جامعة العربي التبسي–تبسة–

كلية الحقوق و العلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر

تخصص:قانون جنائي وعلوم جنائية

بعنوان: جريمة الإبتزاز عبر الوسائل الإلكترونية

إعداد الطالب(ة): برحال آمال

إشراف الأستاذ(ة): شاربي نوال

أعضاء لجنة المناقشة:

الإسم و اللقب	الرتبة العلمية	الصفة في البحث
ياسين جبيري	أستاذ محاضر أ	رئيسا
نوال شاربي	أستاذ مساعد أ	مشرفا ومقررا
عفاف خذيري	أستاذ محاضر ب	مناقشا

السنة الجامعية: 2020/2019

جامعة العربي التبسي–تبسة–

كلية الحقوق و العلوم السياسية

قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر

تخصص:قانون جنائي وعلوم جنائية

بعنوان: جريمة الإبتزاز عبر الوسائل الإلكترونية

إعداد الطالب(ة): برحال آمال

إشراف الأستاذ(ة): شاربي نوال

أعضاء لجنة المناقشة:

الإسم و اللقب	الرتبة العلمية	الصفة في البحث
ياسين جبيري	أستاذ محاضر أ	رئيسا
نوال شاربي	أستاذ مساعد أ	مشرفا ومقررا
عفاف خذيري	أستاذ محاضر ب	مناقشا

السنة الجامعية: 2020/2019

الكلية لا تتحمل أي مسؤولية على ما يرد فى هذه المذكرة من آراء

(بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ)

(وَمَا تَوْفِيقِي إِلاَّ بِاللَّهِ، عَلَيْهِ تَوَكَّلْتُ، وَإِلَيْهِ أُنِيبُ) [هود:88]

شكر و عرفان :

أتوجه الى الله سبحانه و تعالى بالحمد و الشكر،لأنه منّ علي بالتوفيق لإنجاز هذا البحث المتواضع ، فالحمد لله حمدا طيبا مباركا فيه .

كما لا يسعني إلاّ أن أتقدم بجزيل الشكر و الإمتنان الى الأســتاذة الفاضـــــلة **-نوال شارني-** التي تكرمت عليّ بإشرافها، و سديد توجيهاتها إلى غاية إتمام هذا البحث ، كما أتقدم بالشكر إلى جميع أساتذة كلــية الحقوق

بجامعة – العربي التبسي – على المجهودات التي بذلوها من أجلنا .

جزاهم الله عنا كل خير.

إهداء :

إلى الروح الطّاهرة الزّكية ، أبي الغالي(صالح) رحمه الله

و غفر له و عفى عنه وأسكنه فسيح جنانه.

إلى من كرّمها الله في كتابه الكريم ، الوالدة العزيزة حفظها الله و بارك فيها.

إلى أفراد عائلتي الذين كانوا خير عون وسند،

أسأل الله أن يحفظهم و يسدّد خطاهم و يديم شملهم .

أهـــــدي ثمرة جهدي هذا.

قائمة المختصرات

ج ر	الجريدة الرسمية
د د ن	دون دار نشر
د س ن	دون سنة نشر
ط	طبعة
ق ع ج	قانون العقوبات الجزائري
ق إ ج ج	قانون الإجراءات الجزائية الجزائري
ص	صفحة

مقـــــــــدمة

شهد العالم في السنوات الأخيرة ثورة كبيرة في تقنيات المعلومات، و من أهم أوجه إنتفاضتها التقدم المذهل في مجال الحواسيب الآلية و ملحقاتها و البرامج التي تلحق بها حيث أصبح الإعتماد على هذه التكنولوجيا جليا في كل الجهات الرسمية و غير الرسمية ، فأصبحت الدول يقاس تقدمها على مدى قدرتها على امتلاك و التعامل مع التكنولوجيا الحديثة،لكن هذه النعمة صاحبها الاستخدام غير القانوني لهذه التكنولوجيا، فأصبحت تستخدم كمعول هدم لا بناء في أيدي الخارجين عن القانون، ذوو الصفات الخاصة،صاحبو الإجرام الناعم الذي لا يراق فيه نقطة دماء،و بذلك أسهمت في ظهور نوع جديد من الجرائم التي تتصف في الغالب بخطورتها و بسهولة ارتكابها لا سيما أنها جرائم عابرة للحدود و هي ما يطلق عليها الجرائم الإلكترونية.

و هذه الجرائم إما تقع على على الكمبيوتر أو بواسطته حيث يصبح أداة طيعة في يد الجناة يستخدمونها لتحقيق مآربهم الإجرامية مستغلين بذلك تلك التقنيات المستحدثة و التي أصبحت فيما بعد محلا لتلك الجرائم أو وسيلة لارتكابها، فأصبح الوسط الذي ترتكب فيه الجريمة الإلكترونية ومضات كهربائية أو مغناطيسية و رموز و شفرات و لم يعد مسرح الجريمة إلا مسرحا افتراضيا .

إن بعض مجرمي الأنترنت التقليديين قد عزفوا عن جريمة سرقة بطاقات الائتمان ،و معلومات التعريف الشخصية و اتجهوا الى أسلوب أسهل ألا و هو الإبتزاز الإلكتروني، حيث يستخدمون التهديدات التي تحتوي على صور شخصية و أفلام رقمية للضحية للمطالبة بأموال بدلا من سرقتها.

حيث اصبحت جريمة الإبتزاز الإلكتروني ضاهرة تخترق المجتمع و تهدد دعائمه، و تضرب في مقتل أهم أهداف أي مجتمع متحضر في تحقيق الأمن لأفراده،ولعل جوهر تجريم الإبتزاز الإلكتروني هو التهديد ، و التعدي على حقوق الافراد في الخصوصية ، و استغلالهم على غير وجه حق، و الضغط الذي يمارس على الضحية بكشف أسرار من شأنها أن أو تضره ، مما يضطره للإنصياع ،والإذعان لرغبة الجاني و تحقيق مطالبه تحت الإكراه أو الخوف من الفضيحة و هو ما دعى المشرعين في العديد من الدول الى سن قوانين تجرم السلوك الإجرامي الذي يتمثل في جريمة الإبتزاز الإلكتروني ،واهتم شراح القانون بتفسيره، و شرحه، و بيان أركان الجريمة التي تقوم عليها ،و كذلك طرق التحقيق، والإثبات فيها كما ان للدليل الرقمي أسس و قواعد مختلفة في التعامل معه بسبب خطورة هذه الجريمة .

و نظرا الى الآثار المترتبة على انتشار جريمة الإبتزاز الإلكتروني في المجتمع ،وكونها من المستجدات الطارئة عليه فأن للبحث أهمية من الناحيتين العلمية و العملية.

فمن الناحية العلمية ، لفت انتباه الباحثين لدراسة الموضوع و تسليط الضوء على مختلف جوانبه كذلك لفت انتباه المشرع الى إعادة النظر و ضبط النصوص القانونية لمكافحة هذه الجريمة ،أما من الناحية العلمية تبرز أهمية البحث في معرفة مدى كفاية النصوص الجنائية في بعض التشريعات العربية الواردة في قوانين العقوبات إلى الحد من ارتكاب هذه الجريمة و ردع مرتكبيها للتقليل من آثارها و زيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة و ضرورة توخي الحيطة و الحذر في استخدامها.

أما عن أسباب اختيار الموضوع فهي ذاتية ، تتمثل في الرغبة في دراسته كونه يتناول ظاهرة تؤرق المجتمع و تهدد استقراره ، و موضوعية نظرا لكون الجريمة موضوع الدراسة تفشت و تنامت في المجتمع مما يستدعي دراستها باعتبار المجتمعات العربية معروفة بالعادات ، والأعراف الإجتماعية التي تتحفظ على كل ما يتعرض للسمعة و الشرف خصوصا أن هذه الجريمة أغلب ضحاياها فتيات.

تهدف هذه الدراسة الى التعرف الى النقاط التالية :

– التعرف على جريمة الإبتزاز عبر الوسائل الإلكترونية .

– التعرف على طرق ارتكابها و التعرف على دوافع ارتكابها.

– دراسة أركان الجريمة في بعض التشريعات العربية و التشريع الجزائري.

– التعرف على كيفية التحقيق و الإثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية ،و التعرف على الدليل الرقمي و علاقته بهذه الجريمة .

– التعرف على الصعوبات التي تواجه السلطات في التحقيق على هذه الجرائم ،و إثباتهاو التعرف على العقوبات المقررة لهذه الجريمة في بعض التشريعات العربية .

ونظرا لتزايد نسبة ارتكاب هذه الجريمة في الآونة الأخيرة، ونظرا لخصوصية هذه الجريمة ، ووسائل وطرق تنفيذها، أدى إلى إنعكاس هذه الخصوصية على مضمون الأنظمة والقوانين، حتى تتماشى مع طبيعة هذه الجريمة ومعطياتها وآثارها، وبناءا عليه كانت الحاجة ملحة لوضع هذا الموضوع موضع دراسة وتحليل وينبني ذلك على الإجابة على إشكالية الدراسة المتمثلة في :

كيف واجهت بعض التشريعات العربية جريمة الإبتزاز عبر الوسائل الإلكترونية؟

تمحورت هذه الدراسة القانونية العلمية، كان مجال البحث في بعض القوانين العربية ، كالمصري، وبعض دول الخليج العربي، كالمملكة العربية السعودية، و الإمارات المتحدة، الكويت،عمان،العراق ،مع توضيح موقف التشريع المحلي .

لمعالجة هذه الإشكالية إرتكزت الدراسة على المنهج الوصفي لوصف الجريمة ،من خلال تعريفــها ،وآثارها ،وسائل ارتكابها ، و المنهج التحليلي معتمدين على تحليل نصوص كل من نظام مكافحة جرائم المعلومات السعودي و قانون جرائم تقنية المعلومات الكويتي و العماني و قانون مكافحة جرائم تقنية المعلومات الإماراتي و قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و بيان موقفها من جريمة الإبتزاز الإلكتروني والمنهج المقارن للمقارنة بين مختلف النصوص السالفة الذكر .

و لدراسة هذا الموضوع ارتأينا تقسيم البحث إلى فصلين ، الأول بعنوان الإطار الموضوعي لجريمة الإبتزاز الإلكتروني و قد تناولنا في المبحث الأول منه ماهية الإبتزاز الإلكتروني أما المبحث الثاني: تجريم الإبتزاز عبر الوسائل الإلكترونية ،أما الفصل الثاني فقد كان بعنوان : الإطار الإجرائي لجريمة الإبتزاز عبر الوسائل الإلكترونية الذي يحتوي على مبحثين الأول بعنوان التحقيق في جريمة الإبتزاز عبر الوسائل الإلكترونية ، أما المبحث الثاني قتناول الإثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية و في الأخير انتهينا الى توضيح النتائج و المقترحات التي تم التوصل

الفصل الأول:الإطار الموضوعي لجريمة الإبتزاز عبر الوسائل الإلكترونية.

المبحث الأول:ما هية الإبتزاز عبر الوسائل الإلكترونية.

المبحث الثاني : تجريم الإبتزاز عبر الوسائل الإلكترونية.

تعتبر جريمة الإبتزاز الإلكتروني من الجرائم المستحدثة ،و يطلق عليها في علم الجريمة الجرائم الناعمة،التي تخلو من العنف و هي احدى صور الجريمة الإلكترونية فالإبتزاز الإلكتروني هو الوجه الآخر لجريمة الإبتزاز التقليدية التي ترتكب في عالم مادي، و في مسرح جريمة تقليدي حيث يترك الجاني آثار كالبصمات أو الدماء ، لكن الإبتزاز الإلكتروني فيتم في عالم افتراضي مليئ بالرموز و الشفرات تحدده نقاط الاتصال و التكنولوجيا الرقمية،حيث تعتمد هذه الجريمة أساسا على وسائل التكنولوجيا الحديثة ، و إذا ما وقفنا على ماهية ظاهرة الإبتزاز من خلال مفهومها الذي يتطرق الى مختلف تعريفاتها ،و أنواعها و وسائلها و آثارها . و إذا ما وقفنا على هذا السلوك الذي يشكل جريمة كان لزاما علينا ان نتعرض لأركانها و العقوبات المقررة لها في بعض القوانين العربية .

المبحث الأول: ماهية الإبتزاز عبر الوسائل الإلكترونية.

إن الغموض الذي يحيط بجريمة الإبتزاز عبر الوسائل الإلكترونية منذ بدايتها و حتى تمام تنفيذها قد شكل تحديا كبيرا أمام الجهات القضائية حتى أن هذا الغموض قد صاحب تعريف هذه الجريمة.

واختلفت التعريفات لكنها اتفقت في كون استخدام التكنولوجيا و الواقع الإفتراضي كمسرح للجريمة ،و كذلك مرتكبها ذوو المهارات و الصفات المختلفة عن المجرم التقليدي .

كما أنه كان بالأهمية بمكان التطرق الى مفهوم الإبتزاز عبر الوسائل الإلكترونية من خلال تعريفه و أنواعه، و وسائله، و آثاره من خلال مطلبين، المطلب الأول: مفهوم الإبتزاز عبر الوسائل الإلكترونيتة ،أما المطلب الثاني :وسائل الإبتزاز عبر الوسائل الإلكترونية وآثاره .

المطلب الأول:مفهوم الإبتزاز عبر الوسائل الإلكترونية

يعتبر الإبتزاز الإلكتروني هو نتاج الإستخدام السلبي للثورة التكنولوجية التي لحقت العالم حديثا وهي من الآثار غير المرغوب فيها لهذا التقدم العلمي المذهل الذي جعل المجرم يختبئ خلف شاشة ما،و يمارس عملا إجراميا بالإعتداء على مصلحة يحميها القانون للضحية،حيث تتم الجريمة عن طريق الجاني بالضغط على المجني عليه بتهديده تارة و الوعيد تارة أخرى و ذلك بنشر معلومات أو صور أو تسجيلات لا يرغب المجني عليه في إظهارها ، فالإبتزاز الإلكتروني هو أسلوب من أساليب الضغط و الإكراه على المجني عليه يمارسه الجاني لتحقيق مقاصده الإجرامية و ذلك للوصول لهدفه الذي قد يكون هدفا ماديا أو معنويا.

و من خلال هذا المطلب سيتم التطرق الى مفهوم الإبتزاز عبر الوسائل الإلكترونية حيث يحتوي على فرعين، الفرع الأول يتناول تعريف الإبتزاز عبر الوسائل الإلكترونية أما الفرع الثاني يتناول أنواع الإبتزاز عبر الوسائل الإلكترونية .

الفرع الأول:تعريف الإبتزاز

أولا:التعريف اللـــغوي

يرجع أصل كلمة إبتزاز الى الفعل الثلاثي بز بتشديد الزاي، فيقال: بز الشيئ يبزه بزا.

بمعنى اغتصبه ، و البز هو هو السلب ، وابتززت الشيئ: استلبته و من ذلك جاء

المثل (من عز بز) معنى ذلك من غلب سلب.(1)

بز المال:سلبه من الناس بغير حق،او نزعه منهم بقهرو اذلال.(2)

تعريف الابتزاز استعمله العلماء في كتاباتهم فعلا و حديثا و لا يخرج من مفهومه المعاصر .

---

(1) ابو الفضل جمال الدين محمد بن مكرم (ابن المنظور) معجم لسان العرب، دار صابر لبنان،المجلد الثاني ،حرف الباء.

(2) ((العين)) (303/7) باب الزاي و الباء ((جمهرة اللغة)) مادة (بزز) (68/1) ((لسان العرب))

ثانيا : التعريف الاصطلاحي

1/ الحصـــول علـــى معلومـــات ســـرية أو صـــور شخصـــية أو مـــواد فيلميـــة تخـــص الضـــحية و اسـتغلالها لأغـراض ماديـة أو القيـام بأعمـال غيـر مشـروعة و هـو الحصـول علـى المـال او المنـافع من شخص و إبتزازه بواسطة التهديد بفضح بعض أسراره التي يمتلكها.(1)

2/ محاولة تحصيل مكاسب مادية او معنوية من شخص (طبيعي أو اعتباري بالإكراه بالتهديد بفضح سر وقع عليه المبتز).

3/محاولة الإكراه و سلب الإرادة و الحرية لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية او كلاهما معا.

4/استغلال القوة مقابل ضعف إنسان آخر سواء كان مؤقتا ، أو دائما،أما الإبتزاز الإلكتروني فهو مصطلح مكون من كلمتين :

الأولى" الإبتزاز "و قد تم التطرق الى تعريفه و الثانية " الإلكتروني " أي حصول الإبتزاز باستعمال وسائط إلكترونية و عن طريق الشبكة المعلوماتية اذ أن هناك الكثير من المواقع الإلكترونية المنصبة لممارسة الإبتزاز مثل مواقع التواصل الاجتماعي ، أو عن طريق الأجهزة الإلكترونية كالحاسوب و ما في حكمه كالهواتف الذكية و لهذا يمكن القول بأن الإبتزاز الإلكتروني هو التهديد و الظغوطات التي تتم باستخدام الوسائل التكنولوجية الحديثة لإستغلال الضحية ماديا او جنسيا او معنويا.

ثالثا: التعريف الفقهي

تعددت تعريفات الفقه للإبتزاز، فقد عرفه بعض الفقه على أنه الضغط الذي يباشره شخص على إرادة شخص اخر بحمله على ارتكاب جريمة معينه .

وقد عرفه البعض الآخر على أنه فعل يقوم به شخص بتهديد شخص آخر بأي طريقه 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.

(1) محمد بن المحسن بن شلهوب ، جريمة الإبتزاز الإكتروني ، دراسة مقارنة بحث تكميلي لنيل درجة الماجيستير في السياسة الشرعية ، المعهد العالي للقضاء ، قسم السياسة الشرعية ، شعبة الانظمة ، جامعة الامام محمد بن سعود الاسلامية 2011، ص59 .

وقد عرف على أنه (القيام بتهديد شخص بفضح أمره ما لم يستجب المهدد الى تنفيذ طلبات الجاني وغالبا ما تهدف تلك الطلبات إلى أمور غير مشروعه تمس الشرف ، أو الكرامه، أو تتعلق بحرمة الحياة الخاصة للشخص المهدد الذي تم إبتزازه.) (1)

وفي تعريف آخر فقد عرف الإبتزاز الإكتروني (بأنه الحصول على وثائق، و صور، 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 او تهديد يمارسه المبتز على إرادة المجني عليه بهدف الوصول الى تحقيق مراده لأن الإبتزاز مرتبط بالتهديد فدون هذا الأخير لا يتحقق الإبتزاز كما نستطيع القول ان الإبتزاز الإلكتروني يمثل سلوك غير مشروع أو غير اخلاقي ويعد من الجرائم التي تقع عن طريق الشبكة المعلوماتية.

إذ أن هناك الكثير من المواقع الإلكترونية الخاصة بممارسة الإبتزاز كمواقع التواصل الإجتماعي (فيسبوك) أو، عن طريق الأجهزة الإلكترونية الأخرى كالهواتف الذكية و الأجهزة المحمولة الأخرى.

جريمة الإبتزاز الإلكترونية لا تخرج عن نطاق الجرائم العادية لكنها ترتكب بوسيلة معينة والقانون بصفة عامة لا يعتمد بوسيلة اقتراف الجريمة.

فقد سوى كقاعدة عامه بين الوسائل برغم تعريفات ظاهرة الإبتزاز الإكتروني المتعددة إلا أنها تقف جميعا في عنصر التهديد الذي يستخدمه الجاني وينتهي بعمل غير قانوني أوعنف ضد الشخص إن لم يستجب لمطلب المبتز وإذا نظرنا لتعريف جريمة الإبتزاز الإلكتروني فقد نجد أنها جريمة ما تتعلق بالحصول على أموال ، أو ممتلكات ، أو خدمات من فرد ، أو مؤسسة عن طريق التهديد باستخدام وسيلة غير مشروعة كاختراق حاسوب ، أو التقاط صور ، أو فيديوهات لشخص أو قد يكون هو من سلمها الى المبتز بنفسه ثم يقوم المبتز بطلب الأموال في المقابل فإذا ما قمنا بتحليل هذا التعريف فاننا نستنتج:

(1) ممدوح رشيد مشرف الرشيد العنزي ،الحماية الجنائية للمجني عليه من الابتزاز ، مقال منشور على الشبكة الالكترونية ،المجلة العربية للدراسات الامنية ، المجلد 33 ، العدد 70، الرياض 2017، ص199.

(2) المرجع نفسه.

1/ إن تهديد شخص ما أو إكراهه أو القيام بأمر ما ، أو خدمة ، أو تنازل عن ممتلكات فهذا اعتداء صريح على حق الملكية الخاصة المتمثلة في الأموال والممتلكات وكذلك يشكل اعتداء على الحق الفردي من خلال استخدام عنصر التهديد والذي من المفروض أن يكون الشخص آمن على حياته وممتلكاته الخاصة من الإعتداء عليها.

2/ إن اختراق الحواسيب والهواتف الذكية والحصول على المراسلات الخاصة بالأفراد وتهديد الشخص فيه انتهاك لسرية المراسلات ، واعتداء على حرمة الحياة الخاصة التي كفلتها الدساتير والقوانين.(1)

لا خلاف في الفقه ان تعريف الحياة الخاصة امر عسير وصعب وذلك لاختلاف مضمون هذه الحياة واختلاف نطاق الخصوصية من فرد لآخر. (2)

الخلاف يتمحور حول نطاق الحياة الخاصة لكن لابد الى الحق في الخصوصية فهو حقيقة مؤكدة لدى جميع الأفراد وفي كل المجتمعات فهي تعني الحق في الحياة الأسرية والشخصية والداخلية والروحية للشخص عندما يعيش وراء بابه المغلق حسب الفقيه martin .(3)

إن دخول نظام المعالجة الآلية للمعلومات قلب الكثير من الأوضاع وأصبح له اثر بالغ في المجتمع خاصة في مجال الحياة الخاصة فأصبح بنك المعلومات وهو جزء من النظام الآلي للمعطيـــــات ، و مستودعا كبيرا للكثير من الاسرار المتعلقة بالحياة الخاصة للأفراد مما يسمح بالحصول على هذه الأسرار والإطلاع عليها بسهولة وسرعة غير مسبوقة ، وكم هائل ونقل هذه المعلومات من مكان لآخر عن طريق أجهزة الإتصال التي تعمل عن بعد في أماكن مختلفة أن الحق في الحياة الخاصة يتطلب أن يربط بمحاور الحماية الجزائية التي أصبحت أعظم حاجة وأكبر إلحاح خصوصا وقد تجلت الافكار الآتية للمجرمين التقنيين في اتباع وسائل وطرق مستحدثة لتحقيق الإعتداء على الحياة الخاصة للأفراد عن طريق الإبتزاز الإلكتروني.

---

(1) الشحات ابراهيم محمد منصور،الجرائم الالكترونية في الشريعة الاسلامية و القوانين الوضعية، بحث فقهي مقارن،ط1،دار الفكر الجامعي،الاسكندرية ، ص80.

(2) المرجع نفسه، ص81.

(3) اسامة احمد المانعسة،جلال محمدالزعبي،جرائم تقنيةالمعلومات الالكترونية،(دراسة مقارنة)،ط2،دارالثقافة للنشر و التوزيع،عمان،الاردن،2014، ص 241.

الفرع الثاني:أنواع الإبتزاز عبر الوسائل الإلكترونية

تبدأ العلاقة بين طرفي الإبتزاز عن طريق الثقة الوهمية المتبادلة والأساليب الملتوية و المخادعة والوعود الكاذبة ثم تتطور حتى يكون باستطاعة المبتز الحصول على بعض أسرار ضحيته و يحتفظ بها و من ثم تبدا عمليه المساومة و الإبتزاز.(1)

تتعدد أسباب ودوافع الإبتزاز بحسب شخصية الهدف ومدى قابليته للدخول في هذه الدائرة ولكن في أغلب الأحوال هو الخلل السلوكي لدى الطرفين ، المبتز أو الضحية.

تعتبر المرأة الضحية الأبرز في هذه الجريمة و في الغالب كما أن تهاون الأسرة في الرقابة على أبنائها وإعطائهم الحرية دون ضوابط صحيحة، كما يؤدي الفقر والحرمان بالكثير من الأفراد في مختلف المجتمعات في القيام بممارسات تصل في كثير من الأحيان الى حد الإنحراف وارتكاب الجرائم ، كما أن استخدام الوسائل التقنية والإتصالات بشكل سلبي مثل البريد الإلكتروني العشوائي والإيميلات المجهولة و المواقع الإلكترونية العامة والخاصة و مواقع التعارف بين الجنسين ، و مواقع الألعاب و المنتديات الإلكترونية و مواقع الدردشة و الإعلانات المضللة في المواقع الإلكترونية فهي من أكبر الوسائل التي يتم استخدامها لأغراض الإبتزاز. (2)

أما من حيث أساليب الابتزاز التي يمارسها المبتز على الضحية فيعتمد على أسلوب التهديد سواء كان التهديد بالتشهير ، أو التهديد بابلاغ ذوي الضحية ،الأمر الذي يجعل الضحية يقع تحت وطأة ضغوط المبتز ليجبرها على مجاراته في تحقيق غاياته.

---

(1) الحمين عبد العزيز بن حمين بن أحمد ،الابتزاز و دور الرئاسة العامة لهيئة الامر بالمعروف و النهي عن المنكر في مكافحته، بحث مقدم لندوة الإبتزاز(المفهوم،الاسباب،العلاج) ،جامعة الملك سعود ،2011 ، ص58 .

(2) الرويشد أسماء بنت راشد بن عبد الرحمان ،الإبتزاز محليا,بحث مقدم لندوة الابتزاز (المفهوم،الأسباب،العلاج) ، جامعة الملك سعود ،2011، ص137.

ويمثل الإستخدام السلبي للشبكة العنكبوتية عاملا مهما في انتشار جرائم الإبتزاز الذي يستغلها المبتز وتعد جرائم إبتزاز النساء من أكثر انواع الإبتزاز انتشارا وشهرة ، حيث أن جرائم الإبتزاز الإكتروني للنساء تعتبر النموذج المثالي للجريمة لا سيما إذا كان المبتز رجلا وضحية الجريمة امرأة.
هذا لا يمنع من أن جريمة الإبتزاز الإلكتروني من الجرائم ذات الصور المتشعبة حيث أن هذه الصور تتنوع تارة بالنظر الى الهدف المرتقب من الجريمة ، أو المنفعة التي تعود على المبتز.

أولا: الإبتزاز عبر الوسائل الإلكترونية بالنظر لشخص الضحية

و فيه يقسم جرائم الإبتزاز الإلكتروني تبعا لشخصية المجني عليه المحتمل كضحية للجريمة و ذلك على النحو التالي:

أ: الشخصيات الإعتبارية

قد تكون الفئة المستهدفة من الإبتزاز الإلكتروني هي أشخاص اعتبارية كالحكومات ، و الشركات، و المؤسسات ، و ذلك عن طريق الحصول على معلومات سرية خاصة بها ثم يقوم المبتز بالتهديد بالإفصاح عنها ، و افشاؤها ، و نشرها للخرين، فتبدأ الجريمة بمتطفل، أو دخيل على مواقع مهمة أو بالسطو على الموقع الإلكتروني للشخص الإعتباري ، و خاصة، و أن المجرم لديه يقين من ملاءة الضحية المالية ، و بأنه لن يعاني من كونه معسر. (1)

ب: الأحداث

تختلف التشريعات في تعريفها للأحداث، و ذلك يرجع الى اختلاف تحديد سن التمييز، و سن الرشد بسبب العوامل الثقافية الخاصة بكل مجتمع، و تفرده وتكثر جرائم الإبتزاز الإلكتروني للأحداث و ذلك بالضغط على الحدث بتهديده بنشر صور، أو تسجيل مرئي أو محادثات على مواقع الدردشة ،أو أية مادة عن واقعة من شأنها تحقير المجني عليه عند أهله ، و المجتمع .

---

(1) ممدوح رشيد مشرف الرشيد العنزي ،المرجع السابق،ص200 .

و تستهدف هذه الفئة من أجل مطامع جنسية ،أو تسريب معلومات عن الأهل فيستغل المجرم جهل الطفل في التصرف و يمارس جريمة الابتزاز الالكتروني بعد التسلل الى عقل الطفل الحدث لأن الاحداث هم اكثر الفئات اتصالا بالتكنولوجيا و وسائل التواصل الإجتماعي و أكثر ولعا بها حيث باتت تشكل حيزا كبيرا من يومهم مما يسهل انزلاقهم في الجريمة.

