهذا المجال، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لوضع النصوص الكفيلة بمعالجة خصوصية الجرائم الإلكترونية، ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي:

١- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها، وأن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش بضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محلا للتفتيش مع بيان المعلومات التي تم ضبطها، وأن يُسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط و التفتيش، وأن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط أن يكون هذا الإجراء ضروريا.

٢- أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر، وأن تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية و الاحترام للمعلومات التي يفرض القانون لها حماية خاصة، مع وجوب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة و التسجيل.

٣- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة، و إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ الازم للسماح لرجال التحقيق بالاطلاع عليها. وأن تخول سلطات التحقيق بإصدار أوامر مماثلة لأي شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

٤- يجب تطوير و توحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

٥- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

٦- قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات.

٧- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط. ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدها ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة[١].

رابعا: مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية [١]

ناقش المؤتمر في جلسته المنعقدة في البرازيل من ١٢-١٩-٢٠١٠، وفي البند (٨) من جدول الأعمال المؤقت التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية وقد توصل إلى جملة من الاستنتاجات من بينها تلك المتعلقة بالجرائم الإلكترونية فقد نصت التوصية رقم (٤٥) على إن (التحقيق في الجرائم الحاسوبية وملاحقة مرتكبيها قضائيًا يعدّان مصدر تحد لجميع المؤسسات المعنية بهما، ومع مراعاة تعقُّد المسألة والتطور التقني المطَّرد، يبقى التدريب المستدام والمتسع دائما مسألة رئيسية لجميع السلطات المعنية . وقد بينت المناقشة التي جرت في اجتماع فريق الخبراء الذي عقده المكتب المعني بالمخدرات والجريمة عام ٢٠٠٩ بشأن الجريمة الحاسوبية أ ن بناء القدرات المؤسسية واستدامتها البعيدة المدى هما عاملان رئيسيان لقياس

نجاح المبادرات المستقبلية)كما نص في التوصية رقم (٤٦) على (وللقضاء على الملاذات الآمنة وتحسين التعاون الدولي، ينبغي إيلاء الاهتمام لسد الثغرات في التشريعات القائمة، وتعزيز اتساق القوانين وتماسكها وتوافقها. ومع أخذ أهمية مواءمة التشريعات في الحسبان، والاستفادة من نتائج الاجتماعات التحضيرية لمؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، ينبغي النظر في وضع اتفاقية عالمية لمكافحة الجريمة الحاسوبية بعين التأني والقبول)، وقد أشار في التوصيتين (٤٧ و٤٨) إلى ما سيوفره المكتب المعني بالمخدرات والجريمة، بصفته جهة تعنى بوضع المعايير في مسائل منع الجريمة والعدالة الجنائية، من الخبرات الفنية القانونية والتقنية والمتعلقة بإنفاذ القانون، لمكافحة الأنشطة الإجرامية، وذلك إلى جانب الخبرات الفنية المحددة والمتطورة لدى الشركاء الرئيسيين، المنخرطين بالفعل في مكافحة الجريمة الحاسوبية، ويستهدف المكتب الشراكة بالأدوات والخبرات وتجميعها معًا، بما في ذلك من القطاع الخاص (ولا سيما من مزودي خدمة الإنترنت)، لمعالجة المشكلة في بلد معين أو منطقة معينة. وسيستهدف المكتب المعني بالمخدرات والجريمة تحديدًا القيام بمساعدة الدول الأعضاء في اعتماد تشريعات للتحقيق الفعال في الجرائم المتعلقة بالحاسوب وملاحقة الجناة قضائيًا ؛ وبناء المعرفة التشغيلية والتقنية للقضاة والمدعين العامين وضباط إنفاذ القانون، بشأن المسائل المتعلقة بالجريمة الحاسوبية، من خلال التدريب وتكييف/تطوير المواد التدريبية بشأن التحقيق في الجرائم المتعلقة بالحاسوب، وما شابهها، ومقاضاة مرتكبيها وتدريب سلطات إنفاذ القانون لكي تستخدم بفعالية آليات التعاون الدولي لمكافحة الجريمة الحاسوبية؛ ورفع مستوى الوعي لدى المجتمع المدني وإيجاد قوة دفع لدى متخذي القرارات لتوحيد الجهود لمنع الجريمة الحاسوبية ومكافحتها؛ واستبانة الممارسات الجيدة وتعميمها، وتعزيز الشراكات بين القطاعين العام والخاص في مجال منع الجريمة الحاسوبية ومكافحتها.

خامسا: اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة ٢٠٠١

إن الدول الأعضاء في مجلس أوروبا وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية؛ واقتناعا منها بالحاجة إلى إتباع سياسة جنائية مشتركة، كمسألة ذات أولوية، بهدف حماية المجتمع من الجريمة الإلكترونية، من خلال تبني تشريع ملائم ودعم التعاون الدولي ، فقد تبنت هذه الاتفاقية التي، وبعد أن حددت في الفصل الأول والثاني والثالث والرابع الجرائم محل الاتفاقية وذلك في المواد (٢-١٠) من الاتفاقية وما يتعلق بالمحاولة، والمساعدة والتحريض، في المادة(١١) منها، بينت في القسم الثاني الأحكام الإجرائية الواجب اتباعها سواء بالنسبة إلى الجرائم الجنائية المقررة في المواد من ٢ إلى ١١ من الاتفاقية أو الجرائم الجنائية الأخرى التي يتم ارتكابها بواسطة نظام الكومبيوتر أو ما يتعلق بجمع الأدلة الخاصة بجريمة جنائية بشكل إلكتروني (المادة ١٤) ، وذلك بما يتعلق بأحكام التعجيل في حفظ بيانات الكومبيوتر المخزنة والتعجيل في حفظ بيانات الكومبيوتر والكشف الجزئي عن بيانات الحركة الأمر بإبراز البيانات و البحث عن بيانات الكومبيوتر المخزنة ومصادرتها وجمع بيانات الكومبيوتر في الوقت الحقيقي واعتراض بيانات المحتوى والولاية القضائية(المواد ١٦-٢٢)؛ كما بينت ما يتعلق بالتعاون الدولي من خلال تطبيق الصكوك الدولية ذات الصلة والخاصة بالتعاون الدولي في المسائل الجنائية وبالترتيبات المتفق عليها بمقتضى التشريعات الموحدة أو ذات الصلة بالمعاملة بالمثل والقوانين الوطنية، على أوسع نطاق ممكن لأغراض إجراءات التحقيقات أو المتابعات التي تتعلق بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر، أو من أجل جمع أدلة بشأن جريمة جنائية في شكل إلكتروني وما يتعلق بتسليم المجرمين والمساعدة المتبادلة بشان التحقيقات والتدابير المؤقتة (المواد ٢٣-٣٥)[1]

سادسا: اللجنة الاقتصادية والاجتماعية لغربي آسيا(الإسكوا)

وبهدف المساهمة في تطوير البيئة التمكينية لبناء مجتمع المعرفة في المنطقة العربية، أعدت اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) إرشادات الإسكوا للتشريعات السيبرانية التي تغطي ستة محاور أساسية هي :الاتصالات الإلكترونية وحرية التعبير، والمعاملات الإلكترونية والتوقيع الإلكتروني، والتجارة الإلكترونية وحماية المستهلك، ومعالجة البيانات ذات الطابع الشخصي، والجرائم السيبرانية، والملكية الفكرية في المجال المعلوماتي والسيبراني. وقد جاء إعداد هذه الإرشادات لجسر الثغرة القانونية الموجودة في دول المنطقة في مجال التشريعات السيبرانية، وقد تضمنت هذه الإرشادات نصوصا مقترحة لجملة من الجرائم التي عالجت فيها حماية الخصوصية مثل المادة(١٢) التي حددت جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها ، ونصت على (كل من أقدم عن قصد ودون سبب مشروع على الاطلاع بوسائل معلوماتية على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية .يجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة؛ وما ورد في الباب الثامن من هذه الإرشادات التي عالجت الجرائم التي تمسّ المعلومات الشخصية إذ نصت المادة(٣٠) على(كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص مسبق يتيح له القيام بمثل هذه المعالجة من المراجع الرسمية) والمادة (٣١) التي نصت على(كل من أقدم عن قصد على معالجة معلومات ذات طابع

