وزارة التعليم العالي والبحث العلمي
Ministry of high education and scientific research
جامعة محمد البشير الابراهيمي-برج بوعريريج-
University of Mohamed El-Bachir El-Ibrahimi -BBA
كلية الحقوق و العلوم السياسية
Faculty of Law and political Sciences

مذكرة مقدمة لاستكمال متطلبات لنيل شهادة ماستر مهني في القانون العام

تخصص: قانون الاعلام الآلي و الأنترنت

الموسومة بـ:

جريمة الابتزاز الالكتروني-دراسة مقارنة-

من إعداد الطالب:

- بوشعير الحسن
- حداد شعيب

تحت إشراف:

- خرباش جميلة

لجنة المناقشة

الاسم و اللقب	الرتبة	الصفة
• لخضر رفاف	أستاذ محاضر أ	رئيسا
• جميلة خرباش	أستاذ مساعد أ	مشرفا ومقررا
• نسيمة طاجين	أستاذ مساعد أ	مناقشا

السنة الجامعية: 2022-2023

الشكر والعرفان:

قال تعالى:(ومن يشكر فإنما يشكر لنفسه) لقمان:12

أول من يشكر ويحمد آناء الليل وأطراف النهار، هو العلي العظيم القهار الأول والآخر والظاهر والباطن، الذي أغرقنا بنعمه التي لا تحص، وأنعم علينا برزقه الذي لا يفنى، وأنار دروبنا، فله جزيل الحمد والثاء العظيم، هو الذي أنعم علينا إذ أرسل فينا عبده ورسوله محمد ابن عبد الله عليه أزكى الصلوات وأطهر التسليم، أرسله بقرآنه المبين، وأينما وجد.

نحمد الله عزّ وجل الذي وفقنا وألهمنا الصبر على المشاق التي واجهتنا لإنجاز هذا العمل المتواضع، وألهمنا الصحة والعافية والعزيمة فالحمد لله حمداً كثيرا.

والشكر موصول إلى كل معلم أفادنا بعلمه، من أول المراحل الدراسية حتى هذه اللحظة، كما نرفع كلمة شكر والتقدير إلى الأستاذة المشرفة "خرباش جميلة" على كل ما قدمته لنا من توجيهات ومعلومات قيمة ساهمت في إثراء موضوع دراستنا في جوانبها المختلفة، كما نتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة الموقرة، كما نشكر كل من مدّ لنا يد العون من قريب أو بعيد، والشكر لكل أساتذة وعمال كلية الحقوق والعلوم السياسية بجامعة برج بوعريريج على المجهودات التي يبذلوها من أجلنا جزاهم الله عنا كل الخير

وفي الأخير لا يسعينا إلا أن ندعو الله عز وجل أن يرزقنا السداد والرشاد والعفاف والغنى وأن يجعلنا هداة مهتدين.

الإهداء:

الحمد لله وكفى والصلاة على الحبيب المصطفى وأهله ومن وفى أما بعد:

الحمد لله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه ثمرة الجهد والنجاح بفضله تعالى فأهدي ثمرة جهدي التي طالما تمنيت إهدائها وتقديمها إلى الوالدين الكريمين حفظهما الله ورعاهما

لكل العائلة الكريمة التي ساندتني ولا تزال

إلى جميع الزملاء والأصدقاء

إلى كل من ذكرهم قلبي ونسيهم قلمي، إلى كل من كان لهم أثر على حياتي.

إلى كل قسم قانون الإعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج.

إلى كل هؤلاء أهدي ثمرة جهدي.

الطالب: بوشعير الحسن

حداد شعيب

قائمة المختصرات:

ط	الطبعة
ص	الصفحة
ق ع ج	قانون العقوبات الجزائري
د ن	دار النشر
ق إ ج ج	قانون الإجراءات الجزائية الجزائري
ق م ج ت م إ	قانون مكافحة جرائم تقنية المعلومات الإمراتي

مقدمة

عرف العالم تطور هائل في مجال العلمي والتقني بسبب ظهور شبكة الأنترنت، وهذا التطور يمكن أن يكون سلاحا ذو حدين، الأمر الذي دفع بالمشرفين تنظيم هذا المجال بما يخدم حقوق الأنترنت من كل اعتداء، ونتيجة للاستخدام السيئ للشبكة العنكبوتية العالمية ووسائل التكنولوجيا والاتصال الحديثة، أضحت البيئة الافتراضية بؤرة لأنماط جديدة من الجرائم تسمى بالجرائم الالكترونية ومن نماذجها جريمة الابتزاز الإلكتروني.

إلا أنه في هذا العالم الرقمي كرست مجموعة من الفئات المجرمة جهودها للاستغلال هذه التقنيات العالية وتوجيهها لتنفيذ إجرامهم وغرائزهم، حيث جعلت الطرف الآخر سلعة لاستغلالهم عن طريق التهديد والابتزاز عبر وسائل التواصل الاجتماعي من خلال ضغط الذي يمارسه المجرم على الضحية، بتهديده بإفشاء سره ونشر صوره أو فديوهاته أو معلومات عنه مما يفطر معه إلى الإنصياغ والإذعان لرغبة الجاني وتحقيق مطالبه المشروعة أو غير المشروعة تحت إكراه من الخوف من الفضيحة ، وقد يكون الضحية شخصا طبيعيا ، كما يمكن أن يكون شخصا معنويا.

وتعتبر ظاهرة الابتزاز الالكتروني من الظواهر المستحدثة التي ظهرت بظهور تقنيات الاتصال الحديثة والتي نعني بها في ورقتنا البحثية ظهور شبكة الأنترنت ، حيث أصبحت تطالعنا مختلف وسائل الإعلام بأنواع متعددة من الابتزاز، إذ غالبا ما تكون فئة الشباب هي الأكثر تعرضا لمثل هذه المظاهر.

فالانفتاح التقني الذي شهده العالم وبخصوص الدول العربية منذ أواخر التسعينيات وما صاحب هذا الانفتاح من قفزة نوعية في الاتصالات عامة وفي مجال الأنترنت بشكل خاص وقد أوجدت عدة مظاهر سلبية نجمت عن سوء استخدام الوسائل الالكترونية التي من المفروض أنها وجدت حتى تخدم بين البشر لا أن تكون سببا في تعاستهم. كما تعتبر جريمة الابتزاز الإلكتروني كظاهرة اجتماعية تخترق المجتمع، تدق في أعماقها أجراس

الخطر على اعتبار أنها توجه للنيل من الحياة الخاصة للأفراد، معتمدا في ذلك على شبكة الأنترنت بدلالتها التقنية الواسعة كأداة لارتكاب أحد أخطر أصناف الجرائم استفحالا وأكثرها تقعيدا، فقد استغل المجرمون مما أتاحه العصر الحديث من تقدم في مجال الأنترنت لاستحداث أساليب جديدة واستخدام وسائل علمية في تهديد الأشخاص وابتزازهم، وبتالي فإن جريمة الابتزاز الإلكتروني يتعدى الإشكالية التقليدية التي تناولتها الدراسات الفقهية ، وقلة من الدراسات من السلطات الضوء على الجرائم المعلوماتية، ولاسيما بعد انتشار مواقع الدردشة ،وشبكات التواصل الاجتماعي مثل الفيس بوك، التويتر يوتيوب، والمشكلة أن الأفراد يفرطون في خصوصيتهم من خلال وضع معلومات عن أنفسهم وصور شخصية لهم ومقاطع فيديو، والأسوء أن الكثير من الأطفال والمراهقين كانوا فريسة سهلة للابتزاز من قبل مجرمين الأنترنت وهو ما أدى بالمشرعين في العديد من الدول إلى سن قوانين تجرم السلوك الإجرامي الذي يتمثل، في جريمة الابتزاز الإلكتروني، واهتم شراح القانون بتفسيره وشرحه، وبيان أركان الجريمة التي تقوم عليها ، وكذلك طرق التحقيق والإثبات فيها، كما أن للدليل الرقمي أسس وقواعد مختلفة في التعامل معه بسبب خطورة هذه الجريمة.

ونضراً إلى الآثار المترتبة على انتشار جريمة الابتزاز الإلكتروني في المجتمع وكونها من المستجدات الطارئة عليه فإن للبحث أهمية من الناحيتين العلمية والعملية.

من الناحية العلمية؛ لفت انتباه الباحث لدراسة الموضوع وتسليط الضوء على مختلف جوانبه، كذلك لفت انتباه المشرع إلى إعادة النظر وضبط النصوص القانونية لمكافحة هذه الجريمة ، أما من الناحية العملية؛ تبرز أهمية البحث في معرفة مدى كفاية النصوص الجنائية في بعض التشريعات العربية الواردة في قوانين العقوبات إلى الحد من ارتكاب هذه الجريمة ، وردع مرتكبيها للتقليل من آثارها وزيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة وضرورة توحي الحيطة والحذر في استخدامها.

أما عن أسباب اختيار الموضوع، فهي ذاتية؛ تتمثل في الرغبة في دراسته كونه يتناول ظاهرة تؤرق المجتمع وتهدد استقراره، وموضوعية؛ نظرا لكون الجريمة موضوع الدراسة تفشت وتنامت في المجتمع مما يستدعي دراستها باعتبار المجتمعات العربية المعروفة بالعادات، والأعراف الإجتماعية التي تتحفظ على كل ما يتعرض للسمعة والشرف خصوصا أن هذه الجريمة أغلب ضحاياها فتيات.

أما عن أهداف البحث، فتهدف هذه الدراسة إلى التعرف إلى النقاط التالية:

-التعرف على جريمة الإبتزاز الإلكتروني.

-التعرف على أنواعها وطرق ووسائل إرتكابها.

-دراسة أركان الجريمة في بعض التشريعات العربية والتشريع الجزائري والتعرف على الحلول المقترحة للحد من الوقوع ضحية هذه الجريمة

-التعرف على كيفية التحقيق والإثبات في جريمة الإبتزاز الإلكتروني والتعرف على الدليل الرقمي وعلاقته بهذه الجريمة .

التعرف على الصعوبات التي تواجه جهات التحقيق على هذه الجرائم، وإثباتها، والتعرف على العقوبات المقررة لهذه الجريمة في بعض التشريعات العربية.

أما عن حدود البحث فتتمثل في:

الحدود البشرية؛ تقتصر حدود هذا البحث على أولياء أمور الأسر في بعض الدول العربية مثل السعودية والجزائر

الحدود الزمانية؛ طبق هذا البحث في الفترة من 2023/05/20 إلى 2023/08/20.

الحدود المكانية؛ تقتصر حدود البحث على الدول العربية مثل السعودية والجزائر والعراق.

وفي ضوء مراجعة الأدب النظري والدراسات المتعلقة بظاهرة الإبتزاز الإلكتروني، فقد اتضح أن هناك ندرة في الدراسات السابقة التي تناولت هذه الظاهرة، ولعل السبب في ذلك أن مثل هذه الموضوعات تتسم بالخصوصية لحساسيتها الشديدة ولارتباطها بأهم مؤسسات المجتمع وهي الأسرة. ومن بين هذه الدراسات السابقة التي تناولت ظاهرة الإبتزاز الإلكتروني:

دراسة " الغديان وآخرون" هدفت الدراسة إلى الكشف عن أهم صور جرائم الإبتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، واستخدمت ثلاثة مقاييس للحصول على البيانات، وتكونت عينة الدراسة من47 من أعضاء هيئة الأمر بالمعروف والنهي عن المنكر، وعدد 47 من المستشارين النفسيين، وعدد 367 من المعلمين والمعلمات، واعتمدت الدراسة على المنهج الوصفي المقارن، وقد بينت نتائج الدراسة أن الدوافع الجنسية جاءت بالمرتبة الأولى، يليها الدوافع المادية.

ونضرا لتزايد نسبة ارتكاب هذه الجريمة في الآونة الأخيرة، ونظرا لخصوصية هذه الجريمة، ووسائل وطرق تنفيذها أدى إلى إنعكاس هذه الخصوصية على مضمون الأنظمة والقوانين، حيث تتماشى مع طبيعة هذه الجريمة ومعطياتها وآثارها، وبناءاً عليه كانت الحاجة ملحة لوضع هذا الموضوع موضوع دراسة وتحليل وينبني ذلك على الإجابة على إشكالية الدراسة المتمثلة في : كيف واجهت بعض التشريعات العربية جريمة الابتزاز الإلكتروني؟ ونتفرع عنها مجموعة من الإشكاليات الفرعية وهي:

ما مدى كفاية النصوص الحالية في مكافحتها ومواجهتها؟

وهل الحماية التي جاءت بيها التشريعات في بعض الدول العربية كافية لحماية الأشخاص من هذه الجريمة ؟ وماهي الحلول التي قد تحد من انتشار ظاهرة الإبتزاز

الإلكتروني؟

تتمحور هذه الدراسة القانونية العلمية، كان مجال البحث في بعض القوانين العربية، كالقانون المصري، والعراقي، والسعودي مع توضيح موقف التشريع المحلي (التشريع الجزائري).

لمعالجة هذه الإشكالية ارتكزت الدراسة على المنهج الوصفي لوصف جريمة الإبتزاز الإلكتروني، من خلال تعريفها، وأنواعها وأشكالها وآثارها، ووسائل ارتكابها، والمنهج التحليلي معتمدين على تحليل نصوص كل من نظام مكافحة جرائم المعلومات السعودي ، وقانون مكافحة جرائم تقنية المعلومات الإماراتي، والمشرع الجزائري في إصداره لقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وبيان موقفها من جريمة الإبتزاز الإلكتروني والمنهج المقارن للمقارنة بين مختلف النصوص السالفة الذكر.

ولدراسة هذا الموضوع ارتأينا تقسيم البحث إلى فصلين، الأول بعنوان الإطار الموضوعي لجريمة الإبتزاز الإلكتروني، وقد تناولنا في المبحث الأول منه ، ماهية الإبتزاز الإلكتروني أما المبحث الثاني النضرة القانوني لجريمة الإبتزاز الإلكتروني أو (تجريم الإبتزاز الإلكتروني)، أما الفصل الثاني فقد كان بعنوان الإطار الإجرائي لجريمة الإبتزاز الإلكتروني الذي يحتوي على مبحثين الأول بعنوان الآليات القانونية لمكافحة جريمة الإبتزاز الإلكتروني والتي نعني بها إجراءات التحقيق والإثبات في جريمة الإبتزاز الإلكتروني، أما المبحث الثاني فتناول الإجراءات القانونية والعقوبات الردعية لجريمة الإبتزاز الإلكتروني دراسة مقارنة مع بعض القوانين والتشريعات العربية.

وفي الأخير ختمنا هذه الدراسة باستعراض أهم النتائج المتوصل إليها، مع إيراد مجموعة من الاقتراحات القابلة للتجسيد.

الفصل الأول

الإطار الموضوعي لجريمة الابتزاز الإلكتروني

تمهيد وتقسيم:

يعد الإبتزاز الإلكتروني أحد نتائج التطور الهائل والتقدم الكبير في استخدام برامج الأنترنت ومواقع التواصل الإجتماعي ، فعلى الرغم من الأثار الإيجابية التي أحدثتها هذه التكنولوجيا في حياتنا، فإنها أتت ببعض الآفات الإجتماعية والأخلاقية بل والقانونية مثل موضوعنا هذا ما يسمى بالإبتزاز الالكتروني، حيث تعتمد هذه الجريمة أساسا على وسائل التكنولوجيا الحديثة وإذا ما وقفا على ماهية ظاهرة الإبتزاز من خلال مفهومها الذي يتطرق إلى مختلف تعريفاتها، وأنواعها ووسائلها وأشكالها وخصائصها وآثارها.

وإذا ما وقفنا على هذا السلوك الذي يشكل جريمة، كان لازما علينا أن نتعرض لأركانها، وأضرارها والحلول المقترحة للحد من الوقوع ضحية هذه الجريمة.

لهذا نسعى من خلال هذا الفصل إلى دراسة الإطار الموضوعي لجريمة الإبتزاز الإلكتروني، وذلك من خلال التطرق إلى ماهية الإبتزاز الإلكتروني في(المبحث الأول) وتجريم الإبتزاز الإلكتروني أو النضرة القانونية لجريمة الإبتزاز الإلكتروني في (المبحث الثاني).

المبحث الأول: ماهية الابتزاز الإلكتروني

إن الغموض الذي يحيط بجريمة الإبتزاز الإلكتروني منذ بدايتها وحتى تمام تنفيذها قد شكل تحديا كبيراً أمام الجهات القضائية حتى أن هذا الغموض قد صاحب تعريف هذه الجريمة، واختلفت التعريفات لكنها اتفقت في كون استخدام التكنولوجيا والواقع الإفتراضي كمسرح للجريمة، وكذلك مرتكبها ذو المهارات والصفات المختلفة عن المجرم التقليدي .

كما أنه كان بالأهمية التطرق إلى مفهوم الإبتزاز الإلكتروني من خلال تعريفه وأنواعه، ووسائله وخصائصه وأشكاله وآثاره من خلال المطلبين التاليين، المطلب الأول: مفهوم الإبتزاز الإلكتروني والمطلب الثاني: وسائل وأشكال الإبتزاز الإلكتروني وآثاره المترتبة عليه.

المطلب الأول: مفهوم الإبتزاز الإلكتروني

الإبتزاز الإلكتروني هو نوع من الجرائم الإلكترونية لكنه أخطرها وأكثرها إنتشاراً في العالم كله، الذي جعل المجرم يختبئ خلف شاشة ما، ويمارس عملا إجراميا بالإعتداء على مصلحة يحميها القانون للضحية، تتمثل في التهديد والضغط للفرد الضحية بنشر معلومات خاصة له أو صور تسجيلات، لا يرغب المجني عليه في إظهارها، ويجبر المبتز الضحية على دفع مبالغ مالية كبيرة أو استغلال الضحية للقيام بأعمال غير مشروعة وغير أخلاقية كإفشاء أسرار عمل أو علاقات جنسية محرمة أو أي عمل غير محترم، والجميع منا معرضاً إلى الإبتزاز الإلكتروني، حيث لم يسلم منه الرجل والمرأة والصغير والكبير والفرد الواحد والمؤسسات الكبرى، فهناك شركات ومؤسسات أعمال تبتز إلكترونيا لإجبارها على شيء معين عادة ما يخص أمور العمل، لكن الأكثر تعرضا له هم الأفراد على وجه الخصوص والفتيات بالأكثر.

ومن خلال هذا المطلب سيتم التطرق إلى مفهوم الإبتزاز الإلكتروني حيث يحتوي على ثلاث فروع، الفرع الأول يتناول تعريف الإبتزاز الإلكتروني أما الفرع الثاني يتناول أنواع الإبتزاز الإلكتروني والفرع الثالث خصائص الإبتزاز الإلكتروني.

الفرع الأول: تعريف الإبتزاز الإلكتروني

أولا: التعريف اللغوي للإبتزاز

يعرف الإبتزاز لغة بأنه أخذ الشيء بجفاء وقهر، وابتزه، سلبه، ورمى به، ولم يرده.[1]

وابتزت الشيء استلبته ومن ذلك جاء المثل (من عز بز) معنى ذلك من غلب سلب[1]

[1] سليمان بن عبد الرزاق الغديان، يحيى بن مبارك خطاطبة، عزالدين بن عبد الله النعيمي، **صور جرائم الإبتزاز الإلكتروني ودوافعها وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية**، دار المنظومة الرواد في قواعد المعلومات العربية، مجلد27 العدد69 يناير2018 ص166.

ثانيا: التعريف الإصطلاحي للابتزاز

يعرف اصطلاحا بأنه استخدام التهديد بالإيذاء الجسدي أو النفسي، أو الإضرار بالسمعة والمكافحة الإجتماعية بتلقيف الفضائح وإلصاق التهم، ونشر أسرار مما يجبر الشخص(المبتز) على الدفع مكرها لمن يمارس الإبتزاز عليه[2]

الحصول على معلومات سرية أو صور شخصية أو مواد فلمية تخص الضحية، واستغلالها لأغراض مادية أو القيام بأعمال غير مشروعة وهو الحصول على المال أو المنافع من شخص وابتزازه بواسطة التهديد بفضح بعض أسرار التي يمتلكها[3]

ثالثا: التعريف الفقهي للابتزاز

تعددت تعريفات الفقه للإبتزاز، فقد عرفه بعض الفقه على أنه الضغط الذي يباشر شخص على إرادة شخص آخر بجملة على ارتكاب جريمة معينة.

وقد عرفه البعض الآخر على أنه فعل يقوم به شخص بتهديد شخص آخر بأي طريقة ولا يهم نوع عبارات التهديد مادام من شأنها التأثير في نفس المجني عليه بتخويفه، أو ازعاجه من خطر لم يتحقق بعد قد يلحق على المجني عليه، أو نفسه، أو أي شخص آخر له صلة بالمجني عليه وقد عرف على أنه" القيام بتهديد شخص بفضح أمره ما لم يستجيب المهدد إلى تنفيذ طلبات الجاني وغالبا ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس الشرف، أو الكرامة، أو تتعلق بحرمة الحياة الخاصة للشخص المهدد الذي

---

[1] آمال برحال ، **جريمة الإبتزاز عبر الوسائل الإلكترونية**، مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي _تبسة، 2020 ص7.

[2] سليمان الغديان، يحي خطاطبة، وآخرون، المرجع السابق، ص166.

[3] برحال آمال، المرجع السابق، ص 8.

تم ابتزازه[1].

وفي تعريف آخر فقد عرف الإبتزاز الإلكتروني بأنه الحصول على وثائق، وصور، ومعلومات عن الضحية من خلال وسائل الكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة عن طريق استخدام الوسائل الإلكترونية لتحقيق أهداف يسعى لها المبتز.[2]

من خلال التعاريف السابقة للإبتزاز نجد أنها لا تخرج على اعتبار الإبتزاز وسيلة ضغط أو تهديد يمارسه المبتز على إرادة المجني عليه بهدف الوصول إلى تحقيق مراده لأن الإبتزاز مرتبط بالتهديد فدون هذا الأخير لا يتحقق الإبتزاز كما نستطيع القول أن الإبتزاز الإلكتروني يمثل سلوك غير مشروع أو غير أخلاقي ويعد من الجرائم التي تقع عن طريق الشبكة المعلوماتية.[3]

رابعا: التعريف القانوني للإبتزاز

يعرف الإبتزاز في الإصطلاح القانوني بأنه جريمة ترتكب ضد شخص لإجباره على تسليم المال أو التوقيع على وثيقة بتهديد لكشف أمر معين أو لصق تهمة بارتكاب جريمة ما، وتقاس بالدرجة التي يحصل عليها المستجيبون على الأداة المستخدمة في الدراسة الحالية.[4]

ويعرف أيضا: هو تلك الأفعال التي تدفع بالفرد إلى التهديد بكشف معلومات معينة عن شخص، أو فعل شيء ليؤذي الشخص المهدد، إن لم يقم الشخص المهدد بالإستجابة إلى بعض الطلبات، كما يمكن أن تكون هذه المعلومات عادة محرجة أو ذات طبيعة مدمرة

[1] ممدوح رشيد مشرف الرشيد العنزي، **الحماية الجنائية للمجني عليه من الإبتزاز**، مقال منشور على الشبكة الإلكترونية، **المجلة العربية للدراسات الأمنية**، المجلد33، العدد70، الرياض2017، ص199.

[2] المرجع نفسه.

[3] برحال أمال، المرجع السابق، ص9

[4] سليمان الغديان، وآخرون، المرجع السابق، ص_ص،166_167.

اجتماعيا، وهو بمعنى الحصول على أهداف غير مشروعة بإتباع وسائل غير مشروعة أيضا... وقد يستخدم الإبتزاز في أي وظيفة مهما كان نوعها للتأثير على الشخص الذي يكون عرضة لهذا الفعل لتحقيق مكاسب نوعية وغير مشروعة.[1]

خامسا: التعريف التشريعي للابتزاز الإلكتروني:

1/ بالنسبة للمشرع العراقي:

بالنسبة للمشرع العراقي فلم ترد كلمة ابتزاز في متن قانون العقوبات رقم 111 لسنة 1969 وتعديلاته، وعند التدقيق في مشروع قانون جرائم المعلوماتية فإننا نجد أن مسودة المشروع لم تعرف الإبتزاز الإلكتروني بشكل صريح، إلا أنه يتضح من استقراء نص المادة(11/أولا/أ، ب)، أن جريمة الإبتزاز تنطوي على التهديد والترويج لحمل المجني عليه على القيام بالأفعال التي يطلبها الجاني.[2]

المشرع العراقي لم يعرف جريمة الإبتزاز تنطوي على التهديد الإلكتروني كما لم ترد كلمة الإبتزاز في قانون العقوبات العراقي رقم 111 لسنة 1969 ذلك أن القانون المذكور قد تم تشريعه منذ فترة طويلة في عام 1969، ويرى البعض بأن الإبتزاز الإلكتروني هو استخدام وسائل الإتصال وتكنولوجيا المعلومات في تهديد وترهيب ووعيد لحمل شخص على القيام بدفع مال أو طلب أمور أخرى من المجني عليه والذي يخشى من نشر حياته الخاصة خلافا لأحكام القانون والنظم العام والآداب العامة.[3]

---

[1] سعيد زيوش، **ظاهرة الإبتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وأراء نظرية- مجلة العلوم الإجتماعية** ، العدد22، جانفي 2017، ص71.

[2] زينب محمود حسين، **المواجهة الجنائية للإبتزاز الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية**، جامعة كركوك، كلية القانون والعلوم السياسية، قسم القانون الخاص، المجلد10، العدد37،سنة2021، ص574.

[3] كاظم عبد جاسم الزيدي، **جريمة الإبتزاز الإلكتروني،(دراسة مقارنة)**، مكتبة القانون المقارن، طبعة1، بغداد، 2019، ص8.

يلاحظ على نص المادة أعلاه أن الإبتزاز الإلكتروني يتخذ مضمون التهديد فيه شكلا مختلف، ولأغراض شتى، ذلك المضمون، وهذه الغاية قد تكون محددة، وقد أخذت بذلك بعض التشريعات منها: المشرع الفرنسي، حيث بالعنف أو التهديد بالعنف أو الإكراه للتوقيع أو التعهد أو التخلي أو الكشف عن سر أو تحويل أموال أو أوراق مالية أو أي سلعة أخرى.[1]كما عرفته المادة 312-10 من ذات القانون بأنه:" الحصول عن طريق التهديد بكشف أو إدماء وقائع من شأنها أن تضر بالشرف أو الإعتبار بقصد التوقيع أو التعهد أو التخلي أو الكشف عن سر أو تسليم أموال أو أوراق مالية أو أي سلعة أخرى.[2]

ويتضح من ذلك أن المشرع الفرنسي عاقب على الإبتزاز إن كان الغرض محدد وهو الحصول على توقيع أو تعهد أو تخلي أو كشف عن سر أو تحويل أموال أو أوراق مالية أو أي سلعة أخرى، وأن يتم ذلك بالعنف، أو التهديد به، أو التهديد بكشف وقائع، أو ادعائها.[3]

ويحمد للمشرع الفرنسي أنه ذكر هذه الجريمة بصورتها في موضع واحد

2/ بالنسبة للمشرع المصري:

وبالنسبة للمشرع المصري فقد جمع بين تحديد مضمون التهديد في الإبتزاز، والغرض منه كما في المادة 325 من قانون العقوبات التي تنص على أنه" كل من إغتص بالقوة أو التهديد سندا مثبت أو موجوداً لدين أو تصرف أو براءة أو سندا ذا قيمة أدبية أو اعتبارية أو أوراقاً تثبت وجود حالة قانونية أو اجتماعية أو كره أحداً بالقوة أو التهديد على

[1] زينب محمود حسين، المرجع السابق، ص574.