ج: النساء

يعتبر ابتزاز النساء هو النموذج المثالي الأكثر شهرة و انتشارا خاصة إذا كان المبتز رجلا و الضحية امرأة ، و يرجع ذلك أنه غالبا ما يكون تهديد المبتز للمرأة يعتمد على صور ، أو محادثات خادشة بالحياء أو عرضا مرئيا لعلاقة غير شرعية جمعت بين المبتز و ضحيته، أو شخص أخر و قد يكون المبتز قد خطط لجريمته مسبقا، أو قد تزرع الفكرة في رأسه بعد ان وطد أواصر العلاقة مع ضحيته ،و قد تكون الضحية امرأة و من فئة الأحداث و التي غالبا ما تتجاوب مع الإبتزاز خوفا من العار اذا لم ترضخ الى طلبات المبتز. (1)

خاصة اذا كان ما تحرص على إخفاؤه علاقة غير مشروعة ينظر لها الدين ، و المجتمع بالتجريم ، و الرفض، و الاستهجان.

هذا التقسيم حسب نوع الضحية لابد ان يتداخل فيه اكثر من نوع. فقد تكون الضحية امرأة و كونها كذلك لا يعني أن سبب الجريمة دائما هو التهديد بفضح علاقة غير مشروعة فقد تكون الضحية تبتز لأسباب لا علاقة لها بجنسها، أو بسبب علاقة غير مشروعة فقد تهدد المرأة ، و تبتز كونها سيدة أعمال تهدد لفضح أسرار نشاطها التجاري .

---

(1) الحمين عبد العزيز بن حمين بن احمد ، المرجع السابق،ص61.

د: الرجال

قد يقع الرجل ضحية مجني عليه في جريمة الإبتزاز الإلكتروني للعديد من الأسباب فقد يكون ميسور الحال و عرضة للإبتزاز من طرف بعض النساء محترفات ببيع الهوى على المواقع الإلكترونية فتهدده بإذاعة صور، أو مقاطع فيلمية تهدد مركزه، أو بسبب أسرار في مجال عمله، أو عائلته، أو معلومات بنشرها قد تمس في شرفه، و سمعته و مركزه في المجتمع.

ثانيا: بالنظر الى الهدف المرجو من المجني عليه

نتحدث في هذه الجزئية عن الهدف المرجو من عملية الإبتزاز، و الذي يتفرع الى هدف مادي (مالــي) ، هدف نفعي ، هدف انتقامي ، هدف غير اخلاقي (جنسي).

أ: هدف مادي (مالي)

من أهم و أكثر الأهداف التي يرجو المبتز تحقيقها من ارتكابه جريمة الإبتزاز الإلكتروني هي تحقيق منفعة مالية أو عينية ذات قيمة من المجني عليه 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، فيتحقق إبتزاز المال بالطريق المباشر بطلب المبتز من المجني عليه تحويل مبالغ مالية بشكل مستمر، أو لغيره ، أما ابتزاز المال بالطريق غير المباشر فيتحقق عن طريق طلب المبتز من المجني عليه تسديد مبالغ مالية اقترضها من أحد البنوك أو قيامه بدفع أقساط مالية عند الغير و تسديد ديون مستحقة لمصلحة المبتز . (1)

---

(1) المطلق نورة بنت عبد الله بن محمد ،ابتزاز الفتيات احكامه و عقوبته في الفقه الاسلامي ، جامعة الامام محمد بن سعود الاسلامية ، الرياض ،ص 12.

ب: هدف نفعي

يتحقق ذلك بقيام المبتز بتهديد الضحية بإذاعة أسراره و نشرها للملأ و ذلك اذا لم يلبي طلباته أو لم يحقق مصلحة للمبتز، فقد تكون المنفعة المرجوة من الإبتزاز الإلكتروني عمل غير مشروع كتنفيذ سرقة لصالح المبتز، أو ترويج مخدرات، أو يكون عمل مشروع كالتوسط لدى شخص لإتمام عمل، طالما كان العمل ضد إرادة المجني عليه فقد تحققت جريمة الإبتزاز الإلكتروني .

ج: هدف انتقامـــــي

يؤدي الجانب النفسي دورا في عملية الإبتزاز الإلكتروني ، و ذلك باعتبار ان المجني عليه يعيش صراعا داخليا نتيجة أن الجاني سيقوم بتنفيذ تهديداته ضده في أي وقت شاء ما يدفعه الى تلبيه طلبات الجاني تجنبا للفضيحة، حيث يستمتع الجاني بأذية المجني عليه واستماعه لتوسلاته وما يزيد الأمر سوءا أن يقوم الجاني بتصوير المجني عليه، ويطلب منه ذكر أي بيانات تتعلق به كما يكون الدافع لدى الجاني هو الإنتقام من المجني عليه عن طريق الحاق الأذى به وإساءة سمعته بنشر صوره عن طريق شبكة الانترنت. (1)

د: هدف غير أخلاقـــي (جنسي)

تمثل الآداب العامة كل ما يتصل بسلوك الإنسان الحسن ، و تراعي المبادئ الأخلاقية التقليدية المتفق عليها بين عامة الناس ، ووجوب الإلتزام بها في الظاهر، و العلن ، و يعتبر الدافع الجنسي السمة الغالبة في جرائم الإبتزاز باعتباره أكثر أنواع الإبتزاز تحققا عن طريق قيام الجاني بتهديد المجني عليه لفضح أمره ، أو افشاء سر من أسراره، و ينقسم الإبتزاز الجنسي الى قسمين : الإبتزاز الجنسي

(1) ممدوح رشيد مشرف الرشيد العنزي ، المرجع السابق، ص 202 .

الواقعي فيقع هذا النوع من الإبتزاز بقيام المبتز بالحصول على معلومات من الضحية بعد إرتباطه بعلاقة كأن يقوم بالتقاط صور تمس الضحية ، أو يملك مقاطع فيلمية ،أو مقاطع صوتية و بها يصل الأمر الى حصول المبتز على رقم هاتف ولي أمر الضحية و من ثم تهديده بفضح أمره إذا لم يستجب لرغباته الجنسية و الغير أخلاقية.

و مما يدل على وقوع الإبتزاز الجنسي أن كثيرا من قضايا الإبتزاز التي يتم ضبطها ، يضبط معها صور للضحية أو مقاطع مرئية خادشة للحياء بأن يقوم الجاني بتهديد المجني عليه بها مما يجعل إرادة المجني عليه مسلوبة و من ثمّ الإنصياع لطلبات الجاني دون أدنى مقاومة منه.

أما الإبتزاز الجنسي الإلكتروني فيتحقق عن طريق وسائل الإتصال الإكترونية و الأنترنت ، و المبتز في هذا النوع يعتبر مجرما خفيا يسعى للحصول على معلومات تخص الضحية(1)

المطلب الثاني : وسائل الإبتزاز عبر الوسائل الالكترونية و آثاره

إن جريمة الابتزاز هي جريمة قديمة نوعا ما لكنها تطورت لتصبح من أكثر الجرائم خطورة خاصة بعدما اتخذت منحى أكثر خطورة بسبب الثورة التكنولوجية ، و المعلوماتية حيث استغل البعض هذه التكنولوجيا للإعتداء على خصوصية الآخرين و تهديدهم بما يحقرهم في المجتمع حيث يتسلل المجرم إلى تلك الخصوصية ضاربا بعرض الحائط كل الخطوط الحمراء فيقوم باستغلال ما وصل اليه للضغط و التهديد للضحية ، لهذا يرتكب المجرم هذه الجريمة بعد الحصول على ما يمكنه من إبتزاز ضحيته .

فالإبتزاز الإلكتروني هو كل استخدام سيئ صادر من "مجرم" متمرس لوسائل الإتصال التكنولوجية الحديثة لتهديد الضحية بنشر صور، أو مقاطع فيلمية ، أو محادثات ، أو معلومات سرية تخص الضحية عبر الوسائل الإلكترونية خاصة وسائل التواصل الإجتماعي ، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال مشروعة، أو غير مشروعة لصالح المبتز .

(1) ممدوح رشيد مشرف الرشيد العنزي ،المرجع السابق ، ص 201 .

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

- عبر مواقع التواصل الاجتماعي(social media)

- بعض تطبيقات الهواتف الذكية (smart mobile apps)

لإغرائهم بالظهور في أوضاع غير لائقة و تصويرهم دون علمهم ، و تهديدهم بنشر الصور و المقاطع و تهديدهم ماليا و للقيام بما يسبب خطرا على الضحية .(1)

يضع المختصون في مجال مكافحة جرائم الإبتزاز الإلكتروني عدة خصائص، و ملامح لعملية الإبتزاز الإلكتروني فهي :

* نوع من أنواع الجرائم الإلكترونية الحديثة .

* تعد من الجرائم الشائعة للشباب من رواد مواقع التواصل الإجتماعي.

* هي جريمة تستهدف جميع فئات المجتمع.

* يمكن ان تصدر من شخص مبتدئ أو متمرس.

* هي جريمة خطيرة و ارتكابها سهل و متاح لمجتمع الإنترنت .

* هي جريمة غالبا ما يصعب اكتشافها.

* صعوبة تقدير حجم الأضرار النفسية و المادية. (2)

كما يتنوع المجرمون بالإعتماد على عدة معايير مثل الخبرة ، أو علاقتهم بالضحية ، أو من حيث المعرفة التقنية ، أو من حيث كونهم أفراد ، أو ينتمون إلى عصابات منظمة.

فمن حيث الخبرة فقد نجد مجرم متمرس، و مجرم بدائي ، ومن حيث العلاقة بالضحية فقد نجد مجرم معروف ، و معلوم الهوية، و مجرم مجهول الهوية ، من حيث المعرفة التقنية ، لدينا مجرم خبير

(1) مازن سمير الحكيم، حسين فتيخان منسي،المرجع السابق، ص67 .

(2) المرجع نفسه ، ص 71.

يستخدم التكنولوجيا ، و مجرم يستخدم التلاعب بالمشاعر أما من حيث الفئة لدينا مجرم بشكل فردي و مجرم عصابات منظمة

هذا التنوع يؤدي الى تنوع وسائل الإبتزاز الإلكتروني و التالي و تنوع آثاره .

هذا ما سيتم التطرق اليه فالفرع الاول يتناول وسائل الابتزاز الالكتروني و الفرع الثاني الاثار المترتبة عن هذه الجريمة.

الفرع الأول : وسائل الإبتزاز عبر الوسائل الالكترونية

يتم تصيد ضحايا الإبتزاز الإلكتروني بشكل عام عن طريق الحاسب الآلي ، و لواحقه ، و برامجه، و عن طريق شبكة الانترنت (مواقع التواصل الإجتماعي ، أو بعض تطبيقات الهواتف الذكية) .

و من أشهر مواقع التواصل الإجتماعي استخداما لتصيد الضحايا هي :

(facebook , instagram ,twitter ,snapchat , youtube)

ومن أشهر تطبيقات الهواتف الذكية فهي:

(skype , viber , whatsApp)

فضلا عن البريد الإكتروني و أية وسيلة إلكترونية أخرى يمكن من خلالها الوصول الى معلومات سرية أو حساسة عن الضحية.

أولا:الحاسب الآلي

إن الحاسب الآلي (الكمبيوتر) هو جهاز الكتروني قادر على استقبال معطيات المعلومات التي نرغب في إدخالها و تخزينها و كذا تخزين المعلومات الخاصة بالبرامج التطبيقية ، للقيام بمعالجة هذه الأخيرة بسرعة فائقة يستحيل على الإنسان القيام بها و ذلك بعد أن يدخل عليه لإنشاء معلومات مسبقة و برامج متخصصة .

(1) عبد الصبور عبد القوي علي مصري ، الجريمة الالكترونية ،ط 1 ، دار العلوم للنشر و التوزيع ، القاهرة ، 2008، ص22 .

و قد عرف الفقهاء و الدارسون جرائم الكمبيوتر بعدة تعاريف تتمايز و تتعدد تبعا لموضوع العلم المنتمي اليها و تبعا لمعيار التعريف ذاته , فهذه التعريفات تختلف بحسب ما اذا كانت منتمية للقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية أي حق التأليف البرمجي .(1)

يعرف خبراء منظمة التعاون الإقتصادي و التنمية جريمة الكمبيوتر بأنها (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها).

و قد وضع هذا التعريف من قبل مجموعة الخبراء المشار اليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة الإجرام المرتبط بتقنية المعلومات و تبنى هذا التعريف الفقيـــه الألماني (Ulrch Sicher)

و يعتمد هذا التعريف على معيارين :

1- وصف السلوك.

2- اتصال السلوك بالمعالجة الآلية للبيانات ، أو نقلها .

أ: تصنيف الجرائم تبعا لدور الحاسب الآلي في الجريمة

قد يكون هدف الإعتداء بأن يستهدف الفعل لمعطيات المعالجة ، و المخزنة أو المتبادلة بواسطة الكمبيوتر ، و هذا ما يعبر عنه بالمفهوم الضيق (جرائم الكمبيوتر) و قد يكون وسيلة ارتكاب جريمة

(1) عبد الصبور عبد القوي علي مصري ، المرجع السابق، ص23 .

أخرى في إطار (الجرائم المرتبطة بالكمبيوتر) فقد يكون هذا الأخير بيئة لجريمة أو وسطها مخزنا للمادة الإجرامية و في هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور الأول جرائم التخزين ، و يقصد بها تخزين المواد الإجرامية أو المستخدمة في إرتكاب الجريمة أو الناشئة منها .

و الثاني جرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع ، أو غير القانوني ، و الإصطلاح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الأنترنت .

و الحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر ، و الشبكات كبيئة لإرتكاب الجريمة ، و كوسيلة لارتكابها في نفس الوقت ، و هذا التقسيم الشائع و هو تقسيم الجرائم الى جرائم هدف ، و جرائم وسيلة لدى الفقه المصري.أما تقسيمها كجرائم هدف ووسيلة و محتوى فانه الإتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوروبا تحديدا و أفضل ما يعكس هذا التقسيم الإتفاقية الأوروبية لجرائم الكمبيوتر و الأنترنت عام 2001 .

ب: تصنيف الجرائم تبعا لمساسها بالأشخاص و المرتبطة بالحاسب الآلي

نجد هذا التصنيف شائعا في الدراسات و الأبحاث الأمريكية هذا التقسيم يقوم على فكرة الغرض النهائي الذي يستهدفه الإعتداء لكنه ليس تقسيما محددا فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة و الإحتيال و قد تضم كذلك حسب هذا التقسيم: (1)

- أنشطة الاعتداء على الخصوصية computer invasion privacy

(1) عبد الصبور عبد القوي علي مصري ، المرجع السابق، ص24 .

و هي تخرج على مفهوم الجرائم التي تستهدف الأموال فتتصل بجرائم الإختراق و إفشاء كلمة سر الغير و الحيازة غير المشروعة للمعلومات و إساءة استخدام المعلومات و نقل معلومات خاطئة أما الجرائم الماسة بالأشخاص المرتبطة بالكمبيوتر فتضم طائفتين رئيسيتين هما: الجرائم غير الجنسية التي تستهدف الأشخاص و هي تضم التهديد عبر الوسائل المؤمنة و الأحداث المتعمد للضرر العاطفي و الملاحقة عبر الوسائل التقنية و أنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية و بث المعلومات المظللة الزائفة و الانتهاك الشخصي لحرمة الكمبيوتر(الدخول غير المصرح به و طائفة الجرائم الجنسية).(1)

و كمثال على استخدام الكمبيوتر أو، الحاسب الآلي في ارتكاب جريمة الإبتزاز الإلكتروني : فيقوم أحد الموظفين بالدخول على الحاسب الآلي التابع للشركة ثم يقوم بالدخول للمستند الخاص بالمعلومات والبيانات المتعلقة بالموظفين خاصة السرية ثم يقوم بابتزازهم.

ثانيا : برامج الحاسب الآلي.

ورد تعريف لبرامج الحاسب الآلي في نظام مكافحة الجرائم المعلوماتية السعودي بأنه: (مجموعة من الأوامر و البيانات التي تتضمن توجيهات و تطبيقات حين تشغيلها في الحاسب الآلي أو شبكات الحاسب الآلي ، تقوم بأداء الوظيفة المطلوبة).(2)

(1) عبد الصبور عبد القوي على مصري ، الجريمة الالكترونية ،المرجع السابق، ص 26.

(2) أنظر المادة 1 /5 من نظام مكافحة الجرائم المعلوماتية السعودي .

كما جاء في المادة الأولى من القانون الإتحادي الإماراتي في مكافحة جرائم تقنية المعلومات بأنه مجموعة البيانات و التعليمات و الأوامر القابلة للتنفيذ بوسائل تقنية المعلومات ، و المعدة لإنجاز مهمة معينة.(1)

فبرنامج الحاسوب (يعرف أيضا باسم تطبيق أو كيان برمجي) هو عبارة عن مجموعة أو سلسلة من الأوامر تعطى للحاسوب لتنفيذ مهمة معينة في إطار زمني.

ثالثا : الأنترنت

من الطبيعي أن تخلق الأنترنت أنماطا إجرامية مستجدة أو تأثر بالآلية التي ترتكب فيها جرائم الحاسب الآلي ذاتها بعد أن تحقق تشبيك الحواسيب معا في نطاق شبكات محليـة ، و إقليمية ، و عالميـة ، و قد ساد مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود و فواصل في نطاقه بين وسائل الحاسوب و وسائل الإتصال (الشبكات).

و في نطاق هذا المعيار يجري التمييز بين الأفعال التي تستهدف المعلومات في نطاق الكمبيوتر ذاته خلال مرحلة المعالجة و التخزين ، و الإسترجاع ، و بين الشبكات ذاتها ، أو المعلومات المنقولة عبرها و طبعا الأنشطة التي تستهدف مواقع الأنترنت ، و خادمها من نظم الكمبيوتر العملاقة أو تستهدف تطبيقات و استخدامات و حلول الأنترنت، و ما نشأ في بيئتها من أعمال الكترونية و خدمات الكترونية .

عرفت الجريمة بصفة عامة على:(أنها كل فعل غير مشروع صادر عن إرادة اثمة يقرر له القانون عقوبة أو تدبيرا احترازيا، و تعتمد الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت على المعلومة بشكل رئيسي ، هذا الذي أدي الى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم).(2)

(1) أنظر المادة الاولى من القانون الاتحادي الاماراتي لمكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012 .

(2) صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة الماجيستير في القانون ، كلية الحقوق و العلوم السياسية ، مدرسة الدكتوراه " القانون الاساسي و العلوم السياسية " جامعة مولود معمري ، تيزي وزو ، تاريخ المناقشة 2013/03/06، ص 08 .

وقد عرف بعض الفقه الجريمة المرتكبة عبر الأنترنت :(هي نشاط إجرامي تستخدم فيه التقنية الإلكترونية والحاسوب الآلي الرقمي وشبكة الأنترنت، بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف) (1).

هذه الجرائم المستحدثة التي اتى بها التطور العلمي في مجال الإتصالات، فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي حيث ان الجريمة المرتكبة عبر الأنترنت هي أسرع تطورا من التشريعات نظرا للتطور التكنولوجي الهائل ، والمتسارع لشبكه الأنترنت كما تتم عن طريق مجرم يوظف خبراته في التعامل مع الشبكة لكي يقوم بالتجسس والتغرير بالقصر، واختراق خصوصيات الغير دون عنف أو أثر خارجي مادي.

تتم عملية الإبتزاز الإلكتروني كصورة من صور الجرائم المرتكبة عن طريق الأنترنت بواسطة البريد الإكتروني ، مواقع التواصل الإجتماعي و الهواتف الذكيه وملحقاتها وبرامجها.

أ- البريد الإلكتروني.

عرف جانب من الفقه البريد الإلكتروني بأنه طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات ، ويعرف جانب آخر من الفقه بأنه مستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم شرط تأمين هذا الصندوق بعدم الدخول إليه وذلك بطرق التامين المعروفة ومنها التشفير وكلمة المرور وغيرها من تقنيات الحماية الفنية.

ويعرفه جانب آخر من الفقه بأنه عبارة عن خط مفتوح على أنحاء 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 الارضية).

تعريف البريد الإلكتروني قانونا : فقد عربه القانون الإمريكي المتعلق بخصوصية الإتصالات الإلكترونية الصادر عام 1986 اذا جاء فيه : (البريد الإلكتروني وسيلة يتم بواسطتها نقل المراسلات الخاصة عبر

---

(1) صغير يوسف ، المرجع السابق، ص 09 .

شبكة خطوط تليفونية خاصة ،أو عامة وغالبا ما يتم كتابة الرسائل على جهاز الكمبيوتر ثم يتم إرسالها إلكترونيا الى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه إذ يتم إرسالها عبر نظام خطوط التليفون الى الكمبيوتر المرسل اليه).

أما المشرع الفرنسي في القانون الخاص بالثقة في الإقتصاد الرقمي الصادر في يوليو 2004، اذ جاء فيه : (البريد الالكتروني هو كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات ويتم إرسالها عبر شبكه إتصالات عامه وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الصرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها).

ويمكن تعريفه على أنه نظام التراسل باستخدام الحاسبات أما في جميع الدول العربية حتى التي أصدرت قوانين تواكب فيها التطور الحاصل في مجال التقنيات ، لم تعرف البريد الالكتروني.

من خلال التعريفات السابقة يتضح أن القوانين التي عرفت البريد الالكتروني لم تختلف في مضمون هذا الآخير، إنما الإختلاف بالصياغه فقط أما التشريعات العربية لا تزال بعيدة كل البعد عن معالجة التطور الحاصل في مجال التقنية بدليل أن كل القوانين العربية لم تعرف البريد الالكتروني. (2)

من خلال ما سبق ذكره فإن البريد الإلكتروني يحتاج لحماية جزائية نظرا لعدة دواعي أهمها : حمايه الحقوق، وخاصة الحق في الخصوصية التي بها وجهان متلازمان وهما حرية الحياة الخاصة ،وسرية الحياة الخاصة. (3)

1: قصور الحماية التقنية

فعلى الرغم من انتشار الكثير من الصور التقنيه للبريد الإلكتروني (التشفير، كلمه المرور) لكن ذلك لم يمنع قراصنة المعلومات والعابثين بشبكة الانترنت من ارتكاب جرائم بواسطة البريد الإلكتروني.

(1) عدي جابر هادي ، الحماية الجزائية للبريد الالكتروني , دراسة مقارنة ، بحث مقدم بمجلة رسالة الحقوق ، السنة الثانية ، العدد الثالث ، كلية القانون جامعة القادسية 2010 ، ص156 .

(2) المرجع نفسه.

(3) نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط2 ، دار الثقافة للنشر و التوزيع ، عمان، الاردن ،2010 ، ص 167.

2 : تشجيع إقامة حكومة إلكترونية

حيث تعرف الحكومة الإلكترونية على أنها:(البيئة التي تتحقق فيها خدمات المواطنين واستعلاماتهم وتحقق فيها الأنشطة الحكومية للدائرة المعنية من دوائر الحكومة بذاتها أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات، والإتصال عن بعد).(1)

ومن أهم الصعوبات التي تواجه الحماية الجزائية للبريد الإلكتروني نميز بين نوعين :

3 : الصعوبات التقنية

حيث يحدث الإعتداء بواسطه البريد الإلكتروني دون علم الضحية مما جعل من الصعوبة بمكان وصول الجرائم الى علم السلطات خوفا على السمعة.

وفي بعض الأحيان تعرف الجريمة ولكن الجاني مجهول ،لأنه لا يستخدم اسمه الحقيقي بل يستخدم اسما مستعارا عند إرسال الرسالة في البريد الإلكتروني، كما لا يستخدم حاسوبه الخاص وانما يرتاد مقاهي الأنترنت ، وقد تتوفر الخبرة التقنية ومع ذلك لا يمكن التوصل للجاني.

4 : الصعوبات القانونية

يمكن إجمال الصعوبات القانونية التي تواجه الحماية الجزائية للبريد الإلكتروني في النقاط التالية:

قد يكون الجاني من دولة والمجني عليه من دولة أخرى كذلك مسألة تنازع القوانين الجزائية وكذلك إختلاف الأحكام بين قوانين الدول .

فقد يكون الفعل المجرم في دولة وغير مجرما في دولة أخرى.

(1) عدي جابر هادي ، المرجع السابق ، ص159 .

ب: مواقع التواصل الإجتماعي

لقد تعددت أوجه إستخدام شبكة الأنترنت وتنوعت مجالاتها حتى أصبحت جزءا من حياتنا اليومية وهي من أكثر الوسائل المستعملة للتعارف بين الناس عن طريق مواقع التواصل الإجتماعي الذي فتحت أبواب الحوار على مصراعيها مما جعل البعض يعتقد بأنها فضاءا متاحا ومنطقه فوق القانون.

فالواقع الإلكتروني والعالم الإفتراضي أبرز العديد من التجاوزات عن طريق الإستخدام الغير مشروع لمواقع التواصل الإجتماعي فتحولت من فضاءات للتعارف والتقارب الى مناظر للدعوة لبعض الأفعال الماسة بأمن الدولة واستقرارها ، أو شرف الأشخاص واعتبارهم ،أو بالنظام العام والآداب العامة.

إن تشغيل شبكة الأنترنت يتطلب مجموعة من الاشخاص القائمين عليها يعملون على تخزين ونقل وعرض المعلومات فمن يقوم بهذه الأعمال هم من يطلق عليهم الوسطاء في خدمة الأنترنت فهم من يمكن المستخدم من دخول شبكة الأنترنت والتجول فيها والإطلاع على ما يريد عن طريق نقل الخدمة أو تمكينه من الوصول إلى المواقع بالاضافة إلى انتاج المعلومات وتوريدها وتخزينها .

وهو ما يتم عند محاولة شخص الولوج الى الفيسبوك، أو تويتر أو، انستغرام أو، واتساب ،وغيرها من مواقع التواصل الإجتماعي حيث تعتمد في المقام الأول على النظام المعلوماتي عبر شبكة الأنترنت أو أي وسيلة إلكترونية أخرى حيث يعمل على هذا النظام العديد من الأشخاص، أو الوسطاء ودون هؤلاء لا يمكن لمواقع التواصل أن تعمل ومن هنا تشار إليهم أصابع الإتهام عند حصول جريمة في هذا العالم الإفتراضي. (1)

فقد عرف المشرع الفرنسي التواصل الإجتماعي عبر شبكه الإنترنت في المادة الرابعة من القانون رقم 575-2004 الصادر بتاريخ 21 يونيو 2004 بأنه بروتوكول إتصال مفتوح أو ربط بيانات وتبادلها بأي شكل يصل الى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية.(2)

---

(1) بوقرين عبد الحليم ، المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي ، دراسة مقارنة بحث مقدم في مجلة جامعة الشارقة ، دورية علمية محكمة ،المجلد 16 ، العدد 01 ، يونيو ،2016، ص373 .

(2) دنيا عبد العزيز فهمي ، المسؤولية الناشئة عن اساءة استخدام مواقع التواصل الاجتماعي ، بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق، جامعة طنطا، تحت عنوان القانون و الاعلام ، 23-24 افريل 2017، ص 05 .

وقد عرف القانـــــون الاماراتـــي رقم 05 لسنة 2012 (الموقع الإلكتروني هو مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الإجتماعي والصفحات الشخصية والمدونات). (1)

أما مواقع التواصل الإجتماعي فيمكن تعريفها على أنها :(تلك الوسائل التقنية الحديثة التي يستخدمها الأشخاص في ما بينهم لتحقيق التواصل الإجتماعي المشاع عبر شبكة الأنترنت كالفيسبوك، تويتر ، اليوتيوب وغيره...). (2)

كيف يتم تصيد الضحايا عبر مواقع التواصل الاجتماعي؟

حيث يتم جذب الضحايا من خلال تحريض الفرد ببساطة على النقر على رابط من شأنه أن يثير إهتمام أي شخص فيطلب منه معلومات عن الهوية وبعض المعلومات الشخصية كرقم بطاقة الائتمان ، أو رقم الضمان الاجتماعي وقد يظن البعض أنه من السهل اكتشاف أن هذه مجرد عملية احتيال ولكن للأسف حتى أكثر مستخدمي التواصل الإجتماعي ذكاءا قد وقعوا ضحايا لهذه الإحتيالات نظرا لتنوع الوسائل والأساليب التي يستخدمها المجرمون ولجوئهم لأساليب غير مشروعة للحصول على المعلومات.

وقد أدت مجموعة البيانات الضخمة التي يملكها فيسبوك عن المستخدمين والتي لم يتم عرضها إطلاقا عليهم الى إنتهاك خصوصيتهم كما تتوفر مواقع بحث عن الصور المقابلة .