شخصي دون التقيد بالقواعد القانونية المقررة لمعالجة المعلومات ذات الطابع الشخصي) وكذلك المادة (٣٢) حيث نصت على(كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات طابع شخصي، لأشخاص لا يحق لهم الاطلاع عليها). وقد بينت الإرشادات في الباب الثالث عشر منها العقوبات إذ نصت المادة(٥٢)على أن (يُعاقب كل من يرتكب إحدى الجرائم المحددة في هذا الإرشاد بعقوبة السجن وبالغرامة أو بإحدى هاتين العقوبتين. يُترك للدولة المعنية تحديد مدة عقوبة السجن وقيمة الغرامة بحدّيها الأدنى والأعلى)، وكذلك ما نصت عليه المادة (٥٣) بالقول(تُصادر الأجهزة الإلكترونية وخلافها التي استعملت في ارتكاب الجرم) وأيضا ما نصت عليه المادة(٥٤) من أن (تُشدد العقوبة في حال التكرار وفقاً للقواعد العامة المنصوص عليها في قوانين الجزاء، ويتم إبعاد الأجنبي لارتكابه إحدى هذه الجرائم).فضلا عن إن هذه الإرشادات قد أوردت جملة من المصطلحات لتمكين المشرعين من اعتماد مفاهيمها عند إصدار تشريعات مكافحة الجرائم الإلكترونية ومنها:

١- جريمة سيبرانية (cyber crime) يقصد بها أي فعل جرمي أو عمل غير مشروع يستعمل أياً من أدوات وخدمات شبكة الإنترنت مثل غرف المحادثة، المواقع الإلكترونية، الرسائل الإلكترونية الخ.. لارتكاب أعمال غش أو احتيال تطال مالاً معيناً أو تتعرض لشخص ما معنوياً أو مادياً أو تخرب أجهزة أو شبكات أو برامج حاسوب. يدخل ضمنها إرسال الفيروسات وإرسال البريد غير المرغوب به والإباحية لدى الأطفال.

٢- جرم معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص

personal data processing without a license

يقصد به كل من أقدم عن قصد على معالجة معلومات ذات طابع شخصي دون حيازة تصريح أو ترخيص مسبق يتيح له القيام بمثل هذه المعالجة من الجهات الرسمية.

٣- جرم إفشاء معلومات ذات طابع شخصيdissemination of personal data ،يقصد به كل من أقدم، عن قصد أو عن إهمال، على إفشاء معلومات ذات طابع شخصي، لأشخاص لا يحق لهم الاطلاع عليها.

٤- جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها viewing and/or disseminating secret or sensitive data ، ويقصد به كل من أقدم عن قصد ودون سبب مشروع على الاطلاع بوسائل معلوماتية على معلومات سرية أو حساسة أو على إفشاء مثل هذه المعلومات بوسائل معلوماتية. يجوز اشتراط أن يؤدي الفعل إلى إلحاق الضرر بالغير أو بصاحب العلاقة.

٥- بيانات شخصية personal data وهي أي بيانات تتعلق بشخص معروف أو قابل للتعريف مباشرة أو غير مباشرة لا سيما عبر رقم تعريف أو غير ذلك من الميزات الشخصية، الجسدية ، العقلية، الاقتصادية الثقافية أو الهوية الاجتماعية أو عبر البيانات المحفوظة لدى المراقب.

٦- بيانات شخصية حساسةsensitive personal data، هي بيانات شخصية تتعلق بشكل مباشر أو غير مباشر بمعلومات عن الشخص من ناحية العرق، الآراء السياسية، المعتقدات الدينية أو ما شابه، صحته أو حالته الجسدية أو العقلية، وحياته الجنسية، وسجله العدلي[١].

سابعا: جامعة الدول العربية

أصدرت جامعة الدول العربية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢٠١٠/١٢/٢١، وقد الزمت بموجب المادة الخامسة منها الدول الموقعة بتجريم الأفعال الواردة في الاتفاقية ومن بينها ما ورد في المادة الرابعة عشرة وهي **جريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات**[٢]، والتي بلا شك يمثل الابتزاز الإلكتروني أحد صورها.

ثامنا: شرطة الويب الدولية [١]

أنشئت هذه المنظمة في الولايات المتحدة الأمريكية عام ١٩٨٦ وهي تتلقى الشكاوى من مستخدمي شبكة الإنترنيت وتقوم بملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة التي تثبت جرائمهم بغية تقديمهم للمحاكمة، ويعمل في هذه المنظمة العديد من المتخصصين من هيئات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة ومتطوعين فنيين من (٦١) دولة حول العالم، مهماتهم تتبع الأنشطة الإجرامية التي ترتكب من خلال شبكة الإنترنت على مستوى العالم.[٢]

المطلب الثاني مواجهة الابتزاز الإلكتروني في التشريعات الجنائية

لاشك في أن التشريعات الجنائية ما برحت تواكب التطورات المتسارعة لأنظمة التكنلوجيا لما يمكن أن توفره من وسائل قد يستغلها المجرم في تنفيذ مشروعه الإجرامي، وقد عمدت غالبية الدول إلى إصدار تشريعات خاصة بالجرائم الإلكترونية لتلائم خصوصية هذه الجرائم، ولان جريمة الابتزاز الإلكتروني مرتبطة في كثير من جوانبها بالعادات والتقاليد والبنية الثقافية والدينية للمجتمعات، وللتقارب الكبير بين المجتمعات العربية ، فسيتم بحث موقف التشريعات الجنائية العربية لمواجهتها إضافة إلى موقف المشرع العراقي من ذلك، وذلك في فرعين وكما يلي:

الفرع الأول: موقف التشريعات الجنائية العربية

أصدرت العديد من الدول العربية تشريعات جزائية خاصة بجرائم تقنية المعلومات ومنها ما نص صراحة على جريمة الابتزاز الإلكتروني ومنها ما أوجد معالجة خاصة، وهو الأمر الذي سنتولى بيانه بإيجاز فيما يلي:

أولا: في قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم(٥) لسنة ٢٠١٢ المعدل بالمرسوم بقانون اتحادي رقم (٢) تاريخ ٢٠١٨/٠٧/٢٤

صدر المرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الذي الغى القانون الاتحادي الإماراتي رقم(٢) لسنة ٢٠٠٦، فبعد أن عرّف وسيلة تقنية المعلومات في المادة(١) بانها (أي أداة الكرتونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين، حدد صراحة عقوبة ابتزاز أو تهديد شخص للقيام بفعل أو الامتناع عنه باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات وذلك في المادة (١٦) منه بالنص على أن (يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون الف درهم ولا تجاوز خمسمائة الف 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 اذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار).**

كما حدد في المادة (٢٠) عقوبة سبّ الغير وجعله محلاً للعقاب أو الازدراء من قبل الآخرين باستخدام شبكة معلوماتية أو وسيلة تقنية المعلومات بالنص على انه(مع عدم الإخلال بأحكام جريمة القذف المقررة في الشريعة الإسلامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين الف درهم ولا تجاوز خمسمائة الف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلا للعقاب أو الازدراء من قبل الآخرين، وذلك باستخدام شبكة معلوماتية، أو وسيلة تقنية معلومات. فإذا وقع السب أو القذف في حق موظف عام أو مكلف بخدمة عامة بمناسبة أو بسبب تأدية عمله عد ذلك ظرفا مشددا للجريمة) كما بينت المادة (٢١)عقوبة الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا باستخدامه شبكة معلوماتية أو نظام معلومات الكتروني أو احدى وسائل تقنية المعلومات بالقول(يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة الف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في **الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا** بإحدى الطرق التالية:

١- استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية.

٢- التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها.

٣- نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية.

كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة الف درهم أو بإحدى هاتين العقوبتين، **كل من استخدم نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها).**

وحددت المادة (٢٢) عقوبة استخدام شبكة معلوماتية أو موقعا الكترونيا أو وسيلة تقنية المعلومات بدون تصريح لكشف معلومات سرية، بنصها على أن (يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استخدم، بدون تصريح، أي شبكة معلوماتية، أو موقعا إلكترونيا، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه).وقد نصت المادة (٤٠) على عقوبة الشروع في الجريمة بنصها على أن (يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة).كما قضت المادة(٤٢) بإبعاد الأجنبي المحكوم عليه في

الجرائم الواقعة على العرض أو بعقوبة الجناية في جرائم هذا المرسوم بقانون بقولها(مع مراعاة حكم الفقرة الثانية من المادة (١٢١) من قانون العقوبات تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها) وحكمت المادة(٤٣) بوضع المحكوم عليه تحت الإشراف أو المراقبة أو الحرمان من استخدام شبكة معلوماتية أو نظام المعلومات الإلكتروني أو وسيلة تقنية المعلومات بالنص على انه (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).ولاستيعاب خطر جرائم المعلوماتية فقد نصت المادة(٤٦) على أن (يعد ظرفاً مشدداً استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع الكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم بقانون)[١].وواضح من هذا النص أن المشرع قد راعى خطورة وسائل تقنية المعلومات فضلا عن ما يمكن أن يشكله ارتكاب الجرائم بوساطتها من ملابسات قانونية.