[2] المرجع نفسه، ص_ص، 574_575.

[3] المرجع نفسه، ص575.

إمضاء ورقة مما تقدم أو ختمها يعاقب بالسجن المشدد".[1]

وتنص المادة 326 من ذات القانون على أنه:" كل من حصل بالتهديد على إعطائه مبلغا من النقود أو أي شيء آخر يعاقب". المشرع المصري في بعض النصوص الأخرى إلى العقاب على الإبتزاز محدداً مضمون التهديد في الإبتزاز دون تحديد الغرض من التهديد، وبالتالي يقع الإبتزاز طالما تم التهديد بالإفشاء مثلا للقيام بعمل أو الإمتناع عن عمل.[2]

2/ الإبتزاز الإلكتروني بالنسبة للمشرع الجزائري:

يعد الإبتزاز الإلكتروني في القانون الجنائي الجزائري نوعاً من أنواع جريمة السرقة، فهو محوره التهديد بنشر المعلومات الخاصة التي يكون المبتز سرقها من الضحية.[3]

فانتهاك جريمة الإبتزاز الإلكلتروني لمفهوم الخصوصية في نطاق الرقمنة، فالحق في الخصوصية من الحقوق الدستورية الأساسية الملازمة واللصيقة للشخص الطبيعي بصفته الإنسانية كأصل عام.[4]

ولو أن القانون الجزائري لا يحدد هذا المفهوم ومحدداته مما ينبئ عن تعقده وتشعب مراميه، بحيث يصبح الشخص معرضا للإنتهاك متى تم تسجيل محتوى متعلق به في العالم الرقمي، مما يجعله غير قابل للمحو.[5]

فالابتزاز بشكل عام تعرف بأنه: سلوك يتضمن مساومة الشخص للحصول على مكاسب

---

[1] زينب محمود حسين، نفس المرجع، ص575.

[2] المرجع نفسه.

[3] بحث عن جريمة الإبتزاز، اطلع عليه بتاريخ 21ماي 2023 الساعة 10:10.online. Legal-research.

[4] فاطمة العرفي، **حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون الجزائري، مجلة صوت القانون**، المجلد الثامن، العدد خاص 02، 2022 ، ص494.

[5] المرجع نفسه.

مادية أو معنوية أو جنسية أو لمجرد الإنتقام عن طريق وسائل الإكراه والقسر بتهديده بإفشاء أسرار ممكن أن تسيء له أو تلحق الضرر به، وهو أنواع منه الإبتزاز الإلكتروني الذي يعني التهديد والمساومة التي تقع بواسطة آلية إلكترونية، أو هو الحصول على معلومات سرية إلكترونية تتعلق بالمجني عليه لا يرغب وصولها للآخرين والتهديد بإفشاء السر أو نشر المعلومات إن لم تتحقق مطالبه وتنفذ، مما يؤثر على إرادة ونفسية المجني عليه، فيستجيب لرغبات الجاني.[1]

فالإبتزاز في مضمونه طلب خدمة من شخص مع العلم المسبق بعدم قدرته المطلقة على قيامه بها، فهو إذا في معناه الدقيق استخدام المبتز سواء أكان شخصا أم تنظيما أسلوب من أساليب الضغط المادي أو المعنوي لدفع الضحية لنهج سلوك معين يجلب المنفعة للجهة المبتزة، متبعا أسلوب التهديد بالتشهير بالضحية على أوسع نطاق، حتى يجعل الضحية تقع تحت وطأة ضغوط المبتز ليجبرها على مجاراته وتحقيق رغباته الجنسية أو المادية، مما يعني أن محل الإبتزاز خدمة تقترن الفعل المؤذي بالرضا، لذا لابد من توافر القصد الجنائي من خلال اتجاه نية المبتز لاستعمال التهديد والمساومة من أجل الحصول على الخدمة مع العلم المسبق بعدم القدرة على الدفع.[2]

من هذا المنطلق يمكن إعتبار ابتزاز الأشخاص ضمن هذا المفهوم الذي ذكرته المواد 284 و286 و371 من قانون العقوبات الجزائري، ولو أنه كان من الأفضل ذكرها في نصوص قانونية واضحة تأخذ بعين الإعتبار المستجدات التكنولوجية التي أصبحت جزء

---

[1] نجاء المطيري، سامي مرزوق، **المسؤولية الجنائية عن الإبتزاز الإلكتروني في النظام السعودي دراسة مقارنة**، رسالة مقدمة استكمال لمتطلبات الحصول على درجة الماجستير في الشريعة والقانون :إشراف عبد الفتاح باباه، الرياض، أكاديمية نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، ص 13.

[2] ممدوح رشيد مشرف الرشيد العنزي، **الحماية الجنائية للمجني عليه، المجلة العربية للدراسات الأمنية**، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مج 33، العدد70، 2017، ص_ص،193_220.

منها.[1]

وأيضا نظرا لانتشارها وخطورتها على اعتبار أن هذا النوع من المواد المسيئة أصبحت تنتج ثم تروج عبر الوسائط الرقمية، أو تنتج بشكل مباشر أمام جمهور يشاهدها، حيث يتم استغلال قوة الهوية المجهولة للجناة للإساءة للأشخاص، مثل تظاهر المتصيد بأنه صديق حتى يكتسب ثقة الشخص ومن ثم يطلب منه رقم هاتفه بغرض التواصل معه في العالم الحقيقي، لاستغلاله فعليا أو الإكتفاء بالتسجيل أو التصوير أو الدردشة ذات الطابع الإباحي ومن ثم ابتزازه فإن رفض قام بالتشهير به.[2]

سادسا: مفهوم الإبتزاز الإلكتروني

هو كل فعل مبني على الإستخدام السيء للأنترنت الهدف منه تحقيق غرض ما، يختلف هذا الغرض من فرد إلى آخر حسب الظروف المحيطة بكل واحد منهم، إما يكون الغرض ماديا أو جنسيا أو معنويا.[3]

كما يعرف بأنه أسلوب يمارسه المبتز على الضحية عن طريق شبكات التواصل الإجتماعي بهدف الضغط عليه وإجباره على تحقيق مطالبه.[4]

ويعرف الإبتزاز الإلكتروني أيضا بأنه عملية تهديد بنشر صور أو مواد فلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهل العمل أو

[1] فاطمة العرفي، المرجع السابق، ص496.

[2] المرجع نفسه، ص509.

[3] سعيد زيوش، المرجع السابق، ص72.

[4] فيصل بن عبد الله الرويس، **ملخص الوعي الإجتماعي بظاهرة الإبتزاز الإلكتروني لدى الأسرة في المجتمع السعودي، دراسة ميدانية للعوامل والآثار، مجلة كلية الآداب والعلوم الإنسانية**، كلية التربية – جامعة شقراء_ المملكة العربية السعودية، العدد الثالث وثلاثون، الجزء الثاني، ص90.

غيرها من الأعمال الغير قانونية.[1]

و عادة ما يتم تصيد الضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الإجتماعي المختلفة، كالفيس بوك، تويتر، و إنستغرام وغيرها من وسائل التواصل الإجتماعي، نظراً لانتشارها الواسع واسخدامها المتزايد من قبل فئات المجتمع وتزايد عمليات الإبتزاز الإلكتروني في ظل تنامي عدد مستخدمي وسائل التواصل الإجتماعي في إعداد برامج المختلفة.[2]

الفرع الثاني: أنواع الإبتزاز الإلكتروني

تعتبر جريمة الإبتزاز الإلكتروني من الجرائم ذات الأنواع والصور المختلفة والمشبعة، حيث أن هذه الصور تتنوع تارة بالنظر إلى الضحية المستهدفة من الجريمة، وتارة أخرى بالنظر إلى الهدف المترقب من تنفيذه أو المنفعة التي تعود على المجرم.[3]

وتنقسم أنواع الإبتزاز الإلكتروني إلى أكثر من نوع وتم تقسيمها إلى ثلاث أقسام رئيسية، بل هي أكثر هذه الأنواع شيوعا والتي قام الكثير بالإبلاغ عنها بأنهم تعرضوا للابتزاز عبر الكثير من مواقع التواصل الإجتماعي على الأنترنت أو تطبيقات الاتصال المختلفة، ومن أبرز تلك الأنواع هي:[4]

أولا: الإبتزاز الإلكتروني بالنظر لشخصية الضحية

وفيه يتم تقسيم جرائم الإبتزاز الإلكتروني تبعا لشخصية المجني عليه المحتمل كضحية

---

[1] بلال جناجرة، **الأنترنت والإبتزاز الإلكتروني**، دون طبعة، دون دار النشر، 2019، ص14.

[2] المرجع نفسه، ص15.

[3] مريم عراب، **جريمة التهديد والإبتزاز الإلكتروني**، **مجلة الدراسات القانونية المقارنة**، كلية الحقوق والعلوم السياسية، جامعة وهران2، أحمد بن أحمد، المجلد 7، العدد1، 2021/06/28، ص1210.

[4] مطويات عن الإبتزاز الإلكتروني،https://www.eqrae.com،اطلع عليه بتاريخ 2023/05/28،الساعة21:05.

للجريمة وذلك على النحو التالي:

1_ الشخصيات الإعتبارية:

هناك نوع من جرائم الإبتزاز الإلكتروني تكون فيها الفئة المستهدفة كضحية هي الحكومات والشركات والمؤسسات ذات الشخصية المعنوية، وذلك حيث تتم جريمة الإبتزاز عن طريق الحصول على معلومات سرية خاصة بالضحية كمؤسسة أو شركة، والتهديد بالإعلان عن هذه المعلومات ونشرها للآخرين، وقد تبدأ جريمة الإبتزاز بمتطفل أو دخيل على مواقع مهمة، ثم تتمحور شكل الجريمة ليكون التهديد بنشر هذه المعلومات حتى عن طريق السطو على موقع الشخص المعنوي ضحية الجريمة، وابتزازه، لاسيما، وأن المجرم لديه يقين بالجانب المالي للضحية.[1]

2_ الأحداث:

اختلفت التشريعات والأنظمة في تعريف الأحداث، وذلك يرجع إلا اختلاف تحديد سن التمييز وسن الرشد، بسبب العوامل الطبيعية، والإجتماعية، والثقافية الخاصة بكل مجتمع وتفرده.[2]

وتكثر جرائم الإبتزاز الإلكتروني للأحداث وذلك بالضغط على الحديث بتهديده بنشر صور، أو تسجيل مرئي أو محادثات على مواقع الدردشة أو أية مادة عن واقعة من شأنها تحقير المجني عليه عند أهله، والمجتمع.

وتستهدف هذه الفئة من أجل مطامع جنسية، أو تسريب معلومات عن الأهل فيستعمل المجرم جهل الطفل في التصرف ويمارس جريمة الإبتزاز الإلكتروني بعد التسلل إلى عقل الطفل الحدث لأن الأحداث هم أكثر الفئات اتصالا بالتكنولوجيا، ووسائل التواصل

[1] مريم عراب، المرجع السابق، ص1210

[2] المرجع نفسه.

الإجتماعي، بحيث باتت تشكل حيزاً كبيراً من يومهم مما يسهل وقوعهم في الجريمة.[1]

3- النساء:

يعتبر ابتزاز النساء أكثر أنواع الإبتزاز الإلكتروني شهرة وانتشاراً، حيث أن جرائم الإبتزاز الإلكتروني للنساء تعتبر النموذج المثالي للجريمة خاصة إذا كان المبتز رجلا والضحية إمرأة، ويرجع ذلك أنه غالبا ما يكون تهديد المبتز للمرأة يعتمد على الصور، أو محادثات خادشة بالحياء أو عرضا مرئيا لعلاقة غير شرعية جمعت بين المبتز وضحيته...

وقد يكون المبتز قد خطط لجريمته مسبقا، وقد تكون الضحية إمرأة ومن فئة الأحداث والتي غالبا ما تتجاوب مع الإبتزاز خوفاً من العار إذا لم ترفع إلى طلبات المبتز.[2]

4_الرجال:

يقع الرجال مجنيا عليه في جريمة الإبتزاز الإلكتروني للعديد من الأسباب فقد يكون ميسور الحال وعرضة للإبتزاز من بعض النساء، محترفات بيع الهوى على المواقع الإلكترونية، وتهدد بإذاعة صور أو مقاطع مصورة على المواقع الإلكترونية، وتهدده بإذاعة صور أو مقاطع مصورة لتهدد مركزه، كما يكون الرجل عرضة لجرائم الإبتزاز بشكل عام بسبب أسرار في مجال عمله أو عائلته، أو أي معلومات بشكل عام يرى الرجل الضحية أن الإفصاح عنها ونشرها يؤذي شرفه وسمعته.[3]

ثانيا: الإبتزاز الإلكتروني بالنظر إلى الهدف المرجو من المجرم:

[1] آمال برحال، المرجع السابق، ص_ص،12_13.

[2] الحمين عبد العزيز بن حمين بن أحمد، **الإبتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الإبتزاز(المفهوم، الأسباب، العلاج)**، جامعة الملك سعود،2011، ص61.

[3] مريم عراب، المرجع السابق، ص1211.

يختلف الهدف الذي يرجوه المبتز من جريمته باختلاف كل جريمة، وذلك على النحو التالي:

1/ هدف مادي:

من أهم وأكثر الأهداف التي يسعى المبتز إلى تحقيقها من إرتكابه جريمة الإبتزاز هي تحقيق منفعة مادية، وذلك بطلب مبالغ مالية أو عينية ذات قيمة من المجني عليه.[1]

فقد حقق هذا النوع من الإبتزاز بقيام الجاني بتهديد المجني عليه من أجل تسليم أموال أو أشياء أخرى ذات طابع مالي، سواء بطريقة مباشرة أو غير مباشرة...

أما ابتزاز المال بالطريقة غير المباشرة فيتحقق عن طريق طلب المبتز من المجني عليه تسديد مبالغ مالية اقترضها من أحد البنوك أو قيامه بدفع أقساط مالية عند الغير وتسديد ديون مستحقة لمصلحة المبتز.[2]

2/هدف انتقامي:

يؤدي الجانب النفسي دوراً في عملية الإبتزاز الإلكتروني، وذلك باعتبار أن المجني عليه يعيش صراعا داخليا نتيجة أن الجاني سيقوم بتنفيذ تهديداته ضده في أي وقت شاء ما يدفعه إلى تلبية طلبات الجاني تجنبا للفضيحة، حيث يستمتع الجاني بأذية المجني عليه واستماعه لتوسلاته وما يزيد الأمر سواء أن يقوم الجاني بتصوير المجني عليه.[3]

ويطلب منه ذكر أي بيانات تتعلق به كما يكون الدفاع لدى الجاني هو الإنتقام من

---

[1] مريم عراب، نفس المرجع، ص1211

[2] المطلق نورة بنت عبد الله بن محمد، **ابتزاز الفتيات أحكامه وعقوبته في الفقه الإسلامي**، جامعة الإمام محمد بن سعود الإسلامية، الرياض، ص12.

[3] ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص202.

المجني عليه عن طريق إلحاق الأذى به وإساءة سمعته بنشر صوره عن طريق شبكة الأنترنت.

3/ هدف غير أخلاقي (جنسي)

هذا الهدف يبدو واضحا وشائعا حينما تكون الضحية امرأة أو حدث، وأكثر شيوعا حينما تجمع الضحية بين كونها امرأة و حدث في نفس الوقت، ويتحقق هدف المبتز الجنسي حينما يكون المقابل الذي يطلبه لعدم إفشاء أسرار الضحية، وقد يكون الهدف تهديد المجني عليه للقيام بهذه الممارسات مع شخص آخر غير المبتز، ويكون الإبتزاز بطلب المقابل مرة واحدة، أو مرات بحسب ظروف كل جريمة، وإن كان أغلب ضحايا الإبتزاز الجنسي من النساء.[1]

أما الإبتزاز الجنسي الإلكتروني فبتحقق عن طريق وسائل الإتصال الإلكتروني والأنترنت، والمبتز في هذا النوع يعتبر مجرماً خفيا يسعى للحصول على معلومات تخص الضحية.[2]

4/هدف نفعي:

يحقق المبتز هدفه من ارتكاب جريمة الإبتزاز الإلكتروني، بقيامه بتهديد الضحية بإفشاء أسراره ونشرها للملأ، وذلك إذا لم يقم بتحقيق طلب أو مصلحة للمبتز، وقد تكون المنفعة الأمر بتنفيذ سرقة لصالح المبتز، أو ترويج مخدرات، أو التوسط لدى شخص لإتمام عمل سواء كان هذا العمل مشروعاً أو غير مشروع طالما كان العمل ضد إرادة المجني عليه، فقد تحققت جريمة الإبتزاز.[3]

---

[1] مريم عراب، المرجع السابق، ص1211.

[2] ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص201.

[3] مريم عراب، المرجع السابق، ص 1211.

ثالثا: الابتزاز الإلكتروني بالنظر إلى وسائله:

1/ابتزاز مادي:

وهو أن يقوم الجاني بتهديد المجني عليه المرتقب بوسائل مادية ملموسة كالصور والمقاطع المرئية والمستندات، ويكون التهديد مادي الكتروني عن طريق الإتصالات الإلكترونية وهي كل المراسلات والإرسالات التي تقع سواء في شكل علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، يتم تبادلها أو إرسالها بطريق الكتروني عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية.[1]

2/ إبتزاز معنوي:

وهو التهديد بوسائل غير ملموسة، وذلك باستخدام عبارات شديدة للتهديد والوعيد بفضح أمر الضحية.[2]

الفرع الثالث: خصائص الإبتزاز الإلكتروني

لكل ظاهرة إجرامية جديدة أو كل نمط أو سلوك إجرامي حديث خصائص وسمات تميزه عن غيره.[3]

لذلك لابد أن يكون للمجرم المعلوماتي صفات أو خصائص قد لا تتوافر في المجرم الإعتيادي لأن ظاهرة الإجرام المعلوماتي والجريمة الإلكترونية بصفة عامة والإبتزاز

[1] مريم عراب، نفس المرجع، ص- ص، 1211-1212.

[2] المرجع نفسه ص 1212.

[3] محمود أحمد عبانية، **جرائم الحاسوب وأبعاد الدولية**، دار الثقافة للنشر والتوزيع عمان الأردن،2009، ص 4.

الإلكتروني بصفة خاصة هي أنماط إجرامية مستحدثة.[1]

ويمكن القول بأن اختراع الحاسوب وظهور الشبكات المعلوماتية فيما بعد كشبكة الأنترنت، وشيوع وسائل التواصل الإجتماعي أدت إلى تكوين مجرمين يتمتعون بمواصفات ومؤهلات وشخصيات معينة.[2]

فالمجرم الإلكتروني يرتكب جرائمه في أوساط البيئة الحاسوبية والشبكات الإنترنت، ويتمتع بقدر من الذكاء والاحتراف في عمله، كذلك قد يكون هادئ الطباع ولا يميل لاستعمال العنف والقوة وعادة ما يكون المجرم المعلوماتي إنسان اجتماعي بطبعه.

وفيما يأتي نتناول الخصائص العامة للإبتزاز الإلكتروني والسمات التي يتمتع بيها الجاني الذي يقوم بالإبتزاز الإلكتروني على نحو ما يأتي:

أولا: الخصائص العامة للإبتزاز الإلكتروني:

يحتاج الإبتزاز الإلكتروني إلى استخدام تقنية من البرمجيات الحديثة في عالم الإتصال ما بين الأفراد باستخدام الوسائل الإلكترونية الحديثة وشبكة الأنترنت، ولهذا فإن هذه الظاهرة تتمتع بخصائص متعددة تتمثل فيما يلي:

1/الابتزاز الإلكتروني عابر للحدود:

إذا كانت السرقة أو الإحتيال أو الضرب أو غيرها من الجرائم التقليدية الأخرى تتم داخل إقليم الدولة، فإن الإبتزاز الإلكتروني عابر للحدود، فهو لا يحترم الحدود السياسية ومن الممكن ارتكابه عن بعد، مما قد يجعل العالم بأسره مسرحاً جرمياً لمرتكبها، فيمكن

[1] محمد علي العريان، **الجرائم المعلوماتية: انعكاسات دورة المعلومات على قانون العقوبات**، دار الجامعة الجديدة للنشر، الإسكندرية، 2004 ص60.

[2] مدحت رمضان، **جرائم الإعتداء على الأشخاص والأنترنت**، دار النهضة العربية، القاهرة،2000، ص11.

أن يكون الجاني في قارة والمجني عليه في قارة أخرى.[1]

فهذه الخاصية تصنع على الإبتزاز الإلكتروني الصبغة العالمية، حيث يمكن أن يكون الجاني في الإبتزاز الإلكتروني موجوداً في الصين ويكون المجني عليه في العراق، وهو ما يتطلب وجود تعاون دولي في مكافحة هذه الجرائم حول العالم.[2]

إلا أن المشرع الإماراتي قد أشار بصورة صريحة إلى هذه الحالة واعتبر قانون مكافحة جرائم تقنية المعلومات سارياً على كل من ارتكب خارج الدولة إحدى الجرائم الواردة فيه حيث نصت في المادة47 على أنه:"...تسري أحكام هذه المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة، إذا كان محلها نظام معلوماتي الكتروني أو شبكة معلوماتية أو موقع الكتروني أو وسيلة تقنية معلومات خاصة..."[3]

أما بالنسبة للقانون العراقي فقد نص في المادة 6 من قانون العقوبات العراقي رقم 111 لسنة 1999م المعدل على أنه:" تسري أحكام هذا القانون على جميع الجرائم التي ترتكب في العراق وتعتبر الجريمة مرتكبة في العراق إذا وقع فيه فعل من الأفعال المكونة لها أو إذا تحققت فيه نتيجتها أو كان يراد أن تتحقق فيه، وفي جميع الأحوال يسري القانون على كل من ساهم في جريمة وقعت كلها أو بعضها في العراق ولو كانت مساهمته في الخارج سواء أكان فعلا أو شريكة "[4]

ومن خلال النصين القانونين السابقين يمكن للقضاء الإماراتي والعراقي محاسبة الجاني

---

[1] محمد على سالم، حسون عبيد، **الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية**، مجلد 14، العدد2، العراق، 2007، ص92.

[2] عبد الإله محمد النوايسة، **جرائم تكنولوجيا المعلومات–شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية**، ط1، دار وائل للنشر والتوزيع، عمان الأردن،2017، ص_ ص، 78_79.

[3] المادة 47 من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012م.

[4] المادة 6 من قانون العقوبات العراقي، رقم 111 لسنة 1999.

المبتز حتى لو كان خارج حدود البلدين.

أما بالنسبة للمشرع الجزائري تنص المادة الثالثة (03) من قانون العقوبات على ما يلي: "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية"، بمفهوم المخالفة فإن قانون العقوبات الجزائري لا يسري على الجرائم التي تُرتكب في خارج الإقليم الجزائري.[1]

أكد تقنين العقوبات الجزائري مبدأ السريان الإقليمي بنص صريح هو ينص الفقرة الأولى من المادة الثالثة منه، فطبقا لهذا النص فإن تقنين العقوبات الجزائري يسري على كل الجرائم التي ترتكب في الجزائر بغض النظر عن جنسية مرتكبها جزائريا كان أو أجنبيا، وبصرف النظر عن جنسية المجني عليه وبصرف النظر أيضا عن طبيعة الجريمة، وبمفهوم المخالفة فإن هذا التقين لا يسري على ما يرتكب من جرائم خارج الإقليم الجزائري.[2]

2/ الإبتزاز الإلكتروني يمس بحرية الأشخاص:

يتميز الإبتزاز الإلكتروني بكونه من الظواهر الإجرامية التي تمس حرية الأشخاص وحرمتهم، فهي تشبه جرائم السب و القذف أو التشهير وإفشاء الأسرار الشخصية والإعتداء على الحياة الخاصة حيث يقوم الجاني في كثير من الأحوال بالإعتداء على الحياة الشخصية للأفراد ، سواء كانوا أشخاص طبيعيين أو أشخاص معنوية عن طريق إعتداء ملف يحتوي على معلومات أو بيانات شخصية دون علم هذا الشخص.[3]

[1] الفقرة الأولى من المادة 3 من قانون العقوبات الجزائري.

[2] أنظر المادة 3 من قانون العقوبات الجزائري.

[3] زهراء عادل سلبي، **جريمة الإبتزاز الإلكتروني –دراسة مقارنة–**، ط1، دار الأكاديميون للنشر والتوزيع، عمان–الأردن، 2020م، ص61.

ومن ثم يقوم بتهديد بنشر تلك المعلومات الشخصية، مما يمثل إعتداء على الحرية الشخصية والحق في الخصوصية الذي يمثل أهم الحقوق الدستورية.[1]

3/ الإبتزاز الإلكتروني يتم بواسطة الوسائل الإلكترونية الحديثة:

يتم الإبتزاز الإلكتروني عن طريق استخدام الوسائل الإلكترونية الحديثة مما يستلزم لارتكابها وجود أحد الأجهزة الإلكترونية الحديثة كالكمبيوتر أو الهاتف المحمول أو غيرها من الأجهزة الإلكترونية الأخرى...

والدخول إلى أحد برامج التواصل الإلكتروني عبر شبكة الأنترنت من أجل التواصل مع المجني عليه والحصول على الصور أو المقاطع أو البيانات أو المعلومات الشخصية التي يستخدمها المبتز في الإبتزاز، لذلك فإن الجاني يكون بحاجة إلى أدوات تقنية إلكترونية حديثة من أجل القيام بهذه الجريمة، بالإضافة إلى معرفة الجاني لكيفية استخدام تلك الوسائل الإلكترونية التي تتم الجريمة من خلالها.[2]

4/ ظاهرة جرمية بالغة الخطورة:

ظاهرة الإبتزاز الإلكتروني ظاهرة بالغة الخطورة على المجتمع، وهذا يظهر من خلال الخسائر المادية التي تنتج عن هذه الظاهرة كما يصعب معرفة حجم الخسائر المادية الحقيقية التي ترتبت على هذه الظاهرة نتيجة أن الكثير من المنظمات أو الشركات التي تتعرض للإبتزاز الإلكتروني لا تقوم بإبلاغ الجهات المختصة نتيجة خشية التعرض لإساءة السمعة أو التأثير على الوضع المالي لهذه الشركات والمؤسسات وأسهمها في

[1] زهراء عادل سلبي، المرجع السابق، ص61.

[2] بعرة سعيدة، **الجريمة الإلكترونية في التشريع الجزائري –دراسة مقارنة–**، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة الجزائر،2019، ص _ ص، 37_38.

سوق الأوراق المالية.[1]

وبالنسبة للأفراد الطبيعيين تظهر خطورة الإبتزاز الإلكتروني من خلال ما يمسه من شرف الإنسان وسمعته والمساس بحياته الخاصة، علاوة على أنهذه الظاهرة قد تمس الدول في أمنها القومي مما يظهر خطورتها وبالتالي ضرورة مكافحتها من كافة الدول.[2]

لذلك نرى أن المشرع الإماراتي قد نص في المادة 46 من قانون مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012م على أنه:"...كما يعد ظرف مشدداً ارتكاب أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو مصلحة دولة أجنبية أو أي جماعة ارهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة".[3]

5/ صعوبة إثبات الإبتزاز الإلكتروني:

لما كان الإبتزاز الإلكتروني يتم من خلال الوسائل الإلكترونية الحديثة بحيث يقوم الجاني بابتزاز المجني عليه وتهديده عبر هذه الوسائل الإلكترونية فإنه يتعذر إثباته، نظراً لأن عملية الإبتزاز تتم من خلال الوسائل الإلكترونية وهو ما يمكن الجاني من محو أثار فعلته وتدمير كافة الأدلة في وقت قياسي.[4]

كما أن المجني عليه قد يحجم عن التبليغ عن وقوع الجريمة، بالإضافة إلى أن وجود الجاني في دولة أخرى يصعب عملية الإثبات ومن ثم التحقيق أو المعاقبة.[5]

---

[1] زهراء عادل سلبي، مرجع سابق، ص54.