خدمة تتيح للمستخدمين البحث عن صور معينة والعثور على نسخ مماثلة في مكان آخر وقد تم استغلال هذه الأدوات من قبل مجرمو الأنترنت للعثور على حسابات وسائل التواصل الإجتماعي.

ويرتكب مجرموا الأنترنت جريمة الإبتزاز الإلكتروني فيجعل من مواقع التواصل الإجتماعي أداة و وسيلة للوصول الى غايتهم باستدراج ضحاياهم فيستجيب الضحايا للإبتزاز خوفا من التشهير، حيث يعد الإبتزاز

عن طريق مواقع التواصل الإجتماعي جريمة تتم من خلال التهديد بالكشف عن بيانات محرجة أو ضارة عن شخص في الجمهور، أو العائلة ، أو الزملاء ما لم يشتر هذا الأخير صمت المبتز في بعض الدول يعتبر الإبتزاز الإلكتروني عبر الفيسبوك التهديد الرئيسي المرتبط بانتهاك الخصوصية.

---

(1) أنظر المادة الاولى ،المرسوم رقم 05 لسنة 2012، الاماراتي.

(2) أحمد حسن عبد العليم حسن الخطيب ، الجرائم المعلوماتية الواقعة عبر مواقع التواصل الإجتماعي ، مقال منشور بمجلة الدراسات الافريقية و حوض النيل ،مجلة دورية محكمة تصدر عن المركز الديمقراطي العربي ، برلين، المانيا، المجلد 02 ، العدد 06 ، اكتوبر 2019، ص 113 .

كما أن ضبط الخصوصية على الحسابات الإلكترونية لا يعني أن الحساب آمن وخاص كما أن كثيرا من المستخدمين لا يقومون بتعيين إعدادات الخصوصية لحفظ خصوصية حساباتهم لصعوبة القيام بذلك أو ليس لديهم فكرة كافية عن وجود هذه الإعدادات ونظرا لكون التواصل الإجتماعي أصبح جزءا مهما من حياتنا اليومية ، فإن الافراد يجدون أن هذه التقنية وسيلة جذابة لارتكاب الجرائم الإلكترونية خاصة جريمة الإبتزاز الإلكتروني فتسمع خاصة عدم الكشف عن الهوية الحقيقية للشخص عبر مواقع التواصل الإجتماعي فرصة استغلال لهوية شخص آخر فيستغل المجرم هذه الثغرات الأمنية لسرقة بيانات اعتماد المستخدم والتي بدورها يمكن استخدامها لخرق البنية الأساسية لشبكة الشركة.

وتتعدد بذلك الأفعال المجرمة من طرف أصحاب مواقع التواصل الإجتماعي ومن أكثر الجرائم ارتكابا تلك الماسة بالأشخاص والخصوصية وتعد جريمة الإبتزاز الإلكتروني أكثر الجرائم ارتكابا حيث تتزايد معدلاتها بشكل يدعو للقلق حيث تتزايد عمليات الإبتزاز الإلكتروني مع عدد مستخدمي وسائل التواصل الإجتماعي والتسارع المشهود في إعداد برامج المحادثات المختلفة. (1)

رابعا: الهاتف النقـــــال

إن من أبرز مظاهر الجريمة الإلكترونية في عصرنا الحالي الجريمة الإلكترونية المرتكبة بواسطة الهاتف النقال والتي لا تقل خطورة عن الجرائم المرتكبة بواسطة الحاسوب.

و انطلاقا من هذه الخطورة عملت بعض التشريعات الغربية على وضع قوانين تجرم الأفعال التي توصف بأنها جرائم ترتكب بواسطة الهاتف النقال وذلك من خلال إضافة مواد عقابية تجرم هذا النوع من الجرائم على غرار التشريع الفرنسي ، الانجليزي والأمريكي لكن أغلب التشريعات العربية لم تقم بتجريم توظيف الهاتف النقال في ارتكاب جريمة باستثناء المشرع الإماراتي والمنظم السعودي.

بينما المشرع الجزائري لم يقوم بتجريم الافعال المرتكبة بواسطة الهاتف النقال، إلا في جرائم محددة تمس الإساءة لرسول الله ﷺ ،أو المعلوم من الدين ،أو الإساءة لشخص رئيس الجمهورية.

(1) حفيظة سليمان احمد البراشدية ، الفايسبوك و الجرائم الالكترونية في عمان : هل هناك علاقة ؟ مقال بمجلة دراسات المعلومات و التكنولوجيا ، جمعية المكتبات المتخصصة ، فرع الخليج العربي، دار جامعة حمد بن خليفة للنشر ، 30 سبتمبر 2019 ، ص 04 .

وقد واكب الجانب الإجرائي هذا التطور من خلال الإستعانة بالهاتف النقال أو غيره من الوسائط الإلكترونية الأخرى في الكشف عن الجرائم ومرتكبها وهو ما يتجلى في قانون الإجراءات الجزائية الجزائري والقانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال والذي حدد فيه المشرع جميع الإجراءات التي يجب على السلطات التحري والتحقيق والعمل بها في جريمة ذات طابع الكتروني كما أن المشرع الجزائري بموجب هذا القانون قد عمل على تأسيس هيئه وطنية لمكافحة الجريمة الإلكترونية.

يعتبر الهاتف النقال(وسيلة إتصال لاسلكيه تعمل من خلال شبكة من أبراج البث المباشر على تغطية مساحات معينة وتترابط في ما بينها بواسطة خطوط ثابته وأقمار صناعية وهو ما يعرف بشبكة التغطية)

ومع تطور أجهزة الهاتف الخلوي أصبحت الأجهزة أكثر من مجرد وسيلة للإتصال الصوتي حيث أصبحت تستخدم كأجهزة كمبيوتر وتصفح الأنترنت، وللأجهزة الحديثة نفس خصائص ودقة وضوح الكاميرا الرقمية.

يتكون الهاتف النقال من مكونات مادية تنقسم بدورها إلى مكونات مادية خارجية وهي الأدوات التي يحتاجها الهاتف النقال من أجل التشغيل كدائرة الصوت ودائرة الذاكرة التي تختلف حسب نوع الجهاز وجيله أما الأجزاء غير المادية للهاتف النقال فهي تمثل الكيان المنطقي الذي يشغل الجهاز ولا يختلف عن نظيره من الحاسوب حيث يظهر في شكل أنظمة وضعت خصيصا لتشغيل الهاتف النقال أو أنظمة تم تصميمها للحاسوب ولديها قابلية التشغيل بواسطة الهواتف النقالة الذكية. (1)

أما برامج الهاتف النقال مجموعة من التعليمات التي تسمح بمعاينتها على دعامة مقروءة من قبل الآلة لبيان أو أداء أو إنجاز وظيفة مهمة أو نتيجة معينة صادرة عن آلة قادرة على مناقشة المعلومات. (2)

وتنقسم برامج التشغيل للحاسب الآلي أو الهواتف النقالة الذكية إلى برامج أساسية فيظهر في شكل برامج تطبيقية تهدف للقيام بمهام محددة ومن أمثلة على ذلك الماسنجر، الفيسبوك.-

(1) التوجي محمد ،الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال ،رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي ، كلية الحقوق و العلوم السياسية جامعة احمد دراية ، ادرار ،2019 ، ص 03 .

(2) المرجع نفسه، ص 12 .

أما البرامج غير الأساسية وهي المعلومات التي تتميز بها الهواتف الذكية وتظهر في شكل وسيط أو أداة تغطي خدمة معينة كرسائل البريد الالكتروني و البريد النصي و الصور الرقمية ومقاطع الفيديو المخزنة قد تتعلق المعلومات بشخص المستخدم أو تتعلق بوظيفته، وقد تتضمن أسرارا قد تشكل خطرا على المصلحة العامة أو تهديدا لها.

تكون هذه المعلومات محلا لجريمة الإبتزاز الإلكتروني وذلك عندما يقوم المجرم الإلكتروني باستخدام الأنترنت في برامج التواصل الإجتماعي أو المعلومات الموجودة بالهاتف الموجه للتجسس على الآخرين وانتهاك حرمة حياتهم الخاصة أو عن طريق الإستخدام غير المشروع لملحقات الهاتف الذكي : الكاميرا أو البلوتوث أو الآت التسجيل.

الملاحظ خلو نظام مكافحة جرائم المعلوماتية السعودي من تعريف الهاتف الذكي(النقال) باعتباره من أحد أهم الوسائل التي تستخدم في الجريمة الإلكترونية لأنه متاحا للجميع مما قد يسيئ استخدامه للصغار لجهلهم للأنظمة ، لكن المنظم السعودي استدرك بعدم ذكره للتعريف اكتفاءه بذكر العقوبة المقررة على الجاني عندما استخدام الهاتف فقد ذكر في الفترة الرابعة من المادة الثالثة: يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد عن 500 الف ريال او بإحدى العقوبتين كل شخص يرتكب أيا من هذه الجرائم المعلوماتية الآتية... (1)

4-المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها. (2)

كما لم يعرف القانون الإماراتي الهاتف النقال في نصوص مواده العقابية ولعل هذا النقص يرجع إلى الشعور ببداهة التعريف الخاص بالهاتف النقال أين تعتبر جرائم الاعتداء على الخصوصية من بين أكثر الجرائم التي ترتكب بواسطة الهاتف النقال وذلك لسهولة إرتكابها فضلا على إحجام معظم ممن يكونون ضحايا هذا النوع من الجرائم عن الإبلاغ عنها.

(1) أنظر المادة 3 فقرة 4 نظام مكافحة الجرائم المعلوماتية السعودي، رقم 79 الصادر سنة 1428 هجري .

(2) محمد بن عبد االمحسن بن شلهوب ، المرجع السابق، ص 59 .

الفرع الثاني : آثار الإبتزاز عبر الوسائل الإلكترونية

إن لجريمة الإبتزاز الإلكتروني آثار خطيرة و نتناول هذه الآثار على النحو التالي:

أولا: الآثار الاجتماعية

إن ظاهرة الإبتزاز الإلكتروني تشكل خطرا جديا على المجتمع والعائله حيث أن أغلب ضحاياها نساء ، حيث سببت هذه الظاهرة إنفصالهم عن أزواجهم كما ان أغلب الفتيات اللائي تعرضن للإبتزاز يتخوفن من تقديم شكوى في المحاكم خوفا من المشاكل الناجمة كان يحجم الناس من التقدم للزواج منهن خاصة المحيط القريب منهن لمعرفة هذا المحيط بقضياياهن . فقد ترفض الفتاة نفسها الزواج خوفا من أن يعرف الزوج تاريخها السابق ،وقد يؤدي الإبتزاز إلى هدم بيت الزوجية بالطلاق فهو أثر مباشر للإبتزاز .

وقد يتم اغتصاب الفتاة بالانصياع الى 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.

كما يهدد اإابتزاز المستقبل الإجتماعي للضحيه حيث تظل آثاره تلاحقها في المجتمع الذي سمع وشاهد فضيحتها بالصوت والصورة. (1)

ثانيا: الآثار النفسية

نتيجة التزايد المقلق لظاهرة الإبتزاز الإلكتروني أصبح هناك من يعاني بصمت وذلك خوفا من التشهير والفضيحة وتبعاتها.

فالضحية قد يكون عرضها للإبتزاز الالكتروني في أي وقت ومن قبل مجموعة من الأشخاص ومما يزيد من الأثر النفسي.(2)

---

(1) ابتسام كريم و آخرون بحث بعنوان : انتشار ضاهرة الابتزاز الالكتروني في المجتمع العراقي ، استطلاع اراء عينة من المجتمع العراقي حول التعامل معى هذه الضاهرة المؤتمر العلمي الدولي الاول ، نقابة الاكاديميين العراقيين ، مركز التطور الاستراتيجي الاكاديمي جامعة دهوك ، العراق 11-12 فيفري، 2019 ، ص 165.

(2) المرجع نفسه، ص 166 .

ومما يزيد من الآثار النفسية على الضحية عدم قدرة هذه الأخيرة على طلب المساعدة بسبب الإحراج أو الجهل بأساليب الوقاية أو أن هناك من يستطيع تقديم يد العون له والتخفيف عليه.

فعند فئة المراهقين والقصر،لا يفهم ذويهم مشكلتهم فقد يميلون للوحدة والعزلة كما أنهم يتغيبون عن المدرسة والعمل ، وإهمال واجباتهم الدراسية أو العملية كما قد ينتابهم القلق والحزن والكآبة والتوتر والعدوانية تجاه الأخرين وتتفاقم هذه الأعراض مع مرور الوقت لتصل الى الإضطراب والإكتئاب في صورة بكاء وغضب ولوم الذات وقد تصل للرغبة في الإنتحار وكفى به خطرا يستوجب الوقوف عنده .

ومن أبرز العلامات الدالة على تعرض الشخص للإبتزاز الاإكتروني هو التغيير بسلوك هذا الأخير على الشبكات الإلكترونية ممثلا بقله نشاطه أو انعدامه خوفا من التعرف الى المزيد من المعتدين.

كما قد يتحول الضحية في جريمة الإبتزاز الإلكتروني الجنسي من ضحية الى مجرم جنسي آخر ومجرم عادي نتيجة لما حدث له او رد فعل ما أصابه .

ثالثا: الآثار الأمنية

يهدد الإبتزاز الأمن في المجتمع حيث يؤدي إلى تفشي الفساد وانهيار القيم والأخلاق في المجتمع فلا يأمن الفرد على عرضه وشرفه، كما أن جريمة الإبتزاز اذا كان الغرض منها مالي سيؤدي ذلك الى زيادة جرائم النصب والسرقة خاصة إذا كان الضحية معسر ولا يملك ما يقدمه للمبتز لقاء صمته. (1)

أما إذا كان الهدف منه جنسي غير أخلاقي فهذه الجريمة لا تكون منفردة بل تصاحبها جرائم اخرى كالاغتصاب ، السكر ، الزنا ، السرقة كما قد يؤدي الى جرائم القتل حيث يقوم المبتز بقتل ضحيته بعد ارتكاب الفاحشة وتصويره لها، فاذا ما تم تداول صور الجريمة يقوم أهل الضحيه بقتل المبتز المعتدي انتقاما منه خاصة في بعض المجتمعات التي لا ترى غسل العار إلا بسفك الدم.(2)

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق، ص58 .

(2) المرجع نفسه، ص59 .

المبحث الثاني : تجريم الإبتزاز عبر الوسائل الإلكترونية

إن أغلب القوانين العربية والعالمية تعاقب على جنح التهديد بالإبتزاز وكونها من الجرائم الخطيرة التي تلحق الكثير من الضرر للشخص في سمعته ونفسيته وحياته الخاصة لذا فان الكثير من القوانين تنظر الى جريمة الإبتزاز كجريمة مصنفة ضمن الجرائم الخطيرة ، والتي تحدثت معظم القوانين عنها بصراحة وعالجت أغلب وقائعها وفرضت عقوبات على المجرم تصل إلى الحبس لسنوات وغرامات مالية ، حيث تتعامل معها على الأغلب الأجهزة الشرطية في الـدول بكل سرية وبكل دقة وحرفية على أيدي أناس مدربين سواء خبراء في عالم التقنيات أو، خبراء في القبض على المجرم المتخفي.

ولقد أولت معظم القوانين أهمية و مكانة بالغة للخصوصية الشخصية للأفراد أن لا يمسها خدش يطيح بها على المستوى الذي يتمتع به صاحبها ونتج عن ذلك بان تدخل القانون وفرض حمايته الجزائية على هذه المكانة الأدبية واعتبر الإعتداء عليها جريمة تصيب مركز المجني عليه حيث أن الجانب الأخلاقي هو أخطر ما قد تستهدفه الجريمة الإلكترونية وخاصة في المجتمعات العربية التي طالما اعتزت بمبادئها وقيمها الفاضلة فجريمة من هذا النوع كفيلة بأن تقضي على حياة الفرد، أو تفقد عائلته كرامتها وحتى انتمائها للمجتمع ، فالكثير منها ألصقت بها وصمة عار إذا ما تم نشر تلك الصور والبيانات الشخصية والتي لا يوافق على عرض هذه عموم الناس، ولقد تناولنا في هذا المبحث تجريم الإبتزاز الإلكتروني من خلال مطلبين: أولهما هو أركان جريمة الإبتزاز الإلكتروني ،و الثاني يتناول عقوبة جريمة الإبتزاز الإلكتروني.

المطلب الأول : أركان جريمة الإبتزاز عبر الوسائل الإلكترونية

يعتبر الإبتزاز أسلوب من أساليب الضغط يلجأ إليه المبتز للضغط على الضحية وإجباره على الإذعان لمطالبه مستغلا عدة طرق منها التهديد بالمساس بحرمة حياته الخاصة بالتشهير به ، ولكي نكون أمام جريمة إبتزاز إلكتروني لابد من توافر أركان الجريمة المتمثلة في الركن الشرعي ، الذي هو عبارة عن وجود نص قانوني يحدد الفعل المجرم والجزاء الجنائي الذي بوجوده ينقل الفعل من دائرة الإباحة الى دائرة التجريم.

اما الركن المادي فهو كل ما يدخل في كيان جريمة الإبتزاز الإلكتروني وتكون له طبيعة مادية ملموسة سواء كان فعلا أو امتناعا حيث أن للركن المادي مظهر خارجي يعرف من خلاله اما الركن المعنوي فهو داخلي كامن في نفسية الجاني ومن هذا المنطلق يمكن ان نقسم هذا المطلب الى ثلاثة فروع كما يلي :

الفرع الأول : الركن الشرعي لجريمة الإبتزاز عبر الوسائل الإلكترونية

الركن الشرعي في الجريمة هو نص التجريم و العقاب فهو النص الذي نستند اليه لتجريم فعل معين و العقاب عليه ، و أن يكون هذا النص ساريا من حيث الزمان والمكان والأشخاص على مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة: (لا جريمة ولا جزاء ولا إجراء ولا تنفيذ للعقوبة إلا بقانون).

تطبيقا لمبدأ الشرعية فبالرجوع لبعض القوانين العربية نجد أنها قد نصت على هذه الجريمة وحددت العقوبات اللازمة لها أما في البعض الآخر من الدول العربية فلم ينص المشرع صراحة على تجريم الإبتزاز الإلكتروني فلا وجود لقواعد قانونية تخص تلك الجرائم بالذات إلا أن القضاء حاول جاهدا معالجة هذه الجرائم وفق تكييفها القانوني من خلال تطوير القواعد القانونية الموجودة في قوانينها العقابية.

نظام مكافحة الجرائم المعلوماتية السعودية ، يحتوي على نص تجريم الإبتزاز الإلكتروني فقد نص في المادة الثالثة منه على أنه يعاقب بالسجن مده لا تزيد على السنة و غرامة لا تزيد عن 500 ألف ريال او باحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية الاتية : (1)

1- الدخول غير المشروع لتهديد شخص أو ابتزازه بحمله على القيام بفعل، أو الإمتناع عنه حتى ولو كان مشروعا .

2- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقاله المزودة بالكاميرا أو ما في حكمها

---

(1) أنظر المادة 3 نظام مكافحة الجرائم المعلوماتية السعودي.

3- التشهير بالآخرين أو إلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة). (1)

وتعد جريمة الإبتزاز من الجرائم الكبيرة في المملكة العربية السعودية حيث نص المنظم على أن التوقيف منها يكون وجوبا وذلك كما في القرار الوزاري رقم 1900 لسنة 1428هجري ،حيث نص على الجرائم الكبيرة التي تستوجب التوقيف وقد حصرت بخمسة عشرة جريمة ، ونص في الفقرة الرابعة عشر على جريمة انتهاك الأعراض بالتصوير والنشر او التهديد بالنشر . (2)

كما أوضحت المذكرة الايضاحية للقرار الوزاري أن الإبتزاز يتم عن طريق محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه بالتهديد بفضح سر من أسرار الممبتز من شخص أو اشخاص أو مؤسسات كما يدخل في انتهاك الأعراض بالتصوير والحصول على الصور محل الجريمة باي وسيلة كانت كما عاقبه المنظم السعودي الشخص المبتز بعقوبة السجن والغرامة المالية. (3)

كما نصت المادة الثالثة عشر على أنه : (يجوز الحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام أو الأموال المحصلة منها) .

مما سبق يتبين أن المنظم السعودي قد جرم الإبتزاز وجعله من الجرائم الكبيرة المستحقة التوقيف بغض النظر عن الوسيلة المستخدمة في جريمة الإبتزاز بالوسائل التقنية فقد نص المنظم على العقوبة كما جاء في نظام مكافحة جرائم المعلوماتية. (4)

أما في القانون العماني فقد جرم الإبتزاز وعوقب عليه في المادتين 16 و 18 من قانون مكافحة جرائم تقنية المعلومات ، وبالإطلاع على قانون مكافحة جرائم تقنية المعلومات الإماراتي تبين انه نص على تجريم الإبتزاز الذي تم عن طريق تقنية المعلومات حيث تنص المادة 16 منه يعاقب بالحبس مدة لا تزيد عن سنتين والغرامة التي لا تقل عن 250 الف درهم ولا تتجاوز 500 ألف درهم أو إحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر بحمله على القيام بفعل والامتناع عنه وذلك باستخدام شبكة

(1) محمود بن المحسن بن شلهوب ، المرجع السابق ، ص66.

(2) المرجع نفسه .

(3) ممدوح رشيد مشرف العنزي ، المرجع السابق ، ص 207 .

(4) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص 67.

المعلوماتية أو وسيلة تقنية المعلومات وتكون العقوبة بالسجن مدة لا تزيد على 10 سنوات اذا كان التهديد بارتكاب جناية او باسناد أمور خادشة للشرف والاعتبار. (1)

وقد كان معيار المجتمع الإماراتي في الجرائم التي توجب الحبس الإحتياطي معيارا مرنا ،فلم ينص صراحة على اعتبار الجرائم الالكترونية ومنها جريمة الإبتزاز الإلكتروني من الجرائم التي يجب فيها الحبس الإحتياطي حيث لم يحدث قانون الاجراءات الجزائية الإتحادي مبررا للحبس الإحتياطي بل اكتفت المادة 106 على أنه : (يجوز لعضو النيابة العامة ... أن يصدر أمرا بحبسه احتياطيا إذا كانت الدلائل كافية ...) ومع عدم تصريح المشرع الإماراتي بالجرائم التي يجب الحبس الإحتياطي فيها إلا أنه من أكثر المسوغات للحبس الإحتياطي تكمن في منع المتهم من الهرب ومنع المتهم من التأثير في سير التحقيق كما أنه لا يجوز إصدار أمر الحبس الاحتياطي إذا كانت الجريمة جنحة معاقب عليها بالغرامة فقط أو إذا كان المتهم حدثا ويستفيد من كل ذلك جواز الحبس الإحتياطي في جرائم الإبتزاز الإلكتروني وإن لم ينص المشرع الإماراتي على ذلك صراحة.(2)

للتصدي لهذه الجريمة الدخيلة والمهددة للمجتمع فقد أفرد لها المشرع الكويتي حماية وذلك بنص المادة 03 من القانون رقم 63 لسنة 2015 المتعلق بمكافحة جرائم تقنية المعلومات (يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاث الاف دينار ولا تتجاوز عشرة الاف دينار أو، بإحدى هاتين العقوبتين كل من ... استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بعمل أو الإمتناع عنه).

فاذا كان التهديد في ارتكاب جناية أو بما يمس بكرامة الأشخاص ،أو الشرف، أو الاعتبار والسمعة كانت العقوبة الحبس مدة لا تتجاوز خمس سنوات والغرامه التي لا تقل عن 5000 دينار أو باحدى هاتين العقوبتين. (3)

(1) أنظر المادة (16) من القانون الإتحادي لمكافحة جرائم تقنيية المعلومات الإماراتي .

(2) فتيحة محمد قوراري ، غنام محمد غنام ، المبادئ العامة في قانون الاجراءات الجزائية الاتحادي لدولة الامارات العربية المتحدة (معلقا عليه باحكام المحكمة الاتحادية العليا و محكمة تمييز) وفقا لاخر التعديلات بالقانون رقم 29 لسنة 2005 ، ط 3 ، الافاق المشرقة ناشرون ،الاردن ، 2013 ، ص 234 –235 .

(3) أنظر المادة (4) من القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي .

وقد جرم القانون المصري الأبتزاز حيث نصت المادة 326 من قانون العقوبات المصري على أن: (كل من حصل بالتهديد على إعطائه مبلغا من النقود أو ،أي شيء آخر يعاقب بالحبس ويعاقب الشروع في ذلك بالحبس مده لا تتجاوز سنتين).

كما نصت المادة237 على أن كل من هدد غيره كتابة بارتكاب جريمة ضد النفس ،أو بإفشاء أمور، أو نسبه أمور مخدشة بالشرف ، وكان التهديد مصحوبا بطلب أو تكليف بأمر يعاقب بالسجن ، ويعاقب بالحبس إذا لم يكن التهديد مصحوبا بطلب ،أو بتكليف بأمر وكل من هدد غيره شفهيا أو بواسطة شخص آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد عن سنتين، أو بغرامة تزيد عن 500 جنيه سواء كان التهديد مصحوبا بأمر أم لا ، وكل تهديد سواء كان بالكتابة أو شفهي أو بواسطه شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مده لا تزيد على ستة أشهر أو بغرامة لا تزيد على 200 جنيه. (1)

مما سبق يتظح اتفاق القوانين في كل من المملكة العربية السعودية ، عمان ،الإمارات العربية المتحدة ، الكويت ومصر على تجريم الإبتزاز الإلكتروني وايجاب العقاب على مرتكبيه بينما نجد أن بعض القوانين العربية كالعراقي والجزائري لم تتناولها التشريعات بشكل صريح و واضح فلا وجود لقواعد قانونية تخص تلك الجرائم بالذات، إلا أن القضاء العراقي قد حاول جاهدا معالجة هذه الجرائم وفق تكييفها القانوني.

من خلال تطويع القواعد القانونية الموجودة في قانون العقوبات العراقي والخاصة بجريمة التهديد حسب المواد(456 ، 430 ،341) .(2)

فمن خلال تتبع قضايا الإبتزاز الإلكتروني فإن تكييفها القانوني يختلف باختلاف واقعة الإبتزاز فقد تكون عن طريق نصب المبتز واحتياله على الضحية لغرض الوصول الى الغاية محل الإبتزاز فهنا يكون التكييف القانوني لمثل هذه الحالات تحت نص المادة 456 من قانون العقوبات العراقي النافذ حيث تنص على أنه : (يعاقب بالحبس كل من توصل الى تسليم ، أو نقل حيازة مال منقول مملوك للغير لنفسه أو الى شخص آخر وذلك بإحدى الوسائل الاتية :

- استعمال طرق احتيالية

(1)محمد عبد المحسن بن شلهوب ، المرجع السابق، ص 67.

(2) رامي احمد الغالبي ، جريمة الابتزاز الالكتروني و الية مكافحتها في جمهورية العراق ، مقال منشور في مجلة ثقافتنا الامنية ، الاصدار الثاني ،وزارة الداخلية العراقية ، مديرية العلاقات و الاعلام ، دار الكتب و الوثائق ، بغداد، 2019،ص45 .

– اتخاذ اسم كاذب أو صفة غير صحيحة أو تقرير أمر كاذب عن واقعة معينة متى كان من شان ذلك خداع المجني عليه وحمله على التسليم .

أو قد يكيف الإبتزاز وفق احكام المادتين (430)(431) من قانون العقوبات العراقي الخاصة بجرائم التهديد حيث تنص المادة (430) على:

(يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من هدد آخر بارتكاب جناية ضد نفسه أو ماله ،أو ضد نفس أو مال غيره أو باسناد أمور مخدشة بالشرف ،أو إفشائها وكان ذلك مصحوبا بطلب أو، تكليف بأمر ،أو الإمتناع عن فعل، أو مقصود به ذلك .

– ويعاقب بالعقوبة ذاتها إذا كان التهديد في خطاب خال من اسم مرسله أو كان منسوبا صدوره إلى جماعة سرية موجودة أو مزعومة.

كما تنص المادة (431) على أن : يعاقب بالحبس كل من هدد آخر بارتكاب جناية ضد نفسه أو ماله أو، ضد نفس أو، مال غيره أو، باسناد أمور خادجة للشرف أو، الاعتبار أو افشائها بغير الحالات المبينة في المادة 430.