ثانيا: في قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات المصري

في اطار مواجهته الجزائية لجرائم تقنية المعلومات وخاصة فيما يتعلق بمشكلة حجية الأدلة الرقمية في الإثبات الجنائي فقد نص المشرع المصري في المادة(١١) من القانون رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات على أن (يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإلكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون) كما نص في الفصل الثالث من القانون على الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع ومنها ما يشكل جريمة الابتزاز الإلكتروني بعدّها من الجرائم التي تنتهك حرمة الحياة الخاصة، فقد نصت المادة(٢٥) على أن (يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو **انتهك حرمة الحياة الخاصة** أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته, أو **نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة**)كما نصت المادة(٢٦) على أن (يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة, أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه. كما تجدر الإشارة إلى انه قد **اخرج جريمة الابتزاز من الجرائم التي يجوز الصلح فيها** والتي حددتها المادة(٤٢) التي نصت على(يجوز للمتهم في أية حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتا، إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك في الجنح المنصوص عليها في المواد (١٤، ١٥، ١٦،١٧،١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) من هذا القانون؛ولا يُنتج إقرار المجنى عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد (١٤، ١٧، ١٨، ٢٣) من هذا القانون كما لا يُقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين (٢٩، ٣٥) من هذا القانون ، وواضح أن نص المادة (٢٥) المذكورة ليس من بينها. يذكر أن المادة (٣٩) من القانون أعطت للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتا من وظيفته، كما قضت المادة (٤٠)بان يعاقب كل من شرع في ارتكاب الجرائم المنصوص عليها بالقانون، يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة، وقررت المادة(٤١) بان يعفى من العقوبات، المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها، إذا مكن الجاني أو الشريك في أثناء التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال

موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثله لهذا النوع والخطورة ولا يخل حكم هذه المادة، بوجوب الحكم برد المال المتحصل من الجرائم المنصوص عليها بالقانون[١]

ثالثا: نظام مكافحة جرائم المعلوماتية السعودي

أصدر المشرع السعودي بالمرسوم الملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ نظام مكافحة جرائم المعلوماتية وقد أورد الابتزاز الإلكتروني صراحة في نصوصه فقد نصت المادة الثالثة منه على أن (يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

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

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

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

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

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

رابعا: قانون مكافحة جرائم تقنية المعلومات العماني

جاء المرسوم السلطاني رقم (12 /2011) بإصدار قانون مكافحة جرائم تقنية المعلومات، وقد نص في المادة (16) منه على (يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على خمسة آلاف ريال عماني أو بإحدى هاتين العقوبتين ، **كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات كالهواتف النقالة المزودة بآلة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بالتقاط صور أو نشر أخبار أو تسجيلات صوتية أو مرئية تتصل بها ولو كانت صحيحة أو في التعدي على الغير بالسب أو القذف)** ، كما نصت المادة(١٧) على(يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين ، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في المقامرة أو في إنتاج أو نشر أو توزيع أو شراء أو حيازة كل ما من شأنه المساس أو الإخلال بالآداب العامة أو في الترويج لبرامج أو أفكار أو أنشطة من شأنها ذلك) وأيضا ما نصت عليه المادة(١٨) بقولها(يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين 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 مشروعا** ، وتكون العقوبة السجن المؤقت مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على عشرة آلاف ريال عماني إذا كان التهديد بارتكاب جناية أو إسناد أمور مخلة بال شرف أو الاعت [١]

خامسا: قانون جرائم أنظمة المعلومات الأردني لسنة2010

وحسما لأي إشكال قانوني بشأن استخدام تقنية المعلومات في أية جريمة نص المشرع الأردني في المادة(14) من قانون جرائم أنظمة المعلومات الأردني لسنة ٢٠١٠ على أن(كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو أشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع).[٢] ويلاحظ على النصوص التي أدرجتها هذه التشريعات أنها راعت في لفظها العموم الذي تستجوبه الوسائل التي يمكن أن يستخدمها الجناة في الابتزاز فهي دائما ما تذكر عبارة (وسائل تقنية المعلومات) وهو الأمر الذي ندعو المشرع العراقي إلى الالتفات له، في الوقت الذي ندعوها إلى التركيز على ما يتعلق بوسائل الإثبات الرقمية وإيراد نصوص خاصة بها تعالج إشكاليات الإثبات الرقمي مستفيدة من الجهود الدولية بهذا المجال.

الفرع الثاني: موقف التشريع الجنائي العراقي من الابتزاز الإلكتروني

سنحاول تلمس موقف المشرع الجنائي العراقي من الابتزاز الإلكتروني من حيث معالجته للجرائم في بيئة التقنيات العالية و في اطار النصوص التقليدية، وكما يلي:

أولا: موقف المشرع العراقي من مكافحة جرائم تقنية المعلومات

لم يكن المشرع العراقي بعيدا عن مواكبة التطورات المتسارعة في عالم تقنية المعلومات، فقد **صدّق الاتفاقية العربية لمكافحة جرائم التقنية** بالقانون رقم(٣١) لسنة ٢٠١٣ والتي نصت في المادة الرابعة عشرة منها على إن الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات تعد جريمة، والزمت الدولة الطرف بتجريمها وفقا لتشريعاتها وأنظمتها الداخلية وذلك بموجب المادة الخامسة من الاتفاقية[٣]، وقبلها ناقش **مشروع قانون جرائم المعلوماتية** في عام ٢٠١١ وقد تمت قراءته قراءة أولى في مجلس النواب إلا أنه لازال قيد التشريع كحال مشاريع القوانين الأخرى بسبب التجاذب والاختلاف السياسي الذي طال كل شيء؛وعلى أية حال فقد نصت المادة (٢) من مشروع قانون جرائم المعلوماتية بان(يهدف هذا القانون إلى توفير الحماية القانونية للاستخدام المشروع للحاسوب وشبكة المعلومات، ومعاقبة مرتكبي الأفعال التي تشكل اعتداء على حقوق مستخدميها من الأشخاص الطبيعية أو المعنوية ومنع إساءة استخدامه في ارتكاب جرائم الحاسوب)؛كما بيَّنت **المادة(١١)** منه المعالجة التشريعية **لجريمة الابتزاز الإلكتروني** بصورة صريحة بنصها على أن (أولا- يعاقب بالسجن مدة لا تزيد على (٧) سبع سنوات وبغرامة لا تقل عن (٣٠٠٠٠٠٠) ثلاثة ملايين دينار ولا تزيد على (٥٠٠٠٠٠٠) خمسة ملايين دينار كل من: أ- هدد آخر باستخدام أجهزة الحاسوب وشبكة المعلومات بارتكاب جناية ضد نفسه أو ماله أو نفس الغير أو ماله بقصد ترويعه أو من اجل دفعه إلى القيام بعمل أو الامتناع عنه.

ب-**ارسل أو نقل أية رسالة أو خبر أو وثيقة الكرتونية عبر أجهزة الحاسوب أو شبكة المعلومات مع علم ينطوي على تهديد أو ابتزاز لشخص بقصد ترويعه أو من اجل دفعه إلى القيام بفعل أو الامتناع عنه.**

ثانيا-يعاقب بالحبس وبغرامة لا تقل عن (٢٠٠٠٠٠٠) مليوني دينار ولا تزيد على(٤٠٠٠٠٠٠) أربعة ملايين دينار **كل من هدد آخر باستخدام أجهزة الحاسوب وشبكة المعلومات في غير الحالات المنصوص عليها في البند (أولا) من هذه المادة)**،

ومن تحليل نص الفقرة(أولا-ب) من المادة(١١) من المشروع يمكن ملاحظة ما يلي:

١- إن طبيعة الفعل الذي تقوم به هذه الجريمة يتخذ صورة الإرسال أو النقل دون أن يُشترط تحقق العلانية من الإرسال أو النقل من عدمه.