[2] علي حسن الطوالبة، **الجرائم الإلكترونية**، مطبعة جامعة العلوم التطبيقية، البحرين2008، ص60.

[3] المادة 46 من قانون مكافحة جرائم تقنية المعلومات الإماراتي، رقم 5 لسنة 2012.

[4] رحيمة نمديلي، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر "الجرائم الإلكترونية"**، مركز جيل البحث العلمي، طرابلس24-25 مارس2017م، ص102.

[5] المرجع نفسه.

6/ الإبتزاز الإلكتروني من الجرائم الناعمة:

يعد الإبتزاز الإلكتروني أحد أنواع الجرائم الناعمة التي لا تتطلب عنها فالجاني في تلك الجرائم لا يستخدم العنف كما هو الحال في جرائم السرقة أو جرائم الضرب والقتل وغيرها من الجرائم التي يعتمد فيها الجاني على استخدام العنف في تنفيذها، بل تتم هذه الجريمة عبر الوسائل الإلكترونية دون استخدام أي وجه من أوجه العنف، مع المجني عليه...[1]

وهذا ما يراه الباحث أيضا بالنسبة للإبتزاز الإلكتروني فهي من ضمن الجرائم الناعمة التي لا تحتاج أي عنف من قبل الجاني تجاه الشخص المجني عليه.[2]

7/ الإبتزاز الإلكتروني من جرائم الأموال:

ويتحقق ذلك عندما يهدف الجاني الحصول على منافع نقدية أو غيرها، من خلال حصول الجاني على بيانات أو معلومات تجارية ومالية أو براءات اختراع أو غيرها من المعلومات والبيانات التي يترتب على نشرها حدوث خسائر مالية للمجني عليه، مما يجعل محل الإعتداء في تلك الصورة هي الأموال وليس الأشخاص.[3]

ثانيا: سمات الجاني في الإبتزاز الإلكتروني

يتميز المجرم في الإبتزاز الإلكتروني ببعض السمات التي تموه عن المجرمين الآخرين في الجرائم التقليدية وهذه السمات والخصائص تتمثل فيما يلي:

1/المبتز إنسان إجتماعي بطبعه مسؤول عن أفعاله

[1] ذياب موسى البدانية، **الجرائم الإلكترونية المفهوم والأسباب**، ورقة علمية مقدمة خلال الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 2-2014/4، 9م، عمان- الأردن، 2014، ص20.

[2] محمد علي سالم، حسون عبيد، المرجع السابق، ص 92.

[3] زهراء عادل سلبي، المرجع السابق، ص 62.

يجب أن يكون المبتز مسؤولا عن أفعاله الجرمية من الناحية القانونية الجزائية.[1]

ولكي يكون الإنسان مسؤولا جزائيا، يشترط في إرادته أن تكون حرة ومختارة.[2]

وينبغي أن تكون موجهة بصورة محالفة للقانون وهذه الإرادة تسمى بالإرادة الجرمية علما إن المشرع العراقي لم ينص على هذا الأمر بصورة صريحة

فهو إنسان إجتماعي بطبعه ولا تظهر عليه أي علامات الإجرام، يستطيع التحدث واستدراج الضحية من أجل ابتزازها، وتختلف دوافع اللهو أو الكبرياء أو الحصول على منفعة مالية من وراء الجريمة.[3]

2/ المهارة في مجال تكنولوجيا المعلومات:

يتمتع الجاني عادة في جرائم الإبتزاز الإلكتروني بالمهارة في استخدام وسائل الإتصال الإلكترونية الحديثة والإنترنت والمعلومات، بحيث يستطيع الجاني في بعض الأحيان الدخول إلى البيانات الشخصية والصور والفديوهات الخاصة بالمجني عليه عبر استخدام برامج المعلومات والإنترنت ثم ابتزاز المجني عليه، لهذا فإن الجاني يتميز دائما في تلك الجرائم بالمهارة في استخدام تلك الوسائل التي تمكنه من ارتكاب الجريمة ومحو آثارها وأدلتها.[4]

3/ المبتز في الإبتزاز الإلكتروني يتمتع بالذكاء:

---

[1] علي حسين الخلف، سلطان عبد القادر الشاوي، **المبادئ العامة في قانون العقوبات**، مطابع الرسالة، الكويت، 1982، ص328.

[2] أحمد فتحي سرور، **الوسيط في قانون العقوبات –القسم العام–**، الجزء1، دار النهضة العربية، القاهرة ، 1981م، ص465.

[3] المرجع نفسه، ص77.

[4] عبد الإله محمد النوايسة، المرجع السابق، ص 85.

توجد العديد من الدراسات العضوية التي قام بها المختصون بدراسة الظاهرة الإجرامية[1]

للوقوف على أهم العوامل التي تؤدي بالإنسان إلى ارتكاب الجريمة، توصلوا من خلالها إلى نتائج عدة أهمها أنهم قاموا بتقسيم المجرمين إلى أنواع ، وكل نوع يتصف بصفات معينة.

ومما لاشك فيه أن المجرم المعلوماتي يختلف عن المجرم الإعتيادي، فالقيام بارتكاب جريمة معلوماتية يتطلب على الأقل درجة من الدقة والذكاء لكي يتعامل مع جهاز الحاسوب ويختلق الشبكات المعلوماتية ويقوم بوضع فيروسات من شأنها اختراق برامج الحاسوب.[2]

وعليه، يمتاز مرتكبو هذه الجرائم في أغلب الأحيان بالذكاء...، أي أنهم ليسوا كالمجرمين التقليديين، لذا يرغبون في إثبات الذات، وتجربة ما يتمتعون به من قدرة علمية وتسخير ما لديهم من قدرات مالية وتقنية من أجل التفوق على النظم الإلكترونية واختراقها.[3]

وبالتالي يتمتع المجرم في جرائم الابتزاز الإلكتروني بقدر كافي من الذكاء الذي يمكنه من استدراج ضحيته والحصول على الثقة الوهمية والتحايل عليها بفكرة الحب والحنان والعاطفة والأسباب الملتوية المخادعة التي تمكن من استدراج الضحية ثم الحصول على الصور أو مقاطع شخصية فاضحة لها أو بيانات أو غير ذلك مما قد يسيء للفتاة عند نشره ويهددها بالنشر مالم تقوم بدفع أموال أو أن يطلب منها أعمال جنسية غير

[1] محمد شلال العاني، علي حسن طوالبة ، **علم الإجرام والعقاب**، ط1، دار المسيرة، عمان، 1998م، ص57.

[2] محمد علي العريان، المرجع السابق، ص 62.

[3] آمال قارة، **الجريمة المعلوماتية**، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 2002، ص27.

مشروعة، وكل ذلك يستلزم أن يكون هذا المجرم على قدر معقول من الذكاء.[1]

المطلب الثاني: وسائل وأشكال الإبتزاز الإلكتروني وآثاره المترتبة:

إن جريمة الإبتزاز هي جريمة قديمة نوعاً ما لكنها تطورت لتصبح من أكثر الجرائم خطورة خاصة بعدما اتخذت منحنى أكثر خطورة بسبب الثورة التكنولوجية، والمعلوماتية حيث استخل البعض هذه التكنولوجيا للإعتداء على خصوصية الآخرين وتهديجهم بما يحقرهم في المجتمع...

فيقوم المجرم باستغلال ما وصل إليه للضغط والتهديد للضحية.

لهذا فالإبتزاز الإلكتروني يعد أي طريقة تستخدم بواسطة وسائل الإتصال التكنولوجية الحديثة حيث تستدرج الضحية:

- عبر مواقع التواصل الإجتماعي(social media).
- بعض تطبيقات الهواتف الذكية (smart mobile app).

لإغرائهم بالظهور في أوضاع غير لائقة وتصويرهم دون علمهم، وتهديدهم بنشر الصور والمقاطع وتهديدهم ماليا وللقيام بما يسبب خطرا على الضحية.[2]

كما ينوع المجرمون بالإعتداء على عدة معايير مثل الخبرة، أو علاقاتهم بالضحية، أو

---

[1] عبد العزيز بن حمين، **الإبتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، بحوث ندوة الإبتزاز المفهوم، الأسباب، العلاج**، فهرسة مكتبة الملك فهد الوطنية الرياض،1432هـ، ص58.

[2] مازن سمير الحكيم، حسين فتخان منسي، **الإبتزاز الإلكتروني، المفهوم والخصائص وسبل المواجهة، مجلة ثقافتنا الأمنية**، الإصدار الثاني، وزارة الداخلية العراقية، مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد، 2019، ص67.

من حيث المعرفة التقنية، أو من حيث كونهم أفراد، أو ينتمون إلى عصابات منظمة.[1]

فمن حيث الخبرة فقد نجد مجرم متمرس، ومجرم بدائي، ومن حيث العلاقة بالضحية فقد نجد مجرم معروف، ومعلوم الهوية، ومجرم مجهول الهوية، من حيث المعرفة التقنية، لدينا مجرم خبير يستخدم التكنولوجيا، ومجرم يستخدم التلاعب بالمشاعر أما من حيث الفئة لدينا مجرم بشكل فردي ومجرم عصابات منظمة.[2]

هذا ما سيتم التطرق إليه في الفرع الأول الذي يتناول طرق جريمة الإبتزاز الإلكتروني ووسائل ارتكابها، والفرع الثاني يتناول أشكال الإبتزاز الإلكتروني، أما الفرع الثالث تناول أسباب الإبتزاز الإلكتروني وآثاره المترتبة عليه.

الفرع الأول: طرق جريمة الإبتزاز الإلكتروني ووسائل ارتكابها

لكل جريمة خصوصية معينة وطرقاً مختلفة لتنفيذها، وحينما يختار الجاني الطريقة المناسبة التي سيسلكها لارتكاب جريمته فإن لكل طريقة وسيلة مختلفة، وبناء عليه سوف نتعرض لبعض طرق ووسائل الإبتزاز الإلكتروني.[3]

أولا: طرق الإبتزاز الإلكتروني

تتعدد طرق الإبتزاز الإلكتروني على حسب كل مجرم وتخطيط جريمته واحتياجاتها، وذلك على النحو التالي:

1/الحاسب الآلي وملحقاته وبرامجه

يعرف جهاز الحاسب الآلي بأنه: "عبارة عن جهاز إلكتروني كيميائي بصري أو جهاز

[1] آمال برحال، المرجع السابق، ص17.

[2] مرجع نفسه، ص_ص، 17_18.

[3] مريم عراب، المرجع السابق، ص1212.

إعداد معلومات ذات سرعة عالية يؤدي وظائف منطقية حسابية أو تخزينية، ويشتمل على أي تسهيل لتخزين المعلومات أو تسهيل الإتصالات مباشرة سواء المخزنة أو التي تعمل بالاختزان مع هذا الجهاز"[1]

وعرفه البعض الآخر بأنه: "مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة، وهو آلة حاسبة إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة."

وكمثال على استخدام الحاسب كأداة في ارتكاب جريمة الإبتزاز الإلكتروني حيث يقوم أحد الموظفين بالدخول على الحساب الآلي التابع للشركة، ثم يقوم بالدخول إلى المستند الخاص بمعلومات وبيانات الموظفين، فيقوم بالحصول على بيانات ومعلومات سرية عن الموظفين ويبتزهم.[2]

2/ برامج الحاسب الآلي:

ورد تعريف لبرامج الحاسب الآلي في نظام مكافحة الجرائم المعلوماتية السعودي بأنه: "مجموعة من الأوامر والبيانات التي تتضمن توجيهات وتطبيقات حين تشغيلها في الحاسب الآلي أو شبكات الحاسب الآلي، تقوم بأداء الوظيفة المطلوبة".[3]

كما جاء في المادة الأولى من القانون الإتحادي الإماراتي في مكافحة جرائم تقنية المعلومات بأنه: "مجموعة البيانات والتعليمات والأوامر القابلة للتنفيذ بوسائل تقنية

[1] أسامة أحمد المناعسة، وجلال محمد الزعبي، **جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة**، دار الثقافة للنشر والتوزيع، طبعة ثانية، عمان الأردن، 2014، ص27.

[2] مريم عراب، المرجع السابق، ص1212.

[3] المادة5/1 من نظام مكافحة الجرائم المعلوماتية السعودي، الصادر عن مجلس الوزراء، رقم 79، لسنة1428هـ.

المعلومات، والمعدة لإنجاز مهمة معينة."[1]

فبرنامج الحاسوب يعرف أيضا باسم تطبيق أو كيان برمجي وهو عبارة عن مجموعة الأوامر تعطى للحاسوب لتنفيذ مهمة معينة في إطار زمني.

3/ الأنترنت

هو تقنية حديثة، أحدثت ثورة في عالم الإتصالات، حيث تتيح للمستخدمين من كافة أنحاء العالم بالتواصل مع بعضهم البعض، أو الوصول للمعلومات من خلال شبكات الكمبيوتر التي تربط الأجهزة مع بعضها البعض، وقد ظهرت الإنترنت في الولايات المتحدة الأمريكية في عام 1970م، لكن لم يكن استخداما متاحاً للناس إلا في بداية التسعينيات من القرن الماضي.[2]

فالأنترنت هي تلك الشبكة العنكبوتية التي تربط بين كم هائل من الحاسبات، مستعملة في عملية الربط هذه مختلف وسائل الإتصالات السلكية واللاسلكية، مثل الخطوط الهاتفية العامة أو الخطوط الخاصة أو الأقمار الصناعية، أو الكوابل والألياف البصرية، وغيرها من وسائل الإتصالات الحديثة والفائقة السرعة، وتمتد هذه الشبكة حول العالم لتؤلف شبكة دولية هائلة لتبادل المعلومات، بحيث يمكن لمستعملها الدخول إليها في أي وقت ومن أي مكان في العالم على أن يكون معه حاسوب مجهز بوسائط الإتصال بالشبكة لتلقي وإرسال البيانات عبر مزود الخدمة.[3]

وتتم عملية الإبتزاز الإلكتروني كصورة من صور الجرائم المرتكبة في طريق الأنترنت

[1] أنظر المادة الأولى من قانون الإتحادي الإماراتي لمكافحة جرائم تقنية المعلومات رقم 5 لسنة2012.

[2] بلال جناجرة، **الإنترنت والإبتزاز الإلكتروني**، ص2.

[3] ضياء مصطفى عثمان، **السرقة الإلكترونية، دراسة فقهية**، دار النفائس للنشر والتوزيع، الطبعة الأولى 2011، ص25.

بواسطة البريد الإلكتروني، ومواقع التواصل الإجتماعي والهواتف الذكية وملحقاتها وبرامجها.

أ-البريد الإلكتروني:

يعمل البريد الإلكتروني على تبادل الرسائل الإلكترونية بما فيها النصوص والمقاطع الصوتية والصور، وقد وفرت هذه الخدمة كثيرا من الوقت بحيث تصل الرسائل في نفس اللحظة إلى أي مكان في العالم.[1]

فعرفه جانب من الفقه بأنه عبارة عن خط مفتوح على العالم يستطيع الفرد من خلاله إرسال واستقبال كل ما يريد من رسائل، أي رسائل بالصوت والصورة والكتابة.

ويمكن أن نعرف البريد الإلكتروني بأنه: "عبارة عن صندوق بريد مربوط بشبكة الأنترنت يمكن من خلاله نقل واستلام الرسائل بين جميع البشر سواء كان المرسل إليه في البيت المجاور وللمرسل، أو في النصف الثاني من الكرة الأرضية.[2]

تعريف البريد الإلكتروني قانونا: فقد عرفه القانون الأمريكي المتعلق بخصوصية الإتصالات الإلكترونية الصادر عام 1986؛ إذ جاء فيه: "البريد الإلكتروني وسيلة يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تلفزيونية خاصة أو عامة وغالبا ما يتم كتابة الرسائل على جهاز الكمبيوتر ثم يتم ارسالها الكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه إذ يتم إرسالها إلى كمبيوتر المرسل إليه".[3]

أما المشرع الفرنسي في قانون الخاص بالثقة في الإقتصاد الرقمي الصادر في

[1] مريم عراب، المرجع السابق، ص1213.

[2] آمال برحال، المرجع السابق، ص23.

[3] المرجع نفسه، ص_ ص، 23_24.

يوليو2004، إذ جاء فيه: "البريد الإلكتروني هو كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات ويتم إرسالها عبر شبكة الإتصالات عامة وتخزن عند أحكام تلك الشبكة أو في المعدات الصرفية للمرسل إليه ليتمكن هذا الأخير من إستعادتها.[1]

أما المشرع الجزائري فلم يعرف البريد الإلكتروني فقد عرفه رسالة البيانات في المرسوم التنفيذي رقم 11 – 121 بأنها: "تبادل وقراءة وتخزين معلومات في شكل رسالة معطيات بين الموزعات الموجودة في مواقع متباعدة ، ويمكن المرسل إليه أو المرسل إليهم قراءة الرسالة المبعوثة في وقت حقيقي أو في وقت مؤجل".[2]

من خلال التعريفات السابقة يتضح أن القوانين التي عرفت البريد الإلكتروني لم تختلف في مضمون هذا الأخير، إنما الاختلاف بالصياغة فقط، أما التشريعات العربية لا تزال بعيدة كل البعد عن معالجة التطور الحاصل في مجال التقنية.[3]

من خلال ما سبق ذكره فالبريد الإلكتروني يحتاج لحماية جزائية نظراً لعدة دواعي أهمها: حماية الحقوق، وخاصة الحق في الخصوصية التي بها وجهان متلازمان، وهما حرية الحياة الخاصة، وسرية الحياة الخاصة.[4]

وحرية الحياة الخاصة؛ تعني حرية الفرد في اخيار أسلوب حياته دون تدخل من الغير أو السلطة، لكنها ليست مطلقة، بل مقيدة بنظام اجتماعي ويضع القانون حدود لها، أما بالنسبة لسرية الحياة الخاصة؛ فتعني سرية كل ما ينتج عن ممارسة الفرد لحياته

[1] آمال برحال، المرجع السابق، ص24.

[2] أنظر المرسوم التنفيذي 11-121 في التشريع الجزائري.

[3] عدي جابر هادي، **الحماية الجزائية للبريد الإلكتروني، دراسة مقارنة**، بحث مقدم **بمجلة رسالة الحقوق**، لسنة الثانية، العدد الثالث، كلية القانون، جامعة القادسية، 2010، ص156.

[4] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط2، دار الثقافة للنشر والتوزيع، عمان– الأردن، 2010، ص167.

الخاصة...

وهو نطاق شخصي يرتبط بالشخص ذاته، ويشمل جميع البيانات والوقائع التي يقرر الشخص الإحتفاظ بها لنفسه.[1]

ب- مواقع التواصل الإجتماعي (خدمة الدردشة):

خدمة الدردشة هو برنامج يسمح بتجمع عدد من الأشخاص في جميع أنحاء العالم للتواصل مع بعضهم البعض إما كتابة أو صوتاً أو عن طريق الفيديو.[2]

فتشتغل شبكة الأنترنت بتطلب الأشخاص القائمين عليها، على تخزين ونقل وعرض المعلومات، ويطلق عليهم الوسطاء في خدمة الأنترنت وبتالي يمكن للمستخدم من دخول شبكة الأنترنت والتجول فيها والإطلاع على ما يريد، والوصول إلى المواقع، وانتاج المعلومات وتزويدها وتخزينها.[3]

وهذا ما يتم عند محاولة شخص الولوج إلى Facebook أوtwitter أوinstagram أوwhatsaap، وغيرها من المواقع التواصل الاجتماعي، حيث تعتمد على النظام المعلوماتي عبر شبكة الأنترنت...[4]

أما مواقع التواصل الإجتماعي فيمكن تعريفها على أنها: "تلك الوسائل التقنية الحديثة التي يستخدمها الأشخاص في ما بينهم لتحقيق التواصل الإجتماعي المشاع عبر شبكة

---

[1] نهلا عبد القادر المومني، المرجع السابق، ص167.

[2] مريم عراب، المرجع السابق، ص1213.

[3] بوقرين عبد الحليم، **المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الإجتماعي – دراسة مقارنة**، بحث مقدم في **مجلة جامعة الشارقة، دورية علمية محكمة**، المجلد 16، العدد01، يونيو، 2006، ص373.

[4] المرجع نفسه، ص373.

الأنترنت، كالفيس بوك، تويتر، اليوتيوب وغيره...."[1]

4/ الهواتف النقالة وملحقاتها وبرامجها:

يستخدم الهاتف النقال بواسطة المجرم الإلكتروني باعتباره أداة لارتكاب الجريمة، وذلك عندما يستخدم الإنترنت في برامج التواصل، كأن يقوم بالتجسس على الآخرين، بالاستعمال غير المشروع لتكنولوجيا الإتصالات والمعلومات الخاصة بالهاتف النقال والذي من شأنه الإضرار بمصلحة الغير أو تعريضها للخطر، أما ملحقات الهاتف فهي الكاميرا والبلوتوث وآلات التسجيل، أما البرامج فهناك أيضا مجموعة من البرامج الخاصة بالهاتف المحمول.[2]

والتي تسمح بمعاينتها من قبل الآلة لبيان أو أداء أو إنجاز وظيفة مهمة أو نتيجة معينة صادرة عن آلة قادرة على مناقشة المعلومات.[3]

وتنقسم برامج الهواتف الذكية إلى برامج أساسية فيظهر في شكل برامج تطبيقية تهدف للقيام بمهام محددة ومن أمثلة على ذلك الماسنجر، الفيس بوك، أما البرامج غير الأساسية وهي المعلومات التي تتميز بها الهواتف الذكية وتظهر في شكل وسيط أو أداة تغطي خدمة معينة كرسائل البريد الإلكتروني والبريد النصي والصور الرقمية ومقاطع الفيديو المخزنة، وقد تتضمن أسرارا قد تشكل خطرا على المصلحة العامة أو تهديدا لها.[4]

---

[1] أحمد حسن عبد العليم حسن الخطيب، **الجرائم المعلوماتية الواقعة عبر مواقع التواصل الإجتماعي**، مقال منشور **بمجلة الدراسات الإفريقية والنيل، مجلة دورية محكمة تصدر عن المركز الديمقراطي العربي**، برلين–ألمانيا، المجلد 02، العدد06، أكتوبر1019، ص113.

[2] مريم عراب، المرجع السابق، ص1213.

[3] محمد التوجي، **الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال**، رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية جامعة أحمد دراية، أدرار، 2019، ص12.

[4] أمال برحال، المرجع السابق، ص_ص، 29_30.

وقد تكون هذه المعلومات محلا لجريمة الإبتزاز الإلكتروني، بقيام المجرم الإلكتروني باستخدام الأنترنت في برامج التواصل الإجتماعي...[1]

ثانيا: وسائل الإبتزاز الإلكتروني

هناك العديد من الوسائل التي يستخدمها المبتز في سبيل وصوله لهدفه من الجريمة، وهي من ضمن الأسباب الرئيسية التي تجعل المجني عليه يذعن لرغبات المجرم ملبياً إياها، وتتنوع بدءاً من الصورة أو تسجيل صوتي للضحية، وقد تكون الوسيلة تجمع ما بين الصورة والصوت في تسجيل مرئي، وقد تكون أيضا الحصول على أسرار تمس الحياة الخاصة للضحية عن طريق وثائق وبيانات، وهناك وسيلة استخدام الألفاظ والعبارات ذات الوعيد.[2]

كما أن هناك حالات أخرى كاختراق الحسابات الإلكترونية كمواقع التواصل الإجتماعي مثل فيس بوك وماسنجر فيحصل الجاني على معلومات وصور خاصة للضحية ثم يقوم المحتال بابتزاز الضحية وطلب مبالغ طائلة منه أو فضحه.[3]

الفرع الثاني: أشكال الإبتزاز الإلكتروني

يوجد العديد من أشكال الإبتزاز الإلكتروني حيث تتركز أشكاله وتتحدد بتغير الأهداف المرجوة من عملية الإبتزاز، لذلك سنذكر أهم أشكال الإبتزاز الإلكتروني والتي نصنفها كما يلي:

أولا: ابتزاز الكتروني عاطفي

[1] آمال برحال، نفس المرجع، ص30.

[2] مريم عراب، المرجع السابق، ص1213.

[3] سعيد زيوش، المرجع السابق، ص72.

ونقصد بيه تلك الأفعال التي يقوم بيها المبتز الذي لديه معلومات كافية عن الشخص المراد ابتزازه عاطفيا من أجل تحقيق هدف معين، هذا الهدف قد حدده المبتز من أول لقاء بينه وبين ضحيته، وبالتالي تحديد الطرق الكفيلة بإيقاع الضحية لهذا الفخ، ثم المضي قدماً في تحقيق ما حدده سابقاً مع توخي أقصى درجات الحيطة والحذر.[1]

إن الإبتزاز العاطفي عن طريق شبكة الأنترنت هو من أهم الأشكال الفعالة للتلاعب بالضحية، حيث يقوم المبتز بالإساءة للضحية طالباً الرضوخ لتحقيق غاياته التي حددها في عملية البحث عن الضحايا عبر شبكة التواصل الإجتماعي من فيس بوك، تويتر، انستغرام، أو غيرها من شبكات التواصل الأخرى، حيث يستعمل المجرم المبتز معلومات خاصة استطاع أن يجمعها عن طريق التواصل الدائم بينه وبين الضحية المبني على أساس في الظاهر على الثقة المتبادلة، لكن في حقيقة الأمر ما هو إلا وسيلة من وسائل جمع البيانات والمعلومات الخاصة عن الضحية، حتى يتم استعمالها ضدها عندما يحين الوقت.[2]

ثانيا: الإبتزاز الإلكتروني المهني

ونقصد بيه قيام المجرم المبتز الذي يكون عادة مسؤولاً عن الضحية في العمل وبالتالي يمتلك المجرم المبتز المعلومات الكافية عن الضحية، حتى يبدأ بالإبتزاز موجها عدة طلبات أو لتحقيق أهداف معينة كتحقيق ساعات عمل إضافية أو التخلي عن تحفيزات مالية، أو تحقيق رغبات جنسية، وإلا سيكون التهديد بطبيعة الحال بكشف أسراره الخاصة والتي عادة تكون متعلقة بالعمل أو غيره.[3]

[1] سعيد زيوش، نفس المرجع، ص72.

[2] المرجع نفسه.

[3] المرجع نفسه، ص_ ص، 72_73.

ثالثا: الإبتزاز الإلكتروني السياسي

والغرض منه تحقيق مكاسب سياسية على حساب الضحية الذي وقع فريسة لهذا المجرم المبتز، حيث يعمد هذا النوع من المجرمين إلى البحث عن الهفوات والأخطاء، أو إنجاز مواقع تحت أسماء مستعارة ونشر الوثائق المزورة أو الأخطاء التي وقعت فيها الضحية بهدف تحطيم السيرة السياسية للضحية، أو التأثير عليه حتى يتنازل عن بعض ما طلب منه.[1]

رابعا: ابتزاز الكتروني مادي

وهو محاولة الحصول على المكاسب المادية عن طريق الإكراه استغلالا لحالة ضعف، والإبتزاز ضعف العلاقة وهشاشتها بين ضعاف النفوس، كما يبين تأثير المال على هذه النفوس، وكيف يستبطن الحقد والكره مكان الحب والمحبة.[2]

والغرض منه أيضا تحقيق الربح المادي ونيل مبالغ مالية، عن طريق تهديد الضحية بفضح بعض الحقائق الشخصية المتعلقة بيه، مثل تركيب الصورة الشخصية للضحية باستعمال برامج تحسين وتعديل الصور، بصورة إباحية أو في أوضاع مخلة بالحياء، والهدف منه التهديد للضحية للرضوخ لمطالب المجرم المبتز الذي يقوم بطلب مستمر للمبالغ المالية، وفي حالة إعلان الرفض من طرف الضحية سيكون هناك تهديد بنشر هذه الصور والحقائق زوراً وبهتاناً على مستوى شبكات التواصل وعلى مستوى المواقع يكون الضحية مشتركة فيها.[3]

---

[1] سعيد زيوش، نفس المرجع، ص73.