لم يبق القضاء العراقي مكتوف الأيدي أمام جريمة الإبتزاز الإلكتروني بسبب عدم وجود نص تشريعي يجرم ويعاقب على هذا الفعل حيث فوت الفرصة على المبتز من أن يستغل الفراغ التشريعي أو أن يتمسك بقاعدة(لا جريمة ولا عقوبة إلا بالقانون) وذلك لمعالجة هذا الخلل وفق التكييفات آنفة الذكر. (1)

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) رامي احمد غالبي ، المرجع السابق ، ص 46 .

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 و سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة) (1)

وحسب المادة الثانية للقانون 09-04 المؤرخ في 5 اوت 2009، حيث يعرف الجرائم المتصلة بتكنولوجيا الإعلام والإتصال بأنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية. (2)

نص التجريم المادة 303 مكرر (القانون رقم 06 – 23 المؤرخ في 20 ديسمبر 2006). (3)

(يعاقب بالحبس من ستة 6 اشهر إلى ثلاث 3 سنوات وبغرامة مالية من 50,000 دج إلى 300,000 دج كل من تعمد المساس بحرمة الحياة الخاصة للاشخاص بأي تقنية كانت وذلك :

1- بالتقاط أو تسجيل ،أو نقل مكالمات وأحاديث خاصة ،أو سرية بغير إذن صاحبها، أو رضاه

2- بالتقاط ،أو تسجيل، أو نقل صور لشخص في مكان خاص بغير إذن صاحبها ورضاه .

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. ويضع صفح الضحية حدا للمتابعة الجزائية.

المادة 303 مكرر 1 (القانون 06- 23 المؤرخ في 20 ديسمبر 2006) يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور ،أو الغير أو استخدم بأية وسيلة كانت التسجيلات ،أو الصور، أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في الماده 303 مكرر من هذا القانون .

---

(1) أنظر المادة (39) من دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر بتاريخ 7ديسمبر 1996، الجريدة الرسمية رقم 76 المؤرخة في: 8 ديسمبر 1996، المعدل .

(2) أنظر المادة 2 قانون 09-04 من القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها ، مؤرخ في: 14 شعبان 1430 هجري الموافق ل 05 اوت 2009 ، ج ر ج ج رقم 47 ، الصادرة في: 2009/01/15 .

(3) أنظر المادة 303 مكرر من الامر رقم 66-156 المؤرخ في 18 صفر عام 1386 هـ الموافق لـ : 06 يونيو 1966 يتضمن قانون العقوبات المعدل و المتمم ، جريدة رسمية للجمهورية الجزائرية ،عدد 49 ، الصادر في: 1966/06/11 .

.

عندما ترتكب الجنح المنصوص عليها في الفقرة السابقة عن طريق الصحافة تطبق الاحكام الخاصة المنصوص عليها في القوانين ذات العلاقه لتحديد الأشخاص المسؤولين .

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة.

ويضع صفح الضحية حدا للمتابعة الجزائية .) (1)

حيث تضمنت المواد 303 مكرر و 303 مكرر 1 ثلاث صور للتجريم وهي : التقاط وتسجيل ونقل الأحاديث الخاصة والسرية للأشخاص دون موافقتهم ،وكذا جريمة التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص دون رضا أو اذن صاحبها وكذا جريمة الاحتفاظ والوضع في متناول الجمهور أو الغير أو الاستخدام لتلك المكالمات ،أو الاحاديث ،أو الصور المحصل عليها بإحدى تلك الطرق . (2)

أولا: عناصر الحياة الخاصة

حسب المادة 303 مكرر فان المشرع الجزائري قد حصر الحياة الخاصة بمفهومها الضيق في عنصرين هما الحق في سرية المكالمات والمحادثات الخاصة ،والحق في سرية الصور عند التواجد في مكان خاص.

ثانيا: المقصود بالمكالمات والأحاديث الخاصة والسرية

هي تلك الأحاديث التي يتفوه بها الفرد أما مباشرة دون استعمال وسيلة معينة للاتصال وهي الصورة التي يكون فيها المتحدث وجها لوجه مع المتحدث له ،أو أن يتم بشكل غير مباشر في حالة بعد المسافة و اقتضى الأمر لايصال الصوت استعمال جهاز الهاتف أو، الحاسوب وتسمى بذلك مكالمة .

ولا يشترط المشرع أن يكون التفوه بالكلام في إطار مكالمة بين شخصين، أو أكثر بل قد يصدر الكلام من شخص مع نفسه لأن المشرع استعمل مصطلح الأحاديث وليس المحادثات .

(1) أنظر المادة 303 مكرر 1 ق ع ج .

(2) عز الدين طباش ، شرح القسم الخاص من قانون العقوبات ، درائم ضد الاشخاص و الاموال ، د ط ، دار بلقيس ، دار البيضاء ، الجزائر ، د ت ، ص125 .

كما أن الفهم الضيق بعبارة المكالمات ،والأحاديث عن أنه يجب أن يصدر كلام معين فلا تدخل للأصوات في نطاق تطبيق النص (1)

أما بالنسبة لمضمون الحديث الخاص والسري يعني أن يتضمن الكلام مسائل عائلية مرتبطة بالعلاقة الزوجية ،أو العلاقات الشخصية ،أو حتى الكلام المتعلق بالحالة الصحية ولا عبرة بالمكان الذي صدر فيه الحديث . (2)

أما الأحاديث التي قيلت في أماكن عمومية وتضم المسائل المتعلقة بالحياة الخاصة فانها تدخل في نطاق الأحاديث الواردة في المادة 303 مكرر .

ثالثا: المقصود بالحق في سرية الصورة في المكان الخاص

هي تلك الهيئة التي يظهر بها الشخص في مكان خاص لا يريد أن يراه فيها إلا الأشخاص الذين يحددهم بنفسه ، وبالتالي فقيام التجريم المتعلق بانتهاك حرمة الصورة يرتبط بارتباط وثيق بطبيعه المكان الذي يجب ان يتم فيه التصوير وهو المكان الذي لا يجب دخوله إلا بإذن صاحبه وهذا ما يضيق من مجال التجريم بالمقارنه مع المساس بحرمة المكالمات والأحاديث ، أما التصوير في مكان عمومي سواء كان عمومي بطبعه، أو بالتخصيص ،أو المصادفة لا يدخل في نطاق التجريم. (3)

وينصرف مفهوم المكان الخاص إلى كل حيز مكاني ثابت، أو منقول لا يمكن دون استراق ،أو تسجيل أو نقل، أو استماع ما يدور بداخله وإن امكن مشاهدة من بداخله ولا يجوز دخوله إلا بموجب موافقة مالكه أو حائزه، أو ممن تربطهم رابطة وظيفية، أو مهنية.

ومن ثم نسحب أحكام الحماية الجزائية على الحديث الذي يتم في هذا المكان ويتناول أمورا عامة ليست لها صفة الخصوصية. (4)

---

(1)عز الدين طباش ، المرجع السابق ، ص 126 .

(2) المرجع نفسه.

(3) المرجع نفسه، ص 128 .

(4) نبيل صقر ، الوسيط في جرائم الاشخاص ، د ط، دار الهدى عين مليلة – الجزائر ، 2009، ص 174 .

الفرع الثاني : الركن المادي لجريمة الإبتزاز عبر الوسائل الإلكترونية

يقصد بالركن المادي للجريمة السلوك المادي الخارجي الذي ينص القانون على تجريمه أي كل ما يدخل في كيان جريمة الإبتزاز الإلكتروني، وتكون له طبيعة مادية ملموسة وهو ضروري لقيام الركن المادي إذ لا يعرف القانون الجرائم دونه.

وقد عرف قانون العقوبات العراقي النافذ رقم 11 لسنة 1969، في المادة28 الركن المادي بأنه :(سلوك إجرامي بارتكاب فعل جرمه القانون والإمتناع عن فعل أمر به القانون) . (1)

ويتحلل الركن المادي الى ثلاث عناصر وهي : السلوك الإجرامي ،والنتيجة الإجرامية ،والعلاقة السببية .

أولا:السلوك الإجرامي لجريمة الإبتزاز عبر الوسائل الإلكترونية

الفعل محل التجريم هو واقعة مادية ظهرت للعالم الخارجي حيث يتخد صورة السلوك الإجرامي لجريمه الإبتزاز بالقيام بفعل التهديد بنشر بيانات، أو صور، أو مقاطع فيديو للضحية والقانون لا يعير أهمية للتمييز بحيازة تلك البيانات والصور والمقاطع الفيلمية كونها تمت برضى الضحية، أو من خلال اختراق حساب الضحية ،أو عثر في جهاز هاتف مسروق أو ضائع، أو مباع ،أو أنه يستخدم أي من البرامج للدخول غير المصرح به لبيانات وصور الضحية ، ولا يشترط أن يتم التهديد بطريقة معينه سواء تم في غرف الدردشه(الشات) أو عن طريق البريد الإلكتروني ،كما لا عبرة في كون مقابل سكوت المبتز يكون عملا مشروعا ،أو غير مشروعا ، فالعبرة تكون في استخدام الضغط والإكراه المقترن بالتهديد لإرغام المجني عليه على القيام بذلك الفعل. (2)

ويشترط لوقوع جريمة الإبتزاز الإلكتروني أن يكون السلوك الإجرامي للممبتز بطلب أمر رغما عن إرادة الضحية وذلك كأن يطلب منها مالا ليس من حقه ، أو يطلب منها علاقة جنسية ، كما يشترط أن يكون المبتز جادا في ما يطلبه حيث يستشعر المبتز أنه سينفذ تهديده لا محالة إذا لم يقم المجني عليه بتنفيذ مطالبه وهو جوهر الطلب في الإبتزاز.

(1) رامي احمد غالبي ، المرجع السابق، ص 49 .

(2) بعيوي شاكر سعاد ، جريمة الابتزاز الالكتروني ، دراسة مقارنة مقال بمجلة ميسان للدراسات القانونية المقارنة ، كلية القانون جامعة ميسان ، العراق ، نوفمبر 2019 ، ص 129 .

كما يجب أن يكون لفظ التهديد صريحا ،أو ضمنيا ولكن يفهم منه أن المبتز يهدده بأمر هو إفشاء أسرار الضحية إذا لم يلبي رغبته فالعبرة تكمن في الضغط ، والإكراه الذي يقترن بالتهديد لإرغام المجني عليه على القيام بذلك الفعل . (1)

فقد اعتبر القانون العراقي هذا النوع من التهديد في مرتبة إرتكاب جريمة ضد النفس أو المال ، وأوضح عبارة(إسناد أمور مخدشة بالشرف) يقصد بها الأمور غير الصحيحة التي إختلقها الجاني ونسبها كذبا الى الضحية ، أما عبارة إفشائها يقصد بها الأمور الصحيحة الماسة بالشرف.(2)

أما من ناحيه بلوغ التهديد درجة معينة من الجسامة لوقوعه فلم يشترط كل من المنظم السعودي والقانون العماني والإماراتي بلوغ التهديد درجة معينه من الجسامة ، وإنما يكفي أن يؤدي هذا التهديد الى حمل الشخص على القيام بفعل ،أو الإمتناع عنه إلا أنه ينبغي أن تكون وسيلة الجاني على حمل المجني عليه على تنفيذ رغباته التي طلبها منه هي التهديد حيث نجد نصوصهم أن كل شخص هدد شخصا آخر ،أو ابتزه لحمله على القيام بفعل، أو الإمتناع عنه ولو كان القيام بهذا الفعل والإمتناع مشروعا يعاقب بالعقوبات المنصوص عليها قانونا . (3)

(1) رامي احمد غالبي ، المرجع السابق ، ص 50 .

(2) سعاد شاكر بعيوي، المرجع السابق، ص130 .

(3) ممدوح رشيد مشرف الرشيد العنزي ، المرجع السابق ، ص207 .

المادة 3 من نظام مكافحة جرائم المعلوماتية السعودي والمادة 16و 18من قانون مكافحة جرائم تقنية المعلومات الإماراتي في ترويع المجني عليه بحيث تحمله على تنفيذ ما يطلبه منه بل ويعتبر تهديدا قائما سواء كان في مواجهة الشخص المهدد ، أو لم يكن في مواجهته كإخبار شخص آخر وقام هذا الأخير بإخبار التهديد للشخص المهدد. (1)

فماذا يقصد بالتشهير بالآخرين؟

تعد هذه الصورة من صور الركن المادي لجريمة الإبتزاز، لما لها من مساس مباشر بحرية الحياة الخاصة التي يحميها القانون نتيجة لتطور التكنولوجيا ووسائل الاتصال التي ساعدت على إنتشار تلك الصورة. (2)

الأمر الذي يسمح معه لفرصة التسجيل والتصنت ونقل الأحاديث ونسخها وتسجيلها.

فتتحقق تلك الصورة من خلال قيام المبتز باستخدام وسائل تقنيات المعلومات المختلفة كالأنترنت الذي يعد وسيلة للإعتداء على أسرار الحياة الخاصة ، بل ويمتد الأمر للتعرض لأسرهم أو طبيعة عملهم بهدف الإبتزاز أو الإنتقام أو الحصول على منفعة معينة وتتحقق من خلال العديد من الأفعال المادية التي تتمثل في نشر أو عرض أو توزيع صور المجني عليه التي قد تكون خادشة للحياء بقصد التشهير به، كما قد تحصل جريمة الإبتزاز الإلكتروني بقيام الجاني بتهديد المجني عليه من خلال غرف الدردشة والمحادثة أو عبر أحد المنتديات الإلكترونية وقد نص المنظم السعودي على تلك الصوره عندما حددت المادة رقم 03 الفقرة 05 من نظام مكافحة جرائم المعلوماتية ، أن التشهير بالآخرين من الجرائم المعاقب عليها بالسجن والغرامة المالية . (3)

أما ما جاء به القانون العماني والإماراتي يفوق نظيره السعودي من ناحية توسعة في صور التشهير بالاخرين .

فالمنظم السعودي اكتفى بعبارة التشهير بالآخرين عبر وسائل تقنيات المعلومات المختلفة دون أن يعطي تفصيلا كافيا لتلك الصور.

أما القانون العماني والإماراتي فصلا تلك المسألة من خلال تبيان وسائل التشهير كالتقاط الصور أو نشر أخبار أو تسجيلات صوتية ،أو مرئية تتصل بها ولو كانت صحيحة.

(1) ممدوح رشيد مشرف الرشيد العنزي ، المرجع السابق، ص 209 .

(2) المرجع نفسه، ص210 .

(3) المرجع نفسه.

ثانيا : النتيجة الإجرامية لجريمة الإبتزاز عبر الوسائل الإلكترونية

النتيجة الإجرامية هي الأثر المترتب على السلوك الذي يقصده القانون بالعقاب فهي الحقيقة المادية إلى كيان ملموس في العالم الخارجي أو أنها الحقيقة القانونية.

وفي جريمة الإبتزاز الإلكتروني تقع النتيجة الجرمية لمجرد قيام المبتز بتهديد الضحيه بإفشاء سر من أسرارها التي تعتبره أمرا لا يجب الإطلاع عليه أمام الملأ وكان تهديدا بأمر غير مشروع .

طالما يسبب ذلك الخوف والهلع والتأثير على إراده نفسية الضحية بأن يلقي في نفسها قلقا من قيام المبتز بتنفيذ تهديده. (1)

فإذا سعى الجاني بالتهديد إلى مجرد 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 أم لم يفعل. (2)

ثالثا: العلاقة السببية لجريمة الإبتزاز عبر الوسائل الإلكترونية

تعد العلاقة السببية العنصر الثالث من عناصر الركن المادي للجريمة، فهي الصلة التي تربط ما بين السلوك الإجرامي والنتيجة الجرمية ، وتعرف العلاقة السببية بأنها الصلة بين السلوك الذي يعترف به القانون سببا، والأثر الذي يعترف به القانون نتيجة. (3)

ولقيام الركن المادي لابد من أن تنسب النتيجه الإجرامية إلى الفعل أو الإمتناع المؤثرالصادرعن الجاني، معنى ان تحدث النتيجه الجرمية بسبب فعل الجاني أي لولا حصول الفعل لم تحدث تلك النتيجة. (4)

وفي جرائم الإبتزاز الإلكتروني لو أن النتيجة تحققت بإفشاء أسرار المجني عليه ولكن بفعل شخص آخر لم يكن هو المبتز، أو بسبب ضياع هذه الوثائق ،أو الصور، أو الافلام وانتشارها بمحض الصدفة فلا مسؤولية على الفاعل حيث أن علاقة السببية إنتهت ، فقد يسأل عن جريمة أخرى بحسب التكييف القانوني للفعل.

حيث توجد علاقة السببية بين الإبتزاز والتسليم في حال كان الباعث للجاني هو الحصول على المال إذ يلزم أن يكون تسليم المال نتيجة ما أحدثة في نفس المجني عليه من خوف فإذا لم يحدث التهديد هذا الأثر ، وجرى تسليم المال لاعتبارات أخرى انقطعت علاقة السببية.(5)

---

(1) رامي احمد غالبي ، المرجع السابق، ص 41 .

(2) محمد عبد المحسن بن شلهوب ،المرجع السابق ، ص 91.

(3) رامي احمد غالبي ، المرجع السابق، ص51 .

(4) المرجع نفسه، ص 41 .

(5) المرجع نفسه.

أما إذا كان الإبتزاز للقيام بعمل أو الامتناع عن أداء عمل فان النتيجة هنا وقوع الضرر و هو الخوف في نفس المجني عليه وتكون علاقة السببية بينه وبين الإبتزاز هو أن يكون الإبتزاز سببا في إمتهان كرامة المعتدي عليه واحتقارة وتعريضه لبغض أهله والناس واذا امتنع المجني عليه عن أداء عمل ليس على سبيل الخوف من الجاني وإنما لرغبته في الإلتزام بالقانون فهنا لا تقع جريمه الابتزاز وذلك لانتفاء علاقه السببية في الجريمة . (1)

الفرع الثالث: الركن المعنوي لجريمة الإبتزاز عبر الوسائل الإلكترونية

الركن المعنوي هو إرادة الجريمة ولا تخرج الإرادة الإجرامية عن صورتين رئيسيتين هما:

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 ان القانون يجرم تركه. (2)

لهذا يصف بعضهم الركن المعنوي بأنه ركن المسؤولية وعلى ذلك في الركن المعنوي يمثل العلاقة النفسية بين الفعل والفاعل ويقتضي بأن يكون الفاعل أهلا لتحمل المسؤولية الجنائية ، ولا يكون كذلك إلا إذا تجتمع بارادة وإدراك يعتد القانون بهما أو أن تنصرف هذه الإرادة الى ماديات الجريمة .

فالقصد الجنائي لدى المبتز أن تكون إرادته وعلمه قد إتجه الى تهديد الضحية بالمعلومات والصور التي يملكها وهو ما يمثل إعتداء على حرمة الحياة الخاصة. (3)

أولا: القصد العام

ينهض القصد العام في جريمة الإبتزاز الإلكتروني على عنصرين هما :

أ : العلـم

يجب أن يعلم المبتز أن ما يقوم به وما يتصل به من وقائع والتي تعد من عناصر الجريمة والعلم بموضوع الجريمة حيث يجب أن يعلم أن ما يقوم به من الحصول على صور فاضحة لأحد الأشخاص وتهديده بها مقابل الحصول على منفعة جريمة يعاقب عليها القانون ، هنا يتحقق العلم كما ينبغي أن يكون الجاني عالما بماهية الفعل أو الإمتناع المجرم كما أن فعله يلحق ضررا بالمجني عليه. (4)

---

(1) محمد عبد المحسن بن شلهوب ، المرجع السابق، ص 92 .

(2) رامي احمد الغالبي ، المرجع السابق ،ص 52 .

(3) سعاد شاكر بعيوي،المرجع السابق ، ص 212 .

(4) رامي احمد الغالبي ، المرجع السابق ، ص52 .

والجهل هو عكس العلم ويعني انتفاء العلم ،وقد يقع الفاعل في غلط بالوقائع مما يرفع عنه المسؤولية الجزائية وهذا لا يتعارض مع قاعدة عدم جواز الاعتذار بالجهل بالقانون إذ انه إذا بلغ الانسان وتيسر العلم له، مما يجعل هناك إمكانية العلم به مما يمنع معه الاعتذار بالجهل بالقانون اذ ان العلم بالتكييف الجنائي مفترض فيقوم القصد الجنائي في جريمة الإبتزاز الإلكتروني على القصد الجنائي العام باعتبارها من الجرائم العمدية حيث يعلم الجاني أن ما يقوم به من فعل أو خطاب أو قول يترتب عليه بث الرعب والخوف في نفس المجني عليه ، ما يصيبه بقلق نفسي لانتظار ما يسفر عنه فعل الجاني من ضرر يصيب المجني عليه في نفسه أو ماله أو يصيب شخص له صلة به . (1)

ب : الإرادة

هو الإرادة في تحقيق نتيجة غير مشروعة نحو المساس بحق ،أو مصلحة يحميها القانون ومن ثم ينبغي أن تتجه إرادة المبتز الى تحقيق النتيجة الإجرامية المتمثلة في إبتزاز المجني عليه فلا يقف الأمر عند علم الجاني ما يترتب على ذلك من آثار نفسية تلحق بالمجني عليه بل يعتمد قصد الجانب التهديدي إلى تخويف أو حمل المجني عليه على القيام بعمل، أو الإمتناع عنه دون النظر الى تنفيذ العمل ،أو عدم تنفيذه فتتوقع حدوث النتيجة يكفي لرغبة الجاني في حدوثها عند مباشرة نشاطه الإجرامي.

وبما أن الإبتزاز الإلكتروني يعد من الجرائم الشكلية التي تتطلب نصيحة معينة فإن المنظم السعودي والقانون الإماراتي والعماني قد حددوا تلك النتيجة بحمل المجني عليه على القيام بعمل أو الإمتناع عنه. (2)

وتنقسم الإرادة إلى قسمين إرادة الفعل ، وإرادة النتيجة فلكي تقوم المسؤولية يجب إثبات ان إرادة الفعل إتجهت الى القيام بهذا الفعل وذلك دون أن تقع الإرادة في عيب من عيوب الإرادة كأن يكون مختارا ومدركا، أنه يحصل على صور سرية وخاصة بالضحية فاذا كان مكرها فلا يوجد قصد جنائي ولا تقوم المسؤولية الجزائية للفاعل على المكره .

أما إرادة النتيجة فلا بد أن تتجه إرادة الجاني الى تحقيق النتيجة الإجرامية بالحصول على المنفعة المادية أو النفعية أو اللاأخلاقية كما أنه لا أثر للباعث في توافر القصد الجنائي طبقا للقاعدة العامة، فالباعث لا عبرة له في الجريمة، فيستوي في الإبتزاز الإلكتروني أن يكون الباعث شريفا أو وضيعا كانتقامه من المجني عليه أم لتحقيق مصلحة معينة. (3)

---

(1) ممدوح رشيد مشرف الرشيد العنزي ، المرجع السابق ، ص212 .

(2) المرجع نفسه 212 .

(3) محمد عبد المحسن بن شلهوب ، المرجع السابق ، ص107 .

ثانيا : القصد الخاص

بما أن جريمة الإبتزاز الإلكتروني هي من الجرائم التي تحتاج الى 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 ان يكون القصد خاصا. (1)

المطلب الثاني :عقوبة جريمة الإبتزاز عبر الوسائل الإلكترونية

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

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

(1) محمد عبد المحسن بن شلهوب ، المرجع السابق ، ص104 .

الفرع الأول : العقوبات الأصلية والعقوبات التكميلية

أولا : العقوبات الأصلية

نص المنظم السعودي في المادة الثالثة في نظام مكافحة الجرائم المعلوماتية. (1)

على ايقاع عقوبة السجن لمدة لا تزيد على سنة وبغرامة لا تزيد على 500,000 ريال أو باحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية التالية.

وذكر منها الدخول في المشروع لتهديد شخص أو إبتزازه لحمله على القيام بفعل أو الإمتناع عنه ولو كان القيام بهذا الفعل أو الإمتناع عنه مشروعا.

وكون المساس بالحياة الخاصة عن طريق استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها أو بالتشهير بأي شخص عبر وسائل تقنيات المعلومات المختلفة وإلحاق الضرر بهم. فالهواتف المزودة بالكاميرا هي سلاح المعتدي الأسهل والأكثر إنتشارا.

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 . (2)

حسب مجريـات وقائع الدعوى كما أن تعميم وزير الداخلية رقم 2000 لسنة1435 هجري ، إعتبر جرائم الإبتزاز وانتهاك الأعراض بالتصوير ،أو النشر أو التهديد بالنشر من الجرائم الكبيرة الموجبة للتوقيف ، كمـا أوضحت المذكرة الإيضاحية أن الإبتزاز عن طريق محاولة الحصول على مكاسب ماديـة ،أو معنوية عن طريق الإكراه بالتهديد بفضح سر من أسرار المبتز من شخص أو أشخاص أو مؤسسات كما يدخل في انتهاك الأعراض بالتصوير أو الحصول على الصور محل الجريمة في أي وسيلة كانت. (3)

أما المادة (16)من القانون الإتحادي لدولة الإمارات المتحدة . (4)

لقد نصت على : يعاقب بالحبس مدة لا تزيد على سنين والغرامة التي لا تقل عن 250,000 درهم ولا تتجاوز 500,000 درهم أو باحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر بحمله على القيام بفعل أو الإمتناع عنه وذلك باستخدام شبكه معلوماتية أو وسيلة تقنية معلومات .

---

(1) أنظر المادة 3 نظام مكافحة الجرائم المعلوماتية السعودي.

(2) ممدوح رشيد مشرف الرشيد العنزي،المرجع السابق ، ص213 .

(3) المرجع نفسه.

(4) أنظر المادة (16) من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الإماراتي .

وتكون العقوبة بالسجن مده لا تزيد على 10 سنوات إذا كان التهديد بإرتكاب جناية ،أو باسناد أمور خادشة للشرف ،أو الاعتبار كما نجد المشرع الإماراتي في قانون العقوبات الإتحادي في الماده 378 على حماية الحياة الخاصة حيث يعاقب بالحبس وبالغرامة كل من اعتدى على حرمة الحياة الخاصة، أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضى المجني عليه :

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات في مكان خاص أو عن طريق الهاتف أو أي جهاز آخر.

ب- التقاط أو نقل بجهاز أيا كان نوعه صورة شخص في مكان خاص، فإذا صدرت الأفعال المشار إليها في الحالتين السابقتين أثناء إجتماع ،على مسمع و مرأى من الحاضرين في ذلك الإجتماع فإن رضى هؤلاء يكون مفترضا.

كما يعاقب بذات العقوبة من نشر إحدى طرق العلنية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة. (1)

ويعاقب بالحبس مدة لا تزيد على سبع سنوات وبالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته.

ويحكم في جميع الاحوال مصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصل عنها أو إعدامها.

أما القانون العماني فنجد أنه بموجب قانون مكافحة جرائم تقنية المعلومات لعام 2011 والذي عاقب كل من يستخدم الشبكة المعلوماتية ،أو وسائل تقنيه المعلومات مثل الهواتف النقالة التي تحتوي على آلة التصوير في الإعتداء على حرمة الحياة الخاصة ،أو العائلية للأفراد بالسجن مدة لا تقل عن سنة ولا

(1) هذه المادة معدلة بموجب القانون الاتحادي رقم 34 لسنة 2005 م .ونص المادة قبل التعديل يجري على النحو التالي : (يعاقب بالحبس مدة لا تزيد على سنة والغرامة التي لا تتجاوز 10000 درهم في الحالتين أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية أخبارا أو صورا أو تعليقات تتصل بأسرار الحياة الخاصه أو العائليه للأفراد ولو كانت صحيحة).