٢- أن ينطوي فعل الإرسال أو النقل - بالإضافة إلى كونهما إراديان- على علم خاص هو التهديد أو الابتزاز بمعنى أن يكون الإرسال أو النقل لتهديد أو ابتزاز شخص؛ ويلاحظ إنَّ المشرع قد مايز بين التهديد والابتزاز من حيث اللفظ فقط، إذ أن التهديد يتحقق بالوعيد والتخويف بأن ضررا ما سيلحق بالشخص أو بالأشخاص أو الأشياء ذات الصلة بهم، يطلقه الجاني معتقدا بأن ذلك يؤدي إلى الضغط على إرادة من وُجِّه إليه ليتفادى هذا الضرر وهو ما يعرف بالعنف المعنوي والذي يتفق مع الإكراه المعنوي[١]، ويكون ذلك إما بقصد الترويع أو من أجل دفع شخص ما إلى القيام بفعل أو الامتناع عن فعل، وهو ما يمكن أن يتحقق به الابتزاز أيضا وذلك ما يجعلهما على وفق هذه الصيغة مترادفان.

٣- حدد واسطة الفعل أو شكله وهي أجهزة الحاسوب أو شبكة المعلومات، ونرى أن يكون التعبير (بأية وسيلة من وسائل تقنية المعلومات) ليضم جميع الوسائل التقنية دون الاقتصار على الحاسوب أو الشبكة.

٤- حدد محل الفعل(محتواه) وهو رسالة أو خبر أو وثيقة الكترونية، وقد ورد اللفظ عاما دون أن يحدد المشرع أن يكون هذا المحتوى سريا أو خادشا للشرف أو الاعتبار من عدمه.كما وقد حدد في المواد(٢٤-٢٦) إجراءات جمع الأدلة والتحقيق والمحاكمة، و نص في المادة(٢٧) على تطبيق العقوبات الأشد في القوانين الأخرى، وعلى تطبيق أحكام قانون العقوبات وقانون أصول المحاكمات الجزائية في كل ما لم يرد به نص فيه وذلك ما وردة في المادة(٣٠) من مشروع القانون[٢]. وللانتقادات التي وجهت لهذا المشروع تم نشر صيغة أخرى لمشروع قانون حمل اسم (قانون مكافحة الجرائم الإلكترونية)[٣]، وفي هذه النصوص تم تعريف الجريمة الإلكترونية في الفقرة (أولا) من المادة(١) من المشروع بالنص على أنها(هي كل فعل يرتكب باستعمال الحاسب الآلي أو شبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات , معاقب عليها وفق أحكام هذا القانون)؛كما نصت المادة (٦) من المشروع الجديد وتحت عنوان جرائم التهديد والابتزاز على أن (يعاقب بالحبس مدة لا تقل عن ثلاث سنوات ولا تزيد على خمس سنوات وبغرامة لا تقل عن (٥٠٠٠٠٠٠) خمسة ملايين دينار عراقي ولا تزيد على (١٠٠٠٠٠٠٠) عشرة ملايين دينار عراقي كل من استخدم شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد تهديد أو ابتزاز شخص آخر لحملة على القيام بفعل أو الامتناع عنه ولوكان هذا الفعل أو الامتناع مشروعاً).ويلاحظ أن هذا النص يحمل تطورا عن نص المشروع السابق إذ ساوى في الابتزاز بين حمل الضحية على القيام بفعل أو الامتناع عنه سواء أكان ذلك الفعل أو الامتناع غير مشروع أم مشروع، إضافة إلى انه لم يقصر الاستخدام على شبكة المعلومات أو أجهزة الحاسوب وإنما استخدم عبارة (وما في حكمها) وهو امر جيد وان كان الأفضل -كما يرى

الباحث– استخدام العبارة الشائعة وهي (أو أية وسيلة من وسائل تقنية المعلومات).كما نص في الفصل الثالث وفي المواد (٩–١٥) من المشروع على إجراءات جمع الأدلة والتحقيق والمحاكمة، إضافة إلى ما بينته المادة (١٦) من أحكام المساهمة الجنائية في الجريمة بنصها على أن (أولاً– يعد مرتكباً جريمة التحريض كل من حرض أو ساعد أو اتفق أو اشترك مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون فأن لم تقع الجريمة عوقب بنصف العقوبة المقررة لها قانونا. ثانياً– اذا وقعت الجريمة نتيجةً لذلك التحريض يعاقب المحرض بذات العقوبة المقررة لها)، ويلاحظ أن النص قد اطلق وصف جريمة التحريض على أفعال الاشتراك الجرمي، إضافة إلى استخدامه عبارة (من اشترك مع الغير)، وهو الأمر الذي لا ينسجم تارة مع ما جاءت به المادة (٤٨) من قانون العقوبات التي حددت صور المساهمة التبعية في الجريمة بنصها على انه(يعد شريكا في الجريمة: ١ – من حرض على ارتكابها فوقعت بناء على هذا التحريض.٢ – من اتفق على غيره على ارتكابها فوقعت بناء على هذا الاتفاق. ٣ – من أعطى الفاعل سلاحا أو آلات أو أي شيء آخر مما استعمل في ارتكاب الجريمة مع علمه بها أو ساعده عمدا بأي طريقة أخرى في الأعمال المجهزة أو المسهلة او المتممة لارتكابها)، وتارة أخرى لا ينسجم مع ما حددته المادة (٤٧) من قانون العقوبات لصور الفاعل في الجريمة إذ أن أحد صور فاعل الجريمة هي (مَن ارتكبها وحده أو مع غيره) فإن كان قصد المشرع من عبارة (اشترك مع الغير) في ارتكاب الجريمة فانه يعد فاعلا لا شريكا، وهو ما يتطلب إعادة صياغة لهذه المادة، مع الإبقاء على حكم معاقبة المحرض حتى لو لم تقع الجريمة.تجدر الإشارة إلى التفاتة جيدة من المشرع فيما يخص الأدلة الرقمية إذ نصت المادة (٢١) من المشروععلى (أولا– ينشأ بموجب أحكام هذا القانون المركز الوطني للأدلة الرقمية. ثانياً– يحدد بنظام صادر عن مجلس الوزراء آلية تشكيل المركز الوطني للأدلة الرقمية ومهامه خلال ستة اشهر من تاريخ نشر هذا القانون في الجريدة الرسمية. ثالثاً– تعد التقارير الصادرة عن المركز الوطني للأدلة الرقمية من وسائل الإثبات الرسمية التي تعتمدها المحاكم الجزائية عند النظر بالدعوى المتعلقة بالجرائم الإلكترونية) ، ولاشك في أن ذلك سوف يساعد كثيرا في إثبات الجرائم الإلكترونية[1].

ثانيا: مواجهة الابتزاز الإلكتروني في ضوء أحكام قانون العقوبات رقم(١١١) لسنة ١٩٦٩المعدل النافذ

رأينا فيما سبق من البحث، إن فعل الابتزاز الإلكتروني هو الضغط الذي يباشره شخص ما بواسطة وسائل تقنية المعلومات على إرادة شخص آخر لحمله على القيام بعمل أو الامتناع عن عمل وذلك بتهديده بإسناد أو إفشاء أية بيانات أو معلومات سرية خادشة للشرف أو الاعتبار تتعلق به أو بغيره ممن يؤثر عليه، وبذلك فهو يتحقق بسلوك إيجابي من خلال الطلب من الضحية القيام بعمل أو الامتناع عنه، عن طريق تهديده بنشر بيانات أو معلومات لا يريد إعلانها كونها تفشي سرا من أسراره يمكن أن تخدش شرفه أو اعتباره، وهو والأمر كذلك يُعَّد من أفعال الإكراه المعنوي الذي يتجلى بالضغط على إرادة المجني عليه لحمله على إتيان عمل ما أو الامتناع عنه رغما عن إرادته؛ فما حكم الابتزاز الإلكتروني في ضوء نصوص قانون العقوبات رقم (١١١) لسنة ١٩٦٩ المعدل؟وللإجابة على ذلك نجد أن المشرع العراقي قد عالج في الباب الثاني من قانون العقوبات النافذ تحت عنوان الجرائم الماسة بحرية الإنسان وحرمته العديد من الجرائم ومنها جرائم التهديد، وإنَّ فعل الابتزاز –على وفق هذا القانون – يمكن أن ينطبق مع نموذج التجريم الوارد بنص المادة (١/٤٣٠) عقوبات اذا ما تم بالتهديد بإسناد أمور مخدشة بالشرف أو إفشائها متى كان مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل أو مقصود به ذلك، وهو ما نصت عليه هذه المادة بالقول(١ – 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 أو مقصودا به ذلك.** ٢ – ويعاقب بالعقوبة ذاتها اذا كان التهديد في خطاب خال من اسم مرسله أو كان منسوبا صدوره إلى جماعة سرية موجودة أو مزعومة)؛ كما يلاحظ أيضا أن المشرع العراقي قد عالج جريمة التهديد بإسناد أمور مخدشة بالشرف أو إفشائها حتى وإن لم يصاحبه أي طلب أو تكليف بأمر أو الامتناع عن فعل فانه يكون معاقبا بموجب المادة (٤٣١) عقوبات التي نصت على (يعاقب بالحبس كل من هدد اخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره أو بإسناد أمور خادشة للشرف أو الاعتبار أو إفشائها بغير الحالات المبينة في المادة ٤٣٠).