[2] سليمان الغديان، وآخرون، المرجع السابق، ص174.

[3] سعيد زيوش، المرجع السابق، ص73.

الفرع الثالث: أساب الإبتزاز الإلكتروني وآثاره المترتبة عليه

تتعدد أسباب ودوافع الإبتزاز بحسب شخصية الهدف ومدى قابلية للدخول في هذه الدائرة وكذلك بتنوع دوافع وأسباب المبتز، ولكن في جميع الأحوال يبقى الحافز الرئيسي هو الخلل السلوكي، سواء عند المبتز أو الضحية.[1]

وهذا ما سنتناول في هذا الفرع أسباب الإبتزاز الإلكتروني ثم نتطرق إلى آثاره المترتبة عليه.

أولا: أسباب الإبتزاز الإلكتروني

يعد الإبتزاز الإلكتروني من أخطر الجرائم المعلوماتية التي تهدد استقرار وأمن المجتمع، لما يصاحبه من مشكلات سلبية على الفرد والمجتمع، والتي تكون مدفوعة بعدد من الأسباب الدينية أو النفسية أو السياسية أو الإقتصادية أو الإجتماعية.[2]

أساليب الإبتزاز التي يمارسها المبتز على الضحية، فيعتمد على أسلوب التهديد، سواء كان التهديد بالتشهير، أو التهديد بإبلاغ ذوي الضحية، زوجة كان أو أب أو أخاً الأمر الذي يجعل الضحية تقع تحت وطأة ضغوط المبتز ليجبرها على مجاراته في تفي تحقيق غاياته[3]

فهناك أسباب عدة تؤدي إلى بزوغ ظاهرة الإبتزاز بصفة عامة والإبتزاز الإلكتروني

[1] زينب محمود حسين، المرجع السابق، ص577.

[2] مرجع نفسه ، ص577.

[3] المرجع نفسه.

بصفحة خاصة منها:[1]

1/ أسباب إجتماعية:

وتتمثل في الظروف المحيطة بالضحية بجمع مراحله العمرية، من حيث علاقته مع الغير، مثل الأسرة والمدرسة والعمل والأصدقاء وكيفية استثمار أوقات فراغه.[2]

ومن أسباب الإجتماعية الأخرى، الجهل بكثير من الأمور وعدم معرفة الحقائق، سواء ما يتعلق بسوء التنشئة الإجتماعية للأبناء، أو عدم مراقبتهم وتوعيتهم بمخاطر استخدام الأنترنت، هذا بالإضافة إلى ضعف الضبط الإجتماعي وحب التقليد والتجربة والتأثر بالأصدقاء.[3]

2/ أسباب نفسية:

هناك أسباب نفسية التي لها أثر كبير في توجيه الفرد إلى أعمال الخير والشّر، مثل النفس الأمارة بالسوء، وضعف الوازع الديني والفراغ الروحي والعاطفي.[4]

بمعنى آخر ضعف الوازع الديني للمبتز، واللامبالاة في حدود الله التي رسمها لعباده وحذر من الإقتراب منها، ومن أهم تلك الحدود هو عدم قذف المحصنات من النساء، حيث يقول سبحانه في محكم كتابه المجيد: "إن الذين يرمون المحصنات الغافلات

---

[1] محمد سعيد عبد العاطي محمد، محمد أحمد المنشاوي محمد، **دور القانون الجنائي في حماية الطفل من الإبتزاز الإلكتروني –دراسة مقارنة–** ، **مجلة البحوث الفقهية والقانونية**، العدد السادس والثلاثون، إصدار أكتوبر، 2021م، ص137.

[2] محمد سعيد عبد العاطي محمد، وآخرون، المرجع السابق، ص137.

[3] فيصل بن عبد الله الرويس، المرجع السابق، ص93.

[4] محمد سعيد عبد العاطي محمد، وآخرون، المرجع السابق، ص137.

المؤمنات لعنوا في الدنيا والآخرة ولهم عذاب عظيم".[1]والذي يكون سبب قصور أو ضعف في الخلفية الدينية لدى الفرد وتركيزه على الجوانب النظرية دون الإهتمام بالجانب التطبيقي.[2]

3/ أسباب تقنية:

بسبب التقدم المتلاحق لوسائل تقنية المعلومات وهناك أشياء يجب إشباعها لدى الطفل حتى لا يكون فريسة لمجرمي الإبتزاز الإلكتروني منها: الإستقلالية والإعتماد على النفس؛ القبول من الأسرة لطفلهم، وعدم رفضه في شخصيته أو إمكاناته وقدراته، التقدير والإنتماء بحيث تشعره الأسرة بأهمية، وضرورة بناء العلاقات الأسرية على الحوار الفعال، وعدم إطلاق الأحكام، وتحقيق العدالة، ضرورة متابعة الأطفال عند استخدام لوسائل تقنية المعلومات، التربية القاسية التي قد تؤدي إلى تقليل الثقة المتبادلة بين الوالدين والأبناء، مما يترتب عليه عدم الشعور بالأمان وفقدان الجراءة، عدم وجود الحوار الودي بين الأبناء وأسرارهم حول فوائد وأضرار شبكات التواصل الإجتماعي.[3]

التفكك الأسري وتقصير الوالدين في القيام بواجباتها تجاه الأبناء، وخاصة الفتيات بمتابعة سلوكهن، وعدم تأسيس فجوة اجتماعية بين الآباء والأبناء، لئلا تكون فريسة سهلة للإبتزاز، بعد أن تقع في وهم إهتمام المبتز، تمهيداً للإستيلاء على جميع المسائل الشخصية ذات السرية التامة في حياتها الإجتماعية.[4]كما يظهر في عدم قيام الأفراد في

---

[1] زينب محمود حسين، المرجع السابق، ص577.

[2] فيصل بن عبد الله الرويس، المرجع السابق، ص93.

[3] يراجع في هذا الشأن: مقال بعنوان الإبتزاز الإلكتروني –أسباب الوقوع فيه وطرق الحماية منه–، منشور بتاريخ 17 ديسمبر 2019 ، منشور على موقعhttps://comlthread-1210118_Ohtml ، خمس معايير لحماية الأطفال من الإبتزاز الإلكتروني–جدة، منشور بتاريخ 3 يوليو2016.

[4] زينب محمود حسين، المرجع السابق، ص_ص، 577_578.

الأسرة بواجباتهم، والتي نظهر صورة ذلك في عدم كسب الأب لقمة العيش، وعدم توجيهه أيضا الأبناء وزرع القدوة الحسنة داخلهم بحسن التصرف في الحياة.[1]

كما أن اجتياح وسائل التواصل الإجتماعي حياة الأفراد، خاصة بعد انتشار شبكة الأنترنت التي ألغيت بسببها كل الحواجز، وأصبح من السهل استخدامها في أي وقت وأي مكان تعد سببا واضحاً.[2]

4/ أسباب الإقتصادية:

فالجوانب الإقتصادية تؤدي دوراً على سلوكات الناس إما سلباً أو إيجاباً حيث نجد أن الجوانب الإقتصادية لها دور على كل من المبتز والضحية كما يظهر تأثيره من الجانبين جانب الفقر والحاجة والغنى والترف .[3]

أما الضحية فإنها كلما كانت فقيرة محتاجة فإن استغلالها من قبل ضعفاء النفوس يكون أسهل، فيبتز المجرم المرأة أخلاقيا مستغلا حاجتها للوظيفة أو يهددها بالفصل من العمل الذي تحتاجه، وهذا النوع من الإبتزاز يسمى الإبتزاز لاستغلال الحاجة والفقر مقابل العرض والشرف وهو ما قد تلجأ إليه الضحية لسد حاجاتها ودفع الفقر.[4]

وتعد البطالة سبباً أساسيا أيضا ترتبط بها جريمة الإبتزاز، حيث إن الجرائم الإلكترونية شأنها شأن الجريمة التقليدية ترتبط بالبطالة والظروف الإقتصادية الصعبة وتتركز البطالة بين قطاعات كبيرة من الشباب.[5]

5/ أساب سياسية:

[1] فيصل بن عبد الله الرويس، المرجع السابق، ص93.

[2] المرجع نفسه.

[3] سليمان الغديان، وآخرون، المرجع السابق، ص177.

[4] المرجع نفسه.

[5] زينب محمود حسين، المرجع السابق، ص578.

_ انتشار القنوات الفضائية غير المحافظة، حيث ظهرت بعض برامج القنوات الفضائية والإعلام الهابط، من الأفلام والمسلسلات والأغاني...الخ التي تعرض في هذه الفضائيات المشاهد المحرمة التي توجع العواطف وتلهب المشاعر ويشاهدها غير المحصنين. مما حزا كثيرا من الشباب من الجنسين على إقامة علاقات محرمة وجعلهم يستهلون طريق الحرام.[1]

حيث تقوم وسائل الإعلام المختلفة بدور مهم وخطير في توجيه الرأي وتسويق الأفكار والثقافات، فالإعلام دور كبير في قيادة المجتمع نحو الخير أو الشر، وللأسف الشديد أن الواقع الإعلامي الغالب اليوم بوجه المجتمعات عموماً نحو هاوية الإنحراف ويشبع فيها ثقافة الإجرام بكافة صوره وأشكاله، حيث أصبع الوصول سهلا لكافة المعلومات والبرامج بما في ذلك الأفلام المثيرة للغرائز وتدعو لبناء العلاقات غير مشروعة بين الشباب والفتيات.[2]

حيث أظهر استفتاء أجرته الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر من خلال موقعها الإلكتروني عن أسباب جريمة الإبتزاز ذكر من المشاركين أن الإعلام الهابط من أبز أسباب هذه الجريمة.[3]

ثانيا: آثار المترتبة على الإبتزاز الإلكتروني:

تتعدد الآثار الناتجة عن جرائم الإبتزاز الإلكتروني، نظراً لكثرة الأمراض والإضطرابات التي توقعها على الأفراد والمجتمعات.[4]

وجريمة الإبتزاز الإلكتروني آثار خطيرة، ومتنوعة، ونتناول هذه الآثار على النحو التالي:

[1] سليمان الغديان، وآخرون، المرجع السابق، ص176.

[2] مرجع نفسه، ص_ص، 176_177.

[3] المرجع نفسه، 177.

[4] سليمان الغديان، وآخرون، المرجع نفسه، ص179.

1/ الآثار الشرعية:

من أعظم المفاسد والآثار السيئة لجريمة الإبتزاز، الوقوع في معصية الله تعالى، وانتهاك محارمه، الأمر الذي يعرض الفرد و المجتمع لعقاب الله تعالى وسخطه، لاسيما ذا جاهروا بالمعاصي وأعلنوها.[1]

2/ الآثار النفسية:

وهي تؤدي دوراً في الآثار المترتبة على الضحية فإن آثار الإبتزاز الجنسي يتمثل في عدة آثار نفسية تلازم الضحية طول حياته، وقد تتطور لتصبح استمرارية حياته أمراً مستحيلا، مما يفقده الثقة بالآخرين وبالذات، ويجعل من الضحية شخصية غريبة الأطوار وغير سوية، وتصاب بالأمراض النفسية المستعصية كالإكتئاب والإنهيار العصبي والقلق المزمن، والتوتر والشعور الدائم بالذنب، والأرق والسهر، وصعوبات النوم، وتكرار الكوابيس الليلية، وعدم التركيز، والخوف مما يؤدي ذلك إلى قيام حالة نفسية لدى الضحية بسبب الضغوطات تجعله يفكر بالتخلص من ظلم الجاني بأي طريقة كانت، وخاصة إذا تمادى الجاني في ايقاع ظلمه على الضحية فذلك قد يؤدي إلى أن يفكر الضحية بإيذاء نفسه كالإنتحار مثلا، وترك العمل أحيانا رغم الحاجة إلى المال والعصبية التي تنعكس على العمل والبيت، وقلة الإنتاج في العمل كما تؤدي أحيانا إلى الإنهيار العصبي، وقد يصاب بالنظرة العدائية لمجتمع، مما يدفعه للإنتحال الجرم الجنسية نفسية أو غيره.[2]

3/الآثار الأمنية:

تؤدي الجرائم الجنسية وجرائم الإبتزاز وغيرها من الجرائم إلى خلخلة الأمن في المجتمعات ويحول المجتمع إلى غابة وحشية، فلا يأمن الفرد فيه على نفسه وأهله، وكون الأمن

[1] زينب محمود حسين، المرجع السابق، ص579.

[2] نسرين عبد الحمين، نبيه، **الإجرام الجنسي**، دار الجامعة الجديدة، الطبعة الألى، الإسكندرية، 2008.ص39.

والأمان من أهم معايير الحكم على المجتمع القويم والسليم والإجرام بكل أنواعه يؤدي إلى انهيار القيم والأخلاق في المجتمع المسلم وتؤدي إلى فتك كيانه، وزعزعته وانتشار الرذيلة فيه.[1]

كما أن جريمة الإبتزاز إذا كان الغرض منها مالي سيؤدي ذلك إلى زيادة جرائم النصب والسرقة خاصة إذا كان الضحية معسر ولا يملك ما يقدمه للمبتز لقاء صمته، أما إذا كان الهدف منه جنسي غير أخلاقي فهذه الجريمة لا تكون منفردة بل تصاحبها جرائم أخرى كالإغتصاب، الزنا، السرقة...[2]

كما قد يؤدي إلى جرائم القتل حيث يقوم المبتز بقتل ضحيته بعد ارتكاب الفاحشة وتصويره لها، فإذا ما تم تداول صور الجريمة يقوم أهل الضحية بقتل المبتز المعتدي انتقاماً منه خاصة في بعض المجتمعات التي لا ترى غسل العار إلى بسفك الدم.[3]

4/ الآثار الإجتماعية:

تتنوع الآثار الإجتماعية التي تحققها جرائم الإبتزاز وهي على عدة مراتب وأنوع منها:

أ_ ما يترتب على الفرد:

فخاصة إذا كانت الضحية هذه فتاة فإن فرصها في الزواج تصبح قليلة بل معدومة لإعراض الناس عنها وربما ترفض هي الزواج وتحجب عنه إضافة إلى صعوبات التعامل مع الآخرين ورغبتها الجامحة في الإنتقام من المجرم ومن ذاتها والشعور بنقد الذات، إضافة إلى شعورها بالإهانة من الذات، والخجل وتدني مفهوم الذات لديها، وسيطرة

[1] سليمان الغديان، وآخرون، المرجع السابق، ص179.

[2] محمد بن عبد المحسن بن شلهوب، **جريمة الإبتزاز الإلكتروني، دراسة مقارنة –بحث تكميلي– لنيل درجة الماجستير في السياسة الشرعية**، المعهد العالي للقضاء، قسم السياسة الشرعية، شعبة الأنظمة، جامعة الإمام محمد بن سعود الإسلامية، 2011، ص58.

[3] مرجع نفسه، ص59.

الأفكار غير المنطقية على تفكيرها، وكثرة الشكوك، وعدم القدرة على التركيز والإستقرار و الإتجاه السلبي للزواج.[1]

وقد يتم اغتصاب الفتاة بالإنصياغ إلى رغبة المجرم، وقد ينتج عن ذلك حمل الفتاة وقد يترتب عن ذلك قيامها بالإجهاض أو قتل الطفل غير الشرعي، وقد تقوم الفتاة بالتخلص من الطفل بإيداعه للملاجئ أو الشارع ويصبح من أولاد الشوارع والمنحرفين فيكون مصيره إما السجن أو القتل.[2]

كما يهدد الإبتزاز المستقبل الإجتماعي لضحية حيث تظل آثاره تلاحقها في المجتمع الذي سمع وشاهد فضيحتها بالصوت والصورة.[3]

ب/ ما يترتب على المجتمع ككل:

إن انتشار مثل هذه الجرائم وتوسيعها في ضوء التطورات التكنولوجية تؤثر على قواعد بناء وتكوين الأسر والمجتمعات، مما يجعل المجتمعات سلاحاً بين المجرمين الراغبين، بهتكها وهدمها على أهلها، كونها تمس أولى حلقات ومؤسسات المجتمع وهي الأسرة، وتنتقل لبقية المؤسسات التي تسعى إلى تكوين إطار اجتماعي مسلم، ومحافظ قادر على التعدي لمثل هذه الجرائم ومكافحتها.[4]

و وتمثل الآثار الإجتماعية نتاج مجموعة من المواقف والتفاعلات مع بعض الأفراد من مستخدمين وسائل التواصل الإجتماعي، والذي يتعدى تأثيرها الفرد ليشمل الأسرة،

---

[1] سليمان الغديان، وآخرون، المرجع السابق، ص_ ص، 179_ 180.

[2] ابتسام كريم ، وآخرون، **بحث بعنوان: انتشار ظاهرة الابتزاز الإلكتروني في المجتمع العراقي، استطلاع أراء عينة من المجتمع العراقي حول التعامل مع هذه الظاهرة المؤتمر العلمي الأول**، نقابة الأكاديميين العراقيين، مركز التطور الإستراتيجي الأكاديمي جامعة دهوك، العراق 11-12 فيفري 2019، ص165.

[3] المرجع نفسه.

[4] سليمان الغديان، وآخرون، المرجع السابق، ص180.

والمجتمع ككل، مما قد يترتب على ذلك خلل في العلاقات بين الفرد وأسرته وتمزق للنسيج والبناء الإجتماعي وتعاظم أثرها لسنوات لاحقة بسبب انتشار الخلافات والمنازعات وفقدان الثقة، مما يعمل على تدمير كيان المجتمع وهشاشته.[1]

ج/ ما يترتب على القيم والدين والعرض في المجتمع:

تمثل القيم لكل مجتمع الميثاق الأخلاقي الذي يحرك هذا المجتمع ومجتمعنا العربي يستمد قيمة من الشريعة، ولما كانت عمليات الإبتزاز مؤلمة، ومجرمة شرعاً تصبح عملية الإبتزاز سببا في اهتزاز معايير قيم التسامح والتعاون على البر والتقوى، واحترام حقوق الآخرين، والستر.[2]

الأمر الذي ينتج عنه قيم اجتماعية مضادة وسلبية لما هو مأمول، ومنها الضغينة والحقد والكراهية والعدوانية وانتهاك الحرمات.[3]

[1] فيصل بن عبد الله الرويس، المرجع السابق، ص_ص،107_108.

[2] سليمان الغديان، وآخرون المرجع السابق، ص180.

[3] المرجع نفسه.

المبحث الثاني: تجريم الإبتزاز الإلكتروني(النظرة القانونية لجريمة الإبتزاز الإلكتروني)

إن أغلب القوانين العربية والعالمية تجرم، على جنح التهديد بالإبتزاز، وكونها من الجرائم الخطيرة التي تلحق الضرر للشخص في سمعته ونفسيته وحياته الخاصة، فمعظم القوانين العربية صنفتها ضمن الجرائم الخطيرة، وحددت لها أركان خاصة بها، فكل فرد يستخدم الأنترنت معرض لعمليات الإبتزاز أو الإحتيال وغيرها، واهتمامه أيضاً بهذه الظاهرة، فمعظم القوانين تناولت ظاهرة الخصوصية الشخصية للأفراد، ووضعت لها أهمية ومكانة بالغة، وتدخل القانون وفرض حماية الجزائية على هذه المكانة الأدبية، واعتبر الإعتداء عليها جريمة تصب مركز المجني عليه، فقد تستهدف الجريمة الإلكترونية الجاني الأخلاقي خاصة في المجتمعات العربية التي تعتز بمبادئها وقيمها الفاضلة، فهذه الجريمة تقضي على حياة الأفراد، فمعظم القوانين العربية وضعت حدّ لهذه الجريمة وسنت لها أركان وقوانين رادعة لها، كما وضعت حلول مقترحة لتجنب الأضرار المتوقعة من الإبتزاز الإلكتروني، وللحد من الوقوع ضحية الإبتزاز الإلكتروني، وهذا ما سنتطرق إليه في هذا المبحث، تجريم الإبتزاز الإلكتروني من خلال دراسة مطلبيه، المطلب الأول الذي يتناول أركان جريمة الإبتزاز الإلكتروني، والمطلب الثاني، الذي يتناول الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني.

المطلب الأول: أركان جريمة الإبتزاز الإلكتروني

الإبتزاز الإلكتروني الذي يتم عبر الوسائل الإلكترونية هو نوع من أنواع تهديد شخص والضغط عليه، بهدف ابتزازه وجبره على القيام بفعل أو الإمتناع عنه، ولو كان القيام بهذا الفعل أو الإمتناع عنه مشروعاً، وتقضي وجود جريمة الإبتزاز شخصين، أحدهما جاني والآخر مجني عليه، ورغم حداثة عهدها في علم الإجرام إلا أنها في الأساس جريمة كسائر الجرائم الأخرى.

ولقيام جريمة الإبتزاز الإلكتروني، ينبغي توفر أركان متعلقة بالجريمة نفسها، كي تصبح جريمة يعاقب عليها القانون وفق الأنظمة المجرمة لها، والمتمثلة في الركن الشرعي، الذي هو عبارة عن وجود نص قانوني يحدد الفعل المجرم والجزاء الجنائي الذي بوجوده، ينقل الفعل من دائرة الإباحة إلى دائرة التجريم. أما الركن المادي فهو كل ما يدخل في كيان جريمة الإبتزاز الإلكتروني، وتكون له طبيعة مادية ملموسة سواء كان فعلا أو امتناعاً، والركن المعنوي فهو داخلي كامن في نفسية الجاني، ومن هذا المنطلق يمكن تقسيم هذا المطلب إلى ثلاث فروع، كما يلي:

الفرع الأول: الركن الشرعي لجريمة الابتزاز الإلكتروني

هو نص التجريم والعقاب فهو النص الذي نستند إليه لتجريم فعل معين والعقاب عليه، ويكون ساريا من حيث الزمان والمكان والأشخاص على مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة "لا جريمة ولا جزاء ولا عقوبة مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة "لا جريمة ولا جزاء ولا عقوبة إلا بنص".[1]

ومن بين التشريعات العربية التي عنيت بتجريم الأفعال المادية المكونة لجريمة الإبتزاز

[1] آمال برحال، المرجع السابق، ص34.

الإلكتروني واتجهت إلى إصدار قوانين خاصة لضمان جريمة الإبتزاز الإلكتروني بكافة صورها لتجريم والعقاب ووضع ركن شرعي لهذه الجريمة من بينها:

أولا: الركن الشرعي في التشريع الجزائري

في الجزائر قد أولى المشرع أهمية بالغة للخصوصية الشخصية للأفراد، واعتبر الإعتداء عليها جريمة تصيب مركز المجني عليه، حيث أن الجانب الأخلاقي هو أخطر ما قد تستهدفه جريمة الإبتزاز الإلكتروني في المجتمع الجزائري، الذي طالما اعتز بمبادئه وقيمه الفاضلة، فمثل هذه الجريمة كفيلة بهدم حياة المجني عليه، وتفقد عائلته كرامتها وانتمائها للمجتمع.[1]

ولقد تطرق المشرع لتلك الحماية لحرمة الحياة الخاصة في الدستور في نص المادة 39 التي تنص: " لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه يحميها القانون وسرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة.[2]

المشرع الجزائري على غرار باقي التشريعات، تبنى الشمولية في تجريمه للأفعال التي يكون مسرحها الكتروني، وذلك من خلال القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها.[3]

وهو ما يستشف من نص المادة 02 منه التي جرمت كل الأفعال الإجرامية التي ترتكب باستخدام تكنولوجيا الإعلام والإتصال، فتكون جريمة الإبتزاز الإلكتروني بذلك من ضمنها

---

[1] آمال برحال، المرجع السابق، ص38.

[2] أنظر المادة 39 من دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر بتاريخ 7 ديسمبر1996، الجريدة الرسمية رقم 76 المؤرخ في: 8 ديسمبر1996، المعدل.

[3] قانون رقم 09-04 المؤرخ في 14 شعبان عام1430ه الموافق5غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، **الجريدة الرسمية**، العدد 47، الصادر بتاريخ 25 شعبان عام 1430ه، الموافق16 غشت سنة 2009.

إستناداً إلى عمومية النص الذي يحيلنا بدوره إلى القواعد التقليدية المطبقة على جريمة التهديد في صورتها الكلاسيكية.[1]

وما الإبتزاز الإلكتروني إلا صورة مستجدة للتهديد والإبتزاز التقليدي المنصوص عليه في المادة 371، من قانون العقوبات الجزائري.[2]

ثانيا: الركن الشرعي في التشريع الإماراتي

كما حرم المشرع الإماراتي الإبتزاز الإلكتروني قانوناً بموجب المادة 16 من قانون مكافحة جرائم تقنية المعلومات الصادر سنة 2012.[3]

مشيراً إلى الوسيلة المستعملة في ارتكاب الجريمة سواء باستخدام الشبكة المعلوماتية أو أي وسيلة من وسائل تقنية المعلومات، وشدّة العقوبة إذ نتج عن الجريمة مساسا بالشرف والإعتبار.

ثالثا: الركن الشرعي في النظام السعودي

حيث أشار إلى تجريم الإبتزاز الإلكتروني ضمن المادة 03 من نظام مكافحة جرائم

---

[1] أكرم ديب، نورة بن بوعبد الله، **دور الدليل الرقمي الجنائي في إثبات جريمة الإبتزاز الإلكتروني، مجلة الحقوق والعلوم الإنسانية**، جامعة باتنة1 كلية الحقوق والعلوم السياسية، الجزائر، المجلد16، العدد01، 2023/03/31، ص406.

[2] قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427هـ الموافق20 ديسمبر سنة2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386، الموافق 8يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد87، الصادرة بتاريخ 4 ذي الحجة عام 1427هـ الموافق 24ديسمبر سنة 2006.

[3] مرسوم بقانون اتحادي رقم 5 لسنة 2012، في شأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ 25 رمضان سنة 1433 الموافق ل13 أغسطس سنة2012، الجريدة الرسمية، العدد540(ملحق)، السنة الثانية والأربعون، الصادرة في شوال1433هـ الموافق أغسطس 2012.

المعلوماتية السعودي.[1]

ويندرج تحت شمول النص كل ما شأنه المساس بالحياة الخاصة باستخدام وسائل التكنولوجيا والإتصال الحديثة كالهواتف النقالة المزودة بتقنية الكاميرا أو في حكمها، إضافة على ذلك كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

1/ الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على قيام بفعل أو الإمتناع عنه، ولو كان القيام بهذا الفعل أو الإمتناع عنه مشروعا بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا.