تزيد عن 3 سنوات وكذلك بغرامة لا تقل عن 1000 ريال عماني ولا تزيد على خمسة الاف ريال عماني أو

بإحدى هاتين العقوبتين ، وسواء كان ذلك بالتقاط صور، أو نشر أخبار، أو تسجيلات صوتية أو مرئية تتصل بالحياة الخاصة للأفراد وحتى ولو كانت صحيحة أو في التعدي على الغير بالسب أو القذف. (1)

كما أن المادة(18) من القانون نفسه قد أشارت إلى أنه: "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاثة سنوات وبغرامة لا تقل عن 1000 ريال عماني ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في تهديد شخص أو ابتزازه بحمله على القيام بفعل أو امتناع ولو كان هذا الفعل أو الإمتناع عنه مشروعا أو تكون العقوبة السجن المؤقت مدة لا تقل عن 3 سنوات ولا تزيد عن عشر سنوات وغرامة لا تقل عن ثلاثة الآف ريال عماني ولا تزيد على عشرة الآف ريال عماني إذا كان التهديد بارتكاب جناية أو بإسناد أمور مخلة بالشرف،أو الإعتبار." (2)

فالمشرع العماني وضع حدا أقصى ، وحد أدنى للعقوبة أما المشرع الكويتي فحسب نص المادة 03 من قانون مكافحة جرائم تقنية المعلومات، فقد حدد المشرع الكويتي عقوبة الحبس مدة لا تتجاوز ثلاثة سنوات وبغرامة لا تقل عن ثلاثه الآف دينار ولا تتجاوز عشرة الآف دينار أو بإحدى هاتين العقوبتين

من استعمال الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد ،أو إبتزاز شخص طبيعي أو اعتباري بحمله على القيام بفعل ،أو الإمتناع عنه فاذا كان التهديد بارتكاب جناية أو بما يعد مساسا بكرامة الأشخاص أو خادشا للشرف والإعتبار أو السمعة كانت العقوبة الحبس مدة لا تتجاوز خمس سنوات والغرامة التي لا تقل عن خمسة الآف دينار ولا تتجاوز 20 الف دينار أو بإحدى هاتين العقوبتين. (3) أما في القانون المصري فقد نص على العقوبة في جريمة الإبتزاز في حال كانت الجريمة المستخدمة هي من الوسائل التقنية ، وذلك كما جاء في نص الماده 309 بقولها: (يعاقب

(1) أنظر المادة 16 من قانون مكافحة جرائم تقنية المعلومات العماني ، لسنة 2011.
(2) أنظر المادة 18 من القانون نفسه.
(3) أنظرالمادة 3 من القانون رقم 63، لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي .

بالسجن مدة لا تزيد على 5 سنوات كل من هدد بافشاء أمر من الأمور التي يتم التحصل عليها بإحدى الطرق المشار اليها في حمل شخص على القيام بعمل أو الإمتناع عنه ويعاقب بالسجن الموظف الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته ، يحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو إعدامها).

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 اعتمادا على سلطة وظيفته .(1)

أما في العراق فهناك فراغ تشريعي في ما يتعلق بالجرائم المعلوماتية ، وعليه كان للقضاء دور في تحديد عقوبات لهذه الجريمة من خلال تطويع النصوص الحالية والخاصة بجرائم التهديد في حالة ارتكابها بطريق الانترنت. (2)

بالنسبة للمشرع الجزائري فلقد حددت المواد 303 مكرر و 303 مكرر 1 ، 303 مكرر 2 ، العقوبات الخاصة بهذه الجنحة وهي كالاتي :

المادة 303 مكرر (3)

م 303 مكرر: يعاقب بالحبس من ستة أشهر الى ثلاث سنوات وبغرامة مالية من 50 ألف دج إلى 300 الف دج كل من تعمد المساس بحرمة الحياة الخاصة للاشخاص بأية تقنية كانت . (4)

م 303 مكرر1 : يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذه المادة بالعقوبة المقدرة للجريمة الثانية . (5)

ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة.

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق، ص 135.

(2) سعاد شاكر بعيوي ، المرجع السابق ، ص137 .

(3) أنظر المادة 303 مكرر من ق ع ج .

(4) أنظرالمادة 303 مكرر 1 من ق ع ج.

(5) أنظرالمادة 303 مكرر 2 من ق ع ج.

ثانيا: العقوبات التكميلية

العقوبة التكميلية هي تلك العقوبة التي تصيب الجاني بناءا على الحكم بالعقوبة الأصلية وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناءا على الحكم بالعقوبة الأصلية دون الحاجة الى إصدار حكم تبعي فهو مرتبط إرتباطا مباشرا و وثيقا بالعقوبة الأصلية.

ففي جريمة الإبتزاز الإلكتروني نصت المادة 13 من نظام مكافحة جرائم المعلوماتية على أنه يجوز الحكم بمصادرة الأجهزه أو البرامج ،أو الوسائل المستخدمة في أي من الجرائم المنصوص عليها في هذا النظام ، أو الأموال المحصلة منها كما يكون الحكم بإغلاق الموقع الإلكتروني أو مكان تقديم الخدمة إغلاقا نهائيا أو مؤقتا ، متى كان مصدرا لارتكاب هذه الجرائم وكانت الجريمة قد ارتكبت بعلم مالكه . (1)

المصادرة هي الأيلولة النهائية للمال للدولة ،والفرق بين المصادرة والغرامة أن هذه الأخيرة هي عقوبة مالية نقدية وعقوبة أصلية أما المصادرة فهي عقوبة عينية تكميلية، وترد على أشياء حيازتها مشروعة وأن تكون حيازة الأشياء المصادرة مشروعة وذلك بأن تكون بينها وبين الجريمة صلة معينة.

هذه الصلة قد حددتها المادة 13 بقولها (الأجهزة والبرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام).

وبالتالي لا يجوز نظاما أن تحكم بمصادرة أشياء لا صلة لها بالجريمة ، أو لم تكن قد تحصلت منها ،أو من شأنها أن تستعمل فيها ، وأن تكون هذه الأشياء قد تم ضبطها فعلا عند إصدار الحكم بالمصادرة فإذا لم تكن الاشياء محل المصادرة مضبوطة بالفعل وقت الحكم بمصادرتها فلا يجوز للقاضي أن يحكم بمصادرتها. (2)

المصادرة تكون على أشياء حيازتها في الأصل مشروعة ولكنها أستخدمت ،أو كانت وسيلة لارتكاب جريمة فهي مشروعة في الأصل وقد استخدمت في عمل غير مشروع لجريمة الإبتزاز الإلكتروني .

(1) أنظر المادة 13 نظام مكافحة الجرائم المعلوماتية السعودي .

(2) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص 134 .

وللقاضي سلطة تقديرية في توقيع المصادره من عدمه شريطة أن ترتبط بالعقوبة الأصلية على المبتز وهي الحبس، أو الغرامة أو إحداهما. (1)

وإذا لم تكن الأشياء تم استخدامها في الجريمة ليست ملكا للجاني فلا يحكم القاضي بمصادرتها وذلك كما نصت عليه م 13 بقولها ((مع عدم الاخلال بحقوق الغير حسن النية...). (2)

طالما أن تلك الحقوق ثابتة وقت ارتكاب جريمة الإبتزاز الإلكتروني ،أو بعد وقوعها وقبل تحريك الدعوى العمومية.

وبالتالي فإن مصادرة الشيء المضبوط لا تحول دون حق الغير الحسن النية في مطالبة الدولة التي آلت إليها الأشياء.

واستجابة الدولة تأخذ شكل رد الشيء المضبوط إلى صاحب الحق حسن النية كذلك إذا كان هذا الحق للغير من الحقوق العينية وكان خاصا به . (3)

أما في القانون الإماراتي فإن م 41 منه نصت على : (مع عدم الإخلال بحقوق الغير حسنة النية يحكم 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 باغلاق المحل او الموقع الذي يرتكب فيه أي من هذه الجرائم وذلك إما إغلاقا كليا أو لمدة التي تقدرها المحكمة.) (4)

نفس القواعد التي تحكم العقوبة التكميلية في النظام السعودي نجدها في القانون الإماراتي كونها عقوبة عينية وتقديرية للقاضي، وتتبع العقوبة الأصلية وجودا أو عدما وتمتنع في حالة كانت الأجهزة المستخدمة في الجريمة للغير حسني النية ، كما أن المشرع العماني انتهج نفس القواعد فهي عقوبة تكميلية جوازية.

---

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق، ص 134 .

(2) أنظر المادة13 نظام مكافحة الجرائم المعلوماتية .

(3) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص 135 .

(4) أنظر المادة 41 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

أما في القانون المصري فهي عقوبه تكميلية وجوبية وذلك لمصادرة الأجهزه المستخدمة في الجريمة أو الذي تحصل منها وأوجب إزالة الوضع الإجرامي بمحو التسجيلات المتحصلة من الجريمة أو إعدام هذه المواد . (1)

أما في التشريع الجزائري فالحكم بالمصادرة وجوبي حسب المادة 303 مكرر وذلك في ما يخص الأشياء المستعملة في ارتكاب الجريمة كما أن المادة 303 مكرر2 أحالت الى المادة 9 مكرر1.(2) والمادة 18 من قانون العقوبات حيث يجوز للمحكمة أن تحكم على المحكوم عليه بالجرائم المنصوص عليها في المادة 303 مكرر و المادة 303 مكرر 1، وذلك بمنعه من ممارسة حق أو اكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 ق ع ج ، لمدة لا تتجاوز خمس سنوات كما يجوز لها أن تنشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 ق ع ج ، التي تنص على أن للمحكمة عند الحكم بالإدانة أن تأمر في الحالات 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 وأن لا تتجاوز مده التعليق شهرا واحدا. (3)

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص 146 .

(2) أنظر المادة 9 مكرر 1 ق ع ج " يتمثل الحرمان من ممارسة الحقوق الوطنية و المدنية و العائلية في :
1- العزل او الإقصاء من جميع الوضائف و المناصب العمومية التي لها علاقة بالجريمة .
2- الحرمان من حق الانتخاب أو الترشح أو حمل أي وسام .
3- عدم الاهلية لان يكون مساعدا محلفا او خبيرا او شاهدا على اي عقد او شاهدا اما القضاء الا على سبيل الإستدلال.
4- الحرمان من الحق في حمل الأسلحة و في التدريس و في إدارة مدرسة أو الخدمة في مؤسسة التعليم بوصفه أستاذا أو مدرسا أو مراقبا.
5- عدم الأهلية ليكون وصيا أو قيما.
6- سقوط الولاية كلها أو بعضها .

(3) أنظر المادة 18 ق ع ج.

الفرع الثاني : الظروف المشددة للعقاب و المعفية للعقاب لجريمة الإبتزاز عبر الوسائل الإلكترونية

أولا: الظروف المشددة للعقاب لجريمة الإبتزاز عبر الوسائل الإلكترونية

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 أن يحكم بكل العقوبتين الحبس والغرامة معا .

الأصل في عقوبة جريمة الإبتزاز الإلكتروني، أن المنظم السعودي لم يحدد لها حد أدنى واكتفى بوضع حد أعلى لها لا يجوز تجاوزه ومع ذلك فقد جعل المنظم حالات تقع فيها جريمة الإبتزاز عن طريق التقنية شدد فيها بالعقاب بحيث لا تقل عن النصف 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 نظاما فلا يتجاوز السجن مدة السنة ولا يزيد في الغرامة المالية على 500,000 ريال. (1)

ولقد نص المنظم على حالات جعل العقوبة فيها مشددة وذلك كما جاء في نص المادة الثامنة على أنه :

(لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى اذا اقترفت الجريمه بأي من الحالات التالية :

1- ارتكاب الجريمة من خلال عصابة منظمة.

2- شغل الجاني وظيفة عامة واتصال الجريمة الوظيفة أو ارتكابه الجريمة مستغلا سلطانه أو نفوذه.

3- التغرير بالقصر ومن في حكمهم واستغلالهم في جريمة الإبتزاز.

4- صدور أحكام محلية ، أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة. (2)

والعلة في تشديد العقوبة فإذا ارتكبت الجريمة من خلال تنظيم إجرامي حيث استشعر المنظم خطورة الفعل على المجتمع ، وذلك من خلال ممارستها في إطار إجرامي منظم يؤدي إلى استفحال هذه الجريمة كما تشدد في حال ارتكبها موظف عمومي ، فالمفروض أنه شخص مختار بعناية وفيه توضع ثقة الدولة فيجب أن يكون فوق كل شبهة كذلك إذا ارتبط الإبتزاز الإلكتروني بالتغرير بالقصر وأن تقع الجريمة ضد فئه يحق حمايتهم جنائيا بقدر أكبر من الفئات الأخرى كما يعتبر موجبا لتشديد صدور أحكام محلية ،أو أجنبية سابقة في حق المبتز في جرائم مماثلة ، ويبدو أن سبب التشديد هذا يرجع لنفس فكرة التشديد حال العودة والخطورة الإجرامية.

---

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص136 .

(2) أنظر المادة 8 نظام مكافحة الجرائم المعلوماتية السعودي.

بالإطلاع على قانون مكافحة جرائم تقنية المعلومات الإماراتية تبين لنا أن المشرع شدد العقوبة في نفس نص المادة16 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 كل من ابتز شخص أخر بحمله على القيام بفعل أو الإمتناع عنه و ذلك باستخدام شبكة المعلوماتية أو وسيلة تقنية المعلومات وتكون العقوبة بالسجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية ،أو باسناد أمور خادشة للشرف ، و الإعتبار.)(1)

إلا أنه لم يتضح من التشديد أن كان يقع منفردا أم يمكن جمعه مع الغرامة في حدها الأعلى 500,000درهم وبذلك يضع المشرع الإماراتي ردعا قويا حين يتصل التهديد بارتكاب جناية وأن يكون التهديد له علاقه باسناد أمور تمس الشرف والإعتبار.

أما المادة 42 تنص على انه : (تقضي المحكمة بإبعاد الأجنبي الذي حكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوصة عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها). (2) فيتم إبعاد الأجنبي بعد تنفيذه العقوبة الأصلية.

ثانيا: الظروف المعفية من العقاب لجريمة الإبتزاز عبر الوسائل الإلكترونية

إن الإعفاء من العقوبة ليس له علاقة بالسياسة الجنائية أو علاقة بالقواعد العامة للمسؤولية الجزائية لمرتكب الجريمة فقد نص المنظم السعودي م المادة 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 ، و قبل وقوع الضرر وإن كان الإبلاغ بعد العلم بالجريمة تعين الاعفاء حيث يكون من شأن الابلاغ ضبط باقي الجناة في حال تعددهم أو الأدوات المستخدمة في الجريمة.) (3)

كما تنص المادة 12 من القانون رقم 63 لسنة 2015 في شأن مكافحه جرائم تقنية المعلومات على أنه : (للمحكمة ان تعفي من العقوبة كل من بادر من الجناة بابلاغ السلطات المختصة بالجريمة قبل علمها بها وقبل البدء في تنفيذ الجريمة فإن كان الإبلاغ بعد العلم بالجريمة وقبل البدء في التحقيق تعين الإعفاء من العقوبة ان يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم.) (4)

---

(1) أنظر المادة 16 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الاماراتي.

(2) أنظر المادة 42 من القانون نفسه.

(3) أنظر المادة 11 نظام مكافحة الجرائم المعلوماتية السعودي.

(4) أنظر المادة 12 قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي.

ولعل السبب الذي دفع المشرع في كل من المملكة العربية السعودية والكويت الى تقرير هذا الإعفاء هو الرغبه في السيطره على تفاقم جريمة الإبتزاز الإلكتروني بتشجيع فئة من مرتكبيها عن طريق الإعفاء إلى إبلاغ السلطات قبل العلم بالجريمة وقبل وقوع الضرر، كما اشترطت أنه حتى يؤدي الإعفاء دوره يجب أن يكون من شأن هذا الإبلاغ أن تقوم السلطات بضبط باقي الجناة في حالة تعددهم وأيضا ضبط الأدوات المستخدمة في الجريمة كما أن سلطة تحديد العقاب تكون للمحكمة المختصة فالإعفاء من العقوبة ليس مانعا من موانع المسؤولية ، وإنما يهدف في السياسة الجنائية لفرض مزيد من السيطرة على الجريمة وتشجيعا لبعض الأطراف للإبلاغ والاستفادة من الإعفاء لخطورة هذه الجريمة ومحاولة السلطات إغراء فاعليها بالإعفاء عن العقوبة حال الإقرار بمعلومات عنها قبل اتصال علم السلطات بها.

وبالإطلاع على م 45 من القانون الاتحادي الإماراتي(1) : (تقضي المحكمة بناءا على طلب من النائب العام بتخفيف العقوبة أو بالإعفاء منها عن من أدلى من الجناة الى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقا لأحكام هذا المرسوم بقانون متى أدى ذلك الى الكشف عن الجريمة ومرتكبها أو إثباتها عليهم أو القبض على أحدهم .)

أما المادة 44 من نفس القانون : (تعتبر الجرائم الواردة في المواد(4 ,24 ,26 ,28 ,29 ,30 ,38) من هذا المرسوم بقانون من الجرائم الماسة بأمن الدولة. (2)

كما تعتبر من الجرائم الماسة بأمن الدولة أي جريمة منصوص عليها في هذا المرسوم بالقانون إذا ارتكبت لحساب أو مصلحة دولة أجنبية، أو أي جماعه إرهابية ،أو مجموعة ،أو جمعية ،أو منظمة ،أو هيئة غير مشروعة.

في النص الإماراتي إن سلطة تقدير الإعفاء هي المحكمة المختصة، كما أنه أضاف بجانب الإعفاء التخفيف من العقوبة وذلك في الجرائم الخاصة بالإعتداء أو المساس بأمن الدولة ، أما جريمة الإبتزاز الإلكتروني لم يرد لها هذا النص بالإعفاء أو التخفيف من العقوبة مقررا بذلك عدم إستحقاق مرتكب جريمة الإبتزاز الإلكتروني أي إعفاء أو تخفيف .

ويبدو أن المشرع الإماراتي قصد من تقرير الإعفاء أو التخفيف من العقوبة لبعض الجرائم ذات صلة بأمن الدولة وذلك بنفس منطق الحرص على كشف الجريمة قبل حدوث أضرار وكذلك تشجيعا لأطرافها للفوز بالإعفاء ،أو التخفيف أو، القبض على باقي الأفراد الفاعلين المنفذين للجريمة وهي سياسة لكل مشرع يقوم بإنتهاجها لمصلحة خطته في حفظ الأمن والضرب بيد من حديد على كل المجرمين.

(1)أنظر المادة 45 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

(2) أنظر المادة 44 من نفس القانون .

الفرع الثالث : عقوبة الشروع والاشتراك في جريمة الإبتزاز عبر الوسائل الإلكترونية

أولا : عقوبة الشروع في جريمة الإبتزاز الإلكتروني

يقصد بالشروع البدء في التنفيذ في الجريمة التي يعقد الجاني 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 انها 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) . (1)

من خلال نص المادة يتضح 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 .(2)

وهي مرحلة التفكير والتصميم ومرحلة التحضير كأن يقوم الجاني بشراء وسائل الإبتزاز كأن يشتري هاتف نقال بقصد الإبتزاز فهنا لا يعاقب الشخص على هذا الفعل ،أما مرحلة التنفيذ فهنا تعتبر أفعال الجاني مجرمة وليس من الضروري أن يكون الجاني قد بدأ في تنفيذ ركن الجريمة المادي بل يكفي أن يكون الفعل المقصود به تنفيذ الركن المادي .

وينقسم الشروع الى قسمين : شروع تام وشروع ناقص، فالشروع التام يقصد به قيام الجاني بارتكاب جريمة كاملة ولكن النتيجة لم تتحقق وذلك كقيام شخص هدد آخر للحصول على أموال بعد حصوله على مقاطع مصورة له تشينه ، و قبل أن تتحقق النتيجة الإجرامية قبض عليه .(3)

أما الشروع الناقص فيقصد به أن النشاط الاجرامي لم يتم بشكل كامل حيث أن الجريمة هنا ناقصة كأن تتمكن السلطات من القبض على المبتز بعد حصوله على صور لشخص قبل أن يقوم بتهديده. (4)

---

(1) أنظر المادة 10 نظام مكافحة الجرائم المعلوماتية السعودي.

(2) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص 141 .

(3) عبد الرحمن توفيق أحمد، شرح قانون العقوبات ، القسم العام وفق أحدث التعديلات ، ط 3 ، دار الثقافة و النشر و التوزيع ، عمـــان 2012 ،ص159 .

(4) المرجع نفسه، ص 153 .

ويشترط لقيام الشروع توافر ركنين هما : البدء في التنفيذ وعدم إتمام الجريمة لأسباب خارجة عن إرادة المبتز ، فالبدء في التنفيذ هو مرحلة تعقب التفكير والتحضير للجريمة وهو غير معاقب عليه وهو مرحلة تسبق البدء في التنفيذ المعاقب عليها.

أما عدم إتمام الجريمة لأسباب خارجة عن إرادة الفاعل من ذلك قيام المبتز بتهديد ضحيته بحصوله على صور فاضحة له، وذلك بعد اختراق هاتفه النقال وحصوله على الصور وإبلاغ ضحيته بذلك إلا أنه و قبل التهديبد تعطل هاتفه النقال الذي سيرسل إبتزازه عن طريقه فهنا الجريمة وقفت بسبب خارج إرادة الجاني. فقد جعل المنظم السعودي العقوبة على الشروع في مرحلة الإبتزاز الإلكتروني بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة وعليه قد جاء على المنظم العقوبة هنا في حدها الأدنى سلطة تقديرية للقاضي فيكون يوما واحدا ولا يزيد على ستة أشهر والغرامة المالية لا تقل عن ريال واحد ولا تزيد عن 250,000ريال . (1)

وبالإطلاع على المادة 40 من القانون الإتحادي الإماراتي التي تنص على أنه : (لا يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة) .(2)

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

فالمشرع الإماراتي ضمن كلمة إن الشروع على الجنح ، ومنه عقوبة جريمة الإبتزاز الإلكتروني المعتبرة جنحة في القانون الإماراتي .

و من نص المادة يفهم أن الجرائم المعتبرة جنايات في هذا القانون الشروع فيها عقوبته تختلف عن الجنح وليس هناك إختلاف في القواعد الخاصة بالشروع في النظام السعودي والقانون الإماراتي .

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 . (3)

---

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص142 .

(2) أنظر المادة 40 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الإماراتي.

(3) أنظر المادة 303 مكرر ، م 303 مكرر 1 ق ع ج .

الشروع في جريمة الإبتزاز الإلكتروني يتحقيق بالتهديد بإفشاء معلومات أو صور أو مقاطع فيلمية أو أي بيانات خاصة للمجني عليه ، حتى وإن تراجع المبتز عن إكمال جريمته لسبب خارجي طالما أن التهديد بنشر الأسرار قد صدر منه ووقع في نفس المجني عليه موضع التأثير والرهبة التي جعلته يعتقد ان المبتز سينفذ تهديده لا محالة ، وهو الهدف الذي تحقق بالقاء الرعب في قلب المجني عليه . والشروع في الجريمة هنا يتحقق طالما كان الركن المادي فيها قد شرع في تنفيذه وتوافر القصد الجنائي. (1)

ثانيا : عقوبة الإشتراك في جريمة الإبتزاز عبر الوسائل الإلكترونية

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 .

ولقد إتبع المنظم القواعد العامة المقررة في الاشتراك بالتسبب في الجريمة حيث يقع بالتحريض أو الإتفاق أو المساعدة. (2)

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 غذا وقعت الجريمة بناءا على هذا التحريض أو المساعدة أو الاتفاق بما لا يتجاوز الحد الأعلى للعقوبة المقرره لها ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة إذا لم تقع الجريمة الاصلية. (3)

الملاحظ أن المنظم السعودي أقر عقوبة للشريك 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) عبد الرحمن توفيق احمد ، المرجع السابق ، ص 150 .

(2) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص 143 .

(3) أنظر المادة 9 نظام مكافحة الجرائم المعلوماتية السعودي .

وتتعدد صور الإشتراك غير المباشر في الجريمة حسب المادة 9 من النظام السعودي كالتالي :

1/ **الإعانة:** وهي إعانه الغير على ارتكاب الجريمة دون الإشتراك في تنفيذ ركنها المادي كتهيئة المجني عليه وتقديمه للمبتز وتجهيز البرامج المستخدمة لاختراق جهاز الضحية ولكنه لا يشترك في قيام جريمة الإبتزاز الإلكتروني .

2/ التحريض: وهو خلق الفكره وزرعها في ذهن الجاني وترتيب الجريمة والإغراء بتنفيذها وارتكابها والتخطيط المسبق لها بحيث تمكن نسبة الجريمة وعزوها الى التحريض والمؤامرة.

ورغم كل ذلك يبقى بمعزل عن الركن المادي لعدم القيام المباشر بالفعل الجرمي واكتفاءه بالتحريض فقط.

3/الإتفاق: وهو اتفاق إرادة أكثر من جاني على ارتكاب الجريمة باستدراج الضحية وجعلها عرضة للإبتزاز وكذا اتفاق أكثر من جاني للقيام وتقسيم مراحل الجريمة، فلا يشتركون في الركن المادي للجريمة وإنما يشتركون في الإتفاق على الجريمة نفسها . (1)

بالنسبة لقانون مكافحة جرائم تقنية المعلومات الإماراتي نجد أنه لم ينص صراحة على عقاب الشريك كما لم يفرد نصا خاصا بالعقاب على المساهمة الجنائية لجريمة الإبتزاز الإلكتروني ، نفس الأمر بالنسبة للمشرع الجزائري وفي هذه الحالة تطبيق القواعد العامة في المساهمة الجنائية (المواد 41،42،44،45). (2)

(1) محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص143 .

(2) أنظر المواد(41 , 42 , 44, 45) ق ع ج .

ملخص الفصل الأول:

تناول الفصل الأول من الدراسة الإطار الموضوعي لجريمة الإبتزاز الإلكتروني كصورة من صور الجريمة الإلكترونية ، فتم من خلال هذا الفصل التطرق الى لماهية الإبتزاز الإلكتروني لغويا واصطلاحا و فقهيا كما تم التطرق إلى أنواع الإبتزاز الإلكتروني بالنظر لشخص الضحية و الهدف المرجو من المجني عليه ثم تعرضنا الى وسائل الإبتزاز الإلكتروني : الحاسب الآلي، برامجه،الأنترنت و الهاتف النقال.

ثم تجريم ظاهرة الإبتزاز الإلكتروني من خلال التعرض الى أركان الجريمة(الشرعي ، المادي ، و المعنوي).

و في الأخير العقوبات المقررة لجريمة الإبتزاز الإلكتروني في بعض التشريعات العربية (الأصلية، و التكميلية و عقوبة الشروع و الإشتراك).

الفصل الثاني:الإطار الإجرائي لجريمة الإبتزاز عبر الوسائل الإلكترونية

المبحث الأول:التحقيق في جريمة الإبتزاز عبر الوسائل الإكترونية

المبحث الثاني: الإثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية

بالرغم من خصوصية الجريمة الإلكترونية، و منها جريمة الإبتزاز الإلكتروني إلا أنها ما تزال تشكل سلوكا محضورا جرمه المشرع الوضعي، ونص على عقوبته مشددا هذه العقوبة في أحوال معينة و لأسباب نص عليها.

و تمر هذه الجريمة و بعد وقوعها بمراحل،مرحلة جمع الإستدلالات و التحقيق الجنائي، والذي يهدف إلى اكتشاف الجريمة و مرتكبها أو مرتكبيها، فكل هذا البحث و التحقيق تكون أهدافه هو الوصول الى الحقيقة القانونية التي تحتاج الى دليل تتأكد معه نسبة التهمة الى المتهم بها، أو نفي الجريمة عنه لكي تكتمل خصوصية هذه الجريمة فلابد من القول بأن الدليل في الجريمة الإلكترونية و بالأخص في جريمة الإبتزاز الإلكتروني و هو دليل غير تقليدي، حيث يرتبط بالحاسوب و أجهزة الهواتف الذكية و ملحقاتها و البرامج و التطبيقات التكنولوجية، ففي جريمة الإبتزاز الإلكتروني الدليل ليس مضروفا فارغا لطلق ناري و ليس خصلة شعر من الضحية بل هو رموز و شيفرات و أجهزة و عناوين الكترونية، وهذه الأدلة التي يجوز أن يقبلها في حالة معينة و يحظر عليه أن يقبل أدلة سواها.

و نتناول في هذا الفصل التحقيق و الإثبات في جريمة الإبتزاز الإلكتروني و الصعوبات التي تواجه السلطات في التحقيق، و الإثبات من خلال مبحثين ، المبحث الاول : التحقيق في جريمة الإبتزاز عبر الوسائل الإلكترونية و المبحث الثاني : الإثبات في جريمة الإبتزاز عبر الوسائل الالكترونية.

المبحث الأول: التحقيق في جريمة الإبتزاز عبر الوسائل الإلكترونية

إن اختلاف الجرائم الإلكترونية بشكل عام عن الجرائم التقليدية يلقي العبء على سلطات التحقيق بضرورة تطويع إجراءات التحقيق كي تتلائم مع التحقيق في الجرائم الإلكترونية بصفة عامة و في الإبتزاز الإلكتروني بصفة خاصة.

فيضل نظام الإجراءات الجزائية في قواعد التحقيق هو السائد مع ضرورة اعتبار الفوارق الموضوعية في التحقيق .