أما اذا كان هذا التهديد بالقول أو الفعل أو الإشارة كتابة أو شفاها أو بواسطة شخص اخر في غير الحالات الواردة بالمادتين (٤٣٠–٤٣١) عقوبات، بمعنى اذا كان التهديد بإسناد أمور سرية ولكن ليس من شأنها خدش الشرف أو الاعتبار، لو غير مصحوبة بطلب عمل أو الامتناع عنه فان ذلك يعد جنحة يعاقب عليها بالحبس أو الغرامة على وفق المادة(٤٣٢) عقوبات التي نصت على أن (كل من هدد آخر بالقول أو الفعل أو الإشارة كتابة أو شفاها أو بواسطة شخص اخر في غير الحالات المبينة في المادتين ٤٣٠ و٤٣١ يعاقب بالحبس مدة لا تزيد على سنة واحدة أو بغرامة لا تزيد على مائة دينار)؛ تجدر الإشارة أيضا إلى انه اذا تضمَّن فعل الابتزاز ما يمكن أن يُعَّد قذفا عند إسناد

واقعة معينة إلى الغير بإحدى طرق العلانية من شأنها لو صحت أن توجب عقاب من أسندت اليه أو احتقاره عند أهل وطنه، فنكون أمام نموذج التجريم الوارد بنص المادة(٤٣٣) عقوبات التي عاقبت من قذف غيره بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، أو إفشاء للسر بحسب نموذج التجريم الوارد بنص المادة (٤٣٨)عقوبات عند نشر بإحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة اذا كان من شان نشرها الإساءة اليهم، وعاقبت على ذلك بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائة دينار أو بإحدى هاتين العقوبتين، ويتحقق عند ذلك ما يُعرف **بالتعدد المعنوي للجرائم** الذي يتم بموجبة فرض العقوبة الأشد وهو ما نصت عليه المادة(١٤١) بقولها(اذا كون الفعل الواحد جرائم متعددة وجب اعتبار الجريمة التي عقوبتها اشد والحكم بالعقوبة المقررة لها واذا كانت العقوبات متماثلة حكم بإحداها). وقد يقع فعل الابتزاز تحت طائلة التكييف القانوني لنموذج التجريم الوارد بنص المادة (٤٥١) عقوبات اذا تمخض عن التهديد اغتصاب سندا أو محررا أو توقيعا أو ختما أو بصمة إبهام أو الغاء شيء من ذلك أو إتلافه أو تعديله أو على التوقيع على بياض، إذ تكون العقوبة بالسجن مدة لا تزيد على خمس عشرة سنة، أو تحت طائلة نموذج التجريم الوارد في المادة(٤٥٢) عقوبات، اذا كان حمل الآخر بطريق التهديد على تسليم نقود أو أشياء أخرى غير ما ذكر في المادة (٤٥١) ، وتكون العقوبة بالسجن مدة لا تزيد على عشر سنين أو بالحبس[1]. وكل ذلك بحسب الأحوال التي يقع فيها فعل التهديد الذي يقدره القاضي الجنائي من خلال الوقائع المعروضة عليه، وقد اتخذت السلطات العراقية جملة من الإجراءات المتعلقة بالجرائم الإلكترونية من حيث إجراءات التحقيق أو الإثبات.

كما تجدر الإشارة إلى إمكانية شمول هذه الجريمة بالأحكام الآتية:

١- ينمُّ فعل الابتزاز عن **دناءة فاعله:** إذ إن فعل الابتزاز كسلوك إجرامي إيجابي يعتمد التهديد أو الوعيد بنشر بيانات أو معلومات لا يريد الضحية إعلانها لأي سبب كان، وكون النشر بوسائل تقنية المعلومات فهو يجعل المبتز في وضع مريح ومتمكن ويجعل من غايته أن تتحقق بشكل سريع ومؤذي، **ما يجعل المجني عليه عاجزا عن المقاومة** أو في ظروف لا تمَّكن الغير من الدفاع عنه، وكذلك فان فعل الابتزاز غالبا ما يعتمد على بيانات تم الحصول عليها باستغلال ضعف ادراك المجني عليه ، كما لاشك في أن طريقة الحصول على هذه البيانات تستبطن **باعثا دنيئا** للمبتز، وهذا ما يجعل من **فعل الابتزاز ظرفا مشددا للعقاب** عن الجريمة لتوفر أوصاف الظرف المشدد الوارد في المادة(١٣٥) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل التي نصت على (مع عدم الإخلال بالأحوال الخاصة التي ينص فيها القانون على تشديد العقوبة، يعتبر من الظروف المشددة ما يلي: ١ – ارتكاب الجريمة بباعث دنيء. ٢ – ارتكاب الجريمة بانتهاز فرصة ضعف ادارك المجني عليه أو عجزه عن المقاومة أو في ظروف لا تمكن الغير من الدفاع عنه)؛ كما أن هذه الدناءة التي يتصف بها فعل الابتزاز أيضا **لا تجعل من هذه الجريمة جريمة سياسية** حتى لو ارتكبت بباعث سياسي وذلك ما قررته المادة (٢١) من القانون ذاته التي نصت على(..... ومع ذلك لا تعتبر الجرائم التالية سياسية لو كانت قد ارتكبت بباعث سياسي: ١ – الجرائم التي ترتكب بباعث أناني دنيء).

٢- إنَّ فعل الابتزاز يعتمد **التهديد:** وهو ما يجعله **من أفعال التهديد** التي تشكل جناية أو جنحة بحسب المواد (٤٣٠-٤٣٢) عقوبات عراقي ، وهذا ما يعطي المحكمة صلاحية أن تأمر **بوضع المحكوم عليه تحت مراقبة الشرطة**، بعد انقضاء عقوبته، وهو ما قضت به المادة(١٠٩) من قانون العقوبات العراقي، كما يجوز أيضا للمحكمة عند الحكم بإدانة المبتز عن جناية أو جنحة أن تحكم **بمصادرة الأشياء المضبوطة التي تحصلت من الجريمة** أو التي استعملت في ارتكابها أو التي كانت معدة لاستعمالها فيها، دون الإخلال بحقوق الغير الحسني النية، وهو ما قررته المادة (١٠١) من قانون العقوبات؛ كما انه واذا ما تحققت العلانية في النشر- وهو أمر قد يحدث كثيرا في مثل هذه الجرائم- فان المادة (٨٤) من القانون ذاته أجازت لقاضي التحقيق أو المحكمة المنظورة أمامها الدعوى بناء على طلب الادعاء العام أن يأمر بضبط كل الكتابات والرسوم وغيرها من طرق التعبير مما يكون قد اعد للبيع أو التوزيع أو العرض أو يكون قد بيع أو وزع أو عرض فعلا وكذلك الأصول والألواح والأشرطة والأفلام وما في حكمها، وللمحكمة عند صدور الحكم بالإدانة في موضوع الدعوى أن تأمر بمصادرة الأشياء المضبوطة ويجوز لها كذلك أن تأمر بنشر الحكم أو ملخصه في صحيفة أو صحيفتين على الأكثر على نفقة المحكوم عليه).

٣- إنَّ التهديد الواقع بفعل الابتزاز يجعله **من جرائم الخطر** التي لا تستوجب لتمامها أن يقع النشر فعلا، فتقع جريمة الابتزاز بمجرد أن يقوم الفاعل بإيصال التهديد الجدي بالنشر للمجني عليه وتحقق الإثارة النفسية لديه من الخوف بإظهار ما تحتويه المنشورات من بيانات أو معلومات سرية لا يريد نشرها بما يشكل إكراها لإرادته قد تحمله على الاستجابة لطلبات الجاني.