2/ التشهير بالآخرين، والحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.[2]

ووفقا للنظام السعودي تعد جريمة الإبتزاز الإلكتروني من تلك الجرائم الخطيرة الموجبة للتوقيف وذلك بنص القرار الوزاري رقم 2000 بتاريخ 1435هـ بشأن الجرائم الموجبة للتوقيف، تضمنت الفقرة الرابعة: أن الجرائم نظام مكافحة الجرائم المعلوماتية تعد من الجرائم الكبيرة الموجبة للتوقيف.[3]

فكل هذه النصوص نصت بشكل صريح على تجريم الإبتزاز الإلكتروني بصورة مختلفة،

---

[1] المادة 03 من نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ الموافق لسنة2007، مرسوم ملكي رقم م/17 بتاريخ08 ربيع الأول سنة1428هـ، الموافق ل27مارس،آذار سنة2007، قرار مجلس الوزراء رقم 79 الصادر بتاريخ07 ربيع الأول سنة 1428هـ، الموافق ل28 مارس، آذار سنة 2007، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية، متوفر على الموقع الإلكتروني لهيئة الخبراء عبر الرابط: http://LAWS.boe.gov-sa/Boelaw/Law/lawdetails25df3d6-Of49-4de5-b010a5a700feecd/1 الإطلاع بتاريخ 05 ماي 2023، على الساعة 11:40.

[2] المادة 3/الفقرة 2،4،5، من نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/17) بتاريخ:1428/3/8هـ.

[3] الفقرة الرابعة من القرار الوزاري رقم 2000 بتاريخ10/6/1435هـ.

مما يجعل تلك النصوص تمثل الركن الشرعي للجريمة والذي من خلاله يتم العقاب عليها.[1]

رابعا: الركن الشرعي في القانون المصري

اتجه المشرع المصري إلى إصدار قانون مكافحة جرائم تقنية المعلومات كي تتفق النصوص القانونية مع الركن الشرعي لجريمة الإبتزاز الإلكتروني مع الطبيعة الخاصة لتلك الجريمة والوسائل التي تتم من خلالها الجريمة.

حيث اشتمل الفصل الثاني من قانون مكافحة جرائم تقنية المعلومات المصري على الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات.

وتناولت المادة 20 من قانون الجرائم المتعلقة بالإعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع، حيث نصت هذه المادة على أنه: "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 انتهاك حرمة الحياة الخاصة أو ارسال بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات أو أخبار، أو صورة وما في حكمها تنتهك خصوصية أي شخص دون رضاه سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.[2]

وعليه فهذه المواد تمثل الركن الشرعي لجريمة الإبتزاز الإلكتروني في القانون المصري.

---

[1] أحمد كيلان عبد الله، محمد جبار أنويه النصراوي، **العدالة الجنائية في شرحية التجريم والعقاب**، **مجلة الكوفة للعلوم القانونية والسياسية**، المجلد12، العدد41، 2019، ص10.

[2] المادة 20 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175.

الفرع الثاني: الركن المادي لجريمة الإبتزاز الإلكتروني

يعتر الركن المادي للجريمة، السلوك الذي يظهر إلى حيز الوجود، فهو يبرز الجريمة ويجعلها تخرج إلى العالم الخارجي، ولا تختلف جريمة الإبتزاز الإلكتروني في أركانها عن جريمة الإبتزاز التقليدي، فهي تتطلب سلوك إجرامي يصدر من الجاني سواء بالقول أو الكتابة أو أي فعل آخر يتمثل القيام بالتهديد بنشر البيانات أو الصور أو مقاطع فيديو للضحية.[1]

وقد عرف المشرع العراقي في قانون العقوبات العراقي الركن المادي بأنه: "سلوك إجرامي بارتكاب فعل جرمه القانون أو الإمتناع عن فعل أمر به القانون".[2]

بمعنى وجوب أن يكون هناك فعل أو امتناع عن فعل يمكن إثباته، فلا يعتد بما يدور في نفس البشرية كون ذلك خارج نطاق التجريم بحكم القانون.

وبالتالي فعناصر الركن المادي للجريمة ثلاثة: الفعل أو النشاط الإجرامي، والنتيجة والعلاقة السببية بينهما.

فتتطلب سلوك إجرامي يتم عبر وسائل التواص الإجتماعي أو الحاسب الآلي ويعتبر تهديداً كل قول أو كتابة أو رموز أو صور أو شعارات من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد، ولا يهم إن كان الجاني ينوي تنفيذ الأمر المهدد به أم لا، فقط يشترط أن يكون جديا وليس بمجرد هزل.[3]

ترتب على ذلك قيام المسؤولية الجزائية للجاني بتوافر الركن المادي للجريمة، حتى وإن لم

[1] مريم عراب، المرجع السابق، ص 1208.

[2] يوسف خليل يوسف، **الجرائم الإلكترونية في التشريع الفلسطيني**، رسالة ماجستير الجامعة الإسلامية، غزة، 2013، ص50.

[3] مريم عراب ، المرجع السابق ، ص 1208.

تتحقق النتيجة الإجرامية المتمثلة بتنفيذ الجاني لوعيده ونشر وعرض تلك المعلومات والصور والمقاطع المرئية وجعلها معلنة ومتاحة للجمهور....[1]

فالركن المادي لجريمة الإبتزاز الإلكتروني إذن، يقوم على ثلاثة عناصر: النشاط الإجرامي يأتيه الجاني ونتيجة إجرامية سواء تحققت أو لم تتحقق واقتصرت على التهديد فقط، إضافة إلى العلاقة السببية بتنفيذ الجاني لتهديده بالنشر والعلانية لتلك المعلومات التي تتعلق بالشخص المجني عليه على المنصات الإلكترونية ووسائل التواصل الإجتماعي.[2]

أولا: السلوك الإجرامي للإبتزاز الإلكتروني

الفعل محل التجريم هو واقعة مادية ظهرت للعالم الخارجي، حيث يتحذ بالقيام بفعل التهديد بنشر بيانات أو صور أو مقاطع فيديو للضحية، والقانون لا يميز ولا يهمه من أين حصل عليها، فيمكن أن يكون قد حصل عليها باختراق حساب الضحية أو أنه عثر عليها في جهاز الضحية المسروق أو المعثور عليه أو المباع.[3]

ولا يشترط أن يتم التهديد بطريقة معينة، فيمكن أن يتم عن طريق غرف الدردشة (الشات) أو عن طريق البريد الإلكتروني أو التسجيل الصوتي، كما لا يهم بأن كان الإبتزاز لمصلحة المبتز المشروعة أو غير المشروعة، فالعبرة في استخدام الضغط والإكراه المقترن بالتهديد لإرغام المجني عليه للقيام بذلك الفعل.[4]

---

[1] أكرم ديب، بن بوعبد الله نورة، المرجع السابق، ص 407.

[2] سهام عكوش، المرجع السابق، ص1301.

[3] شاكر سعاد بعيوي ، **جريمة الإبتزاز الإلكتروني، دراسة مقارنة**، مقال منشور **بمجلة ميسان للدراسات القانونية المقارنة**، كلية القانون، جامعة ميسان العراق، نوفمبر 2019، ص129.

[4] عراب مريم، المرجع السابق، ص 1208.

ثانيا: النتيجة الإجرامية لجريمة الإبتزاز الإلكتروني

النتيجة الإجرامية هي الأثر المترتب على السلوك الذي يقصد القانون بالعقاب، فهي الحقيقة المادية إلى كيان ملموس في العالم الخارجي أو أنها الحقيقة القانونية.[1]

وتقع النتيجة الجرمية في جريمة الإبتزاز الإلكتروني لمجرد قيام المبتز بتهديد الضحية بإفشاء سر من أسرارها التي تعتبره أمراً لا يجب الإطلاع عليه أمام الملأ وكان تهديداً بأمر غير مشروع.

ويسبب الخوف والهلع والتأثير على إرادة نفسية بأن يلقي في نفسها قلقا من قيام المبتز بتنفيذ تهديده.[2]

فإذا قام الجاني بالتهديد بمجرد ترهيب الضحية أو طلب منفعة أو أن يحمل المجني عليه على أداء عمل أو الإمتناع عن عمل فهنا تقع النتيجة، سواء فعل المجني عليه ما طلب منه أو لم يفعل.[3]

ثالثا: العلاقة السببية لجريمة الإبتزاز الإلكتروني

تعرف العلاقة السببية بأنها الصلة بين السلوك الذي يعترف به القانون سببا، والأثر الذي يعترف به القانون نتيجة، وتعد العنصر الثالث من عناصر الركن المادي للجريمة، فهي الصلة التي تربط ما بين السلوك الإجرامي والنتيجة الجرمية.[4]

---

[1] آمال برحال، المرجع السابق، ص45.

[2] رامي أحمد غالبي، **جريمة الإبتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق**، مقال منشور في **مجلة ثقافتنا الأمنية**، الإصدار الثاني، وزارة الداخلية العراقية، مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد، 2019، ص41.

[3] محمد عبد المحسن بن شلهوب، المرجع السابق، ص 91.

[4] رامي أحمد غالبي، المرجع السابق، ص51.

ولقيام الركن المادي لابد أن تحدث النتيجة الجرمية بسبب فعل الجاني، أي لو لا حصول الفعل لم تحث تلك النتيجة الإجرامية.[1]

حيث تقوم علاقة سببية بين الإبتزاز والتسليم في حال كان الباعث للجاني هو الخصول على المال، إذ يلزم أن يكون تسليم المال نتيجة ما أحدثه في نفس المجني عليه من الخوف فإن لم يحدث التهديد هذا الأثر، وجرى تسليم المال لإعتبارات أخرى انقطعت علاقة السببية.[2]

أما إذا كان الإبتزاز للقيام بعمل أو الإمتناع عن أداء عمل فإن النتيجة هنا وقوع الضرر وهو الخوف في نفس المجني عليه، وتكون علاقة سببية بينه وبين الإبتزاز، هو أن يكون الإبتزاز سببا في امتهان كرامة المعتدي عليه واحتقاره وتعريضه لبعض أهله والناس وبامتناع المجني عليه عن أداء عمل ليس على سبيل الخوف من الجاني، وإنما لرغبته في الإلتزام بالقانون، فهنا لا تقع جريمة الإبتزاز وذلك لانتقاء علاقة السببية في الجريمة.[3]

الفرع الثالث: الركن المعنوي لجريمة الإبتزاز الإلكتروني

تتطلب جريمة الإبتزاز الإلكتروني لقيامها ركناً معنوياً إلى جاب الركن المادي والشرعي لها، فهي تعد من الجرائم العمدية تأخذ صورة القصد الجنائي الذي يقوم بتوافر عنصري العلم والإرادة.[4]

أي لابد أن يعلم الجاني بنتيجة السلوك الذي اقترفه وأن ينصب علمه على أن ما يقوم به من حصوله على الصور الفاضحة وبيانات سرية لأحد الأشخاص وتهديده بها مقابل

[1] رامي أحمد غالبي، المرجع السابق، ص41.

[2] المرجع نفسه.

[3] محمد عبد المحسن بن شلهوب، المرجع السابق، ص 92.

[4] أكرم ديب، نورة بن بوعبد الله ، المرجع السابق، ص 407.

الحصول على منفعة جريمة يعاقب عليها القانون.[1]

أما العنصر الثاني المتمثل في الإرادة المنصرفة إلى السلوك الإجرامي وتوقع النتيجة الإجرامية في الوقت نفسه.[2]

ويقصد بالركن المعنوي إدراك الجاني وقت اقترافه للفعل المادي المكون للجريمة أن قوله أو كتابته من شأن أي من هما أن يسبب انزعاج الضحية، وهو تهديد مصحوب بطلب أو تكليف بالقيام بأمر ما، والركن المعنوي مسلك ذهني ونفسي للجاني، يوفر معلومات قيام المسؤولية مع اعتبار حق الدولة في العقاب.[3]

ومن هنا يمكن القول بأن الركن المعنوي هو إرادة الجرمية ولا تخرج الإرادة الإجرامية عن صورتين أساسيتين وهما:

1/ القصد الجنائي: وبه تكون الجريمة عمدية.

2/الخطأ غير العمدي: وبه تكون الجريمة غير عمدية.

فالقصد الجنائي هو تعمد إتيان الفعل المجرم أو تركه مع العلم أن القانون يجرم تركه.[4]

فالقصد الجنائي لدى المبتز أن تكون إرادته وعلمه قد إتجه إلى تهديد الضحية بالمعلومات والصور التي يملكها، وهو ما يتمثل إعتداء على حرمة الحياة الخاصة.[5]

أولا: القصد العام

[1] مريم عراب، مرجع سابق، ص 1208.

[2] سيف مجيد العاني، **مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الإجتماعي (دراسة مقارنة)**، دون طبعة، دروب المعرفة للنشر والتوزيع، الإسكندرية، مصر، لسنة 2022، ص 117.

[3] زينب محمود حسين، المرجع السابق، ص584.

[4] رامي أحمد الغالبي، المرجع السابق، ص 52.

[5] سعاد شاكر بعيوي، المرجع السابق، ص 212.

ينهض القصد العام في جريمة الإبتزاز الإلكتروني على عنصرين هما:

أ_ العلم:

وهي من عناصر الجريمة والعلم بموضوع الجريمة أنه يعلم المبتز أن ما يقوم به وما يتصل به من وقائع، ويجب أن يعلم أن ما يقوم به من الحصول على صور فاضحة لأحد الأشخاص وتهديده بها، مقابل منفعة جريمة يعاقب عليها القانون.

وبالتالي يتحقق العلم كما يجب أن يكون الجاني عالماً بماهية الفعل أو امتناع المجرم كما أن فعله يلحق ضرراً بالمجني عليه.[1]

ب_ الإرادة:

هو الإرادة في تحقيق النتيجة غير مشروعة نحو المساس بحق، أو مصلحة يحميها القانون، ومن ثم ينبغي أن تتجه إرادة المبتز إلى تحقيق النتيجة المتمثلة في ابتزاز المجني عليه.[2]

وتنقسم الإرادة إلى قسمين إرادة الفعل، وإرادة النتيجة، فلكي تقوم المسؤولية يجب إثبات أن إرادة الفعل اتجهت إلى القيام بهذا الفعل وذلك دون أن تقع الإرادة في عيب من عيوب الإرادة كأن يكون مختار ومدركاً، أنه يحصل على صور سرية وخاصة بالضحية فإن كان مكرها فلا يوجد قصد جنائي ولا تقوم المسؤولية الجزائية للفعل على المكره.[3]

أما إرادة النتيجة فلا بد أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية بالحصول على المنفعة المادية أو النفعية أو اللاأخلاقية، فالباعث لا عبرة له في الجريمة، فيستوي في

[1] رامي أحمد الغالبي، المرجع السابق، ص52.

[2] ممدوح رشيد المشرف الرشيد العنزي، المرجع السابق، ص212.

[3] محمد عبد المحسن بن شلهوب، المرجع السابق، ص 107.

الإبتزاز الإلكتروني أن يكون الباعث شريفا كانتقامه من المجني عليه أو لتحقيق مصلحة ما.[1]

ثانيا: القصد الخاص

بما أن جريمة الإبتزاز الإلكتروني من الجرائم التي تحتاج إلى معرفة خاصة وعالية بتكنولوجيا المعلومات من أجل تنفيذها فلا يمكن تصور حصولها من دون قصد، فهي من الجرائم العمدية التي يكتفي فيها بالقصد العام، ولا يشترط أن يكون القصد خاص.[2]

المطلب الثاني: الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني

غالبا ما تنشأ مشكلة الإبتزز الإلكتروني بسبب ممارسات خاطئة وتصرفات لا أخلاقية، فقد يكون ذلك بسبب ضعف الوازع الديني لدى الأشخاص، وقد يكون بسبب الإستخدام الخاطئ لوسائل التواصل الإجتماعي، وقد ينتج عن منح الثقة للأشخاص الذين لا يستحقونه.

الأمر يحتاج فقط للوعي والمعرفة والثقافة الإلكترونية التي تمكنك من عدم الوقوع في فخ أحد المجرمين الذين يتصيدون المجني عليه عن طريق جهلهم ببعض الأمور البسيطة وتكاد تكون بسيطة حيث أنك فقط تحتاج إلى أن تتحقق من بعض أمور وعندما تتأكد من عدم صحتها، يجب عليك فوراً أن تبتعد عن إتخاذ أي إجراء من قبلك.[3]

وتنقسم حلول الإبتزاز الإلكتروني إلى حلول تخص أفراد مستخدمين الأنترنت، وحلول

[1] محمد عبد المحسن بن شلهوب، نفس المرجع، ص107.

[2] المرجع نفسه، ص 104.

[3] بلال جناجرة، المرجع السابق، ص 21.

تخص الدولة، كذلك ومن بين أهم الحلول التي نرها قد تلعب دوراً مهما في الحد من الوقوع ضحية ابتزاز الكتروني الإهتمام بالجانبين التاليين، الجانب الوقائي الداخلي، والذي سنتطرق إليه في الفرع الأول والجانب الخارجي في الفرع الثاني.

الفرع الأول: الجانب الوقائي الداخلي

وهي حلول تقع على مستخدمين الأنترنت فهناك مجموعة من الأسس الواجب اتخاذها من طرف الفرد الذي يستخدم شبكة الأنترنت، سواء في مكان علمه أو في الأماكن العامة أو حتى في بيته، حيث سنبين هذه الأسس كما يلي:[1]

يجب على الأشخاص الذين يستخدمون شبكة الأنترنت في الأماكن العامة والخاصة، أن يكون على قدر كاف من الحيطة والحذر، كأن يحذروا عندما يكتبون إسم المستخدم وكلمة السر لموقع ما.[2]

وأن يختاروا كلمة سر قوية لحسابات مواقع التواصل الإجتماعي والبريد الإلكتروني.[3]

بحيث يطالبهم الموقع المعين بحفظ كلمة المرور فبمجرد كبسة واحدة على الزر موافق يكون الموقع قد احتفظ بكلمة السر حتى ولو تم مسح بيانات المتصفح في نهاية العمل، لذا يجب أن يكون حفظ كلمات السر للمواقع المسجل فيها في الأجهزة الشخصية الموجودة في البيت فقط.[4]

ونشير في هذا الصدد إلى أن كل ما يقوم به الفرد الذي يستخدم جهاز الكمبيوتر المتصل

---

[1] سعيد زيوش، المرجع السابق، ص 84.

[2] المرجع نفسه.

[3] أنظر بحث عن جريمة الإبتزاز الإلكتروني في 23-06-2022،بحوث قانونية جنائية-http://www.legal-researche.online.com، اطلع عليه بتاريخ 20ماي2023، الساعة 21:00.

[4] سعيد زيوش، المرجع السابق، ص_ص، 84_85.

بشبكة الأنترنت، يكون عرضة لمجموعة من الهجمات المقصودة وغير المقصودة، كأن يسجل في موقع لتعليم اختراق المواقع أو البريد الإلكتروني، فيكون هو ضحية أو أنه يقوم بمشاركة ملف من الملفات والتي تكون صورة أو فيديو أو برنامج معين، يحتوي على شفرات مخفية لا تظهر إلا بعد أن يتم النقر على الملف، وبالتالي يصبح جهازه عرضة لكل أنواع الإختراق و الجوسسة الإلكترونية.[1]

إن جهاز الحاسوب عبارة عن أداة وليست غاية، حيث أن سرعة معالجة المعطيات ومختلف العمليات التي تدخل في تبويب وتصنيف البيانات بالإعتماد على برامج رئيسية وأخرى ثانوية تساهم في حل الكثير من مشاكلنا اليومية.[2]

لذا لا يجب أن نغفل عن مدى تعرض هذه البرامج للإصابة بنوع معين من الفيروسات التي قد لا تظهر للعيان في الوهلة الأولى، حتى باستخدام أقوى البرامج التي تكافح الفيروسات التي يتعرض بها الفرد للقرصة أو للإستحواذ في جهازه بما يحتويه من ملفات حتى ولو كانت تلك الملفات محمية بكلمات مرور.[3]

لذا وجب تحصين جهاز الذي تتعامل معه سواء كان حاسب آلي أم هاتف محمول بأحد برامج الحماية من الفيروسات.[4]

لذا يجب على الشخص المستعمل للأنترنت، الإبتعاد عن المواقع المشبوهة، والإبتعاد عن تصفح المواقع الجنسية مثلا، غالبا ما يكون هدفها تتبعك وسرقة معلوماتك وسرقة معلومات المتصفح الخاص بك ناهيك عن زرع برامج التجسس من غير علمك وتعتبر

[1] سعيد زيوش، نفس المرجع، ص85.

[2] المرجع نفسه، ص85.

[3] المرجع نفسه.

[4] أنظر بحث عن جريمة الإبتزاز الإلكتروني، المرجع السابق.

وسيلة إلى إسقاط الكثير من الأشخاص.[1]

كما يجب أن لا يسجل الفرد المستخدم للأنترنت في مواقع غريبة ومريبة ، خاصة تلك التي توهمك بتعليم اختراق المواقع أو البريد الإلكتروني، أو توهمه بتحصيل المال عن طريق تبادل الملفات وغيرها من أساليب وطرق الإحتيال الإلكتروني.[2]

وفي حالة حدوث خلل في الحاسوب أو الهاتف المحمول لا تقم في تصليحه إلا عند فني موثوق بسبب زرع برامج تجسس وفيروسات تنقل معلومات الجهاز للشخص الآخر.[3]

_ ابتعد تماما عن الفضول في الأنترنت خاصة إن لم تكن محترف في التعامل مع المواقع الغير موثوقة، كأن تجد رابط في بريدك أو في مواقع التواصل الإجتماعي بعنوان فاضح أو مثير للفضول بشكل غريب ويطلب منك إدخال معلومات خاصة بك كتسجيل الدخول مجدداً للبريد أو الحساب أو حتى أحياناً لا يحتاج الأمر إلى إرسال بياناتك إذ كان منشئ رابط التصيد الإحتيالي محترف فيرسلك إلى رابط يقوم بتحميل ملفات بشكل تلقائي إلى جهازك.[4]

_ لا ترسل أي صور شخصية لك لأي شخص كان، حتى لو صديقك أو صديقتك فربما هاتفه أو جهازه يتعرض للسرقة أو الإختراق وتقع أنت الضحية، فضلا على تغير نفوس الأشخاص.[5]

---

[1] بلال جناجرة، المرجع السابق، ص21.

[2] سعيد زيوش، المرجع السابق، ص 85.

[3] بلال جناجرة، المرجع السابق، ص 22.

[4] المرجع نفسه.

[5] أنظر بحث عن جريمة الإبتزاز الإلكتروني، المرجع السابق.

لذا تجنب مشاركة معلوماتك الشخصية حتى مع أصدقائك في فضاء الأنترنت.[1]

_ تجنب قبول طلب صداقة من قبل أشخاص غير معروفين، وعدم الردود والتجاوب على أي محادثة ترد من مصدر غير معروف، والرفض التام لطلبات إقامة محادثات الفيديو مع أي شخص، مالم تكن تربطك به صلة وثيقة.[2]

_ لا تعط كلمة السر الخاصة ببريدك الإلكتروني أو حساباتك لأي شخص كان، ولا تجعل أحد يستخدم جهازك أو هاتفك خاصة إذا كان من خارج أفراد أسرتك، والقيام بفعل خاصية الغلق لحساباتك على مواقع التواصل الإجتماعي.[3]

_ الحضور والإستماع للمحاضرات والندوات التي تنبه الناس باستخدام الأمن للأنترنت وخبايا مواقع التواصل الإجتماعي.[4]

_ زيادة المستوى الثقافي لدى الأفراد ويأتي هنا دور المؤسسات الإجتماعية في توعية الأفراد ونشر حملات توعية ضد مخاطر الإبتزاز الإلكتروني.

_ قبل شراء جهاز الكمبيوتر وجب على أفراد الأسرة أن يكونوا على إطلاع تام وواسع بمجال شبكة الأنترنت ومخاطرها وسلبياتها، وبفوائدها وإيجابياتها، وأن يكون جهاز الكمبيوتر المتحصل بشبكة الأنترنت الموجودة بالبيت تحت رقابة الأسرة وأن لا يكون في غرفة المراهق والأطفال.[5]

لذا يجب توعيتهم بالإستخدام الصحيح للأنترنت ومتابعة ما يتابعونه ومع من يتحدثون،

---

[1] بلال جناجرة، المرجع السابق، ص21.

[2] المرجع نفسه.

[3] أنضر بحث عن جريمة الإبتزاز الإلكتروني. المرجع السابق.

[4] المرجع نفسه.

[5] سعيد زيوش، المرجع السابق، ص85.

فالأطفال من أبرز ضحايا الإبتزاز الإلكتروني.[1]

لذا يجب أن يكون جهاز الكمبيوتر تحت مراقبة الأولياء، كما يجب أن يكون هناك توقيتا مخصصاً لاستعمال الجهاز.[2]

كما يجب أن يكون الجهاز أو الأجهزة المتحصلة في البيت تحتوي على برامج لمكافحة الفيروسات، ويجب أن تكون خاضعة لنظام التحيين اليومي(La mise à jour)، وهذا لإثراء قاعدة البيانات لدى هذه البرامج.[3]

كما يجب على الأجهزة أن يكون بها جدار الحماية(Le pare feux) مفعل ومنتظم وهذا حتى يتم التعامل مع البرامج الخبيثة والضارة التي يقوم الجهاز بكشفها ومن ثم منعها من التجوال بحرية داحل الجهاز.[4]

الفرع الثاني: الجانب الخارجي

ونقصد به " كل الأفعال التي من شأنها أن تؤدي إلى الحماية من التدخلات التي قد يتعرض لها الفرد جراء ولوجه المستمر لشبكة الأنترنت (بما فيها من مواقع، ومنتديات، وبرامج،...)؛ وبالتالي يكون عرضة للعديد من الهجمات الإلكترونية وتكون ضارة وخطيرة أحيانا." [5]

ونشير في هذا الصدد إلى مجموعة من الإجراءات الواجب القيام بها بعدما يتأكد الفرد أن وقع ضحية ابتزاز عبر شبكة الأنترنت حيث سنعرضها كما يلي:

---

[1] أنظر، بحث عن جريمة الإبتزاز الإلكتروني، المرجع مذكور سابقا.

[2] سعيد زيوش، المرجع السابق، ص85.

[3] المرجع نفسه ص85.

[4] المرجع نفسه.

[5] المرجع نفسه، ص86.

_ يجب على الضحية التقرب من أقرب مصلحة أمنية (مقر شرطة، مقر الدرك الوطني) وتقديم شكوى مؤسسة على وقائع مبينة.[1]

لذا يجب الإهتمام بتزويد جهاز الشرطة بأحدث الأجهزة التقنية التي تراقب من يفعل فعلا ينتهك الأخلاق عبر الأنترنت، وزيادة الرقابة على مواقع التواصل الإجتماعي، فهي أكثر الأماكن التي ينتشر عليها الإبتزاز الإلكتروني.[2]

لذا يجب على الدولة وضع رادع قانوني للأشخاص الذين يقومون بالإبتزاز الإلكتروني يمنعهم من هذا الفعل، ومحاسبتهم حسابا عسيراً على ما يفعلوه.[3]

ووضع قانون أو لائحة تقنن من استخدام الأطفال الصغار للأنترنت فنجد كثيراً أطفال في عمر 3 سنوات و4 سنوات يستخدمون ألعابا وبرامج قد تكون خطيرة وتعرض أجهزة أهلهم إلى الإختراق ومن ثم الإبتزاز.[4]

_ يجب على الضحية عدم التمادي مع المبتز كأن يحاول أن يستعطفه أو يحاول أن يلبي رغباته، نتيجة ما يملكه هذه المبتز من ملفات شخصية (قد تكون صوتية، أو صور، أو فيديو).

_ ويجب على الضحية إخبار أفراد الأسرة بما وقع له من مشكل، كي يجد كل المساندة والدعم من طرف أهله.[5]

---

[1] سعيد زيوش، نفس المرجع، ص 86.

[2] أنظر بحث عن جريمة الإبتزاز الإلكتروني، المرجع مذكور سابقا.

[3] أنظر، أضرار الإبتزاز الإلكتروني، متوفر على الموقع،https://cyberone.com، اطلع عليه بتاريخ 22ماي2023، الساعة10:30.

[4] أنظر، بحث جريمة الإبتزاز الإلكتروني، المرجع السابق.