ونظرا لخصوصية جريمة الإبتزاز الإلكتروني فإن هناك صعوبات تثار أثناء التحقيق في هذه الجريمة و سنتعرض لهذه النقاط من خلال مطلبين، لأول يتناول إجراءات التحقيق في جريمة الإبتزاز عبر الوسائل الإلكترونية و المطلب الثاني يتناول الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز عبر الوسائل الإلكترونية .

المطلب الأول: إجراءات التحقيق العامة و الخاصة في جريمة الإبتزاز عبر الوسائل الإلكترونية

الفرع الأول :إجراءات التحقيق العامة في جريمة الإبتزاز عبر الوسائل الإلكترونية

تتشابه إجراءات التحقيق في الجريمة الإلكترونية مع إجراءات التحقيق في الجريمة التقليدية فكلاهما، يحتاج الى المعاينة و التفتيش و الإستجواب و جمع وسائل الإثبات و فحصها و المحافظة عليها من العبث بها أو ضياعها.(1)

فقد تكون إجراءات التحقيق عملية كالتفتيش أو فنية كمضاهاة البصمات ،أو برمجية لتحديد كيفية الدخول الى المعطيات المخزنة في أجهزة الحاسوب.

(1) داليا عبد العزيز، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي،دراسة مقارنة، مجلة البحث العلمي ، العدد 25 ،2018 .

أولا:الخبرة الفنية و تدريب 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 و الدولي كآلية من آليات التعاون ، فالكوادر قد يستعينون بالخبراء و بعد تدريبهم في المجال المعلوماتي يصبحون خبراء في عملهم .

أ:الخبرة الفنية

الخبرة هي وسيلة لتحديد التفسير الفني و التقني، بالإستعانة بالمعلومات العلمية فهي مستقلة عن الدليل القولي أو المادي و إنما هي تقييم لهذا الدليل. (1) و قد تعتمد الخبرة من أجل كشف الجريمة المعلوماتية و لابد ان تتماشى هذه الخبرة مع خصوصية الجريمة الإلكترونية .

و قد تعمل بعض البلدان على إعادة تأهيل بعض المجرمين المعلوماتيين من أجل الإستفادة من خبرتهم في الإختراق .

و على الخبير أن يتمتع بمؤهلات عالية و مقدرة فنية في تركيب الكمبيوتر و شبكة الأنترنت و التعامل مع الجريمة التي خلفتها التقنية الحديثة، و كيفية عزل النظام المعلوماتي و الحفاض على الأدلة دون تلف. (2)

المشرع الجزائري أجاز للمحقق الإستعانة بالخبرة ، و منه يطلب خبير في أي وقت الى أن ينتهي التحقيق و هو أمر وجوبي في مجال الجرائم المعلوماتية التي تتطلب خبرة فنية بحتة لا يكشف غموضها إلا المتخصصون.

و من خلال نص المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها التي تنص على انه : (...يمكن للسلطات المكلفة بتفتيش المنظومة المعلوماتية التي تتظمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها).

(1) رابحي عزيزة،الأسرار المعلوماتية و حمايتها الجزائية،أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص،جامعة أبو بكر بلقايد ، تلمسان، 2018 ،ص271 .

(2) المرجع نفسه .

و الجدير بالذكر ان المشرع الجزائري قرر الحماية اللازمة للخبير إذا ما سببت له المعلومات التي أفاد بها للقضاء أي خطر حول حياته، أو سلامته الجسدية ،أو سلامة أفراد عائلته ،أو اقاربه ،أو مصالحه الأساسية ، وذلك بموجب الأمر 02/15 المعدل و المتمم لقانون الإجراءات الجزائية بموجب المواد 65 مكرر الى 65 مكرر 28.

ب:تدريب الكوادر

طبيعة الجرائم الواقعة على الأسرار المعلوماتية تقتضي معرفة بنظم المعلوماتية و كيفية تشغيلها من قبل مستخدميها، ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري و التحقيق في مجال الجرائم المعلوماتية .

ففي الجزائر و، على مستوى جهاز الشرطة أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة و مخبرين جهويين في كل من قسنطينة و وهران، أما على مستوى الدرك الوطني للأدلة الجنائية و علم الإجرام قسم الإعلام و الإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية .(1)

كما تسعى الأجهزة الأمنية المعنية بالتحقيق في استقطاب المتخصصين و الكفاءات في المجال المعلوماتي لضمهم إليها ليكونوا ضمن كوادرها و الإستفادة منهم.

و التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المعلوماتية قد يكون بين الدول و أجهزة العدالة لديها، فمثلا يتم إرسال أعضاء النيابة العامة من مختلف الدرجات في برامج خارجية و ذلك بالتعاون معى أجهزة النيابة العامة في الدول الأخرى و الهيئات الدولية بهدف الإطلاع على أحدث الأنظمة المقارنة من خلال عقد ندوات و مؤتمرات وورشات عمل جماعي متخصصة في مواجهة تلك الجرائم، تعقد على المستوى الدولي أو الإقليمي .

حيث نسلط الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال مناقشة أبعادها،أخطارها و وسائل الوقاية بأساليب ووسائل تفوق تلك التي يستعملها مرتكبوها، فالتعاون الدولي في مجال تدريب

(1) رابحي عزيزة،المرجع السابق، ص273 .

الكوادر العاملين في أجهزة العدالة الجزائية و المعنيين بمكافحة الجريمة على المستوى الدولي و الإقليمي يستهدف توحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة ، من خلال تبادل الخبرة . (1)

ثانيا: الإنتقال و معاينة مسرح الجريمة المعلوماتية

فالإنتقال هو:ذهاب مأموري الظبط القضائي، أو المحقق الجنائي الى مكان ارتكاب الجريمة ،حيث توجد آثارها و أدلتها.

أما المعاينة فهي تخص مكان أو شيئ أو شخص له علاقة بالجريمة وإثبات حالته، فالمعاينة تستلزم الإنتقال إلى محل الجريمة ،أو الواقعة، أو إلى أي محل آخر توجد به اشياء أو آثار يرى المحقق أن لها صلة بالجريمة غير أن المحقق قد ينتقل الى غرض آخر غير المعاينة كالتفتيش مثلا، و في جريمة الإبتزاز الإلكتروني يقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، و تشمل الرسائل المرسلة منه أو التي يستقبلها و كافة الإتصالات التي تمت من خلال الكمبيوتر أو الأنترنت، و المعاينة جوازية للمحقق ، شأنها شأن سائر إجراءات التحقيق فهي متروكة لتقديره، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في الجريمة التقليدية و ذلك لسببين:

– الجرائم التي تقع على نظم المعلومات قلما يترتب على ارتكابها آثار مادية .

– قد يتردد على مسرح الجريمة عدد كبير من الأشخاص خلال الفترة الزمنية التي تتوسط ارتكاب الجريمة واكتشافها مما يغير ،أو يتلف الآثار المادية ،أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة.

و كي تكون المعاينة لها فائدة في كشف الحقيقة عنها و عن مرتكبها فإنه ينبغي مراعاة عدة قواعد و ارشادات فنية ابرزها ما يلي:

– تصوير الحاسب و الاجهزة الطرفية المتصلة به و المحتويات و الأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب الآلي و ملحقاته ، و يراعي تسجيل وقت، و تاريخ و مكان التقاط كل صورة .

(1) رابحي عزيزة،المرجع السابق،ص274 .

– ملاحظة الطريقة التي تم بها إعداد النظام و الآثار الإلكترونية خاصة السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الإتصال و نوع الجهاز الذي تم عن طريقه الولوج الى النظام و موقع الإتصال أو الدخول معه في حوار.(1)

– ملاحظة و إثبات حالة التوصيلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة و التحليل حين عرض الأمر على القضاء .

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء إختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن ان تتسبب في محو البيانات المسجلة. (2)

– التحفظ على محتويات سلة المهملات من الأوراق الملقاة ، أو الممزقة و أدوات الكربون المستعملة و الشرائط ، و الأقراص الممغنطة ، و غير السليمة أو المحطمة و فحصها و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

– التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع و مضاهاة ما قد يوجد من بصمات ، و يلاحظ أن الآثار المعلوماتية ، و الرقمية المستخلصة من اجهزة الكمبيوتر من الممكن أن تكون ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة و البريد الإلكتروني،الفيديو الرقمي، الصوت الرقمي،غرف الدردشة،المحادثات،الملفات المخزنة في الكمبيوتر،الصور المرئية.

و لفهم المعاينة لابد من التعرف على المقصود من مسرح الجريمة في الجريمة الإلكترونية.

عموما لم تهتم معظم التشريعات الجنائية المعاصرة بتعريف مسرح الجريمة أو وضع معايير ثابتة لتحديد نطاقه المكاني، فمعظم التشريعات تعبر مسرح الجريمة بمحل الواقعة و يتفق معظم الفقه على أن مسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها .

و يرجع عدم الإهتمام التشريعي بتعريف مسرح الجريمة إلى إعتبارين:

– معظم القوانين الجنائية لا ترتب آثار قانونية بالبطلان على تجاوز الحدود المكانية بما هو معروف بمصطلح مسرح الجريمة عند إجراء معاينة تاركا للمحقق السلطة تقديره .

– لا تقوم بشأن تحديد المجال الميداني لمسرح الجريمة ضاربة بين أطراف الدعوى العمومية .

(1) هشام فريد رستم،الجوانب الإجرائية للجرائم المعلوماتية ،دط ،مكتبة الآلات الحديثة،أسيوطن مصر، 1994 ،ص 59 .

(2) صغير يوسف،المرجع السابق،ص86 .

فلا يجوز لأي طرف من أطراف الدعوى العمومية أن يعترض على إجراء معاينة لمسرح الجريمة ،أو طريقة ،أو أسلوب تنفيذها، أو مجالها الميداني فهي إجراء يستهدف التعرف على أبعاد الجريمة ، و أركانها، و ظروفها ، و كشف الحقيقة بشأنها و ليست إجراء موجه ضد شخص معين تمس بحرمة حياته الخاصة حتى ينسب له حق الطعن فيه بالبطلان.

و مسرح الجريمة في جريمة الإبتزاز الإلكتروني هو مسرح سيبراني يقع داخل بيئة الحاسوب ،أو ما في حكمه ، و يكون في البيانات الرقمية التي تتواجد و تنقل داخل بيئة الحاسوب و شبكاته و في ذاكرته و في الاقراص الصلبة الموجودة بداخله ، و التعامل مع الأدلة الموجودة في هذا المسرح لا يتم إلا على يد خبير متخصص في التعامل مع هذا النوع من الأدلة الرقمية.

ثالثا: التفتيش

التفتيش في قانون الإجراءات الجزائية هو البحث عن شيئ يتصل بجريمة وقعت، و يفيد في كشف الحقيقة عنها، و عن مرتكبيها, و قد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة .

و قد أحاط القانون التفتيش بضمانات، فمحل التفتيش أما أن يكون مسكنا أو شخصا، و قد يكون متعلقا بالمتهم أو بغيره و هو في كل أحواله جائز مع الإختلاف في بعض الشروط .

التساؤل المطروح كيف نكون بصدد تفتيش عن حيثيات جريمة الإبتزاز الإلكتروني و مدى قابلية مكونات و شبكات الحاسب الآلي للتفتيش.

أ: مدى خضوع المكونات المادية للحاسب الآلي للتفتيش

تفتيش المكونات المادية للحاسب الآلي بحثا عن شيئ ما يتصل بجريمة من جرائم الأنترنت يفيد في كشف الحقيقة عنها و عن مرتكبيها و تخضع للإجراءات القانونية الخاصة بالتفتيش، كما أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه و هل هو مكان عام أم خاص.

و للمكان أهمية كبيرة فإذا كانت في مسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يكون فيها تفتيش مسكنه و بنفس الضمانات و الإجراءات المقررة قانونا مع مراعات

(1) صغير يوسف،المرجع السابق،ص76 .

التمييز بين ما اذا كانت مكوانت الحاسب الآلي المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أو متصلة بحاسب آلي آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم.

فلو وجد شخص يحمل مكونات الحاسب الآلي المادية ،أو كان مسيطرا عليها ،أو حائزا لها في مكان ما من الأماكن العامة سواء كانت عامة بطبيعتها كالطرق العامة، أو الميادين ،أو الشوارع ،أو عامة بالتخصيص كالمقاهي ، و المطاعم ، و السيارات العامة فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها التفتيش للأشخاص و بنفس الضمانات و القيود المنصوص عليها في هذا المجال . (1)

فالتفتيش على المكونات المادية للنظام المعلوماتي لا إشكال فيه ، حيث نصت المادة 44 من قانون الإجراءات الجزائية الجزائري ، ورد فيه بأن التفتيش يكون على الأشياء و هي كلمة تنصرف على الأرجح على المكونات المادية، مع الأخذ بعين الإعتبار الإجراءات الخاصة بظبط هذه الأجهزة لحساسيتها و إمكانية إتلافها.

و الجدير بالذكر فإذا كانت المكونات المادية للحاسب الآلي، موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه ،و بنفس الضمانات المقدرة قانونا، فالقانون الجزائري في نص المادة 64 من ق إ ج ج .(2)

والتي قيدت ممارسة هذا الإجراء بالشروط التالية:

– الحصول على إذن تفتيش من وكيل الجمهورية ،واستضهار هذه المذكرة قبل بدء العملية و تتضمن مذكرة التفتيش البيانات التالية : وصف الجريمة محل البحث و التحري، عنوان الأماكن التي سيتم تفتيشها ،عدم ذكر هذه البيانات يؤدي الى بطلان إجراء التفتيش.

– أن يجري التفتيش بحضور صاحب المسكن ، و إن تعذر وجب تعيين ممثل له و إن تعذر الأمر كذلك يقوم ضابط الشرطة القضائية بتعيين شاهدين لا علاقة لهما. (3)

– أن يجري التفتيش بعد الساعة الخامسة 05 صباحا ، و قبل الساعة 08 مساءا غير أنه يجوز التفتيش في أي وقت إذا طلب صاحب المسكن ذلك و إذا سمعت نداءات من داخل المسكن كما يجوز تفتيش

(1) صغير يوسف ، المرجع السابق، ص77 .
(2) أنظر المادة 64 ق إ ج ج.
(3) أنظر المادة 45 ق إ ج ج .

الفنادق ، و المحلات ، و النوادي ، و المقاهي، و أماكن المشاهدة العامة (المسرح,السينما) و كل مكان مفتوح للجمهور في أي ساعة ليلا و نهارا.

هذا و قد استثنى عن القاعدة العامة في المادة 64 السالفة الذكر في فقرتها الثالثة ، تطبيق هذه الضمانات على بعض الجرائم ، محيلا ذلك الى المادة 47 في الفقرة 3 حيث أجازت أن يتم التفتيش و المعاينة في المساكن كل ساعة ليلا و نهارا ، و دون التقيد لشرط حضور صاحب المسكن أو ممثليه إذا تعلق الأمر بالجرائم التالية : "...الجرائم الماسة بأنظمة ممارسة المعالجة الآلية للمعطيات. (1)

ب:مدى خضوع مكونات الحاسب المعنوية للتفتيش

أثار تفتيش المكونات المنطقية للحاسب الآلي جدلا كبيرا لدى الفقه بشأن جواز تفتيشها. فذهب جانب من الفقه الى جواز تفتيشها ولابد من ضبط البيانات الإلكترونية بمختلف أشكالها المحسوسة و غير المحسوسة.

أما جانب آخر من الفقه فيرى عدم انطباق المفهوم المادي على بيانات الحاسب الآلي غير المرئية أو غير الملموسة ، لذا فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن يفتش الحاسب الآلي لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي ، لأن الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الإتصالات ترتكز على البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي. (2)

أما المشرع الجزائري فإنه استجاب للرأي القائل بأن طبيعة المعلومات المعالجة تتطلب قواعد خاصة و على هذا الأساس أجاز تفتيش المعطيات و لكن بموجب نص جديد و هو المادة 05 من القانون 04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، حيث سمح

(1) رابحي عزيزة،المرجع السابق،ص280 .

(2) صغير يوسف،المرجع السابق،ص78 .

لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 من هذا القانون ، و من بين هذه الحالات توفر معلومات عن احتمال الإعتداء على منظومة معلوماتية على نحو يهدد النظام ،أو الدفاع الوطني، أو مؤسسات الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المخزنة فيها و كذا منظومة تخزين معلوماتية .(1)

ج: مدى خضوع شبكات الحاسب الآلي للتفتيش

عقدت طبيعة التكنولوجيا الرقمية التحدي أمام أعمال التفتيش فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة و بعيدة تماما عن الموقع المادي للتفتيش، و إن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها ، و قد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو بلد آخر مما يزيد من تعقيد الإجراءات المتعلقة بالجريمة خاصة العابرة للحدود و يزيد من أهمية تبادل المساعدة القانونية. (2)

و في هذه الأيام يتم التمييز بين ثلاثة احتمالات:

الإحتمال الأول : إتصال حاسب المتهم بحاسب ،أو نهاية طرفية موجودة في مكان آخر داخل الدولة فهناك من الدول من وجدت حلا للإشكالية المتعلقة بمدى جواز امتداد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم أو المشتبه فيه أم على جهازه فقط؟

بالنسبة للمشرع الجزائري، حيث نصت المادة 05 في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعوا للإعتقاد بأن المعطيات المبحوث عنها في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة ،أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك. (3)

(1) رابحي عزيزة،المرجع السابق،ص282 .
(2) صغير يوسف،المرجع السابق،ص79 .
(3) رابحي عزيزة،المرجع السابق،ص282 .

الإحتمال الثاني: ايصال حاسب المتهم بحاسب ،أو نهاية طرفية موجودة في مكان آخر خارج الدولة، فطبقا لهذا الإحتمال يمكن أن يقوم مرتكبوا الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكة الإتصال البعيدة بهدف عرقلة سلطات الإدعاء في جمع الأدلة .

وقد أجاز المشرع الجزائـــري تفتيش الأنظمة و لو كانت خارج إقليم الدولة و ذلك بموجب المادة 5 في فقرتها 03 من القانون 04/09 حيث أجاز النص الحصول على المعطيات المبحوث عنها و المخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني، و التي يمكن الدخول إليها إنطلاقا من المنظـومة الأولى و ذلك بمساعدة السلطات الأجنبيـــة المختصة طبقا للإتفاقيات الدوليـــــة ذات الصلة وفقا لمبـدأ المعاملة بالمثل. (1)

و حسب م 2/16 من نفس القانون : من واجب سلطات التحقيق الجزائرية أن تقدم جميع التسهيلات لمراقبة الإتصالات و تفتيش المنظومات المعلوماتية الموجودة على التراب الوطني متى طلب منها ذلك مع مراعاة مبدأ المعاملة بالمثل ، و الإتفاقيات الدولية. (2)

و حسب المادة 18 من نفس القانون (3) أورد المشرع الجزائري استثناءات على طلب المساعدة القضائية و هي الحالة التي يمكن أن تؤدي الى المساس بالسيادة الوطنية ،أو النظام العام كما اشترط المشرع الجزائري قبول المساعدة القضائية بضرورة الالتزام بالمحافظة على سرية المعلومات المبلغة و بشرط عدم استعمالها في غير الأغراض التي أدت الى تجميعها.

الإحتمال الثالث: التنصت و المراقبة الالكترونية لشبكات الحاسب الآلي ، فالتنصت و الأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا مثلما هو الأمر بالنسبة للمشرع الجزائري في المادة 04 الفقرة ج من القانون 04/09 أجاز النص استثناءا المراقبة الالكترونية للوصول الى الحقيقة و اشترط ان تكون هي الحل الوحيد للوصول الـى الحقيقة .(4)

(1) أنظر المادة 5.ق 04/09 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها .
(2) أنظر المادة 16.ق 04/09 من القانون نفسه.
(3) أنظر المادة18 ق 04/09 من القانون نفسه.
(4) أنظر المادة4. ق 04/09 من القانون نفسه .

أما عن السلطة المختصة بالتفتيش فيختص قاضي التحقيق أصلا بإجراء التفتيش تساعده النيابة العامة بتوليها تتبع الجرائم واتخاذ الإجراءات الملائمة بصددها، ثم يحضر قاضي التحقيق الذي يتولى مباشرة التحقيق، فالنيابة العامة توجه الإتهام و قاضي التحقيق يباشر إجراءات التحقيق.

و قد نصت المادتين 81 و 82 من قانون الإجراءات الجزائية على أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد فيه أشياء يفيد اكتشافها في إظهار الحقيقة و لقد أجازت المادة 83 من قانون الإجراءات الجزائية لقاضي التحقيق القيام بنفسه بالتفتيش في أي مكان آخر و بالتالي أي مسكن آخر غير مسكن المتهم ليضبط أدوات الجريمة أو ما نتج عن ارتكابها و كل شيئ آخر يفيد في في كشف الحقيقة، كما منحته المادة 48 من قانون الإجراءات الجزائية حق إنابة أحد ضباط الشرطة القضائية للقيام بهذا التفتيش بنفسه ، و طبقا للشروط التي نصت عليها المواد 138 الى 142 من قانون الإجراءات الجزائية حيث ان قاضي التحقيق سلطته مقيدة بمنح الإنابة بشرط إستحالة قيامه بالإجراء بنفسه نظرا لخطورة السلطات التي يمتلكها قاضي التحقيق و منها التفتيش.

اما ضابط الشرطة القضائية فإن من الممكن أن يقوم بعملية التفتيش حيث يتم بمعرفة ضباط الشرطة القضائية في الجرائم المتلبس بها و لقد نصت المادة 15 من قانون الإجراءات الجزائية على أعظاء الضبطية القضائية الذين لهم صفة ضباط الشرطة القضائية، إذ نص القانون على ضرورة إجراء التفتيش من طرف ضابط يساعده أعوان ولكن يتم الإجراء بحضوره و تحت إشرافه و إلا وقع باطلا . (1)

الفرع الثاني: إجراءات التحقيق الخاصة في جريمة الإبتزاز عبر الوسائل الإلكترونية

نظرا لسرعة إرتكاب الجريمة الالكترونية و سهولة محو آثارها ، جعل أمر إكتشافها صعب للغاية، لذا استحدث التشريع الجزائري على غرار التشريعات الحديثة إجراءات خاصة من أجل ضبطها قبل تفاقم خطرها، و يمكن تقسيم هذه الإجراءات الخاصة الى نوعين، الإجراء الأول: مراقبة الإتصالات الإلكترونية أما الإجراء الثاني : حفظ المعطيات المتعلقة بحركة السير.

(1) رابحي عزيزة, المرجع السابق , ص286 .

أولا مراقبة الإتصالات الإلكترونية

تعتبر المراقبة من أهم مصادر التحري سواءا في الجرائم التقليدية أو المستحدثة كجرائم الأنترنت و هي ما يعرف بالمراقبة الإلكترونية، و قد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية في اعتراض المراسلات ، و تسجيل الأصوات والتقاط الصور .

و قد اختلف المشرع الجزائري في إعطاء مصطلح واحد للمراقبة الإلكترونية فأحيانا يقر بمصطلح المراقبة الإلكترونية كما قررها في القانون 04/09 و أحيانا أخرى بمصطلح أساليب التحري الخاصة إلا أنها نفس الإجراءات تختلف في التسمية و في القانون الذي أقرها.

إن أساليب التحري الخاصة تمس حرمة الحياة الخاصة المكفولة دستوريا. (1)

و من أجل ذلك قرر المشرع في قانون الإجراءات الجزائية خلال تعديل 2006 الذي طرأ عليه وفق قانون 22/06 الذي حصر وجوبية اللجوء إلى مثل هذا الإجراء على الجرائم الستة الخطيرة و من بينها الجريمة المعلوماتية . (2)

و تتمثل هذه الاساليب في :

- اعتراض المراسلات
- التقاط الصور
- تسجيل الاصوات

(1) المادة 39 من دستور 1996 ،المعدل.
(2) قانون رقم 06-22 مؤرخ في 29 ذي القعدة 1427 الموافق ل 20 ديسمبر 2006يعدل و يتمم قانون الاجراءات الجزائية .

أ- اعتراض المراسلات

المراسلات هي جميع الخطابات و الرسائل و الطرود و البرقيات، و المشرع الجزائري في المادة 65 مكرر ق إ ج ج حصر مفهوم المراسلات في تلك التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية فقط ، و بالتالي استبعد المراسلات العادية .

ب: تسجيل الأصوات

يقصد به مراقبة الأحاديث ،و تسجيلها و كل الإتصالات التي تتم عن طريق سلكي، أو لا سلكي أي أن عمليات المراقبة تشمل كل أدوات الإتصال سواء سلكية ،أو لا سلكية ،و تتمثل في وضع تقنية دون موافقة المعنيين من أجل التقاط، و تثبيت ،و بث و تسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة اشخاص . (1)

ج: إلتقاط الصور

هي تلك العملية التقنية التي يتم بواسطتها إلتقاط صور لشخص أو عدة اشخاص يتواجدون في مكان خاص.

و تتسم هذه الإجراءات بالسرية التامة لأنها بها مساس بحرمة الحياة الخاصة للاشخاص المكفولة دستوريا.

وقد عرفت الفقرة 03 من قانون 04/09 مراقبة الإتصالات الإلكترونية حيث تشمل الإتصالات السلكية و اللاسلكية ،و الخلوية كالفاكس، و البريد الإلكتروني، و مواقع الدردشة حتى المنتديات، و ساحات الرأي و النقاش التي تسمح بنقل الأفكار و المعلومات. (2)

ثانيا:حفظ المعطيات المتعلقة بحركة السير

قرر المشرع الجزائري على غرار التشريعات الحديثة إلزام مقدمي الخدمات حفظ المعطيات المتعلقة بحركة السير لضمان الوصول الى آثار الجريمة مهما كانت.

(1) أنظر المادة 65 مكرر 5و م65 مكرر 10 ق.إ.ج.ج تعديل 2006 .
(2) أنظر المادة 11 فقرة "هـ" قانون 04/09 .

أ:تعريف المعطيات المتعلقة بحركة السير

المعطيات المتعلقة بحركة السير هي تلك المعطيات المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها تلك الأخيرة باعتبارها جزء من حلقة الإتصال، توضح مصدر الإتصال و الوجهة المرسلة إليها و الطريق الذي سيسلكه ووقت و حجم الإتصال و نوع الخدمة. (1)

أما مقدمي الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو مستعمليها . المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال و كذا عناوين المواقع المطلع عليها.

أما بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة و كذا تلك التي تسمح بالتعرف على مصدر الإتصال و تحديد مكانه .

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداءا من تاريخ التسجيل.

ولا تعرض مقدمو الخدمة الى العقوبات المقدرة في المادة 11 من القانون 09-04. (2)

المطلب الثاني:الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز عبر الوسائل الإلكترونية

تتميز الجرائم التي ترتكب عبر الأنترنت بكون محلها معلومات أو برامج معالجة آلية عبر الحواسيب ،أو جرائم تتعلق بالأشخاص عبر عالم إفتراضي غير متناهي و غير محدود مما يعطيها طابع خاص ليس فقط في طريقة إرتكابها ، و بل كذلك في الوسيلة التي ترتكب بها، الأمر الذي ينجم عنه صعوبات إكتشاف الجريمة و التحقيق فيها .

فهي تتنوع بين صعوبات متعلقة بالجريمة و الجهات المتضررة ، و صعوبات متعلقة بالجانب القضائي.

الفرع الأول: صعوبات إكتشاف الجريمة المرتكبة عبر الأنترنت (الإبتزاز عبر الوسائل الالكترونية)

يعترض إكتشاف الجريمة المرتكبة عبر الأنترنت عدة صعوبات و ذلك راجع الى عدة اعتبارات منها ما هو متعلق بفقدان الآثار المادية للجريمة ، و منها ماهو راجع لتكتم الضحية ،و منها ما هو راجع لنقص الخبرة لدى سلطات التحقيق.

(1) أنظر المادة 12 فقرة "د" قانون 04/09 .
(2) أنظر المادة 11 من القانون نفسه.