٤- كما يمكن أن يتصور **الشروع في هذه الجريمة** متى أوقف النشر أو خاب اثره لأسباب خارجة عن إرادة الفاعل أو كان تنفيذها مستحيلا أما لسبب يتعلق بموضوع الجريمة أو بالوسيلة التي استعملت في ارتكابها ما لم يكن اعتقاد الفاعل صلاحية عمله لإحداث النتيجة مبنيا على

وهم أو جهل مطبق سندا لأحكام المادة (٣٠) من قانون العقوبات، و بذلك يمكن معاقبة الفاعل عن جريمة الشروع بالابتزاز على وفق أحكام المادة (٣١) من القانون ذاته، فضلا عن انه تسري على الشروع الأحكام الخاصة بالعقوبات التبعية والتكميلية والتدابير الاحترازية المقررة للجريمة التامة وهو ما قررته المادة (٣٢) من هذا القانون، مع مراعاة انه لا يعد شروعا مجرد العزم على ارتكاب الجريمة ولا الأعمال التحضيرية لذلك ما لم ينص القانون على خلاف ذلك، كما يمكن معاقبة **كل من حرَّض أو اتفق أو ساعد بأية وسيلة كانت على الابتزاز** بعقوبة المبتز بوصفه شريكا ،استنادا لأحكام المادة (٥٠ /١) من قانون العقوبات.

٥- إنَّ فعل الابتزاز فعل عمدي ما يجعل من الجريمة الواقعة منه **جريمة عمدية يتحقق فيها القصد الجنائي العام** وهو انصراف إرادة المبتز إلى التأثير على إرادة المجني عليه بالضغط والترويع من خلال نشر بيانات لا يريد إعلانها للحصول على منفعة مادية أو معنويه له أو لغيره وهو يعلم بذلك. جدير بالذكر الإشارة إلى أن مجرد النشر المقصود بإحدى طرق العلانية دون أن يصاحبه ابتزاز أو تهديد متى شكَّل إساءة لمن وقع بحقه فانه يُعَّد جريمة على وفق المادة (٤٣٨) عقوبات التي نصت على أن (يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائة دينار أو بإحدى هاتين العقوبتين.١ – من نشر بإحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة اذا كان من شان نشرها الإساءة اليهم....) وقد بيَّن المشرع العراقي وسائل العلانية في المادة (٣/١٩) من قانون العقوبات بالقول(تعد وسائل للعلانية:

ا – الأعمال أو الإشارات أو الحركات اذا حصلت في طريق عام أو في محفل عام أو مكان مباح أو مطروق أو معرض لأنظار الجمهور أو اذا حصلت بحيث يستطيع رؤيتها من كان في مثل ذلك المكان أو **اذا نقلت اليه بطريقة من الطرق الآلية.**

ب – القول أو الصياح اذا حصل الجهر به أو ترديده في مكان مما ذكر أو اذا حصل الجهر به أو **اذا أذيع بطريقة من الطرق الآلية وغيرها** بحيث يسمعه من لا دخل له في استخدامه.

جـ – الصحافة والمطبوعات الأخرى وغيرها من وسائل الدعاية والنشر.

د – الكتابة والرسوم والصور والشارات والأفلام ونحوها عرضت في مكان مما ذكر أو اذا وزعت أو بيعت إلى اكثر شخص أو عرضت للبيع في أي مكان). وبناء على ما تقدم وإن كنا نجد في نصوص قانون العقوبات التقليدية نصوصا يمكن لها ان تعالج جرائم الابتزاز الإلكتروني، إلا أن الطابع الخاص الذي يميز جميع جرائم تقنية المعلومات وخصوصا في وسائل الإثبات وما يتعلق بالأدلة الرقمية، تقتضي معالجتها بصورة اكثر دقة وعمقا وهو ما ندعو له المشرع في ضرورة استكمال مراحل تشريع قانون مكافحة جرائم تقنية المعلومات والاستفادة من التجارب الإقليمية والدولية بهذا الخصوص سواء بوضع نص خاص يحتوي الابتزاز الإلكتروني وكذلك بإيراد نص يشير إلى إن استخدام وسائل تقنية المعلومات يعدُّ ظرفا مشددا لأي جريمة منصوص عليها في القوانين الجزائية، إضافة إلى إيجاد النصوص الإجرائية التي تساعد سلطات التحقيق والمحاكمة في مواكبة البيئة المعلوماتية .

الخاتمـــة

سيتم بيان أهم النتائج التي توصل لها هذا البحث وما يمكن أن يُعَّد مقترحات غايتها الوصول إلى حماية جنائية ناجعة في مواجهة هذه الجريمة وذلك فيما يلي:

أولا: الاستنتاجات

١- تبين من خلال البحث إنَّ جريمة الابتزاز الإلكتروني تقع عن طريق قيام الجاني بالضغط على المجني عليه بالتهديد والوعيد ، وذلك بنشر معلومات أو صور أو تسجيلات لا يرغب المجني عليه في إظهارها علنا، في حال عدم استجابته للجاني، فهو أسلوب من أساليب الضغط والإكراه على المجني عليه، يمارسه الجاني لتحقيق مقاصده الإجرامية، وذلك للوصول إلى هدفه الذي قد يكون هدفاً مادياً أو معنوياً؛

٢- توالت الجهود الدولية والإقليمية الرامية إلى معالجة هذا النوع من الجرائم بوضع رؤى للتعاون الدولي وإيجاد نصوص جزائية تواكب التعقيد من حيث نماذج التجريم ومن حيث وسائل الإثبات وإجراءات التحقيق الذي تتصف به بيئة تقنية المعلومات وظروف مستخدميها، وإنَّ المشرع العراقي بصدد إصدار قانون خاص لمكافحة هذه الجرائم الذي ندعو أن تتم الاستفادة فيه من كل التجارب الدولية بالخصوص.

٣- كما اتضح أن جريمة الابتزاز تشكل جريمة من جرائم الاعتداء على حرمة الحياة الخاصة والتي عالجها المشرع العراقي في الباب الثاني من قانون العقوبات النافذ تحت عنوان الجرائم الماسة بحرية الإنسان وحرمته، وإنَّ فعل الابتزاز –على وفق قانون العقوبات العراقي النافذ –

يمكن أن ينطبق مع نموذج التجريم الوارد بنص المادة (١/٤٣٠) عقوبات؛ اذا ما تم بالتهديد بإسناد أمور مخدشة بالشرف أو إفشائها متى كان مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل أو مقصود به ذلك .

٤- كذلك فان المشرع العراقي بصدد تشريع قانون خاص بمكافحة الجرائم المعلوماتية، وقد نص صراحة على هذه الجريمة في المادة(١١/ب) من مشروع القانون، والتي بيَّنا جملة من الملاحظات على النص فيها، وكما وردت في ثنايا البحث.

ثانيا: المقترحات

١- إذ تبقى مسألة استمكان ظروف الجريمة المادية والشخصية المتعلقة بتقنية المعلومات كافة ، فضلا عن ما يتعلق بالجوانب الإجرائية من حيث التحقيق والإثبات الرقمي بحاجة إلى تطوير، ندعو المشرع إلى الالتفات له في مشروع القانون والنص على أحكام خاصة بالأدلة الرقمية بما ينسجم وخصوصية هذه الجرائم، وذلك بان يجعل للدليل الرقمي الحجية ذاتها بالإثبات.

٢- الدعوة إلى اعتبار استخدام وسائل تقنية المعلومات ظرفا مشددا عاما في جميع الجرائم.

٣- إذ إنَّ جريمة الابتزاز الإلكتروني كغيرها من الجرائم التي تؤشر انحرافا قيميا وأخلاقيا وقد لا ينحصر هذا الانحراف بالجاني المبتز فانه لطالما كان الضعف الأخلاقي للضحية سببا حاكما في مثل هذه الجرائم لذا ندعو أولياء الأسرة والشرطة المجتمعية لاتخاذ تدابير تربوية تتناسب وحجم الأخطار التي يتعرض لها مستخدمي الحاسوب والهاتف النقال وشبكة الإنترنيت،

٤- ندعو المشرع العراقي إلى تشريع قانون يختص بجرائم تقنية المعلومات يعالج صورها من الناحية الموضوعية من حيث صور الأفعال الجرمية والإجرائية من حيث الضبط والتحقيق والمحاكمة ووسائل الإثبات مستفيدا من الخبرات والتجارب الدولية والإقليمية.