[5] سعيد زيوش، المرجع السابق، ص86.

ويجب أن لا يخاف أبدا من التحدث إلى أهله وأصدقائه في حال تعرض لأي نوع من الإبتزاز أو الإهانة.[1]

يجب فصل الأنترنت عن الجهاز أو الأجهزة المتصلة في البيت تحت ما يسمى بالشبكة المحلية (Le réseau local)، حيث لا يقوم المبتز بالسطو على الأجهزة الأخرى.

يجب عمل نسخة احتياطية(Une sauvegarde)، عن كل البرامج والملفات التي يراها الفرد مهمة، وهذا كي يسهل الوصول إليها فيما بعد، خاصة إذا عمل مسح تام للجهاز والأقراص الصلبة التي تحتوي على المعلومات.[2]

وبالفعل حكومات بعض الدول نجدها لا تتأخر بتاتاً عن الإستجابة لشكوى في الإبتزاز الإلكتروني، فتقوم بدعم الضحية وتطمئنه، وخلال ساعات معدودة يكون المبتز مقبوضاً عليه لينال جزاءه.

ونظراً للإنتشار الكبير للإبتزاز الإلكتروني ، خاصة في السنوات الأخيرة ونتيجة لما يترتب عليه من الآثار لا حصر لها، فجريمة الإبتزاز الإلكتروني جريمة معقدة متلفة الجوانب.[3]

[1] بلال جناجرة، المرجع السابق، ص22.

[2] سعيد زيوش، المرجع السابق، ص86.

[3] أنضر، بحث جريمة الإبتزاز الإلكتروني،المرجع السابق.

خلاصة الفصل الأول:

وفي ختام هذا الفصل يمكن القول أن هذا الفصل (الأول)، تناول الإطار الموضوعي لجريمة الإبتزاز الإلكتروني، من خلال دراسة أحكامه العامة، كصورة من صور الجرائم الإلكترونية، فتم من خلال هذا الفصل إلى التطرق إلى دراسة ماهية الإبتزاز الإلكتروني من خلال تعريفه لغويا واصطلاحا، وشرعيا، وفقهيا، أين تم تحديد أنواعه بالنظر لشخص الضحية، والهدف المرجو من المجني عليه، ثم تعرفنا على خصائصه والسمات التي يتميز بها الجاني في جريمة الإبتزاز الإلكتروني، ثم تعرضنا إلى وسائل الإبتزاز الإلكتروني وأشكاله وآثاره المترتبة عليه، من خلال التطرق إلى طرق جريمة الإبتزاز الإلكتروني عبر وسائله الإلكترونية من حاسب آلي وملحقاته، الهاتف النقال وبرامجه، والأنترنت... ثم التطرق إلى أشكال الإبتزاز الإلكتروني من (ابتزاز عاطفي الكتروني، ابتزاز الكتروني مادي...)، والأسباب التي تؤدي إلى ارتكاب هذه الجريمة من (أسباب إجتماعية، وأسباب نفسية، وأسباب تقنية، وأسباب اقتصادية...).

ثم تجريم الإبتزاز الإلكتروني من خلال التعرض لدراسة أركانه (الشرعي، المادي، المعنوي)

وفي الأخير تم معالجة الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني، من خلال دراسة جانبيه (الجانب الوقائي الداخلي، والجانب الخارجي).

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني –دراسة المقارنة–

المبحث الأول: الإجراءات القانونية لعقوبات جريمة الإبتزاز الإلكتروني دراسة مقارنة مع بعض القوانين العربية.

المبحث الثاني: الآليات (الإجراءات) القانونية لمكافحة جريمة الإبتزاز الإلكتروني (إجراءات التحقيق والإثبات في جريمة الإبتزاز الإلكتروني).

تمهيد وتقسيم:

شكل الإنفجار المعلوماتي الذي نشهده، والتطور المتسارع والمتلاحق لهذه التكنولوجيا تنوعا في الأنشطة الإجرامية تفرغ في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها، فعدم كفاية التشريعات الخاصة بها وصعوبة التكييف القانوني لها وإجراءات متابعتها من أهم الصعوبات التي تعتري بالنسبة لمكافحة هذه الجريمة.

وبالرغم من خصوصية الجريمة الإلكترونية، ومنها جريمة الإبتزاز الإلكتروني إلا أنها ما تزال تشكل سلوكاً محضوراً جرمه المشرع الوضعي، كما نص على عقوباته مشدداً هذه العقوبة في أحوال معينة ولأسباب نص عليها وعقوبات مخففة منها، والعقوبات الأصلية والتكميلية المقررة في بعض القوانين العربية، كما نص أيضاً على عقوبة الشروع والإشتراك في هذه الجريمة، هذا من ناحية الإجراءات القانونية لعقوبات جريمة الإبتزاز الإلكتروني، أما من ناحية الإجراءات أو الآليات القانونية لمكافحة هذه الجريمة، وذلك من خلال القيام بإجراءات التحقيق والإثبات في هذه الجريمة، بحيث تمر هذه الجريمة وبعد وقوعها بمراحل، مرحلة جمع الإستدلالات، والتحقيق الجنائي، والذي يهدف إلى إكتشاف الجريمة ومرتكبها، فكل إجراءات البحث والتحقيق تكون أهدافها هو الوصول إلى الحقيقة القانونية التي تحتاج لدليل تأكد معه نسبة التهمة للمتهم بها، ولكي تكتمل خصوصية هذه الجريمة، فلا بد من القول بأن الدليل في الجريمة الإلكترونية وبالأخص في جريمة الإبتزاز الإلكتروني هو دليل غير تقليدي، ويرتبط بالحاسوب وأجهزة الهواتف الذكية وملحقاتها والبرامج والتصنيفات التكنولوجية، ففي جريمة الإبتزاز الإلكتروني الدليل ليس مظروفا فارغاً لطلق الناري، وليس خصلة شعر من الضحية، بل هو رمز وشيفرات وأجهزة وعناوين الكترونية، وهذه الأدلة التي يجوز أن يقبلها في حالة معينة ويخطر عليه أن يقبل أدلة سواها.

كما يخضع الإثبات في المسائل الجنائية لقواعد مخالفة عن تلك المحتكم لها في السائل المدنية، ويعود ذلك لاعتبارات موضوعية ومنها ما يرجع لأهمية الدعوى الجنائية، فالقواعد التي تحكم المسائل الجنائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة الجريمة، في إثبات نشاط إجرائي موجه للوصول إلى اليقين القضائي قطعاً وفقاً لمعيار الحقيقة الواقعية، والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة الإلكترونية، وبين الواقعة المعروضة، ولتحقيق ذلك يستعمل وسائل معينة ووسيلة جريمة الإبتزاز الإلكتروني هي الدليل الإلكتروني.

من خلال هذا الموقف ارتأينا أن تكون نقطة الإنطلاق من عنوان هذا الفصل "الإطار الإجرائي لجريمة الإبتزاز الإلكتروني" وذلك من خلال التطرق إلى تقسيمه إلى مبحثين، المبحث الأول تناول الإجراءات القانونية لعقوبة جريمة الإبتزاز الإلكتروني دراسة مقارنة مع بعض القوانين العربية، أما المبحث الثاني فتناول الإجراءات(الآليات) القانونية لمكافحة جريمة الإبتزاز الإلكتروني (إجراءات التحقيق والإثبات في جريمة الإبتزاز الإلكتروني).

المبحث الأول: الإجراءات القانونية لعقوبة جريمة الإبتزاز الإلكتروني

إن أغلب القوانين العربية والعالمية تعاقب على جريمة الإبتزاز الإلكتروني، فكثير من القوانين تنظر إليها كجريمة مصنفة ضمن الجرائم الخطيرة والتي تحدثت معظم القوانين عنها بصراحة وعالجت أغلب وقائعها وفرضت عقوبات على المجرم لتصل إلى الحبس لسنوات وغرامات مالية، حيث تتعامل معها على الأغلب الأجهزة الشرطية في الدول بكل سرية وبكل دقة وحرفية على أيدي أناس مدربين سواء خبراء في عالم التقنيات، أو خبراء في القبض على المجرم المتخفي.

ومن خلال دراساتنا السابقة لجريمة الإبتزاز الإلكتروني نتطرق في هذا المبحث إلى معرفة عقوبات جريمة الإبتزاز الإلكتروني دراسة مقارنة مع بعض الدول العربية التي تشمل نوعين منها ، العقوبات الأصلية والتكميلية، إضافة إلى ذلك معرفة عقوبة الشروع والإشتراك في هذه الجريمة وفي الأخير ندرس الظروف المشددة والمعفية من العقاب، بحيث يمكن تقسيم هذا المبحث إلى مطلبين، الأول تناول عقوبة جريمة الإبتزاز الإلكتروني الأصلية والتكميلية، والثاني تناول عقوبة الشروع والإشتراك في جريمة الإبتزاز الإلكتروني والظروف المشددة والمعفية من العقاب.

المطلب الأول: عقوبة جريمة الإبتزاز الإلكتروني (الأصلية والتكميلية)

تعد العقوبة من أهم الآثار التي تترتب على تجريم السلوك المعتدي، إذا نظم المشرع كل فعل أو ترك مخالفين لنصوصه الموضوعية وجعل مقابل هذا الفعل أو الترك المجرمين عقوبة، هذه العقوبة لضمان تحقيق الردع الخاص للمجرم وتحقيق الردع العام للمجتمع ككل، فلعقوبة وجهين العلاجي والوقائي.

وتختلف الأنظمة والقوانين المجرمة في كل دولة، وذلك باختلاف كل سياسة جنائية يتخذها المشرع ما بيم التخفيف والتشديد في العقوبة وقد أكد ذلك المنظم السعودي والمشرع في أغلب الدول العربية في قناعتهم الشديدة واهتمام المجتمعات العربية بأغلب فئاتها، وتخويفهم من جريمة الإبتزاز الإلكتروني حيث جرم هذا السلوك بكل صورة وتعدياته فوضعت لها عقوبات تتناسب مع الجريمة فتنوعت بين عقوبات أصلية وعقوبات تكميلية.

الفرع الأول: العقوبات الأصلية لجريمة الإبتزاز الإلكتروني

تباين موقف التشريعات محل الدراسة بشأن العقوبة الجنائية المقررة لجريمة الإبتزاز الإلكتروني.[1]

حيث نصت العديد من النصوص القانونية والتشريعية على عقوباتها نذكر منها:

أولا: العقوبات الأصلية في النظام السعودي

على الرغم من تمسك السعودية بالأعراف والتقاليد وثبات الوازع الديني لدى أغلب أفرادها، فإن جرائم الإبتزاز الإلكتروني انتشرت بها، ولحرص المملكة السعودية والنظام السعودي على التصدي لأي جريمة أو جنحة تعرقل الأمن وتروع الأفراد ولو عن طريق الإنترنت

[1] محمد سعيد عبد العاطي محمد، وآخرون، المرجع السابق، ص161.

فتضع عقوبات قاسية للجرائم كافة[1]

تنص المادة رقم(3) من نظام مكافحة الجرائم المعلوماتية في السعودية على " يعاقب بالسجن لمدة سنة وبغرامة لا تزيد على 500,000 ألف ريال أو بعقوبة واحدة منهما كل من يرتكب أي من الجرائم المعلوماتية الآتية:[2]

- يتنصت على المعلومات المتبادلة بين الأفراد عبر الأنترنت.
- ابتز شخصا بنية سيئة.
- دخول إلى موقع إلكتروني بهدف تغيير تصميمه أو تعكيره.
- المساس بحرية الأشخاص عبر مواقع التواصل الإجتماعي.
- التشهير بالأشخاص أو تهديدهم بذلك.

الملاحظ أنه بالرغم من معاقبة المنظم السعودي للمبتز بالعقوبة الأصلية فإنه لم يضع حد أدنى للغرامة المالية، أو للعقوبة السالبة للحرية كما جعل للقاضي السلطة التقديرية ما بين السجن أو الغرامة المالية أو الجمع بينهما.[3]

ثانيا: العقوبات الأصلية عند المشرع العماني

حيث نص المشرع العماني بأنه " يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد عن ثلاث سنوات وبغرامة لا تقل عن ألف ريال ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين...، وبالتالي فإن المشرع جعل العقوبة تخييرية للقاضي؛ 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

[1] بحوث قانونية جنائيةadmin23-06-2023بحث عن جريمة الإبتزاز الإلكتروني وأركانها وكيفية إثباتها

[2] أنظر المادة 3 نظام مكافحة الجرائم المعلوماتية السعودي.

[3] ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص213.

بإسناد أمور مخلة بالشرف أو الإعتبار"[1]

ولخطورة الجريمة في هذه الحالة جعل المشرع سلطة القاضي تخييرية حيث لم يتضمن النص عبارة "أو بإحدى هاتين العقوبتين"، كما جعلها من مصاف الجنايات، وتشدد العقوبة إلى السجن المؤقت الذي لا تقل عن خمس سنوات ولا يزيد على خمس عشرة سنة، إذا كان المجني عليه طفلاً، كما خفف العقوبة إذا كان المتهم طفلاً.[2]

ثالثا: العقوبات الأصلية عند المشرع المصري:

حيث نصت المادة رقم 428 من قانون العقوبات المصري على " أن كل شخص هدد غيره بفضحه أو التشهير به أو نشر معلومات شخصية عنه أو الإستيلاء على ممتلكاته وتحجيم حريته، سواء كان هذا التهديد مكتوباً أو منطوقاً، يعاقب بالسجن مدة 7 سنوات، وإذ نفذ المجرم تهديده يعاقب بالسجن 9 سنوات"[3]

وقد نصت المادة رقم 18 من قانون مكافحة جرائم تقنية المعلومات على "كل شخص استولى أو إخترق أو سرق بريداً الكترونياً لشخص آخر يعاقب بالسجن شهر وغرامة تتراوح بين 50 إلى 100 ألف جنيه، وإذا كان الضحية من الأشخاص المشهورين بسجن المبتز مدة 6 أشهر ويغرم مبلغا من 100 إلى 200 ألف."

والملاحظ أن القانون المصري جعل عقوبة الإبتزاز السجن مدة لا تزيد على خمس سنوات ولم ينص القانون المصري على الحد الأدنى للعقوبة كما يعاقب الموظف العام الذي يرتكب أحد الأفعال في هذه المادة اعتماداً على سلطة وظيفته.[4]

---

[1] المادة 17 من قانون مكافحة جرائم تقنية المعلومات العماني.

[2] محمد سعيد عبد العاطي محمد، مرجع سابق، المرجع السابق، ص161.

[3] أنظر المادة 428 من قانون العقوبات المصري.

[4] محمد بن عبد المحسن بن شلهوب المرجع السابق، ص135.

رابعا: العقوبات الأصلية في القانون العراقي:

يعد العراق من البلدان التي تعاني الإبتزاز الإلكتروني بكثرة لذا تصدى المشرع العراقي في القوانين الموضوعية تجاه جريمة الإبتزاز، وتتمثل عقوبة جريمة الإبتزاز الإلكتروني في العراق وفقا للمادة 430 من قانون العقوبات العراقي في أن " كل من هدد شخصاً بارتكاب جناية في حقه أو التشهير به أو بأحد ذويه يعاقب بالسجن مدة 7 سنوات أو بالحبس، سواء كان المبتز هذا معروفا للضحية أو غير معروف له، وسواء تم الإبتزاز في الواقع أو عبر الإنترنت".[1]

خامسا: عقوبة الأصلية للإبتزاز الإلكتروني في الإمارات:

تنص المادة رقم 16 من قانون مكافحة جرائم المعلومات في الإمارات على" كل من ابتز شخصاً أو أجبره على فعل شيء غير قانوني وغير أخلاقي عبر الإنترنت يعاقب بالسجن مدة سنتين وغرامة قدرها يتراوح بين 25 إلى 500 ألف درهم، وبواحدة من هاتين العقوبتين، وتصل العقوبة إلى السجن 10 سنوات، في حال كان طلب الإبتزاز يخص أمور الشرف".[2]

سادسا: العقوبات الأصلية للإبتزاز الإلكتروني بالنسبة للمشرع الجزائري:

بالنسبة للمشرع الجزائري فقد حددت المواد 303 مكرر1 و 303 مكرر2، العقوبات الخاصة بهذه الجنحة وهي كالآتي: المادة 303 مكرر: يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية من 50 ألف إلى 300 ألف دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت.[3]

---

[1] أنظر المادة 430 من قانون العقوبات العراقي

[2] أنظر المادة 16 من قانون الإتحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

[3] المادة 303 مكرر من قانون العقوبات الجزائري.

المادة 303 مكرر 1: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذه المادة بالعقوبة المقدرة للجريمة الثانية، ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة.[1]

الفرع الثاني: العقوبات التكميلية (التبعية) لجريمة الإبتزاز الإلكتروني

العقوبات التكميلية هي تلك العقوبات التي تصيب الجاني بناءاً على الحكم بالعقوبة الأصلية وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناءاً على الحكم بالعقوبة دون الحاجة إلى إصدار حكم تبعي فهو مرتبط ارتباطاً مباشراً ووثيقاً بالعقوبة الأصلية.[2]

فالعقوبة التبعية هي العقوبة التي تتبع العقوبة الأصلية للجريمة المحكوم بها في المتهم بقوة القانون دون الحاجة لنص عليها في الحكم، وعليه فتطبيق العقوبة التبعية سواء تضمنتها أو لم يتضمنها الحكم ولذلك نلحظ أن النصوص التشريعية المتعلقة بالعقوبة التبعية لجريمة الإبتزاز الإلكتروني، قد استخدم مصطلح يدل على وجوبية تطبيق هذه العقوبات.[3]

أولا: عقوبات التبعية (التكميلية) عند المشرع العماني والمصري:

حيث نص المشرع العماني: "... على المحكمة المختصة الحكم في جميع الأحوال بالآتي..."

وكذا المشرع المصري قضى بأنه "...على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي..."[4]

---

[1] أنظر المادة303 مكرر من قانون العقوبات الجزائري.

[2] آمال برحال، المرجع السابق، ص53.

[3] محمد سعيد عبد العاطي، وآخرون، المرجع السابق، ص165.

[4] المادة 37 من قانون مكافحة جرائم تقنية المعلومات المصري حيث استخدم المشرع المصري مصطلح "العقوبة التبعية" صراحة في هذا القانون كمسمى للفصل الثامن منه.

القانون المصري فهي عقوبة تكميلية وجوبية وذلك لمصادرة الأجهزة المستخدمة في الجريمة أو الذي تحصل منها وأوجب إزالة الوضع الإجرامي بمحو التسجيلات المتحصلة من الجريمة.[1]

بقراءة النصوص الخاصة بالعقوبة التبعية لجريمة الإبتزاز الإلكتروني يتضح لنا أن للقاضي عند الحكم في جريمة من الجرائم المنصوص عليها في هذا القانون أن يحكم بإحدى العقوبات التبعية المنصوص عليها في هذا القانون صراحة وإذا لم يتضمن الحكم أي من هذه العقوبات وجب على الجهات المختصة تطبيق هذه العقوبات على الرغم من عدم نص الحكم عليها.[2]

كما تبين لنا أن المشرع العماني كان أكثر وضوحا من الشرع المصري في بيان هذه العقوبات، لأن المشرع المصري حصرها فقط على مصادرة الأدوات والآلات والمعدات والأجهزة التي لا يجوز حيازتها قانونا، وبالتالي تخرج عن دائرة المصادرة، إلا إذا لجأنا إلى قواعد العامة في قانون الجزاء المنظمة لهذه العقوبات.[3]

كما نصت على عقوبة الغلق للشخص المعنوي إذا لم يحصل على الترخيص اللازمة لممارسة النشاط، وبالتالي إذا كان الشخص المعنوي قد حصل على التراخيص اللازمة فلا يجوز الغلق، وهذه مفارقة غريبة من قبل المشرع المصري التي يجب عليه أن يتدخل ويرفع هذا النقص الموجود في هذا النص الخاص بالعقوبة التبعية.

كما تضمن أيضا العزل المؤقت من الوظيفة في حالة ارتكاب الجريمة من قبل الموظف العام أثناء أو بسبب وظيفته، ويكون وجوبيا في حالة لو ارتكب الجريمة بغرض الإخلال

[1] محمد عبد المحسن بن شلهوب، المرجع السابق، ص146.

[2] محمد سعيد عبد العاطي محمد، وآخرون، المرجع السابق، ص165.

[3] المرجع نفسه.

بالأمن العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد.[1]

ثانيا: العقوبة التكميلية في القانون الإماراتي:

حيث نصت المادة41 من القانون الإماراتي على: "مع عدم الإخلال بحقوق الغير حسنة النية بحكم في جميع الأحوال بمصادرة الأجهزة، والبرامج والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوصة عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب في أي من هذه الجرائم وذلك إما إغلاقا كليا أو لمدة التي تقدرها المحكمة."[2]

ثالثا: العقوبات التكميلية في النظام السعودي:

تضمنت القواعد التي تحكم العقوبة التكميلية في النظام السعودي نجدها في القانون الإماراتي كونها عقوبة عينية وتقديرية للقاضي، وتتبع العقوبة الأصلية وجوداً أو عدماً وتمتنع في حالة كانت الأجهزة المستخدمة في الجريمة للغير حسني النية.[3]

رابعا: العقوبة التكميلية في التشريع الجزائري:

أما في التشريع الجزائري فالحكم بالمصادرة وجوبي حسب المادة303 مكرر وذلك في ما يخص الأشياء المستعملة في ارتكاب الجريمة كما أن المادة 303 مكرر2 أحالت إلى المادة9 مكرر1.[4]

---

[1] محمد سعيد عبد العاطي محمد، وآخرون، نفس المرجع، ص_ص، 165_166.

[2] أنظر المادة 41 من القانون الإتحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

[3] آمال برحال، المرجع السابق، ص54.

[4] أنظر المادة 9 مكرر 1 من ق ع ج "يتمثل الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية في:–العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي بها علاقة بالجريمة–الحرمان من حق الإنتخاب أو الترشح،– الحرمان من حق في حمل الأسلحة وفي التدريس وفي إدارة مدرسة أو الخدمة في مؤسسة التعليم بوصفه أستاذ أو مدرساً أو مراقب– عدم الأهلية يكون وصيا أو قيما، – سقوط الولاية كلها أو بعضها..

وذلك بمنعه من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 من قانون العقوبات الجزائري، لمدة لا تتجاوز خمس سنوات كما يجوز لها أن تنشر حكم الإدانة طبقاً للكيفيات المبينة في المادة 18 من ق ع ج، التي تنص على أن للمحكمة عند الحكم بالإدانة أن تأمر في حالات التي يحددها القانون بنشر الحكم بأكمله أو مستخرج منه في جريدة، أو أكثر أو بتعليقه في الأماكن التي يبينها وذلك كله على نفقة المحكوم عليه على أن لا تتجاوز مصاريف النشر المبلغ الذي يحدده الحكم بالإدانة بهذا الغرض، أو لا تتجاوز مدة التعليق شهرا واحداً.[1]

المطلب الثاني: الظروف المشددة والمعفية من العقاب في جريمة الإبتزاز الإلكتروني وعقوبة الشروع والإشتراك في هذه الجريمة:

هناك حالات تشدد فيها العقوبة في جريمة الإبتزاز الإلكتروني وذلك حال تحقق شروط معينة كما توجد حالات معفية من العقوبة يتم فيها الإعفاء من عقوبة في جريمة الإبتزاز الإلكتروني كما تضمن عقوبة الشروع التي نعني بها البدء في تنفيذ في الجريمة والإشتراك في الجريمة الذي يتم عن طريق أحد صور المساهمة كالإنفاق مع الفاعل الأصلي أو مساعدة المبتز بأي صورة من صور المساعدة حتى يصل إلى النتيجة الإجرامية المستهدفة، هذا ما سنتناوله في هذا المطلب، بحيث يمكن تقسيمه إلى فرعين، الفرع الأول تناول الظروف المشددة والمعفية من العقاب لجريمة الإبتزاز الإلكتروني، والفرع الثاني تناول عقوبة الشروع والإشتراك في جريمة الإبتزاز الإلكتروني.

الفرع الأول: الظروف المشددة والمعفية من العقاب لجريمة الإبتزاز الإلكتروني

[1] أنظر المادة 18 من قانون العقوبات الجزائري.

أولا: الظروف المشددة للعقاب لجريمة الإبتزاز الإلكتروني

هناك حالات تشدد فيها العقوبة في جريمة الإبتزاز الإلكتروني وذلك حال تحقق شروط معينة، ويقصد بالتشديد هنا أن يحكم القاضي بالحكم الأعلى للعقوبة المقدرة أو يحكم بكل العقوبتين الحبس والغرامة معاً.

الأصل في عقوبة جريمة الإبتزاز الإلكتروني، أن المنظم السعودي لم يحدد لها حد أدنى واكتفى بوضع حد أعلى لها لا يجوز تجاوزه، لذا فقد جعل المنظم حالات تقع فيها جريمة الإبتزاز عن طريق التقنية شدد فيها بالعقاب، وللقاضي سلطة تقديرية في تحديد مدة السجن وله سلطة تقديرية في تحديد الغرامة المالية التي يدفعها الجاني شرط أن لا تتجاوز الحد الأعلى المقرر للعقوبة نظاماً فلا يجوز السجن مدة السنة ولا يزيد في الغرامة المالية على500,000 ريال.[1]

بالإطلاع على قانون مكافحة جرائم تقنية المعلومات الإماراتية تبين لنا أن المشرع شدد العقوبة في نص المادة 16 بتجريم الإبتزاز حيث نصت على أنه: "يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن 250,000 درهم ولا تتجاوز 500,000 درهم أو بإحدى هاتين العقوبتين كان من ابتز شخص آخر بحملة على القيام بفعل أو الإمتناع عنه وذلك باستخدام شبكة المعلوماتية أو وسيلة تقنية المعلومات ونكون العقوبة بالسجن مدة لا تزيد على عشر سنوات، إذا كان التهديد بارتكاب جناية، أو بإسناد أمور خادشة للشرف، والإعتبار".[2]

ثانيا: الظروف المعفية من العقاب لجريمة الإبتزاز الإلكتروني:

إن الإعفاء من العقوبة ليس له علاقة بالسياسة الجنائية أو علاقة بالقواعد العامة

[1] محمد بن عبد المحسن بن شلهوب، المرجع السابق، ص136.

[2] أنظر المادة 16 من قانون الإتحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

للمسؤولية الجزائية لمرتكب الجريمة فقد نص المنظم السعودي والمادة 11 من نظام مكافحة الجرائم المعلوماتية على أنه: " للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجنات بإبلاغ السلطة المختصة بالجريمة قبل العلم بها، وقبل وقوع الضرر وإن كان الإبلاغ بعد العلم بالجريمة تعين الإعفاء حيث يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم أو الأدوات المستخدمة في الجريمة" .[1]

الفرع الثاني: عقوبة الشروع والإشتراك في جريمة الإبتزاز الإلكتروني:

أولا: عقوبة الشروع في جريمة الإبتزاز الإلكتروني:

يقصد بالشروع البدء في تنفيذ في الجريمة التي يعقد الجانب العزم على ارتكابها ولكنه لا يصل إلى النتيجة التي يريد تحقيقها، فهي جريمة ناقصة لعدم إكتمال النتيجة الإجرامية المرجوة.