أولا:فقدان الآثار المادية للجريمة

تضل الجريمة المرتكبة عبر الأنترنت مجهولة ما لم يبلغ عنها للجهات المعنية بالإستدلالات ،أو التحقيق الجنائي، فهي جرائم غير تقليدية لا تخلف آثار مادية حيث تضع الوسيلة التي ترتكب بها الجريمة ضمن قالب غير تقليدي نظرا إلى أن ارتكابها يتم عن طريق نقل معلومات على شكل نبضات الكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي ، و شبكة الإتصالات بصورة آلية كما تنساب بالكهرباء عبر الأسلاك. (1)

و يكفي الضغط على زر في لوحة الإستخدام لزوال ملفات أو حتى قواعد بيانات أو أنظمة بأكملها ، فتأتي من هنا مشكلة ضبط هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل إلا انها تتطلب خبرة عالية ، و إمكانيات قد لا تتواجد عادة لدى مصالح الشرطة القضائية المكلفة بالبحث ، و حتى حال حجز المعطيات الرقمية، فإن البيانات التي تشمل عليها لا تتضمن آثار أو بصمات يمكن الإستدلال من خلالها على صاحبها بل تحتاج للوصول الى هذا الهدف إلى عمليات بحث و تحري أخرى للحصول على نسق من القرائن المادية الأخرى التي يمكن أن تعزز دلالتها و قيمتها في الإثبات .(2)

ثانيا:فرض الجناة لتدابير أمنية

يعمد المجرمون الى إزالة آثار الجريمة عن طريق التلاعب بقواعد البيانات في جهاز الكمبيوتر، و البرامج دون ترك أثر، ولا سيما أن التخزين الإلكتروني غير مرئي,و البيانات بلغة رقمية لا تفهمها إلا الآلة ، و هذا يشكل عقبة أمام إقامة الدليل على الجريمة المرتكبة إلكترونيا لأن هؤلاء المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة هم فئة الأذكياء حيث يضربون سياجا أمنيا على افعالهم غير المشروعة قبل إرتكابها كي لا يقعوا تحت طائلة العقاب، كما يقوم المجرمون عبر الأنترنت بإخفاء هويتهم أو انتحال شخصيات أخرى حتى لا يمكن التعرف عليهم حال إكتشاف الجريمة ، حيث توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته ، كما يقوم المجرمون بانتحال الشخصية عبر البريد الإلكتروني و هي من أكثر الطرق استعمالا من طرف المجرمون. (3)

(1) صغير يوسف،المرجع السابق، ص117 .
(2) المرجع نفسه،ص118 .
(3) المرجع نفسه،ص119 .

ثالثا:التكتم عليها من قبل المجني عليه

غالبا ما يلجأ الضحية في هذه الجريمة الى التكتم ، و غالبا ما يكون مصرفا أو مؤسسة مالية أو شركة أو مشروعا صناعيا ضخما.

و يحرض المجرمون على عدم الإبلاغ عن الجريمة التي راحت ضحيتها من أجل إخفاء أساليب إرتكابها للحيلولة دون تقليد الآخرين للجناة ،كذلك للتستر على معلومات لا يجب الإبلاغ عنها خاصة إذا كانت الضحية شركات التأمين أو البنوك.

رابعا: نقص خبرة سلطات الإستدلال

قد تكون شخصية المحقق مثل التهيب من إستخدام الكمبيوتر و التهيب من إستخدام الإنترنت ، و عدم الخبرة الكافية و عدم الإهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية ، صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم ، كذلك عدم توفر المعرفة بأساليب ارتكاب الجريمة الإلكترونية و كذا قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية . (1)

كذلك أجهزة العدالة المقاومة لهذه الجرائم المرتبطة بالتقنية يبدأ بالتكوين و التشكيل عقب ظهور هذه الجرائم و هو أمر يستغرق الوقت فعدم توازي سرعة تقدم التقنية ذاتها والحركة التشريعية، أو الثقافة القانونية أو الأمنية،حيث لا تسيران بذات المعدل مما يعكس سلبا على إجراءات الإستدلالات، و التحقيقات في الدعوى الجنائية مما يستدعي ضرورة تأهيل سلطات الأمن و جهات التحقيق و الإدعاء و الحكم في شأن هذه الجرائم .

(1) خالد عياد الحلبي،إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، ط 1، دار الثقافة للنشر و التوزيع ، د ب ن ،2011، ص224

الفرع الثاني : صعوبات متعلقة بالجانب القضائي

يفترض الطابع الخاص لهذا النوع من الجرائم تعاون أكثر من دولة لكن هذا القصور مقارنة بتفاقم و تطور هذه الجريمة يشكل فارق شاسع بين الجريمة ، و بطء الإجراءات.

و قد نجم عن هذه الإشكالية أيضا صعوبات تتمثل في القانون الواجب التطبيق ، و المحكمة المختصة (تنازع الاختصاص) حيث ترى كل دولة أن لها الحق في ملاحقة ، و متابعة مرتكب هذه الجريمة لعدة إعتبارات:

أولا : قصور التعاون القضائي الدولي في مكافحة جريمة الإبتزاز عبر الوسائل الإلكترونية

يعتبر التعاون الدولي في مجال مكافحة الجريمة الإلكترونية عموما و جريمة الإبتزاز الإلكتروني من أصعب المواضيع المطروحة على هذا المستوى بسبب الإختلافات القائمة في الممارسات بين الدول و التشريعات ، و كذلك سبب العدد المحدود نسبيا من المعاهدات ، و الإتفاقيات المتاحة للدول بشأن التعاون الدولي الذي يعد مطلبا تسعى لتحقيقه كل دولة ، إلا أنه له معوقات تقف دون تحقيقه .

ثانيا: عدم وجود نموذج موحد للنشاط الإجرامي

نظرا لاختلاف المفاهيم الخاصة بالجريمة واختلاف التقاليد ، و الأعراف القانونية الدولية فإن ذلك يضعف منظومة القانون الدولي في مجال ضبط تلك الجرائم، مما يسهل إفلات الجناة من المسائلة الجنائية ، و ذلك بسبب عدم توفر تعريف موحد للجريمة فتكون مجرمة في تشريع و في تشريع آخر مباحة. (1)

فالطبيعة الدولية لهذه الجريمة تثير إشكالية تحديد القانون الواجب التطبيق هل هو قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيها الآثار الضارة .

(1) صغير يوسف، المرجع السابق، ص133 .

كذلك تعارض القوانين من الناحية الموضوعية و الإجرائية يتطلب العمل على توحيد التشريعات المتعلقة بمكافحة هذا النوع من الجرائم إضافة الى إبرام اتفاقيات في هذا المجال .(1)

ثالثا: تنوع واختلاف النظم القانونية الإجرائية

إن اختلاف النظم القانونية الإجرائية و التحقيق و المحاكمة قد تثبت فاعليتها في دولة ما و قد تكون عديمة الفائدة في دولة اخرى و قد لا يسمح بإجرائها كما هو الشأن بالنسبة للمراقبة الإلكترونية و التسليم المراقب ، و غيرها من الإجراءات.

رابعا:عدم وجود قنوات إتصال

إن عدم الإتصال بين الدولة لجمع الأدلة ، و المعلومات يعيق التعاون الدولي في مجال مكافحة الجريمة ، فعدم التعاون و التنسيق بين الدول فيما يخص الأجراءات ، و جمع الإستدلالات و التحقيق خاصة ، و أن الحصول على دليل في هذه الجريمة قد يكون خارج نطاق الدولة هو أمر غاية في الصعوبة. (2)

خامسا:مشكلة الإختصاص في جريمة الإبتزاز عبر الوسائل الإلكترونية

ينجم عن اختلاف التشريعات و النظم القانونية تنازع في الإختصاص بين الدول فقد يحدث أن ترتكب هذه الجريمة في إقليم دولة من طرف أجنبي فهنا تكون هذه الجريمة خاضعة للإختصاص الإقليمي للدولة الأولى طبقا لمبدأ الإقليمية و تخضع للإختصاص للدولة الثانية على أساس مبدأ الإختصاص الشخصي و قد تهدد أمن ،و سلامة دولة اخرى فتدخل في اختصاصها إستنادا لمبدأ العينية. و يرتبط بمشكلات الإختصاص و القانون الواجب التطبيق مشكلات إمتداد انشطة الملاحقة و التحري و الضبط و التفتيش خارج الحدود مما أعاق التعاون الدولي و شتت الجهود في مكافحة هذه الجريمة.

(1) رابحي عزيزة، المرجع السابق،ص329 .
(2) صغير يوسف، نفس المرجع ، ص135.

سادسا:التجريم المزدوج

يجد شرط التسليم المزدوج أساسه في أن الدولة طالبته التسليم الذي تهدف به إلى متابعة من نسب إليه السلوك الإجرامي أو تنفيذ العقوبة عليه ، و بالتالي لابد أن يكون السلوك مجرما في تشريعها و إلا فلا يتصور وجود دعوى عمومية، أو ملاحقة جزائية أو تنفيذ عقوبة جزائية و منه لا يمكن مطالبة الدولة المطلوب إليها التسليم إيقاع عقوبة على ارتكاب سلوك ماهو في الأساس غير محرم وفقا لقانونها و ذلك راجع لعدم وجود معاهدات ثنائية للتعاون في هذا المجال.

سابعا:صعوبات الإنابة القضائية الدولية

إنبثقت الإنابة القضائية الدولية من الواجبات، و الإلتزامات التي يفرضها القانون الدولي على الأمم المتحدة و بموجبها يعهد للسلطات القضائية المطلوب منها اتخاذ إجراء القيام بالتحقيق لمصلحة السلطة القضائية المختصة في الدولة الطالبة مع احترام حقوق، و حريات الإنسان المعترف بها عالميا و مقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل واحترام النتائج القانونية المتوصل إليها من طرف الدولة المطلوب منها المساعدة القانونية .

تتسم اعمال الإنابة القضائية بالبطء و التعقيد مما يتعارض مع سرعة الجريمة.

الفرع الثالث: اشكالية القانون الواجب التطبيق و المحكمة المختصة بالجريمة

نظرا لكون هذه الجريمة قد ترتكب خارج الحدود الوطنية، يبرز أهمية إختبار مدى ملائمة قواعد الإختصاص و القانون الواجب التطبيق ، و ما إذا كانت النظريات ، و القواعد القائمة في هذا المجال تطال هذه الجرائم او يتعين إفراد قواعد خاصة بها مما تثيره من مشكلات في مجال الإختصاص القضائي.

أولا: تحديد القانون الواجب التطبيق

أ:المبادئ التقليدية في تحديد القانون الواجب التطبيق

و تتمثل في مبدأ اقليمية النص الجنائي، و مبدأ عينية النص الجنائي، و مبدأ شخصية النص الجنائي .

---

(1) صغير يوسف،المرجع السابق،ص 138 .

ب: انقضاء المبادئ التقليدية أمام خصوصية جريمة الإبتزاز عبر الوسائل الإلكترونية

نظرا لعدم تبعية شبكة الأنترنت لأي جهة أو شخص محدد، و نظرا لعدم وجود مقر لها في دولة محددة تخضع لرقابتها و نظرا لعدم وجود نص جنائي موحد يحكم هذه الشبكة، فان القوانين الجنائية التي تطبق عليها تتعدد بتعدد الدول المرتبطة بها، باعتبار أن القانون الجنائي يتعلق بسيادة الدولة.(1)

ثانيا: تحديد المحكمة المختصة

تنوعت المعايير الفقهية التي إعتمدت لتحديد المحكمة المختصة بنظر الجرائم المرتكبة عبر الأنترنت الى ثلاث معايير.

أ:معيار الاختصاص المكاني

وتضبطه ثلاث ضوابط هي مكان وقوع الجريمة، محل اقامة المتهم أو مكان القاء القبض عليه، و في حال اجتماع أكثر من ضابط تكون المحكمة المختصة بنظر الدعوى هي التي رفعت اليها الدعوى أولا، و يقصد بمكان ارتكاب الجريمة ، المكان الذي ارتكب فيه السلوك ليس الذي تحققت فيه النتيجة.(2)

ب:معيار القانون الأكثر ملاءمة

يرى أصحاب هذا الإتجاه بأنه نظرا للطبيعة الخاصة للجرائم الالكترونية ، و الأضرار الناجمة عنها التي تمتد لتشمل أكثر من دولة واحدة، و أحيانا قد تتفاوت نسبة الضرر بين دولة و أخرى ، يجب التوسع في تفسير قاعدة الاختصاص (وقوع الفعل و حصول الضرر) ليجعل الإختصاص لمحكمة الدولة الأكثر تعرضا للضرر، بشكل فعلي مع التركيز على مبدأ التخلي.

(1) صغير يوسف،المرجع السابق،ص144 .

(2)رابحي عزيزة،المرجع السابق،ص 330.

ج: معيار الضرر المرتقب

نظرا لكون الجريمة تتم في عالم افتراضي لا يخضع لأي سلطة اقليمية و بالتالي فالضرر الذي تسببه الجريمة المرتكبة الكترونيا يمكن أن يحدث في أي دولة متصلة بالأنترنت و هذا هو معيار الضرر الإفتراضي أو المرتقب.

فتطبيق معيار (الارتقاب) لا يمكن إيجاده إلا من خلال إيجاد صلة أو علاقة للقانون المختص مع مبدأ موضوعي، و ذلك بعيدا عن تذرع كل دولة بإختصاصها المحتمل.

و أول المعالم الموضوعية في الاختصاص هي محل تمركز الموقع الذي نشرت فيه الأقوال، و المعلومات والصور و الأفلام ، و هو أكيد و يمكن التحكم فيه بخلاف مكان تلقيها الذي يبقى احتماليا. (1)

(1) صغير يوسف،المرجع السابق،ص146 .

المبحث الثاني: الإثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية

لمكافحة جريمة الإبتزاز الإلكتروني أصبح من الضروري استحداث وسائل حديثة تختلف عن ما يتم اعتماده في الجريمة التقليدية، و هذا راجع الى عجز إجراءات التحقيق التقليدية في مجاراة نسق تطور هذه الجريمة، بالإضافة إلى عجز الأدلة الجنائية المادية في اثبات وقوعها، مما يستلزم اعتماد الأدلة الجنائية الرقمية و قد تناول هذا المبحث مطلبين، المطلب الأول ماهية الدليل الجنائي الرقمي ، أما المطلب الثاني صعوبات الإثبات في جريمة الإبتزاز الإلكتروني.

المطلب الأول: ماهية الدليل الجنائي الرقمي

للتعرض الى ماهية الدليل الجنائي الرقمي لابد من توضيح مفهومه و ذلك من خلال تعريفه و تبيان خصائصه ،كذلك شروط صحة الدليل الرقمي، و مصادر الحصول عليه لذا سيتم تخصيص الفرع الأول لمفهوم الدليل الجنائي الرقمي أما الفرع الثاني سيتم التطرق فيه الى شروط صحة الدليل الرقمي و مصادر الحصول عليه.

الفرع الأول: مفهوم الدليل الجنائي الرقمي

يشمل مفهوم الدليل الرقمي على عدة عناصر لابد من ذكرها ، و حتى يتضح هذا المفهوم سنتناول تعريف الدليل الرقمي ثم خصائصه.

أولا: تعريف الدليل الرقمي

يعرف على أنه "الدليل المأخوذ من أجهزة الكمبيوتر، و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تحميلها ، و تحليلها

---

(1) ممدوح عبد الحميد بن عبد المطلب،البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت،دار الكتب القانونية،مصر، 2006، ص77 .

باستخدام برامج تطبيقات و تكنولوجيا، و هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة، أو الصور، أو الأصوات ،أو الأشكال و الرسوم ، و ذلك من أجل اعتماده أمام أجهزة التحقيق"(1)

و قد عرفه البعض الأخر على أنه مجموعة من البيانات أو المعلومات التي تمكن من أن تثبت أن جريمة ما وقعت أو وجود صلة بين الجريمة و الجاني أو علاقة بين الجريمة و المجني عليه.(2)

فالدليل الرقمي هو الدليل المشتق من أو بواسطة البرامجية و المعلوماتية و أجهزة و معدات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية و فنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة ،أو رسومات، أو صور ،أو أصوات ، لاثبات وقوع الجريمة، أو لتقرير البراءة أو الإدانة.(3)

و يحتاج إثبات الجرائم الإلكترونية إلى دليل رقمي كوسيلة لإثبات الإبتزاز الإلكتروني، فيتطلب إجراء خطوات جمع الأدلة .

ثانيا : خصائص الدليل الرقمي.

الدليل الرقمي له خصائص تميزه عن غيره من الأدلة الجنائية التقليدية، و هذا يعود للبيئة الافتراضية التي يستخلص منها هذا الدليل، حيث أن هذه البيئة هي بيئة متطورة بطبيعتها و التي تنعكس على هذا الدليل مما أضفت عليه خصائص لا تتوفر في باقي الأدلة الجنائية .

و هذا ما سيتم توضيحه من خلال العناصر الأتية:

(1) ممدوح عبد الحميد بن عبد المطلب،المرجع السابق ، ص78 .

(2) محمد الأمين البشري،التحقيق في الجرائم المستحدثة،ط1،جامعة نايف العربية للعلوم الامنية،السعودية،2004،ص234 .

(3) ثنيان ناصر آل ثنيان ،إثبات الجريمة الالكترونية ،دراسة تأصيلية تطبيقية،رسالة ماجيستير،جامعة نايف العربية للعلوم الامنية، كلية الدراسات العليا السعودية،2012، ص74 .

أ:دليل علمي غير مرئي

فهو يتميز بالطبيعة الفنية ، حيث يتكون من بيانات و معلومات ذات صفة الكترونية غير ملموسة ولا تدرك بالحواس العادية، فتقوم الجهات القضائية بتمريره على البرامج المختصة لمعرفة ما اذا تم العبث بهذا الدليل، و هذه الدليل كالدليل العلمي يخضع لقاعدة لزوم التجاوب مع الحقيقة كاملة وفق قاعدة (أن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة) فبحكم الطبيعة الخاصة للدليل الإلكتروني فإنه لا يجب أن يخرج عما توصل إليه العلم الرقمي وإلا فقد معناه.

ب:دليل قابل للنسخ

حيث تتيح التكنولوجيا المعلوماتية استخراج نسخ من الأدلة الرقمية محقق جنائي، و فني متخصص لديه المهارة الفنية و التقنية لاستخلاص ، و جمع الأدلة الرقمية ، لأن الفصل في دعاوي الجرائم الإلكترونية بصفة عامة و جريمة الإبتزاز الإلكتروني بصفة خاصة يتوقف على الرأي الفني الذي يثبت أو ينفي قيام الجريمة من قبل المشتبه به.

فالدليل الرقمي يتكون من بيانات و معلومات الكترونية غير ملموسة و يتطلب إدراكها الإستعانة بأجهزة و برامج معينة لتقديم معلومات بشكل نصوص مكتوبة، أو صور ،أو أصوات ،أو غيرها ،بترجمة البيانات الرقمية المخزنة على الأجهزة الالكترونية و شبكة الأنترنت لاثبات الواقعة المطلوب اثباتها في الجرائم الالكترونية ، و نسبتها إلى الشخص المشتبه فيه.(1)

و قد استدعى واقع التقدم التقني الإستعانة بالخبراء و المختصين .

ويختلف الإعتبار بحجية الدليل الرقمي و اعتبارها حجة في إثبات الدعوى أو نفيها ، باختلاف النظم القانونية فنجد الدول التي تأخذ بمبدأ التقييم الحر لهذه الأدلة الرقمية فيكون لدى القاضي الجنائي الأخذ بجميع الأدلة، و تقييم مدى اعتماد المحكمة على تلك الأدلة و يكون هذا في النظام الأنجلوساكسوني،أما في النظم الأخرى التي تأخذ بمبدأ الترافع بحيث يكون لدى الخصم مناقشة الشاهد لدحض افادته و يكون للقاضي حرية تقييم الأدلة.

(1) ثنيان ناصر آل ثنيان،المرجع السابق،ص74 .

ج: صعوبة طمس الأدلة الرقمية

الأدلة الالكترونية (الرقمية) يمكن استرجاعها بعد محوها و إصلاحها بعد إتلافها ، مما يؤدي الى صعوبة التخلص منها ، و هي من أهم الخصائص التي تميزه مقارنة بالدليل التقليدي، فهناك الكثير من البرامج الحاسوبية التي وظيفتها استعادة البانات التي تم حذفها، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن و العدالة طالما وصل الى علم رجال البحث و التحقيق الجنائي بوقوع الجريمة، و الأكثر من ذلك فان محاولة الجاني محو الدليل الإلكتروني بذاتها تسجل عليه كدليل، و أن قيامه بذلك يتم تسجيله في ذاكرة الآلة و هو ما يمكن استخراج نسخ منه لها نفس الحجية و القوة الثبوتية، الأمر الذي لا يتوافر في أنواع الأدلة التقليدية الأخرى مما يشكل ضمانة فعالة ضد الفقد و التلف.

د: الدليل الجنائي الرقمي متنوع و متطور

إن مصطلح الدليل الرقمي يشمل جميع البيانات الرقمية التي يمكن تداولها رقميا، سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها من الأجهزة ، أو شبكة الأنترنت، أو شبكات الاتصال السلكية أو اللاسلكية، و منه فالآثار الرقمية المستخلصة متنوعة بما تحتويه من معلومات عن وقائع قد تشكل جريمة، فتصبح أدلة براءة أو ادانة، و من بينها صفحات المواقع الالكترونية ، الصور، الفيديوهـات الرقمية ، والملفات المخزنة في الحاسب الآلي الشخصي أو المعلومات المتعلقة بمستخدم شبكة الأنترنت و غيرها.

فهذا التنوع يدل على اتساع قاعدة الدليل الجنائي الرقمي الذي يمكن أن يكون دليل براءة أو إدانة .(1)

أما خاصية التطور فهي ناتجة عن تزايد استعمال تقنية المعلومات الرقمية ، لتلبية احتياجات المستخدمين الأمر الذي أدى الى ظهور أنواع جديدة من الأدلة.

(1) رابحي عزيزة،المرجع السابق،ص270 .

الفرع الثاني: شروط صحة الدليل الرقمي و مصادر الحصول عليه

أولا: شروط صحة الدليل الرقمي

هناك شروط في الدليل الرقمي لقبوله كأساس تقوم عليه الحقيقة في الدعاوي الجنائية و هذه الشروط تتمثل في النقاط التالية: لابد أن يكون الدليل الرقمي غير قابل للشك، يجب الحصول على هذا الدليل بصورة مشروعة، كما يجب أن يكون الدليل قابلا للمناقشة، و هذا ما سنستعرضه في الآتي:

أ:يجب أن يكون الدليل الرقمي غير قابل للشك

أي لابد أن يكون يقيني، ذلك أنه لامجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي الى يقين، حيث يصل إليه القاضي بعد عرض الأدلة الرقمية، فمن خلال ما يعرض عليه من مخرجات الكترونية، فما ينطبع في ذهنه من تصورات و احتمالات بالنسبة لها، سيحدد قوتها الإستدلالية على صدق نسبة الجريمة المعلوماتية الى شخص معين من عدمه.(1)

ب: يجب أن يكون الدليل الرقمي متحصل عليه بصورة مشروعة

فالمشروعية هي التوافق والتقيد بأحكام القانون في إطاره و مضمونه العام فهي تهدف الى تقرير ضمانة أساسية لحماية الحقوق و الحريات الشخصية ضد تعسف السلطة، و التطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي و تحقيق حماية مماثلة للفرد .

وعليه ينبغي على القاضي أن يستقي قناعته في الحكم من خلال أدلة مشروعة ، أما الأدلة التي جاءت ناتجة عن إجراءات غير قانونية و باطلة، فلا يجوز الإعتماد عليها، كما يجب استبعاد كل دليل معيب حتى وإن استندت في إصدارها الى أدلة أخرى مشروعة إلى جانب الدليل الباطل و المعيب.(2)

(1) ممدوح عبد الحميد بن عبد المطلب،المرجع السابق،ص125 .

(2) رابحي عزيزة،المرجع السابق،ص255 .

ج:يجب أن يكون الدليل الرقمي قابلا للمناقشة

و يعني ذلك أن القاضي لا يعتمد إلا الدليل الذي تم مناقشته في معرض المرافعة ، وجاهيا ، علنيا حضوريا من قبل أطراف الدعوى.(1)

فالأدلة المتحصلة من جرائم الحاسب الآلي و الأنترنت، ستكون محلا للمناقشة عند الأخذ بها كوسيلة اثبات أمام المحكمة فيجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي،لكن بصفة مباشرة أمام القاضي الجزائي.

فلا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة اليه في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه .

و متى كان للأدلة أصل في ملف الدعوى ولا يمكنه بناء اقتناعه على مادار خارج التحقيقات، أو أدلة لم يطلع عليها الخصوم و لم يتمكنوا من مناقشتها.(2)

ثانيا: مصادر الحصول على الدليل الرقمي

تعتمد جهات التحري و التحقيق على مصادر لتحصيل الدليل الرقمي من المصادر التي يسمح لها القانون، و المتمثلة في: اجراء الارشاد الجنائي ، و اجراء الوضع تحت المراقبة الالكترونية، و تعاون مقدمي خدمات الانترنت مع السلطات القضائية.

أ:إجراء الإرشاد الجنائي

الذي يقوم بمقتضاه ضباط الشرطة القضائية بتجنيد أحد عناصرها للولوج للعالم الافتراضي و بالأخص عبر حلقات النقاش و قاعات الدردشة و الاتصال المباشر، مستعملين صفات وهمية من أجل الكشف عن هذه الجرائم و كشف المجرمين.

(1) أنظر المادة212 ق إ ج ج المعدل و المتمم.

(2) رابحي عزيزة،المرجع السابق،ص296 .

فهذا الإجراء لا يتطلب جهد مادي كبير، حيث يقوم به ضباط الشرطة القضائية ، أو يكلف غيره من ذوي الاختصاص و هذا بعد الحصول على إذن رسمي للقيام بمهام البحث و التحري عن الجرائم و ضبط مرتكبيها.

و قد أتاح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت اسم التسرب من خلال نصوص المواد 65 مكرر 05 الى غاية المادة 65 مكرر 18 (ق.إ.ج.ج) بعد الحصول على اذن مسبب من وكيل الجمهورية أو قاضي التحقيق تحت رقابة وكيل الجمهورية لمدة 04 أشهر قابلة للتجديد. (1)

ب:إجراء الوضع تحت المراقبة الالكترونية

و هي من أهم مصادر البحث و التحري سواء في الجرائم التقليدية أو المستحدثة، و يقصد بها مراقبة شبكة الجرائم المعلوماتية (Cyber surveillance) ، و تسمى بذلك بالمراقبة الالكترونية.

فهي العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع البيانات و المعلومات عن المشتبه فيه، من أجل تحقيق غرض أمني، أو أي غرض آخر ، و هي مرتبطة بالزمن. وقد أجاز المشرع الجزائري المراقبة الالكترونية في الجرائم المعلوماتية عن طريق اعتراض المراسلات التي تتم بواسطة وسائل الإتصال السلكية و اللاسلكية ، كما أجاز كل الترتيبات التقنية لها دون علم المعنيين و لا موافقتهم، بغية الحصول على تسجيلات الكلام الصادر عنهم بصفة سرية أو خاصة ، وذلك باذن من وكيل الجمهورية.

ج:تعاون مقدمي خدمات الانترنت مع السلطات القضائية

يقصد بمزود الخدمة كل شخص يقدم خدمة الى الجمهور بوجه عام في مجال الاتصالات الالكترونية التي لا تقتصر في آدائها على طائفة معينة من المتعاملين معه بعقد من العقود, وقد عرف المشرع الجزائري مقدم الخدمة بموجب المادة 02 في القانون 04/09 بأنه: (2)

(1) أنظر المادة من ق إ ج ج المعدل و المتمم .
(2) أنظر المادة 2/د قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها .

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام للاتصالات .

2- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها.

و نظرا لضلوع الشبكة المعلوماتية في أغلب جرائم العالم الافتراضي ، فإن المشرع الجزائري قد فرض على مقدمي خدمات الانترنت مجموعة من الإلتزامات من أجل مساعدة السلطات القضائية في أعمال التحقيق و ذلك من خلال القانون رقم 04.09 في فصله الرابع تحت عنوان "التزامات مقدمي الخدمات " و من بين الإلتزامات الواردة نجد: الإلتزام بمساعدة السلطات و الإلتزام بحفظ المعطيات المتعلقة بحركة السير.

المطلب الثاني : صعوبات الإثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية

نظرا لكون هذه الجريمة تتم في الخفاء، و من يرتكبها يتصف بمعرفة التقنية و الذكاء، و بالرغم من الجهود المبذولة لمكافحة الجريمة الالكترونية ، و جريمة الإبتزاز الإلكتروني بوجه خاص ، إلا أنه هناك بعض المعوقات و الصعوبات التي تواجه السلطات المختصة في الإثبات بالدليل الرقمي و ذلك لعدة أسباب أهمها:

الفرع الأول: معوقات مرتبطة بالدليل ذاته

أولا: سهولة محو الدليل

حيث أن الجناة بعد ارتكابهم للجريمة يحرصون على محو أي آثار للتهديد و الإبتزاز مما يجعل الوصول للدليل صعب وفي بعض الأحيان يكون مستحيل.(1)

(1) نهلا عبد القادر المومني،المرجع السابق،ص54 .