٥- إبعاد هذا التشريع عن الأهداف السياسية المتعلقة بجدلية الصراع بين السلطة والحرية والنظر له على وفق السياسة الجنائية فقط.

٦- كما وندعو إلى ضرورة مواكبة التطور التكنولوجي وتزويد جهات الضبط والتحقيق بالوسائل التقنية التي تسهل عملها، فضلا عن وضع برامج تدريبية للجهات ذات العلاقة بما يجعلها قادرة على مكافحة هذه الجرائم بصورة فعالة.

٧- ندعو أيضا الحكومة العراقية إلى التنسيق مع الدول الأخرى نحو إبرام معاهدة دولية شارعة تلزم الأطراف بالتعاون الجنائي لمكافحة هذه الجرائم من حيث الضبط والتحقيق والمحاكمة والعقاب وتسليم المجرمين.

٨- ندعو الجهات المختصة إلى الاستفادة من منظمة(شرطة الويب) وإيجاد وسائل التنسيق معها لتسهيل عملية القبض على الجناة وإثبات الأدلة ضدهم.

٨- وأخيرا ندعو وسائل الإعلام كافة إلى ضرورة التركيز في برامجها الإعلامية المختلفة على نشر الوعي حول مخاطر هذه الجريمة وتبصير أفراد المجتمع بأساليب المبتزين وطرقهم كي لا يكونوا صيدا سهلا لإجرامهم.

مصادر البحث

أولا: الكتب

١- احمد شوقي أبو خطوة ، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣ .

٢- د. احمد عمر مختار، معجم اللغة العربية المعاصرة، الفقرة (٣٢٣٤١)، كتاب الكتروني، marqoon.org

٣- د. جمال إبراهيم الحيدري، الوافي في شرح أحكام القسم العام من قانون العقوبات، مكتبة السنهوري،بغداد،٢٠١٢ .

٤- د. زينب عبد العزيز المحرج، الابتزاز في المجتمع السعودي وضوابط الحد منه، مكتبة القانون والاقتصاد، الرياض،٢٠١٥

٥- عبد الرحمن عبدالله السند، جريمة الابتزاز ، مكتبة الملك فهد الوطنية،الرياض،١٤٣٩ هـ

٦- د. علاء الدين زكي مرسي ، نظم القسم الخاص في قانون العقوبات – جرائم الاعتداء على العرض، الكتاب الثاني، مصر، ٢٠١٣.

٧- د. مأمون محمد سلامة، إجرام العنف، بحث منشور في مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ع٢، القاهرة،١٩٧٤.

٨- محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح، دار الرسالة، الكويت، دون سنة نشر

٩- د. محمود صالح العادلي، ، موسوعة القانون الجنائي للإرهاب، ج١، دار الفكر الجامعي، الإسكندرية ،٢٠٠٣.

١٠- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط ٢٠٠٠ ، ص ٨٠ وما بعدها.

١١- د. ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، المستودع الرقمي المؤسسي لجامعة نايف العربية للعلوم الأمنية.

١٢- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر،عمان،٢٠٠٨

١٣- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،١٩٩٢

١٤- وليد الزيدي، القرصنة على الأنترنت والحاسوب، دار أسامة للنشر ،عمان،٢٠٠٣

ثانيا: البحوث والمجلات

١- بلال حناجره، الإنترنت والابتزاز الإلكتروني،www.goldenacadimy.net،2019

٢- د. جورج لبكي، المعاهدات الدولية للإنترنت: حقائق وتحدّيات، مجلة الدفاع الوطني اللبناني ،العدد ٨٣ ، كانون الثاني ٢٠١٣

٣- د. داليا عبد العزيز، لمسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة ،مجلة جيل الأبحاث القانونية المعمقة العدد ٢٥/https://jilrc.com

٤- *شيخه حسين الزهراني* ، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، *المجلد* ١٧ *العدد* ١، الشارقة – الإمارات العربية المتحدة ،*يونيو*، ٢٠٢٠

٥- فايز عبد الله الشهري ، دور مؤسسات المجتمع في مواجهة ظاهرة الابتزاز وعلاجه، الابتزاز الإلكتروني نموذجا، بحث مقدم لندوة الابتزاز (المفهوم–الأسباب– العلاج)، جامعة الملك سعود ،٢٠١١.

٥- عبد العزيز حمين أحمد الحمين ،الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الابتزاز (المفهوم–الأسباب– العلاج)، جامعة الملك سعود،٢٠١١ ،ص٥١.

ثالثا: الوثائق والمواقع الإلكترونية

١- إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢

٢- موقع الأمم المتحدة، القرارات.

٣- موقع مجلس أوروبا

٤- موقع مجلس القضاء الأعلى، قاعدة التشريعات العراقية

رابعا: التشريعات

١- قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم(٥) لسنة ٢٠١٢ المعدل بالمرسوم بقانون اتحادي رقم(٢) تاريخ ٢٠١٨/٠٧/٢٤، الجريدة الرسمية رقم ٥٤٠ ملحق ص ١٩.

٢- قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات المصري

٣- المرسوم الملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ نظام مكافحة جرائم المعلوماتية السعودي

٤- المرسوم السلطاني رقم (١٢) / ٢٠١١ بإصدار قانون مكافحة جرائم تقنية المعلومات العماني

٥- قانون جرائم أنظمة المعلومات الأردني لسنة2010

٦- قانون العقوبات العراقي رقم(١١١) لسنة ١٩٦٩ المعدل

خامسا: مشروعات القوانين

١- مشروع قانون جرائم المعلوماتية، موقع مجلس النواب العراقي

٢- مشروع قانون الاتصالات والمعلوماتية، موقع مجلس النواب

Resources

Firstly: Books:

1- Ahmad Shawqi Abu Khotwa, Explanation of General Provisions of the Penal Code, Dar Al-Nahda Al-Arabiya, Cairo, 2003, p. 559. 2- Dr. Ahmed Omar Mukhtar, Dictionary of Contemporary Arabic Language, Paragraph (32341), electronic book, marqoon.org.

2- Dr. Jamal Ibrahim Al-Haidari, Al-Wafi in Explaining the Provisions of the General Section of the Penal Code, Al-Sanhouri Library, Baghdad, 2012.

3- Dr. Zainab Abdulaziz Al-Muharj, Extortion in Saudi Society and Controls to Reduce It, Law and Economy Library, Riyadh, 2015.

4- Abdul Rahman Abdullah Al-Sanad, the crime of extortion, King Fahd National Library, Riyadh, 1439 AH.

5- Dr. Alaa El Din Zaki Morsi, Organized the Special Section in the Penal Code - Assaults on Show, Book Two, Egypt, 2013.
6- Dr. Mamoun Muhammad Salama, Crime of Violence, a research published in the Journal of Law and Economics, Faculty of Law, Cairo University, Volume 2, Cairo, 1974
7- Muhammad bin Abi Bakr bin Abdul Qadir al-Razi, Mukhtar As-Sahih, Dar Al-Risala, Kuwait, without a year of publication.
8- Dr. Mahmoud Saleh Al-Adly, The Criminal Law Encyclopedia of Terrorism, Part 1, University Thought House, Alexandria, 2003.
9- Dr. Mamdouh Rashid Musharraf Al-Rasheed Al-Anzi, Criminal Protection of the Victim from Extortion, Institutional Digital Repository of Naif Arab University for Security
Sciences.
10- Dr**.** Medhat Ramadan, Assault Crimes and Internet.University of Thought,Alexandria.2003
11- Nahla Abdel Qader Al-Momani, Information Crimes, House of Culture for Publishing, Amman, 2008.
12- Hoda Hamid Qashqoush, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Cairo, 1992.
13- Walid Al-Zaidi, Internet and Computer Piracy, Usama Publishing House, Amman, 2003.