وبالإطلاع على المادة العاشرة من نظام مكافحة الجرائم المعلوماتية السعودي نجد أنها نصت على أنه: "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة".[2]

من خلال نص المادة يتبين أن النظام قد عاقب على الشروع في جريمة الإبتزاز إذا كانت الوسيلة المستخدمة هي من الوسائل التقنية، ولكن لم ينفذ الجريمة، فالعقاب على الشروع هنا يكون فقط في مرحلة التنفيذ بمعنى أن النظام السعودي لا يعاقب على المراحل الأولى التي تمر بها الجريمة.[3]

وبالإطلاع على المادة 40 من قانون الإتحادي الإماراتي التي تنص على أنه: "لا يعاقب

[1] أنظر المادة 11 من نظام مكافحة الجرائم المعلوماتية السعودي.

[2] أنظر المادة 10 من نظام مكافحة الجرائم المعلوماتية السعودي.

[3] محمد عبد المحسن بن شلهوب، المرجع السابق، ص141.

على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة".[1]

ويتضح من خلال النص أن المشرع الإماراتي ساير نظيره السعودي في نفس الرأي إذ جعل عقوبة الشروع نصف عقوبة الجريمة التامة.

وحسب القانون الجزائري يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في المادة 303 مكرر بالعقوبات المقررة للجريمة التامة، ولذا نص المادة 303 مكرر 1.[2]

ثانيا: عقوبة الإشتراك في جريمة الإبتزاز الإلكتروني:

الإشتراك في الجريمة يتم عن طريق أحد صور المساهمة كالإتفاق مع الفاعل الأصلي أو مساعدة المبتز بأي صورة من صور المساعدة حتى يصل إلى النتيجة الإجرامية المستهدفة.

يعاقب نظام مكافحة جرائم المعلوماتية على الإشتراك في جريمة الإبتزاز في حال كانت الوسيلة المستخدمة هي من وسائل التقنية والعقاب هنا يشمل الفاعل الأصلي للجريمة وكذلك الشريك بالتسبب، واتبع المنظم القواعد العامة المقررة في الإشتراك بالتسبب في الجريمة حيث يقع بالتحريض أو الإتفاق أو المساعدة (الإعانة).[3]

وكذلك كما جاء في نص المادة التاسعة من نظام مكافحة جرائم المعلوماتية، على أنه يعاقب كل من حرض غيره أو ساعده أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام إذا وقعت الجريمة بناء على هذا التحريض أو المساعدة أو الإتفاق لما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ويعاقب بما لا يتجاوز نصف

[1] أنظر المادة 40 من قانون الإلحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

[2] أنظر المادة 303 مكرر، مادة 303 مكرر 1 من قانون العقوبات الجزائري.

[3] محمد بن عبد المحسن بن شلهوب، المرجع السابق، ص143.

الحد الأعلى للعقوبة المقررة، إذا لم تقع الجريمة الأصلية.[1]

الملاحظ أن المنظم السعودي أقر عقوبة لشريك بما لا يتجاوز عقوبة الفاعل الأصلي، كما عاقب النظام الشريك المتسبب بنصف العقوبة الأصلية، وإن لم تقع الجريمة الأصلية مع أن القواعد العامة تقضي بأن لا يعاقب الشريك إلا إذا قام الفاعل الأصلي بارتكاب الجريمة أو الشروع فيها على الأقل.

[1] أنظر المادة 9 من نظام مكافحة الجرائم المعلوماتية السعودي.

المبحث الثاني: الآليات القانونية لمكافحة جريمة الإبتزاز الإلكتروني (إجراءات التحقيق والإثبات)

الجرائم الإلكترونية بصفة عامة وجريمة الإبتزاز الإلكتروني بصفة خاصة هي في الأصل جريمة محضورة تشكل سلوك إجرامي يجرمه المشرع، فجريمة الإبتزاز الإلكتروني مثل غيرها من الجرائم لها عناصرها، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى الجنائية في الجرائم العادية (التقليدية).

كما هو الحال في القصور التشريعي لتحديد كل جريمة معلوماتية على حدى، لإزالة كل غموض يحيط بها، فإن مظاهر الفراغ التشريعي تظهر أيضا في المجال الإجرائي الذي يواجه الطبيعة الخاصة للجريمة المعلوماتية بصفة عامة وجريمة الإبتزاز الإلكتروني بصفة خاصة.

وبالرغم من قيام الكثير من الدول بسن تشريعات جديدة، القائمة لمواجهة الجريمة المعلوماتية، إلا أنها لم تتوصل إلى تدارك كل ما يحيط بالجريمة من الجانب الإجرائي، كذلك بالنسبة للمشرع في الدول العربية لم يتدخل جديا لمواجهة هذا النوع من الجرائم بنصوص إجرائية خاصة، وأمام هذا القصور التشريعي تبرز مسألة صعوبة جمع الأدلة في مجال الجريمة المعلوماتية من جهة، ومن جهة أخرى صعوبة في تطبيق الإجراءات الجنائية التقليدية.

إلا أن هناك إشكالات تطرح أمام رجال القانون حول كيفية ملاحقة المجرمين ومسألة الإختصاص مروراً بأعمال الإستدلال والتحقيق وإنتهاء بقضية الإثبات، وبهذا نقسم هذا المبحث إلى مطلبين، الأول تناول إجراءات التحقيق في جريمة الإبتزاز الإلكتروني والصعوبات التي تواجه المحقق أو جهات التحقيق، والثاني الذي تناول الإثبات في جريمة الإبتزاز الإلكتروني.

المطلب الأول: إجراءات التحقيق في جريمة الإبتزاز الإلكتروني والصعوبات التي تواجه المحقق:

رغم اختلاف الجرائم الإلكترونية بشكل عام عن الجرائم التقليدية، وهو ما يلقي بعبء على سلطات التحقيق، من ضرورة تطوير إجراءات التحقيق لكي تتناسب مع التحقيق في الجرائم الإلكترونية بصفة عامة وفي الإبتزاز الإلكتروني بصفة خاصة، فأيضا يظل نظام الإجراءات الجزائية في قواعد التحقيق هو السائد، مع ضرورة اعتبار الفوارق الموضوعية في التحقيق، حيث أن هناك صعوبات تثار أثناء التحقيق تتبع من طبيعة جريمة الإبتزاز الإلكتروني.[1]

الفرع الأول: إجراءات التحقيق العامة والخاصة في جريمة الإبتزاز الإلكتروني:

تتشابه إجراءات التحقيق في الجرائم الإلكترونية مع إجراءات التحقيق في الجرائم التقليدية، بأن كليهما يتطلب المعاينة والتفتيش والإستجواب وجمع الأدلة وفحصها.[2]

والمقصود بالتحقيق هو مجموع الإجراءات التي يقوم بها المحقق وتؤدي لكشف الجريمة ومعرفة مرتكبها تمهيداً لتقديمه إلى المحاكمة كي ينال عقابه وقد تكون هذه الإجراءات، كالتفتيش أو فنية كالبصمات أو برمجية لتحديد كيفية الدخول إلى المعطيات المخزنة في الحاسوب.[3]

---

[1] مريم عراب، المرجع السابق، ص1215.

[2] رايز سالم الحقبا ، **مهارات البحث والتحقيق في الجرائم المعلوماتية**، رسالة دكتوراه، جامعة نايف للعلوم الأمنية.

[3] وائل سليم عبد الله شاطر، **الإطار القانوني لجريمة الإبتزاز الإلكتروني في الألعاب الإلكترونية " دراسة مقارنة وفق النظام السعودي والقانون الكويتي"**، **المجلة العربية لنشر العلمي**، المملكة العربية السعودية، تاريخ الإصدار:2 شباط2020، ص 438.

نصت المادة 40 الفقرة الأولى من قانون الإجراءات الجزائية المعدل بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 والمرسوم التنفيذي رقم 06-348 المؤرخ في 10/05/ 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق على أن اختصاص قاضي التحقيق المحلي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد المشتبه في مساهمتهم في اقترافها، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.[1]

أولا: إجراءات التحقيق العامة:

1/ الخبرة الفنية وتدريب الكوادر

إن الخبرة هي إجراء أما تدريب الكوادر فهو آلية من آليات مكافحة الجريمة الإلكترونية، فيخضع الكوادر إلى دورات تدريب لتبادل الخبرات على المستوى الإقليمي والدولي كآلية من آليات التعاون.

أ_ الخبرة الفنية:

هي وسيلة لتحديد التفسير الفني والتقني، بالإستعانة بالمعلومات العلمية، فهي مستقلة عن الدليل القولي أو المادي وهي تقييم لهذا الدليل.[2]

وعلى الخبير أن يتمتع بمؤهلات عالية ومقدرة فنية في تركيب الكمبيوتر وشبكة الأنترنت والتعامل مع الجريمة التي خلقتها التقنية الحديثة وكيفية عزل النظام المعلوماتي والحفاض على الأدلة دون تلف.[3]

---

[1] أنظر المادة 40، الفقرة 1 من قانون الإجراءات الجزائية الجزائري.

[2] عزيزة راجي، **الأسرار المعلوماتية وحمايتها الجزائية**، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2018، ص271.

[3] المرجع نفسه.

ب_ تدريب الكوادر:

طبيعة الجرائم الواقعة على الأسرار المعلوماتية تقضي معرفة بنظم المعلوماتية وكيفية تشغيلها من قبل مستخدميها، ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري والتحقيق في مجال الجرائم المعلوماتية.

2. الإنتقال ومعاينة مسرح الجريمة المعلوماتية:

فالانتقال هو ذهاب مأموري الضبط القضائي، أو المحقق الجنائي إلى مكان ارتكاب الجريمة، حيث توجد آثارها وأدلتها.

أما المعاينة فهي تخص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، فالمعاينة تستلزم الإنتقال إلى محل الجريمة أو الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة غير أن المحقق قد ينقل إلى عرض آخر غير المعاينة كالتفتيش مثلا، وفي جريمة الإبتزاز الإلكتروني يقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الأنترنت.[1]

3/ التفتيش:

التفتيش في قانون الإجراءات الجزائية هو البحث عن الشيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة.[2]

ثانيا: إجراءات التحقيق الخاصة:

يمكن تقسيم هذه الإجراءات الخاصة إلى نوعين؛ الإجراء الأول مراقبة الإتصالات

[1] آمال برحال، المرجع السابق، ص69.

[2] المرجع نفسه، ص71.

الإلكترونية، أما الإجراء الثاني حفظ المعطيات المتعلقة بحركة السير.

1/ مراقبة الإتصالات الإلكترونية:

تعتبر المراقبة من أهم مصادر التحري سواء في الجرائم التقليدية أو المستحدثة كجرائم الأنترنت وهي ما يعرف بالمراقبة الإلكترونية، وقد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية في اعتراض المراسلات، وتسجيل الأصوات والتقاط الصور.

أ_ اعتراض المراسلات:

المراسلات هي جمع الخطابات والرسائل والطرود والبرقيات، والمشرع الجزائري في المادة 65 مكرر من ق إ ج ج حصر مفهوم المراسلات في تلك التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية فقط، وبالتالي استبعد المراسلات العادية.[1]

ب_ تسجيل الأصوات:

يقصد به مراقبة الأحاديث وتسجيلها وكل الإتصالات التي تتم عن طريق سلكي، أو لا سلكي، من أجل التقاط ، وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية، من طرف شخص أو عدة أشخاص.[2]

ج_ التقاط الصور:

هي عملية تقنية تتم بواسطتها التقاط صور لشخص، يتواجد في مكان خاص، وتتم هذه الإجراءات بالسرية التامة لأنها بها مساس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا.[3]

---

[1] أنظر المادة 65 مكرر من قانون الإجراءات الجزائية الجزائري.

[2] آمال برحال، المرجع السابق، ص78.

[3] المرجع نفسه.

2/ حفظ المعطيات المتعلقة بحركة السير:

المعطيات المتعلقة بحركة السير هي تلك المعطيات المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها تلك الأخيرة بإعتبارها جزء من حلقة الإتصال؛ توضح مصدر الإتصال ونوع الخدمة.[1]

الفرع الثاني: الصعوبات التي تواجه المحقق (جهات التحقيق) في جريمة الإبتزاز الإلكتروني:

يعتبر التحقيق في جرائم الإبتزاز الإلكتروني، أمرا ليس بالهين بسبب الصعوبات التي تواجه المحقق أمام جريمة ما زالت غامضة، حتى أن عدم التمكن من السيطرة على مجريات التحقيق، قد يؤدي إلى فقط أن الثقة في المجتمع وزيادة نسبة الجريمة، وتتمثل هذه الصعوبات في:

أولا: الحق في الخصوصية:

كثير من التشريعات في الدول جرمت التعدي على حياة الإنسان الخاصة باستخدام شبكة الأنترنت، وقد نص عليها ميثاق الأمم المتحدة سنة 1948م، ومنها المادة 15 " لا يعرض أي شخص لتدخل تعفسي في حياته الخاصة، أو أسرته، أو مسكنه، أو رسائله أو شن حملات على شرفه وسمعته، ولكل شخص الحق في طلب حماية القانون له من هذه التدخلات أو تلك الحملات".[2]

ثانيا: نقص الخبرة:

[1] أنظر المادة 12 فقرة "د" من قانون 04/09.

[2] أنظر المادة 15 من ميثاق الأمم المتحدة سنة 1948.

الخبرة في التحقيق هي مهارة تتطلب توفرها لرجال التحقيق للوصول إلى مراحل متقدمة من الخبرة والمعرفة للعمل في مثل هذه الجرائم، ومازالت جهات التحقيق والضبط تعاني من قلة الخبرة الفنية وقلة التدريب على التعامل مع الأدلة الإلكترونية وكيفية البحث والإستدلال وهو بمثابة ثغرة كبيرة في النظام الجنائي.[1]

كما أن خبرة التحقيق مع المجرم الذكي له طبيعة خاصة، سيما أنه يحاول الهرب من الجريمة، حيث أن المحقق الجنائي في جرائم الإبتزاز الإلكتروني يجب أن يكون له تكوين تقني، فيجب أن يجمع بين مهارة استخدام التقنية الحديثة، وكذلك مهارة تقييم الجريمة الإلكترونية ومدى الخطورة الإجرامية لمرتكبها، وكذلك مهارة التعرف على المكونات المادية للأجهزة وعلى ملحقاتها من طابعات ومساحات ضوئية وكاميرات.[2]

ثالثا: تنازع الإختصاص:

هي مشكلة تؤرق عمل جهات الضبط والتحقيق لأن جريمة الإبتزاز الإلكتروني من إحدى مشكلاتها أنها قد تكون عابرة للحدود الإقليمية للدولة، بحيث يكون الجاني من دولة والمجني عليه من دولة أخرى، بحيث يتنازع كل قانون في محل تطبيق العقوبة المقررة في حق الجاني بحسب النظام الذي تتضمنه العقوبة والقانون الواجب التطبيق.[3]

المطلب الثاني: الإثبات في جريمة الإبتزاز الإلكتروني

الإثبات هو كل ما يؤدي إلى كشف الحقيقة أما في معناه القانوني هو كل ما يؤدي إلى كشف الحقيقة وإقامة الدليل على وجود قاعدة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون، ويعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية،

[1] وائل سليم عبد الله شاطر، المرجع السابق، ص439.

[2] عراب مريم، المرجع السابق، ص1216.

[3] المرجع نفسه.

ويزداد صعوبة في الجريمة الإلكترونية بصفة عامة، لأن اكتشاف الجريمة الإلكترونية بصفة عامة وجريمة الإبتزاز الإلكتروني ليس بالسهل، بل وحتى عند اكتشاف الجريمة والإبلاغ عنها يتبقى عبء الإثبات به الكثير من الصعاب، فالجريمة الإلكترونية تتم في بيئة غير تقليدية، لأنها تقع في إطار غير ملموس، لأن أركانها تقوم بين بيئة حاسب آلي أو جهاز الكتروني تقني واستخدام الأنترنت وسيلة أخرى، مما يزيد من الصعوبات التي تواجه رجال الضبط الجنائي والقضائي لأن العمل في هذه البيئة تكون فيها البيانات والمعلومات عبارة عن نبضات الكترونية، ترسل عبر نظام الكتروني، مما يسهل من محو الأدلة الإلكترونية من قبل الجاني أمراً يسيراً.[1]

كما أن وسائل الإثبات التقليدية لا تفلح دائما في إثبات مثل هذا النوع من الجرائم نظراً لاختلافها بطبيعتها الخاصة عن الجريمة التقليدية ولاختلاف العناصر المادية التي تقوم عليها الجريمة الإلكترونية.

كان من الضروري تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام الإلكتروني، وأصبح متطلبا من أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي خاصة مسألة حجية الدليل الإلكتروني.[2]

وبالتالي يمكن تقسيم هذا المطلب إلى فرعين، الأول يتناول طرق الإثبات في جريمة الإبتزاز الإلكتروني، والثاني تناول صعوبات الإثبات في جريمة الابتزاز الإلكتروني.

الفرع الأول: طرق الإثبات في جريمة الإبتزاز الإلكتروني :

[1] ثنيان ناصر الثنيان، **إثبات الجريمة الإلكترونية؛ دراسة تأصيلية تطبيقية**، رسالة ماجستير، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012.

[2] فيصل بن زحاف ، **مقال قانوني بعنوان الحماية الجنائية للحكومة الإلكتروني، مجلة القانون المجتمع والسلطة**، العدد رقم 03، 2014، ص82.

خصوصية متابعة جريمة الإبتزاز الإلكتروني تكمن في صعوبة إثباتها لأنها تتم عن طريق وسائل تقنية معقدة، وتتم في مسرح رقمي، وكل هذا ينعكس على مدى حجية الدليل الرقمي المتحصل عليه من سلسلة إجراءات التحري والإستدلال، وهل تكفي لتكوين قناعة تسمح بتحريك دعوى عمومية ضد الجاني ومن ثم التحقيق معه؟.[1]

ولم تسلم طرق الإثبات من تأثيرات ثورة المعلومات والتكنولوجيا فقد أفرت إلى حيز الوجود نوعاً جديداً من الأدلة يتماشى مع طبيعة جرائم الأنترنت، وهو ما يعرف بالدليل الرقمي، أي الدليل الناتج عن فحص المكونات المعنوية أو البرمجية للحواس وشبكة الأنترنت، وهذا الدليل تبنته معظم التشريعات وذلك بتحديد الشروط التي يجب توافرها في الدليل الرقمي حتى يمكن قبوله من قبل القضاء الجزائي.[2]

أولا: الدليل الرقمي (الدليل الجنائي الرقمي):

بالرجوع للدليل الرقمي المأخوذ من منظومة معلوماتية نجده يكون في شكل مجالات أو نبضات مغناطيسية أو تطبيقات تكنولوجية خاصة، ويتم تقديمها في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأشكال و الرسوم، وذلك من أجل الربط بين الجريمة والمجرم والضحية وبشكل قانوني يمكن الأخذ به أمام أجهزة انقاذ وتطبيق القانون.[3]

1/ تعريفه:

يعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات مغناطيسية أو نبضات كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات

[1] فاطمة العرفي، المرجع السابق ص 499.

[2] مريم عراب، المرجع السابق، ص 1222.

[3] عبد المطلب ممدوح، **البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت**، دار الكتب القانونية، دون طبعة، مصر، ص 88.

وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، ويتطلب البحث في ماهية الدليل الرقمي التعرض لتعريفه، ثم التعرض على حجيته.[1]

فالدليل الرقمي يتكون من بيانات ومعلومات الكترونية غير ملموسة التي بدورها تدل على وجود الجريمة وحقيقة ارتكابها، ويمكن استخدامها في أي مرحلة من مراحل التحقيق لإثبات واقعة قانونية.[2]

وهناك عدة تعريفات للدليل الرقمي، تباينت بين التوسع والتضيق نذكر منها:

_ هو" أية بيانات مخزنة أو منقولة بواسطة الحاسوب؛ تدعم أية نظرية حول كيفية ارتكاب الجريمة، وتتعلق بعناصر هامة في الجريمة."

_ هو " المعلومات والبيانات ذات القيمة الإستقصائية والمأخوذة أو المنقولة عبر جهاز الكتروني"[3]

2/ خصائصه:

يتميز الدليل الرقمي بخصائص تميزه عن الدليل المادي تتمثل في:

أ_ دليل علمي:

فهو يتميز بالطبيعة الفنية، حيث يتكون من البيانات والمعلومات ذات صفة الكترونية غير ملموسة، ولا تدرك بالحواسب العادية.

ب_ صعوبة محو الأدلة الرقمية:

[1] مريم عراب، المرجع السابق، ص1222.

[2] بشرى، محمد الأمين، **التحقيق في الجرائم المستحدثة**، أكاديمية النايف العربية للعلوم الأمنية، ط1، الرياض، ص 234.

[3] مريم عراب، المرجع السابق، ص 1222.

الأدلة الإلكترونية الرقمية يمكن استرجاعها بعد محوها وإصلاحها بعد إتلافها، مما يؤدي إلى صعوبة التخلص منها.[1]

ج_ دليل قابل للنسخ:

حيث تتيح التكنولوجيا المعلوماتية استخراج نسخ الأدلة الرقمية محقق جنائي، وفني متخصص لديه المهارة الفنية والتقنية لاستخلاص وجمع الأدلة الرقمية.[2]

الفرع الثاني: صعوبة الإثبات في جريمة الإبتزاز الإلكتروني:

كما عهدنا على هذا النوع من الجرائم حدوثه في الخفاء ويكون الجاني أو الجناة ممن يتصفون بالذكاء ويمتلكون أدوات المعرفة التقنية وبالرغم من الجهود المبذولة لمكافحة الجريمة الإلكترونية، إلا أن هناك بعض المعوقات التي تواجه رجال السلطة في الإثبات بالدليل الرقمي وذلك للعديد من الأسباب نذكر أبرزها:[3]

أولا: معوقات مرتبطة بالدليل ذاته:

1/ سهولة محو الدليل:

حرص الجاني الإلكتروني في جرائم الإبتزاز الإلكتروني على محو أي آثار للإبتزاز بعد القيام بتهديد المجني عليه مما يصعب الوصول إلى الدليل، وفي بعض الأحيان يكون مستحيل.[4]

2/ صعوبة الكشف عن هوية الجاني من خلال الدليل الرقمي:

---

[1] رشيدة بوكر، **جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن**، منشورات المحلي، الطبعة الأولى، 2012، ص 398.

[2] آمال برحال، المرجع السابق ص 89.

[3] وائل سليم عبد الله شاطر، المرجع السابق، ص442.

[4] المرجع نفسه.

تختلف جريمة الإبتزاز الإلكتروني عن جرائم الإبتزاز التقليدية لأنها تحدث في عالم الكتروني افتراضي تحكمه الرموز والبيانات ويخلو من العنف الظاهر والآثار المادية كالجريمة التقليدية مما يصعب عمل الوصول لدليل مادي.[1]

3/عرقلة الوصول إلى الدليل:

وضع العقبات الفنية من قبل الجناة كتشفير الملفات الرقمية لمنع الكشف عن جريمته واكتشاف أدلتها.

ثانيا : صعوبات متعلقة في نقص الخبرة:

نقص الخبرة بعض العاملين في جهات التحقيق؛ مما يؤثر على عملية التحقيق برمتها من حيث ضبط الأدلة، حمايتها واحرازها حتى لا يتم إتلافها وضياعها، مثل اتلاف القرص الصلب، الأقراص الممغنطة أو أوعية المعلومات التي تخزن فيها البيانات.[2]

ثالثا: صعوبات متعلقة في احجام المجني عليه:

عدم الإبلاغ من قبل المجني عليه وخوف المجني عليه من الإبلاغ سبب رئيسي في تشكيل الصعوبة التي تواجه رجال الضبط والمحققين في هذا النوع من الجرائم، وبالتالي فإن هذا الأحجام يساعد على اختفاء الدليل الرقمي الذي يدل على الجاني ويكون هذا سبب في تكوين عقبة تتفق عثرة في طريق الإثبات عن طريق الدليل الرقمي.[3]

رابعا: صعوبة التعاون الدولي:

حيث أن اختلاف تشريعات الدول في تجريم أفعال الإبتزاز الإلكتروني بصفة عامة مختلفة من دولة لأخرى، وهذا مما يزيد العراقيل في ملاحقة الجناة، ورغم المناداة بضرورة التعاون

[1] وائل سليم عبد الله الشاطر، نفس المرجع، ص 442.

[2] فاطمة العرفي، المرجع السابق، ص 503.

[3] وائل سليم عبد الله شاطر، المرجع السابق، ص443.

الدولي في مكافحة الجريمة الإلكترونية، إلا أن هناك عوائق تحول دون تحقيق ذلك، ومن هذه العوائق[1]:

1/ عدم وجود نموذج واحد متفق عليه يتعلق بالنشاط الإجرامي:

لم تتفق لم تتفق الأنظمة القانونية في الدول على صورة واحدة محددة كما يسمى "اساءة استخدام نظم المعلومات الواجب اتباعها"، كما أنه لا يوجد تعريف متفق عليه ومحدد للجريمة تتفق جميع الدول على تجريمه.

2/ عدم وجود تنسيق دولي يتعلق بالإجراءات الجنائية في شأن الجريمة الإلكترونية:

كأعمال الضبط والتحقيق والإستدلال، خاصة في إمكانية الحصول على الدليل في الجرائم التي تقع خارج حدود الدولة فضلا عن الصعوبة الفنية في الحصول على الدليل بعينه.

3/ عدم وجود معاهدات ثنائية أو اجتماعية بين الدول تسمح بالتعاون المثمر في مجال الجرائم الإلكترونية:

وحتى وإن وجدت معاهدات وأقيمت الندوات المتعلقة بالأمن السيبراني الدولي مؤخراً كمؤتمر الأمن السيبراني المنعقد في الرياض في 14، 13، فيبراير عام 2019، الذي كان هدفه مناقشة سبل المعالجة الإستباقية لتحديات الأمن السيبراني وكيفية حماية البيانات والمعلومات الحساسة للمملكة العربية السعودية.[2]

4/ مشكلة الإختصاص في الجريمة الإلكترونية:

ما يعرقل الوصول إلى الجريمة الإلكترونية هي عيب الإختصاص في المستوى المحلي والدولي بسبب تداخل وترابط شبكة المعلومات فقد يكون مكان نشأة الجريمة في دولة

[1] وائل سليم عبد الله الشاطر، نفس المرجع، ص 443.

[2] المرجع نفسه، ص_ص، 443_444.

والجاني في دولة والمجني عليه في دولة والدليل الرقمي يتبع نظام دولة أخرى في مكان ما، ومن هنا تنشأ مشكلة البحث على الدليل الرقمي على شبكة الإنترنت، مما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدول.[1]

[1] وائل سليم عبد الله شاطر، نفس المرجع، ص 444.

خلاصة الفصل الثاني:

نستخلص من خلال هذا الفصل الإطار الإجرائي لجريمة الإبتزاز الإلكتروني، وذلك من خلال هذه الدراسة أن جريمة الإبتزاز الإلكتروني متميزة عن باقي الجرائم، ليس فقط في تعريفها وخصوصيتها، بل تعدى الأمر ذلك حتى في إجراءات الردعية لعقوبتها، وذلك بتسليط الضوء على دراسة الإجراءات العامة والعقوبات الردعية لهذه الجريمة، ولم تغفل التشريعات العربية في بعض الدول إلى خطورة هذه الجريمة، وخطورة مرتكبها، فبادرت بسن مختلف النصوص القانونية التي جاء في أحكامها عقوبات مشددة وأخرى معفية من العقاب، كما سنت عقوبة الشروع والإشتراك في الجريمة، وعقوبات أصلية وأخرى تكميلية لمرتكب جرائم الإبتزاز الإلكتروني، بغض النضر عن كون الفاعل شخصاً طبيعياً أو معنوياً، ذلك بهدف تحقيق الردع والحد من هذه الجرائم التي دخلت إلى مجتمعنا كفيروس خبيث، انتقلت عدواه إلى بقاع العالم وتشتت فيه، وأضحى من الصعب اليوم التخلص منها، كما أن لا ننسى الإشكالات الإجرائية التي تثيرها هذه الجريمة من ناحية إجراءات التحقيق فيها، وذلك من خلال التطرق إلى صعوبات إكتشاف جريمة الإبتزاز الإلكتروني والصعوبات التي تواجه المحقق أو جهات التحقيق فيها، وكذا الإجراءات المرتبطة بالإثبات في الجريمة موضوع الدراسة والتي تناولنا فيها خصوصية هذه الإجراءات، كما تعرضنا إلى أهم طرق الإثبات التي تخص هذه الجريمة، وهو الدليل الرقمي، وذلك من خلال التطرق إلى تعريفه وخصائصه، وكذا صعوبات الإثبات المرتبطة بالدليل الرقمي في حد ذاته، وكذا صعوبات التعاون الدولي، والصعوبات المتعلقة في نقص الخبرة...