ثانيا:صعوبة الكشف عن هوية الجاني من خلال الدليل الرقمي

تتم جريمة الإبتزاز الإلكتروني في بيئة افتراضية تحكمها الرموز و البيانات و تخلو من العنف الظاهر و الآثار المادية كالجريمة التقليدية مما يصعب الوصول لدليل مادي، كبصمات الأصبع أو نقاط الدم مما يجعل الوصول للجاني معترض بالعقبات.(1)

ثالثا: عرقلة الوصول للدليل

قد يضع الجاني عقبات فنية لمنع كشف جريمته من خلال أدلتها و ذلك بتشفير الملفات الرقمية قصد حجب المعلومات عن التداول و منع الوصول الى مصدر الارسال.(2)

رابعا: صعوبات متعلقة بنقص الخبرة

من بين الصعوبات التي تواجه عملية الحصول على دليل رقمي في جريمة الابتزاز الالكتروني، نقص الخبرة لدى بعض العاملين في جهات التحقيق،و من رجال الضبط القضائي و رجال النيابة العامة ، فيما يخص مهارة استخدام أجهزة الحاسب الآلي و ملحقاتها و مهارات الاستجواب للمجرم الالكتروني في جرائم الإبتزاز الإلكتروني، لذا من الضروري جدا الإهتمام و تطوير و تأهيل العنصر البشري من محققين و رجال الضبط القضائي لمواكبة مثل هذا النوع من الجرائم و يتطلب أيضا متابعة العنصر البشري للأمور التقنية و كل مستجد على الساحة.

خامسا: صعوبات متعلقة في إحجام المجني عليه على الإبلاغ

إن عدم الإبلاغ من قبل المجني عليه سبب رئيسي في تكوين الصعوبة التي تواجه السلطـات المخـتصة، و بالتالي فإن هذا الإحجام يساعد على إختفاء الدليل الرقمي ، و بالتالي يكون هذا سبب في تكوين عقبة تقف كحجر عثرة في طريق الاثبات عن طريق الدليل الرقمي.

(1) غنية باطلي،الجريمة الالكترونية دراسة مقارنة،الدار الجزائرية للنشر و التوزيع، د ط ،الجزائر، 2016 ،ص45 .

(2) المرجع نفسه ،ص46.

فكل ذلك يعود إلى خوف المجني عليه من الإبلاغ كي لا يفتضح أمره ، فهذه الجريمة أرتكبت أساسا بسبب خوف المجني عليه من أن يكتشف أسراره .

الفرع الثاني: صعوبة التعاون الدولي

إن اختلاف تشريعات الدول في تجريم أفعال الإبتزاز الإلكتروني يزيد في عراقيل ملاحقة الجناة، و رغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الالكترونية ، إلا أنه هناك عوائق تحول دون تحقيق ذلك، و من هذه العوائق.

أولا:عدم وجود نموذج موحد للنشاط الإجرامي و اختلاف النظم القانونية الإجرائية

فهذا الأمر يعتبر من أهم الصعوبات التي تعترض التعاون الدولي في مجال مكافحة الجريمة المعلوماتية و سنحاول التفصيل فيه على النحو التالي:

أ:عدم وجود نموذج موحد للنشاط الإجرامي

عدم وجود إتفاق مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات ، حيث أن الإختلاف في تجريم الإبتزاز الإلكتروني من دولة لأخرى ، مما يجعل ملاحقة الجاني تمر بعقبات و عراقيل ، فما تراه دولة مباح تراه دولة أخرى مجرم.(1)

ب: تنوع و اختلاف النظم القانونية الإجرائية.

حيث نجد أن طرق التحري و التحقيق و المحاكمة التي تثبت فائدتها في دولة ما تكون عديمة الفائدة في دولة أخرى أو لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية و غيرها، حتى إن تم الحصول عليه في إختصاص قضائي و بشكل مشروع.(2)

(1)رابحي عزيزة،المرجع السابق،ص315 .

(2) المرجع نفسه،ص316 .

ثانيا : مشكلة الإختصاص

ينعقد الإختصاص القضائي المكاني أو المحلي للمحاكم الجزائية من خلال القاعدة الثلاثية، حيث يرجع الإختصاص إما لمحكمة ارتكاب الجريمة ، أو محكمة القاء القبض على المجرم ،أو أحد مشاركيه أو محكمة موطن إقامة المجرم، فالإختصاص هو مباشرة المحكمة ولايتها القضائية في نظر الدعوى في الحدود التي رسمها القانون.

فتطبيق القواعد التقليدية التي تحدد معايير الإختصاص لا يتلائم مع طبيعة الجريمة الإلكترونية العابرة للحدود ، حيث يصعب تحديد مكان وقوع الفعل الجرمي في هذه الجرائم، لأن الطبيعة الخاصة لهذا

الصنف من الجرائم المستحدثة تتطلب تجاوز المعايير التقليدية التي لا تتلائم مع تحديد محل وقوع الجريمة في العالم الإفتراضي، لأن هذه الجرائم لا تعترف بالحدود الجغرافية ، و السياسية للدول و لا سيادتها ، فهي جرائم عابرة للحدود تتم في فضاء الكتروني معقد عبارة عن شبكة إتصلات لامتناهية غير مجسدة ، و غير مرئية متاحة لأي شخص في العالم ، و غير تابعة لأي سلطة حكومية.(1)

فقواعد الإختصاص القضائي المنصوص عليها في قانون الإجراءات الجزائية صيغت كي تحدد الإختصاص المتعلق بجرائم قابلة للتحديد المكاني و لا يمكن إعمالها بشأن الجريمة الإلكترونية.

و هذا ما يجعل التعاون الدولي لضمان الفعالية بمحاربة هذه الجرائم حتمية لا ينبغي غض الطرف عنها، فلابد من توحيد التشريعات أو على الأقل تقليص الفوارق بينها لتعزيز هذه الأليات كي لا يفلت المجرمون من المتابعة الجزائية.(2)

إذن فمشكلة الإختصاص في الجريمة الإلكترونية، أصبحت الحاجة فيها ملحة الى إبرام اتفاقيات دولية ثنائية أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الإختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالأنترنت بالاضافة الى تحديث القوانين الجنائية الموضوعية و الإجرائية بما يتناسب و التطور الكبير الذي تشهده تكنولوجيا المعلومات و الإتصالات.

---

(1)رابحي عزيزة،نفس المرجع،ص316 .

(2) صغير يوسف،المرجع السابق،ص133 .

وهوما قام به المشرع الجزائري عندما عالج مشكلة امتداد التفتيش خارج الدولة الجزائرية بموجب ما أرساه القانون 04/09 ، أيضا عندما توصل الى حل إشكالات الاختصاص بالنسبة لبعض الجرائم و منها الجرائم الخاصة بالأنظمة المعلوماتية حيث تم تمديد الاختصاص ليشمل اختصاص محاكم أخرى عن طريق التنظيم، مثلما هو الأمر بالنسبة للمشرع الجزائري حينما عدل نص المادة 329 من قانون الإجراءات الجزائية و أيضا تم تمديد الاختصاص الإقليمي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق ليتجسد فعليا موجب المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الإختصاص المحلي لبعض وكلاء الجمهورية ، و قضاة التحقيق الذي أنشأ الجهات القضائية ذات الإختصاص الموسع أو (الأقطاب القضائية).(1)

و قد عدل هذا الأخير بالمرسوم التنفيذي رقم 16/267 المؤرخ في 17 أكتوبر 2016 حيث تم تعديل هذا الاختصاص الموسع.

ثالثا: الصعوبات الخاصة بالمساعدات القضائية الدولية و تدريب الكوادر

تتعدد الصعوبات الخاصة بالمساعدات القضائية الدولية و تدريب الكوادر و سيتم تفصيلها فيما يلي:

أ:الصعوبات الخاصة بالمساعدات القضائية الدولية

تعتبر الانابة الدولية من أهم صور المساعدات القضائية الدولية في المجال الجنائي، و التي تتم عن طريق الطرق الدبلوماسية التي تتسم بالبطء مما لا يتناسب مع طبيعة جرائم الأنترنت التى تتسم بالسرعة. (2)

ب:الصعوبات الخاصة بالتعاون الدولي في مجال التدريب

تتمثل هذه الصعوبات في الفوارق الفردية بين المتدربين و تأثيرها في عملية الاكتساب للمهارات بطريقة متكافئة لدى المتدربين ، و تأثيرها في عملية اكتساب المهارات المستهدفة سيما في مجال التكنولوجيا الرقمية .

. (1) صغير يوسف،نفس المرجع،ص133 .

(2) رابحي عزيزة،المرجع السابق،ص319

ملخص الفصل الثاني:

يعالج هذا الفصل الإطار الإجرائي لجريمة الإبتزاز عبر الوسائل الالكترونية و ذلك بتسليط الضوء على الإجراءات العامة والخاصة وكذا الإشكالات الإجرائية التي تثيرها هذه الجريمة من ناحية التحقيق من خلال التطرق إلى صعوبات إكتشاف الجريمة والصعوبات المتعلقة بالجانب القضائي وإشكالية القانون الواجب التطبيق و كذا الإجراءات المرتبطة بالإثبات في الجريمة موضوع الدراسة والتي تعرضنا فيها إلى خصوصية هذه الإجراءات كما تعرضنا لأهم وسائل الإثبات التي تخص هذه الجريمة و هو الدليل الرقمي وذلك من خلال التطرق إلى مفهومه وشروط صحته وكذا صعوبات الإثبات المرتبطة بالدليل الرقمي في حد ذاته و كذا صعوبات التعاون الدولي والصعوبات المتعلقة بالمساعدات القضائية وتدريب الكوادر.

خـــــاتمة

جريمة الإبتزاز الإلكتروني من الجرائم المستحدثة ، و يطلق عليها في علم الجريمة الجرائم الناعمة، التي تخلو من العنف ، و هي احدى صور الجريمة الإلكترونية ، فجريمة الإبتزاز الإلكتروني هي الوجه الآخر لجريمة الإبتزاز التقليدية التي تنشأ و ترتكب في عالم مادي و في مسرح جريمة تقليدي حيث يترك فيه الجاني أثر، أما الابتزاز الالكتروني فيتم في عالم افتراضي مليء بالرموز و الشيفرات و يزداد التحدي حين نجد العقبات و الصعوبات التي تواجه أجهزة التحقيق في التعامل مع الدليل الرقمي.

و قد أصبحت هذه الجريمة تشكل هوسا لدى مستخدمي التكنولوجيا الحديثة، بعد التطور السريع للتكنولوجيا الرقمية ، و أمام هذه الثورة حاولت الدول تطوير تشريعاتها لتواكب هذه الجرائم المستحدثة، ثم تنبهت لضرورة افراد نصوص تشريعية خاصة بهذه الجريمة الالكترونية.

وبعد الإنتهاء من دراسة موضوع البحث (جريمة الابتزاز عبر الوسائل الالكترونية) التي استعرضنا من خلالها الإطار الموضوعي للجريمة الذي تحدث عن ماهية الإبتزاز عبر الوسائل الإلكترونية و تجريمه كما تطرقنا الى الجانب الإجرائي للجريمة موضوع البحث من خلال التطرق الى التحقيق في الجريمة و الإثبات فيها، نصل في الأخير الى أهم النتائج و المقترحات.

النتائـــــج:

1- جريمة الإبتزاز عبر الوسائل الإلكترونية صورة من صور الجريمة الإلكترونية حيث تتم باستخدام الوسائل التقنية الحديثة .
2- لجريمة الإبتزاز عبر الوسائل الإلكترونية وسائل و طرق مختلفة في ارتكابها تختلف عن الإبتزاز التقليدي ، كالهواتف النقالة المزودة بآلة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد، وذلك بالتقاط الصور أو نشر أخبار أو تسجيلات صوتية، أو مرئية تتصل بها و لو كانت صحيحة.
3- تتحقق جريمة الإبتزاز عبر الوسائل الإلكترونية باستخدام الجاني سلوكا واحدا أو متعددا ، إذ لا عبرة بالطريقة التي لجأ اليها الجاني لتهديد المجني عليه، فقد تتم عن طريق البريد الإلكتروني أو غرف المحادثة ، أو المنتديات أو أي طريقة أخرى تهدف لحمل المجني عليه على إحداث نتيجة معينة تتمثل في القيام بفعل أو الإمتناع عنه.

4- جريمة الإبتزاز عبر الوسائل الإلكترونية قد تتسبب في جرائم بعدها، كالزنا أو القتل أو جريمة عنف أو سرقة.

5- جريمة الإبتزاز عبر الوسائل الإلكترونية جريمة عابرة للحدود، فقد يكون المبتز في دولة و الضحية في دولة أخرى.

6- لم تشترط التشريعات كالسعودي و العماني و الإماراتي أن يبلغ التهديد درجة من الجسامة ، إذ نجد نصوصهم بينت أن كل شخص هدد شخصا آخر أو ابتزه لحمله على القيام بفعل أو الإمتناع عنه و لو كان القيام بهذا الفعل أو الإمتناع مشروعا، كما أنه لاعبرة لموضوع و نوع التهديد، فقد يكون بالقول أو بانزال ضرر بالمجني عليه عن طريق التشهير به عبر إرسال مجموعة من الرسائل النصية عبر الهاتف النقال لمجموعة من الأشخاص بهدف حمل المجني عليه للقيام بعمل

7- جريمة الإبتزاز عبر الوسائل الإلكترونية لها خصوصية في التحقيق و تستلزم فريق عمل من المختصين أو المؤهلين لاستيعاب التطورات الحديثة في التحقيق مع مجرم ذكي له صفات تختلف عن صفات المجرم التقليدي.

8- جريمة الإبتزاز عبر الوسائل الإلكترونية جريمة صعبة الإثبات، حيث أنه من السهل محو آثارها و تحتاج لعمل شاق كي يتم إثباتها.

9- الدليل الرقمي أهم أدلة الاثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية إلا أن التعامل معه يحتاج إلى خبرات معينة و أجهزة متخصصة و فريق عمل متكامل الخبرة.

10 -الأساس النظري لجريمة الإبتزاز عبر الوسائل الإلكترونية بين بعض التشريعات العربية يتشابه كثيرا، و قد تفوق القانون الإتحادي الإماراتي على التنظيم السعودي في تجريم الإعتداء على حرمة الحياة الخاصة، حتى ولو لم يحدث ابتزاز أو تهديد حيث أفرد نصا خاصا لذلك في قانون العقوبات بالاضافة الى تجريم الإبتزاز الإلكتروني في قانون مكافحة جرائم تقنية المعلومات.

11- اختلفت التشريعات في مقدار العقوبة المقررة لجريمة الإبتزاز عبر الوسائل الالكترونية فالمشرع الإماراتي ضاعف مدة الحبس بحده الأعلى سنتين، أما المشرع السعودي فجعل الحد الأعلى سنة في عقوبة جريمة الإبتزاز عبر الوسائل الالكترونية، وقد خرج المنظم السعودي عن القواعد العامة حين قرر عقوبة للمساهم في الجريمة حتى وان لم تتم الجريمة.

12- المشرع الإماراتي شدد عقوبة السجن في جريمة الإبتزاز عبر الوسائل الالكترونية ،اذا ارتبطت بجناية.

13 - تقرير الإعفاء في بعض التشريعات العربية لفاعل الجريمة حال الإبلاغ ، وهو إخبار السلطات قبل العلم بالجريمة و الإخبار عن الشركاء.

14- وجود فجوة تشريعية بين تشريعات العالم في تجريم الإبتزاز عبر الوسائل الإلكترونية مما سهل التهرب من المتابعة و العقاب خاصة الدول التي لم تفرد نصوص خاصة تجرم هذا السلوك على غرار المشرع الجزائري والعراقي .

المقترحـات:

1- إصدار قانون خاص يجرم الإبتزاز عبر الوسائل الإلكترونية في الدول التي لا يوجد في تشريعها نص ليكون الردع بشقيه العام و الخاص ذا فاعلية أكبر.

2- لابد من تعاون كل مؤسسات التعليم و التعليم العالي ، و دور العبادة لاقامة دراسات وندوات حول مخاطر هذه الجريمة الدخيلة على المجتمعات العربية و الاسلامية .

3- أن يعين أخصائيين نفسانيين و اجتماعيين تكون مهمتهم التواصل مع كل من تعرض للابتزاز مهما كان جنس و سن الضحية.

4- تدريب و تأهيل العاملين بجهات التحقيق و الجهات 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.

5- انشاء وحدات لمعالجة جرائم الإبتزاز عبر الوسائل الالكترونية في الجهات الأمنية لاستقبال بلاغات الابتزاز وتتبع أثر المبتزين بحرفية عالية.

6- زيادة التعاون الدولي، وذلك بوضع آلية موحدة تجرم الإبتزاز عبر الوسائل الالكترونية كي لا يفلت المجرم من العقاب نتيجة تساهل بعض الأنظمة و تشدد أخرى.

قائمة المصادر والمراجع

قائمة المصادر و المراجع

I/قائمة المصادر

أ. الدساتير

1-الدستور الجزائري الصادربتاريخ 07 ديسمبر 1996 في الجريدة الرسمية رقم 76 المؤرخة في 08 ديسمبر 1996 ، المعدل بمقتضي:

- القانون رقم 02-03 المؤرخ في 15 نوفمبر2002 ، الجريدة الرسمية رقم 25 المؤرخة في24 افريل 2002.
- القانون رقم 08-19 المؤرخ في 15 نوفمبر 2008 ، الجريدة الرسمية رقم 63 المؤرخة في 16 نوفمبر 2008.
- القانون رقم 01/16 المؤرخ في 06 مارس 2016 ، الجريدة الرسمية رقم 14 المؤرخة في 07 مارس 2016.

ب. القوانين

1- الأمر رقم 66-155 المؤرخ في 18 صفر1386 هـ الموافق ل 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل و المتمم ،الصادر بالجريدة الرسمية عدد 48 ،الصادرة في 09 يونيو 1966.

2- الأمر رقم 66-156 المؤرخ في 18 صفر 1386 هـ الموافق ل 8 يونيو 1966 يتضمن قانون العقوبات المعدل و المتمم ، الصادر بالجريدة الرسمية عدد 49 ، الصادرة في 11 يونيو 1966.

3- نظام مكافحة الجرائم المعلوماتية السعودي الصادر عن مجلس الوزراء رقم 79 لسنة1428 هجري .

4- القانون رقم 09-04 المؤرخ في 14 شعبان 1430 هـ الموافق ل 05 أوت2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، الجريدة الرسمية عدد 47 الصادرة في 16 أوت 2009.

5- قانون مكافحة جرائم تقنية المعلومات الإتحادي الاماراتي رقم 05 لسنة 2012.

6- قانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات الكويتي.

II/ قائمة المراجع

أ .الكتب العامة

1- أبو الفضل جمال الدين محمد بن مكرم (إبن منضور) معجم لسان العرب ، دار صادر، لبنان .

2- عبد الرحمان توفيق احمد ، شرح قانون العقوبات ، القسم العام وفق أحدث التعديلات، ط3 ، دار الثقافة و النشر و التوزيع ، عمان 2012.

3- عز الدين طباش ، شرح القسم الخاص من قانون العقوبات ، جرائم ضد الأشخاص و الاموال ، د ط ، دار بلقيس ، الدار البيضاء ، الجزائر ، د ت ن.

4- نبيل صقر ، الوسيط في جرائم الأشخاص ، د ط ، دار المهدي ، عين مليلة ، الجزائر، 2009

ب .الكتب المتخصصة

1- الشحات ابراهيم محمد منصور ، الجرائم الإلكترونية في الشريعة الإسلامية و القوانين الوصفية ، بحث فقهي مقارن ، ط1 ، دار الفكر الجامعي ، الإسكندرية 2011.

2- أسامة احمد المناعسة ، جلال محمد الزعبي ، جرائم تقنية المعلومات الالكترونية (دراسة مقارنة) ، ط2 ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن 2014.

3- خالد عياد الحلبي ، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت ، الطبعة الأولى ، دار الثقافة للنشر و التوزيع ، د ب ن ،2011.

4- صالح العقيلي و آخرون ، الحاسوب البرمجيات و المعدات ، د ط ، دار الشروق للنشر و التوزيع ،عمان ، الاردن 1995.

5- عبد الصبور عبد القوي على مصري ، الجريمة الالكترونية ، ط1 ، دار العلوم للنشر و التوزيع ، القاهرة 2008.

6- غنية باطلي ، الجريمة الالكترونية ، دراسة مقارنة ، الدار الجزائرية للنشر و التوزيع ، د ط ، الجزائر 2016.

7 - فتيحة محمد قوراري ، غنام محمد غنام ، المبادئ العامة في قانون الإجراءات الجزائية الإتحادي لدولة الإمارات العربية المتحدة ، (معلق عليه بأحكام المحكمة الإتحادية العليا و محكمة تمييز) وفقا لآخر التعديلات بالقانون رقم 29 لسنة 2005 ، ط 3 ، الآفاق المشرقة ناشرون ، الأردن 2013.

8- محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، ط1، جامعة نايف العربية للعلوم الأمنية ، السعودية 2004.

9- ممدوح عبد الحميد بن عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الأنترنت ، دط، دار الكتب القانونية ، مصر 2006.

10- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط 2 ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن 2010.

11- هشام فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة ،أسيوط، مصر، د ط ، 1994 .

ج .الأطروحات و المذكرات الجامعية

1.أطروحات الدكتوراه

1- التوجي محمد ، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال ، رسالة مقدمة لنيل شهادة الدكتوراه (LMD) في الحقوق ، تخصص قانون جنائي ، كلية الحقوق و العلوم السياسية ، جامعة احمد دراية ، أدرار،2019 .

2- رابحي عزيزة ، الأسرار المعلوماتية و حمايتها الجزائية ،اطروحة لنيل شهادة الدكتوراه ، علوم في القانون الخاص ، جامعة ابو بكر بلقايد ، تلمسان، 2018.

2. رسائل الماجستير

1- ثنيان ناصر آل ثنيان ، إثبات الجريمة الإلكترونية ، دراسة تأصلية تطبيقية ، رسالة ماجيستير ، جامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا ، السعودية، 2012.

2- صغير يوسف الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة الماجيستير في القانون ، كلية الحقوق و العلوم السياسية ، مدرسة الدكتوراه ، "القانون الأساسي و العلوم السياسية" ، جامعة مولود معمري ، تيزي وزو ، تاريخ المناقشة 2013/03/06.

3- محمد بن عبد المحسن بن شلهوب ، جريمة الإبتزاز الالكتروني ، دراسة مقارنة ، بحث تكميلي لنيل درجة الماجيستير في السياسة الشرعية ، المعهد العالي للقضاء ، قسم السياسة الشرعية ، شعبة الأنظمة ، جامعة الإمام محمد بن سعود الإسلامية ، 2011 .

د .المقالات

1- أحمد حسن عبد العليم حسن الخطيب ، الجرائم المعلوماتية الواقعة عبر مواقع التواصل الإجتماعي ، مقال منشور بمجلة الدراسات الإفريقية ، و حوض النيل ، مجلة دورية محكمة تصدر عن المركز الديمقراطي العربي في برلين ، المانيا ، المجلد 02 ، العدد 06 ، أكتوبر 2019.

2- المطلق نورة بنت عبد الله بن محمد ، إبتزاز الفتيات أحكامه و عقوبته في الفقه الإسلامي ، جامعة محمد بن سعود الإسلامية ، الرياض .

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

4- 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.

5- حفيظة سليمان أحمد البراشدية ، الفيسبوك و الجرائم الالكترونية في عمان ، هل هناك علاقة ؟ مقال بمجلة دراسات المعلومات و التكنولوجيا ، جمعية المكتبات المتخصصة ، فرع الخليج العربي ، دار جامعة حمد بن خليفة للنشر ، 30 سبتمبر،2019.

6- داليا عبد العزيز ، المسؤولية الجنائية عن جريمة الإبتزاز الالكتروني في النظام السعودي ، دراسة مقارنة ، مجلة البحث العلمي ، العدد25، 2018.

7- رامي احمد الغالبي ، جريمة الإبتزاز الالكتروني و آلية مكافحتها في جمهورية العراق ، مقال منشور في مجلة ثقافتنا الأمنية ، الإصدار الثاني ، وزارة الداخلية العراقية ، مديرية العلاقات و الإعلام ، دار الكتب و الوثائق ، بغداد، 2019.

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

9- مازن سمير الحكيم ، حسين فتيخان منسي ، الإبتزاز الإلكتروني ، المفهوم و الخصائص و سبل المواجهة ، مجلة ثقافتنا الأمنية ، الإصدار الثاني ، وزارة الداخلية العراقية ، مديرية العلاقات و الإعلام ، دار الكتب و الوثائق ، بغداد، 2019.

10- ممدوح رشيد مشرف الرشيد العنزي ، الحماية الجنائية للمجني عليه من الإبتزاز ،المجلة العربية للدراسات الأمنية ، الرياض ، المجلد 33 ، العدد 70، 2017.

هـ .المداخلات

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

2- أسماء بنت راشد بن عبد الرحمان الرويشد الإبتزاز محليا ، بحث مقدم لندوة الإبتزاز (المفهوم ، الأسباب ، العلاج) ، جامعة الملك سعود ،2011.

3- الحمين عبد العزيز بن حمين بن أحمد، الإبتزاز و دور الرئاسة العامة لهيئة الأمر بالمعروف و النهي عن المنكر في مكافحته ، بحث مقدم لندوة الإبتزاز (المفهوم ، الأسباب ، العلاج) ، جامعة الملك سعود 2011.

4- دنيا عبد العزيز فهمي ، المسؤولية الناشئة عن إساءة إستخدام مواقع التواصل الإجتماعي ، بحث مقدم للمؤتمر العلمي الرابع لكلية الحقوق ، جامعة طنطا تحت عنوان القانون و الإعلام، 23-24 افريل 2017.

الفـــــهرس

ملخص:

تعرض هذه الدراسة لجريمة الإبتزاز عبر الوسائل الإلكترونية في كل من النظام السعودي و القانون الإماراتي و بعض القوانين العربية ، و قد تناولت في البداية هذه الجريمة كصورة من صور الجريمة الإلكترونية ، و عرض لتعريف ماهيتها و أنواع الجريمة و طرق إرتكابها و تلك الوسائل الحديثة المستخدمة في تنفيذ الجريمة بعرض أركانها كما يتعرض البحث لدوافع الجريمة و الآثار التي تترتب عليها ، و كان عرض جريمة الإبتزاز الإلكتروني إيذانا بعرض الأركان المكونة لها الركن الشرعي و الركن المادي و الركن المعنوي و كذا عرض العقوبات المقررة لجريمة الإبتزاز الالكتروني و لحالات التشديد و الإعفاء و لعقاب الشروع و المساهمة الجنائية ، مقارنة بينهما عارضة لأوجه النقص و القصور و لأوجه التمام بغرض الإفادة من هذا النقص و ذلك التمام في النواحي التشريعية.

و تعالج الدراسة الإشكاليات التي تثيرها جريمة الإبتزاز الإلكتروني من الناحية الإجرائية من إجراءات التحقيق و خصوصية هذه الإجراءات التي تلقي بعراقيل و صعوبات أمام جهات التحقيق ، كما نتعرض لأهم طرق الإثبات التي تختص لجريمة الإبتزاز عبر الوسائل الالكترونية و نعني الدليل الرقمي بتعريفه و الوقوف على ماهيته و أقسامه و الصعوبات التي تواجه جهات التحقيق في إعتبار الدليل الرقمي و التعامل معه كدليل إثبات.

Summary :

This study deals with crime of electronic extortion in both of the Saoudi system and UAE law and some arab legislation , it first dealt with this crime , the types of crime , the ways of commiting it , and the modern means used in escecuting the crime .

The study of the motives of this crime and the implications thereof , and the presentation of the crime of electronic extortion , the presentation of the elements of constituent elements of the text (the legal corner,the physical and moral corner) , and penalties for extortion , for cases of emphasis and criminal contribution , punishment of initiation and criminal contribution .

A comparison between them is symptomatic deferences and completness , in order to benefit from this deficiency , lesgislative expects.

The study adress the problems raised by the crime of electronic blackmail in procedural terms of the procedures of the investigation , and specificity of these procedures , whitch give obstecles and difficulties to the investigation bodies.

We also present the most important methods of proof of the crime of electronic blackmail , namely the digital evidence , definition and identification of what it is and its divisions and the difficulties facing the investigation bodies in concidering the digital evidence and dealing with it as proof.