Secondly: Research and Journals:

1- Bilal Hanajreh, Internet and Electronic Blackmail: goldenacadimy.net.www, 2019.
2- Dr. George Labaki, International Internet Treaties: Facts and Challenges, Lebanese National Defense Magazine, Issue No. 83, January 2013.
3- Dr. Dalia Abdulaziz, Criminal Responsibility for the Crime of Electronic Blackmail in the Saudi System, a Comparative Study, Journal of the Generation of In-depth Legal Research, Issue 25, https://jilrc.com.
4- Sheikha Hussein Al-Zahrani, International Cooperation in Confronting Cyber Attack, University of Sharjah Journal of Legal Sciences, Volume 17, Issue 1, Sharjah, United ArabEmirates, June, 2020
5- Fayez Abdullah Al-Shehri, The Role of Community Institutions in Confronting the Phenomenon of Extortion and its Treatment, Electronic Blackmail as a Model, Research presented to the Blackmail Seminar (Concept - Reasons - Treatment), King Saud University, 2011
5- Abdulaziz Hamin Ahmad Al-Hamin, blackmail and the role of the General Presidency of the Commission for the Promotion of Virtue and Prevention of Vice in combating it, research presented to the Blackmail Symposium (concept - causes - treatment), King Saud University, 2011, p. 51.

Thirdly: Documents and Websites:

1- ESCWA Guidelines for Cyber Legislation, Cyber Legislation Coordination Project to Encourage Knowledge Society in the Arab Region, Beirut, 2012.
2- United Nations website, resolutions
3-Council of Europe Website.
4- The Supreme Judicial Council website, the base for Iraqi legislation.

Fourthly: Legislation:

1- UAE Information Technology Crimes Law No. (5) of 2012 amended by Federal Decree Law No. (2) dated 07/24/2018, Official Gazette No. 540 Appendix p.19.
2- Law No. 175 of 2018 in the matter of combating Egyptian information technology crimes.
3- Royal Decree No. M / 17 of 3/8/1428 AH, the Saudi Anti-Information Crime Law.
4- Royal Decree No. (12) / 2011 issuing the Omani Law to Combat Information Technology Crimes.
5- The Jordanian Information Systems Crimes Law of 2010.
6- Iraqi Penal Code No. (111) of 1969, as amended.

Fifthly: Draft Laws:

1- Information Crimes Draft Law, website of the Iraqi Parliament.
2- Communications and Informatics Bill, Parliament website

الهوامش

(١) محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح، دار الرسالة، الكويت، دون سنة نشر، ص ٥١، ود. احمد عمر مختار، معجم اللغة العربية المعاصرة، الفقرة(٣٢٣٤١)،كتاب الكتروني،marqoon.org، ص٩٢ .

[1] احمد شوقي أبو خطوة ، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٠٣، ص٥٥٩ ود. جمال إبراهيم الحيدري، الوافي في شرح أحكام القسم العام من قانون العقوبات، مكتبة السنهوري، بغداد،٢٠١٢،ص٧٣٠ وما بعدها .

[2] عبد الرحمن عبدالله السند، جريمة الابتزاز، مكتبة الملك فهد الوطنية،الرياض،١٤٣٩ ه، ص ١٥، و فايز عبد الله الشهري ، دور مؤسسات المجتمع في مواجهة ظاهرة الابتزاز وعلاجه، الابتزاز الإلكتروني نموذجا، بحث مقدم لندوة الابتزاز (المفهوم-الأسباب- العلاج)، جامعة الملك سعود ،٢٠١١ ،ص١٤١.

[3] بلال حناجره، الإنترنت والابتزاز الإلكتروني،www.goldenacadimy.net،2019،ص١٤، وهدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،١٩٩٢، ص١٨٥

[4] وليد الزيدي، القرصنة على الإنترنت والحاسوب، دار أسامة للنشر ،عمان،٢٠٠٣،ص٧٢، و عبد العزيز حمين أحمد الحمين ،الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الابتزاز (المفهوم-الأسباب- العلاج)، جامعة الملك سعود،٢٠١١، ص٥١.

[1] د. ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، المستودع الرقمي المؤسسي لجامعة نايف العربية للعلوم الامنية،ص٢٠٠، و د. زينب عبد العزيز المحرج، الابتزاز في المجتمع السعودي وضوابط الحد منه، مكتبة القانون والاقتصاد، الرياض،٢٠١٥، ص٩٢

[1] د. داليا عبد العزيز، لمسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة ،مجلة جيل الأبحاث القانونية المعمقة العدد ٢٥ https://jilrc.com/ و ، د. علاء الدين زكي مرسي ، نظم القسم الخاص في قانون العقوبات – جرائم الاعتداء على العرض، الكتاب الثاني، مصر، ٢٠١٣، ص ١٣٦.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر،عمان،٢٠٠٨،ص٣٦

[1] موقع الأمم المتحدة، الوثيقة UNODC/CCPCJ/EG

[1] موقع الأمم المتحدة، القرارات.

[2] د. جورج لبكي، المعاهدات الدولية للإنترنت: حقائق وتحدّيات، مجلة الدفاع الوطني اللبناني ،العدد ٨٣ ، كانون الثاني ٢٠١٣،ص ٥ وما بعدها.

[3] المجلس الأوربي هو قمة لرؤساء الدول ورؤساء الحكومات في الاتحاد الأوربي ويمثل الجهاز التنفيذي لهذا للاتحاد.

[1] د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط ٢٠٠٠ ، ص ٨٠ وما بعدها.

[1] الأمم المتحدة ، الوثيقة رقم A/CONF.213/٩

[1] موقع مجلس أوروبا ،سلسلة المعاهدات الأوروبية رقم ١٨٥..

[1] إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢

[2] موقع مجلس القضاء الأعلى، قاعدة التشريعات العراقية

[1] انظر موقع المنظمة http://www.web-police.org

[2] *شيخه حسين الزهراني* ، التعاون الدولي في مواجهة الهجوم السيبراني، بحث منشور في مجلة جامعة الشارقة للعلوم القانونية، *المجلد* ١٧ *العدد* ١، الشارقة – الإمارات العربية المتحدة ،*يونيو*، ٢٠٢٠

[1] قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم(٥) لسنة ٢٠١٢ المعدل بالمرسوم بقانون اتحادي رقم(٢) تاريخ ٢٠١٨/٠٧/٢٤، الجريدة الرسمية رقم ٥٤٠ ملحق ص ١٩.

[1] قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات المصري

[1] المرسوم الملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨هـ نظام مكافحة جرائم المعلوماتية السعودي

[1] المرسوم السلطاني رقم ١٢ / ٢٠١١ بإصدار قانون مكافحة جرائم تقنية المعلومات العماني

[2] قانون جرائم أنظمة المعلومات الأردني لسنة2010

[3] موقع مجلس القضاء الأعلى ، قاعدة التشريعات العراقية

[1] د. مأمون محمد سلامة، إجرام العنف، بحث منشور في مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ع٢، القاهرة،١٩٧٤، ص٢٦٥، و د. محمود صالح العادلي، ، موسوعة القانون الجنائي للإرهاب، ج١، دار الفكر الجامعي، الإسكندرية ،٢٠٠٣، ص ٤٤.

[2] مشروع قانون جرائم المعلوماتية، موقع مجلس النواب العراقي-القوانين قيد التشريع

[3] نص المشروع تم نشره في موقع aliraqnet.net

[1] جدير بالذكر أن المشرع العراقي بصدد تشريع قانون الاتصالات والمعلوماتية الذي تم إعداده في عام ٢٠٠٩ ولازال قيد التشريع إذ حظر بموجب المادة (١٠/ رابعا) من المشروع على الحاصل على ترخيص تردد أو إجازة اتصالات القيام باي تصرف أو اتخاذ أي إجراء أو استخدام أي جهاز يمكن أن يرتب ضررا لأمن أو مصلحة الدولة أو للمواطنين أو مصلحة المنافسين له، وعاقب على ذلك بموجب المادة(٢٥) بالسجن مدة لا تزيد على (١٠) عشر سنوات وبغرامة لا تقل عن (٥٠٠٠٠٠٠٠) خمسين مليون دينار ولا تزيد على (١٠٠٠٠٠٠٠٠) مئة مليون دينار أو بإحدى هاتين العقوبتين كل من ارتكب ذلك عمدا، كما جرّم التنصت أو إفشاء المعلومات والبيانات وتسبب بالحاق الضرر بمصلحة الدولة أو المصالح الخاصة للمواطنين وعاقب على ذلك بنصه في المادة(٢٨) على أن (يعاقب بالحبس وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) عشرة ملايين دينار ولا تزيد على (١٥٠٠٠٠٠٠) خمسة عشر مليون دينار كل من قام بالتنصت أو إفشاء المعلومات والبيانات وتسبب بالحاق الضرر بمصلحة الدولة أو المصالح الخاصة للمواطنين).

[1] قانون العقوبات العراقي رقم(١١١) لسنة ١٩٦٩ المعدل