الخاتمة

في ختام هذه الدراسة المتعلقة بجريمة الإبتزاز الإلكتروني والذي لا أعتبره محاول الإلمام بالموضوع، وما يطرح من إشكالات عديدة ومبادئ جديدة، يمكن أن نقول أن هذه الجريمة تتميز باختلاف تعريفاتها وتطورها وإرهاقها للمجتمعات الحديثة عرفنا أنها جريمة مستحدثة يكون الحاسب الآلي فيها كأداة لارتكاب هذه الجريمة (جريمة الإبتزاز الإلكتروني)، ويطلق عليها في علم الإجرام بالجرائم الناعمة، التي تخلو من العنف، وهي أحد صور الجريمة الإلكترونية، والإبتزاز الإلكتروني هو الوجه الآخر لجريمة الإبتزاز التقليدية التي تنشأ وترتكب في عالم مادي، وفي مسرح الجريمة التقليدية، حيث يترك الجاني أثاره، أما الإبتزاز الإلكتروني فيتم في عالم افتراضي مليء بالرموز والشفرات، وشبكات المعلومات والأجهزة الحديثة، وتطبيقاته.

ورغم التطور السريع للتكنولوجيا الرقمية، حاولت الدول تطوير تشريعاتها لتواكب هذه الجرائم المستحدثة، فقامت بسن نصوص تشريعية خاصة بهذه الجريمة الإلكترونية.

وبعد الإنتهاء من دراسة موضوع البحث (جريمة الإبتزاز الإلكتروني) التي عرضنا من خلالها الإطار الموضوعي لجريمة الإبتزاز الإلكتروني الذي تحدث عن ماهية الإبتزاز الإلكتروني، وتجريمه أو النضرة القانونية لجريمة الإبتزاز الإلكتروني، كما تطرقنا إلى الجانب الإجرائي لجريمة الإبتزاز الإلكتروني موضوع البحث، من خلال التطرق إلى الإجراءات القانونية الردعية لعقوبة جريمة الإبتزاز الإلكتروني بدراسة مقارنة بين بعض الدول العربية، وكذا الإجراءات القانونية لمكافحة هذه الجريمة من خلال إجراءات التحقيق والإثبات فيها.

لنصل في الأخير من خلال هذا البحث إلى جملة من النتائج والمقترحات:

النتائج:

1-جريمة الإبتزاز الإلكتروني هي صورة من صور الجرائم الإلكترونية، إذ تتم باستخدام

شبكة إنترنت وأجهزة الإتصال الحديثة وتطبيقاتها المختلفة كوسائل التواصل الإجتماعي، والتي بلغت خطورتها على الأفراد والمجتمعات حداً كبيراً وتعني اجبار المجني عليه على تنفيذ أوامر الجاني عبر التهديد والإبتزاز المقترن بطلب، سواءا كان تهديد بالإفشاء أم الإسناد بارتكاب أذى يصيب مال المجني عليه.

2- تعد جريمة الإبتزاز الإلكتروني من جرائم التي تكون تتكون من سلوك مادي ذي مضمون نفسي.

3- لجريمة الإبتزاز الإلكتروني وسائل وطرق مختلفة في ارتكابها تختلف عن الإبتزاز التقليدي، كالهواتف النقالة المزودة بآلة تصوير في الإعتداء على حرمة الحياة الخاصة أو العائلية للأفراد، عن طريق التقاط الصور أو نشر أخبارها أو تسجيلات صوتية، أو مرئية.

4- تجدر الإشارة أن جريمة الإبتزاز الإلكتروني قد تسبب في حدوث جرائم بعدها، كالقتل والزنا، أو أي جريمة عنف أو اعتداء أو سرقة.

5- من أهم النتائج المترتبة على الوسيلة الإلكترونية وهي وسيلة ارتكاب جريمة الإبتزاز سهولة ارتكاب الجريمة عبر تلك الوسيلة، وهي من الجرائم الصعبة الإكتشاف، كما أنها تحتاج إلى فريق عمل من الخبراء والمختصين والمؤهلين في التحقيق فيها لاستعاب التطورات الحديثة مع التحقيق مع المجرم الذكي له صفات تختلف عن صفات المجرم التقليدي، فالمجرم المعلوماتي يتمتع بنوع عالي من الذكاء، والإعتماد بشكل كبير على أساليب تقنية كأنظمة الحاسب الآلي والأنترنت والهواتف الذكية، وكل أشكال الأجهزة الإلكترونية، لأن المجرم لا يترك أثرا مادياً عند ارتكابها.

6- صعوبة تحديد هوية المجرم المعلوماتي واستحالة التوصل إلى أدلة مادية ملموسة، رغم التحديات التي تواجه المشرع، والإمتداد الجغرافي للجريمة فهي عابرة الحدود، فقد

يكون المبتز في دولة والضحية في دولة أخرى.

7- جريمة الإبتزاز الإلكتروني جريمة صعبة الإثبات، حيث أنه من السهل محو آثارها وتحتاج لعمل شاق كي يتم إثباتها.

8- الدليل الرقمي أهم أدلة الإثبات في جريمة الإبتزاز الإلكتروني إلا أن التعامل معه يحتاج إلى أجهزة وخبرات متخصصة وفرق عمل متكامل الخبرة.

9- عجز النصوص التقليدية لتصدي لهذا النوع المستحدث للإجرام، وعدم وجود نصوص قانونية صارمة تجرم هذه الأفعال وتجبر مرتكبها على التفكير قبل تنفيذهم لجرائمهم.

10- وجود فجوة تشريعية بين تشريعات دول العالم في تجريم الإبتزاز الإلكتروني مما سهل التهرب من المتابعة والعقاب خاصة الدول التي لم تفرد نصوص خاصة تجرم هذا السلوك الإجرامي على غرار المشرع الجزائري والعراقي.

11- اختلفت بعض تشريعات العربية في مقدار العقوبة المقررة لجريمة الإبتزاز الإلكتروني فالمشرع الإماراتي ضاعف مدة الحبس بحده الأعلى سنتين، أما المشرع السعودي فجعل الحد الأعلى سنة، و المنظم السعودي خرج عن القواعد العامة حين قرر عقوبة للمساهم في الجريمة حتى وإن لم تتم الجريمة.

12- تقرير الإعفاء في بعض التشريعات لفاعل الجريمة حال الإبلاغ عنها؛ بمعنى إخبار السلطات قبل العلم بالجريمة والإخبار عن شركاء الجريمة.

المقترحات:

في ضوء النتائج التي أظهرتها الدراسة نستخلص بعض التوصيات والإقتراحات تتمثل في:

1_ ضرورة استحداث نصوص قانونية إجرائية تتلائم مع مجال الضبط والتحقيق في المجال الإفتراضي، لأن جريمة الإبتزاز الإلكتروني أكثر تطور مستقبلا، والأجيال القادمة تكون أكثر خبرة.

2_ لابد من ضرورة نشر الوعي داخل المجتمع بأخطار جريمة الإبتزاز الإلكتروني، مع اتخاذ كل الإجراءات الإحترازية للحيلولة دون وقوع الأشخاص ضحايا للإبتزاز الإلكتروني، وتشجيع من يتعرض للإبتزاز بالإبلاغ عن الجريمة، للتخلص منها دون إبلاغ المجرم عن نية التحريك ، فالتصرف بحكمة يمكن إيقاع المجرم في شباك القضاء.

3_ الإتصال فورا بالجهة المختصة لأنها الأقدر للتعامل مع الجاني، مع عدم مسح المحتوى محل الإبتزاز مهما كان جد حميمي وحساس ومحرج، وتسليمه للجهات الأمنية لأنه يشكل دليل إدانة الجاني.

4_ ضرورة عدم بقاء الضحية لوحده والإسراع بطلب الدعم المادي والمعنوي من شخص موثوق فيه؛ من أخصائيين نفسانيين واجتماعيين حتى يتم تجاوز المحنة.

5_ تدريب وتأهيل العاملين بجهات التحقيق والجهات القضائية، بكل أساليب التحقيق الحديثة، و التعامل مع الدليل الرقمي حتى لا تفلت الجرائم من بين يدي رجال التحقيق بسبب قلة الخبرة في التعامل مع الدليل الرقمي.

6_ ضرورة رفع مستوى التعاون الدولي وتعزيز هذا التعاون في مجال مكافحة هذه الجرائم من خلال الإتفاقيات الدولية، لأن جرائم الإبتزاز الإلكتروني عابرة للحدود.

قائمة المصادر والمراجع

I. قائمة المصادر:

أ/ القوانين:

1- قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012.
2- قانون العقوبات العراقي، رقم 111 لسنة 1999.
3- نظام مكافحة الجرائم المعلوماتية السعودي الصادر عن مجلس الوزراء، رقم 79، لسنة 1428هجري.
4- قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة في بتاريخ 16 غشت 2009.
5- قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427هـ الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 87، الصادة بتاريخ 4 ذي الحجة عام 1427هـ الموافق 24 ديسمبر 2006.
6- قانون مكافحة جرائم تقنية المعلومات المصري رقم 175.
7- قانون مكافحة جرائم تقنية المعلومات العماني، من المادة 17.
8- قانون العقوبات الجزائري من المادة 303 مكرر.
9- قانون الإجراءات الجزائية الجزائري من المادة 40 الفقرة1.
10- المادة الثالثة من قانون العقوبات الجزائري.

ب/ المراسيم:

1- مرسوم بقانون إتحادي رقم 05 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، صادر ب25 رمضان سنة 1433 الموافق ل13 أغسطس 2012،

الجريدة الرسمية، العدد 540(ملحق)، السنة الثانية والأربعون صادر في شوال 1433هـ الموافق أغسطس 2012.

2- نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/2هـ.

3- أنظر المرسوم التنفيذي 11-121 في التشريع الجزائري.

ج/ القرارات:

1- القرار الوزاري رقم 2000 الصادر بتاريخ 1435/06/10هـ.

II. قائمة المراجع:

أ/ الكتب:

1- أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، الجزء الأول، دار النهضة العربية، القاهرة، 1981.

2- أسامة أحمد المناعسة، وجلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، طبعة ثانية، عمان الأردن، 2014.

3- جناجرة بلال، الأنترنت والإبتزاز الإلكتروني، 2019.

4- بشرى، محمد الأمين، التحقيق في الجرائم المستحدثة، أكاديمية النايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض.

5- بوكر رشيدة، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات المحلي، الطبعة الأولى، 2012.

6- زهراء عادل سلبي، جريمة الإبتزاز الإلكتروني – دراسة مقارنة – طبعة الأولى، دار الأكاديميون للنشر والتوزيع، عمان الأردن، 2020.

7- سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل

الإجتماعي – دراسة مقارنة – ، دون طبعة، دروب المعرفة للنشر والتوزيع، الإسكندرية، مصر، 2012.

8- ضياء مصطفى عثمان، السرقة الإلكترونية، دراسة فقهية، دار النفائس للنشر والتوزيع، الطبعة الأولى، 2011.

9- علي حسن الطوالبة، الجرائم الإلكترونية، مطبعة جامعة العلوم التطبيقية، البحرين 2008.

10- علي حسين خلف، سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت،1982 .

11- عبد العزيز بن حمين، الإبتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحة مركز باحثات لدراسة المرأة، بحوث ندوة الإبتزاز المفهوم، الأسباب، العلاج، فهرسة مكتبة الملك فهد الوطنية الرياض، 1432.

12- ممدوح عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت، دار الكتب القانونية، دون طبعة، مصر.

13- عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، طبعة الأولى دار وائل للنشر والتوزيع، عمان الأردن، 2017.

14- كاظم عبد جاسم الزيدي، جريمة الإبتزاز الإلكتروني، دراسة مقارنة، مكتبة القانون المقارن، طبعة الأولى، بغداد 2019.

15- محمد علي العريان، الجرائم المعلوماتية: انعكاسات دورة المعلومات على قانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

16- مدحت رمضان، جرائم الإعتداء على الأشخاص والأنترنت، دار النهضة العربية، القاهرة، 2000.

17- محمود أحمد عبانية، جرائم الحاسوب وأبعاد الدولية، دار الثقافة للنشر والتوزيع، عمان الأردن، 2009.

18- محمد شلال العاني، علي حسن طوالبة، علم الإجرام والعقاب، طبعة الأولى، دار المسيرة، عمان، 1998.

19- نهلى عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان– الأردن، 2010.

20- نسرين عبد الحمين نبيه، الإجرام الجنسي، دار الجامعة الجديدة، الطبعة الأولى، الإسكندرية، 2008.

ب/ البحوث والدراسات العلمية:

أولا: الأطروحات، والمذكرات الجامعية:

1/ أطروحات الدكتوراه:

1. التوجي محمد، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية جامعة أحمد دراية، أدرار 2019.
2. راجي عزيزة، الأسرار المعلوماتية وحمايتها، أطروحة نيل شهادة الدكتوراه في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان 2018.
3. رايز سالم الحقبا، مهارات البحث والتحقيق في الجرائم المعلوماتية، رسالة الدكتوراه، جامعة نايف للعلوم الأمنية.

2/ رسائل الماجستير:

1. قارة أمال، الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق جامعة الجزائر، 2002.
2. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، رسالة

ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة الجزائر، 2019.

3. ثنيان ناصر الثنيان، إثبات الجريمة الإلكترونية، دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012.
4. محمد بن عبد المحسن بن شلهوب، جريمة الإبتزاز الإلكتروني دراسة مقارنة، بحث تكميلي لنيل درجة الماجستير في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية، شعبة الأنظمة جامعة الإمام محمد بن سعود الإسلامية، 2011.
5. نجاء المطيري، سامي مرزوق، المسؤولية الجنائية عن الإبتزاز الإلكتروني في النظام السعودي دراسة مقارنة، رسالة مقدمة استكمال لمتطلبات الحصول على درجة الماجستير في الشريعة والقانون :إشراف عبد الفتاح باباه، الرياض، أكاديمية نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون.
6. يوسف خليل يوسف، الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير، الجامعة الإسلامية غزة، 2013.

3/ مذكرات التخرج ماستر:

1. برحال آمال، جريمة الإبتزاز عبر الوسائط الإلكترونية، مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، تبسة 2020.
2. عكوش سهام، القانون الأجنبي إثباتاً وتفسيراً: دراسة مقارنة، مذكرة مقدمة لنيل شهادة الماستر القانون الدولي، جامعة محمد بوقرة، بومرداس، 2010.

ج/ المقالات:

1- المطلق نورة بنت عبد الله بن محمد، إبتزاز الفتيات أحكامه وعقوبته في الفقه

الإسلامي، جامعة محمد بن سعود الإسلامية، الرياض.

2- أحمد حسن عبد العليم حسن الخطيب، الجرائم المعلوماتية الواقعة عبر مواقع التواصل الإجتماعي، مقال منشور بمجلة الدراسات الإفريقية وحوض النيل، مجلة دورية محكمة تصدر عن المركز الديمقراطي العربي، برلين_ ألمانيا، المجلد 02، العدد 06، أكتوبر 2019.

3- أكرم ديب، نورة بن بوعبد الله، دور الدليل الرقمي الجنائي في إثبات جريمة الإبتزاز الإلكتروني، مجلة الحقوق والعلوم الإنسانية، جامعة باتنة 1، كلية الحقوق والعلوم السياسية الجزائر، المجلد 16، العدد 01، 2023/03/31.

4- أحمد كيلان عبد الله، محمد جبار أنويه النصراوي، العدالة الجنائية في شرحية التجريم والعقاب، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 12، العدد41، 2019.

5- بعيوي شاكر سعاد، جريمة الإبتزاز الإلكتروني، دراسة مقارنة، مقال منشور بمجلة ميسان للدراسات القانونية المقارنة، كلية القانون، جامعة ميسان العراق، نوفمبر 2019.

6- بن زحاف فيصل، مقال قانوني بعنوان الحماية الجنائية للحكومة الإلكترونية، مجلة القانون المجتمع والسلطة، العدد رقم 03، 2014.

7- بوقرين عبد الحليم، المسؤولية الجنائية عن الإستخدام غير المشروع لمواقع التواصل الإجتماعي دراسة مقارنة ، بحث مقدم في مجلة جامعة الشارقة ، دورية علمية محكمة، المجلد 16 ، العدد 01 ، يونيو 2016.

8- رامي أحمد غالبي، جريمة الإبتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق، مقال منشور في مجلة ثقافتنا الأمنية الإصدار الثاني، وزارة الداخلية العراقية، مديرية العلاقات والإعلام، دار الكتب والوثائق ، بغداد ، 2019.

9- زينب محمود حسين، المواجهة الجنائية للإبتزاز الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، كلية القانون والعلوم السياسية، قسم القانون الخاص، المجلد 10، العدد37، 2021.

10- زيوش سعيد، ظاهرة الإبتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الإجتماعية، العدد 22، جانفي 2017.

11- سليمان بن عبد الرزاق الغديان، يحي بن مبارك خطاطبة، عز الدين بن عبد الله النعيمي، صور جرائم الإبتزاز الإلكتروني وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، دار المنظومة رواد في قواعد المعلومات العربية، مجلد 27، العدد 69، يناير2018.

12- عدي جابر هادي، الحماية الجزائية للبريد الإلكتروني، دراسة مقارنة، بحث مقدم بمجلة رسالة الحقوق السنة الثانية، العدد الثالث، كلية القانون، جامعة القادسية، 2010.

13- العرفي فاطمة، حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون، مجلة صوت القانون، المجلد 8، العدد خاص 2، 2022.

14- الرويس، فيصل بن عبد الله ، ملخص الوعي الإجتماعي بظاهرة الإبتزاز الإلكتروني لدى الأسرة في المجتمع السعودي، دراسة ميدانية للعوامل والآثار، مجلة كلية الآداب والعلوم الإنسانية، كلية التربية جامعة شقراء، المملكة العربية السعودية، العدد الثالث وثلاثون، الجزء الثاني.

15- العنزي ممدوح رشيد مشرف الرشيد ، الحماية الجنائية للمجني عليه من الإبتزاز، مقال منشور على الشبكة الإلكترونية، المجلة العربية للدراسات الأمنية، المجلد 33،

العدد 70، الرياض، 2017.

16- عراب مريم، جريمة التهديد والإبتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة وهران2 أحمد بن أحمد، المجلد 7، العدد 1، 2021/06/28.

17- محمد علي سالم، حسون عبيد، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، مجلد 14، العدد 2، العراق، 2007.

18- مازن سمير الحكيم، حسين فتيخان منسي، الإبتزاز الإلكتروني، المفهوم والخصائص و سبل المواجهة ، مجلة ثقافتنا الأمنية ، الإصدار الثاني، وزارة الداخلية العراقية ، مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد، 2019.

19- محمد سعيد عبد العاطي محمد، محمد أحمد المنشاوي محمد، دور القانون الجنائي في حماية الطفل من الإبتزاز الإلكتروني دراسة مقارنة، مجلة البحوث الفقهية والقانونية، العدد السادس والثلاثون، إصدار أكتوبر 2021.

20- وائل سليم عبد الله شاطر، الإطار القانوني لجريمة الإبتزاز الإلكتروني في الألعاب الإلكترونية دراسة مقارنة وفق النظام السعودي والقانون الكويتي، المجلة العربية لنشر العلمي، تاريخ الإصدار2 شباط 2020، المملكة العربية السعودية.

د/ المداخلات العلمية:

1. إبتسام كريم وآخرون، بحث بعنوان: إنتشار ظاهرة الإبتزاز الإلكتروني في المجتمع العراقي، إستطلاع آراء عينة من المجتمع العراقي حول التعامل مع هذه الظاهرة، المؤتمر العلمي الدولي الأول، ثقافة الأكاديميين العراقيين، مركز التطور الإستراتيجي الأكاديمي، جامعة دهوك، العراق، 11-12 فيفري 2019.

2. البداينة ذياب موسى، الجرائم الإلكترونية المفهوم والأساب ، ورقة علمية مقدمة خلال الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 2-2014/4، عمان الأردن.
3. عبد العزيز بن حمين، الإبتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، بحوث ندوة الإبتزاز (المفهوم ، الأسباب ، العلاج) ، فهرسة مكتبة الملك فهد الوطنية، الرياض ، جامعة الملك سعود 2011.
4. نمديلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة أعمال المؤتمر الدولي الرابع عشر" الجرائم الإلكترونية"، مركز جيل البحث العلمي، طرابلس 24-25 مارس 2017.

هـ/ المواقع الإلكترونية:

1. https://www.eqrae.com، مطويات عن الإبتزاز الإلكتروني، أطلع عليه بتاريخ 2023/05/28، الساعة 21:05.
2. https://comthread-1210118-ohtml، يراجع في هذا الشأن مقال بعنوان الإبتزاز الإلكتروني أسباب الوقوع فيه وطرق الحماية منه، منشور بتاريخ 17 ديسمبر 2019، خمس معايير لحماية الأطفال من الإبتزاز الإلكتروني، جدة، منشور بتاريخ 03 يوليو 2016.
3. https://www.legal-researche.com ، بحث عن جريمة الإبتزاز الإلكتروني في 23-06-2022، اطلع عليه بتاريخ 20 ماي 2023، الساعة 21:00.
4. https://www.cyberone.com ، أضرار الإبتزاز الإلكتروني، إطلع عليه بتاريخ 22 ماي 2023، الساعة 10:30.

الفهرس

الفهرس:

ملخص المذكرة

تتحدث هذه الدراسة عن جريمة الإبتزاز الإلكتروني ودراسة مقارنة لها، والسبل الكفيلة لمحاربتها، بتحديد حجم هذه الدراسة ومعرفة العوامل المختلفة التي تتدخل فيها، وأهم المخاطر وهول الخسائر الناجمة عنها وهو الأمر الذي استلزم تدخل التشريعات في بعض الدول من أجل التصدي لمثل هذه الظواهر، ومن بين هذه التشريعات كل من النظام السعودي والقانون الإماراتي والمشرع الجزائري وبعض القوانين العربية، وقد تناولت هذه الجريمة في بدايتها كصورة من صور الجريمة الإلكترونية، بعرض تعريف لماهيتها وأنواعها وخصائصها وطرق إرتكابها وتلك الوسائل وأشكال الحديثة المستخدمة في تنفيذ جريمة الإبتزاز الإلكتروني، كما تناولت أسباب الإبتزاز الإلكتروني والآثار المترتبة عليه، كما تناولت الأركان المكونة لها من ركن شرعي في بعض التشريعات دول العربية ودراسة مقارنة بينهما، وكذا الركن المادي والركن المعنوي، وكذا معالجة الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني وذلك من خلال دراسة جانبيه الجانب الوقائي الداخلي والجانب الخارجي.

كما تناولت هذه الدراسة السبل الكفيلة لمحاربة هذه الجريمة، وذالك بتسليط الضوء على دراسة الإجراءات العامة والعقوبات الردعية لجريمة الإبتزاز الإلكتروني، ولم تغفل الشريعات العربية في بعض الدول إلى خطورة هذه الجريمة وخطورة مرتكبها، فبادرت بسن مختلف النصوص القانونية التي جاء في أحكامها عقوبات مشددة وأخرى معفية وكذا عقوبة الشروع و المساهمة الجنائية، مقارنة بينهما في بعض التشريعات العربية، ومعاقبة مرتكبها ذلك بهدف تحقيق الردع والحد من هذه الجرائم التي دخلت إلى مجتمعنا كفيروس خبيث، انتقلت عدواه إلى بقاع العالم وتشتت فيه، وأضحى من الصعب اليوم التخلص منها، كما أن لا ننسى الإشكالات الإجرائية التي تثيرها هذه الجريمة من ناحية الإجراءات التحقيق فيها، وذلك من خلال التطرق إلى صعوبات إكتشاف جريمة الإبتزاز

الإلكتروني والصعوبات التي تواجه المحقق أو جهات التحقيق فيها، وكذا الإجراءات المرتبطة بالإثبات في الجريمة موضوع الدراسة والتي تناولنا فيها خصوصية هذه الإجراءات، كما تعرضنا إلى أهم طرق الإثبات التي تخص هذه الجريمة، وهو الدليل الرقمي، وذلك من خلال التطرق إلى تعريفه وخصائصه، وكذا صعوبات الإثبات المرتبطة بالدليل الرقمي في حد ذاته، وكذا صعوبات التعاون الدولي، والصعوبات المتعلقة في نقص الخبرة...

الكلمات المفتاحية:

1/ الجرائم الإلكترونية 2/ الإبتزاز الإلكتروني

3/ المشرع 4/ التحقيق

5/ الإثبات 6/ المجرم التقليدي

7/ الشبكة المعلوماتية 8/ المجرم المعلوماتي

9/ الدليل الرقمي 10/ العالم الإفتراضي

Summary of note (Abstract) :

This study talks about the crime of electronic blackmail and a comparative study of it, and ways to combat it, by determining the size of this study and knowing the various factors that interfere with it, and the most important risks and the horrific losses resulting from it, which necessitated the intervention of legislation in some countries in order to confront such phenomena, and among them These legislations include the Saudi system, the Emirati law, the Algerian legislator, and some Arab laws. They dealt with this crime at its beginning as a form of electronic crime, by presenting a definition of its nature, types, characteristics, methods of committing it, and those means and modern forms used in implementing the crime of electronic blackmail. It also addressed the causes of electronic blackmail and the effects. The consequences of it, as well as its components, including a legal element in some legislation in Arab countries and a comparative study between them, as well as the material element and the moral element, as well as addressing the proposed solutions to reduce falling victim to electronic blackmail by studying its two sides, the internal preventive side and the external side. This study also addressed ways to combat this crime, by highlighting the study of general procedures and deterrent penalties for the crime of electronic extortion. Arab laws in some countries did not ignore the seriousness of this crime and the danger of its perpetrator, so they took the initiative to enact various legal texts whose provisions included severe penalties and others that were exempt. As well as the punishment for criminal attempt and participation, comparing it in some Arab legislation and punishing the perpetrator with the aim of achieving deterrence and reducing these crimes

that have entered our society like a malicious virus whose infection has spread throughout the world and has spread in it, and it has become difficult today to get rid of it. We should also not forget the procedural problems raised by this crime in terms of the procedures for investigating it, by addressing the difficulties of discovering the crime of electronic blackmail and the difficulties facing the investigator or the investigating authorities, as well as the procedures associated with proving the crime under study, in which we discussed the specificity of these procedures. We also discussed the most important methods of proof related to this crime, which is digital evidence, by addressing its definition and characteristics, as well as the difficulties of proof associated with the digital evidence itself, as well as the difficulties of international cooperation, and the difficulties related to the lack of experience...

key words:

1/ Electronic crimes. 2/ Electronic blackmail

3/ The legislator 4/ Investigation

5/ Proof 6/ The traditional criminal

7/ The information network 8/ The information criminal

9/ Digital Evidence 10/ Virtual World