الحماية الجنائية للطفل من جرائم الابتزاز الالكتروني

إعـــداد الدكتور

محمــود رجــب فتــح الله

دكتوراه القانون العام

والمحاضر بكلية الحقوق جامعة الاسكندرية

٢٠٢٢

عدد خاص بالمؤتمر الدولى

قال تعالى :

(وَلَا يَأْتِينَ بِبُهْتَانٍ يَفْتَرِينَهُ بَيْنَ أَيْدِيهِنَّ وَأَرْجُلِهِنَّ) (*)

صدق الله العظيم

(*) القرآن الكريم – سورة الممتحنة، الآية ١٢ .

أولا : مقدمة عامة:

لقد عرف القرن العشرين تطورا مذهلا في مجال الاتصالات، وشكلت الشبكة المعلوماتية الدولية مثار هذا القرن التي امتدت عبر كامل أنحاء المعمورة وربطت بين شعوبها، فأصبحت وسيلة التعامل اليومي بين أفراد مختلف الطبقات والمجتمعات.

وأمام اختلاف العقليات والمستويات العلمية لمستعملي شبكة الانترنت ظهرت ممارسات غير مشروعة، فأصبحت هذه الشبكة أداة ارتكابها أو محلا لها حسب الحالة، مما أدى إلى ظهور طائفة جديدة من الجرائم المستحدثة، والمختلفة عن باقي الجرائم التقليدية، وقد سميت بجرائم الابتزاز الالكتروني .

وهكذا جاء التقدم الفني مصحوباً بصور مستحدثة لارتكاب الجرائم، التي تستعير من هذه التقنية أساليبها المتطورة، فأصبحنا أمام ظاهرة جديدة هي ظاهرة جرائم الابتزاز الالكترونيCyber extortion crime .

ثانياً: أهمية الدراسة:

تكمن أهمية دراسة هذا الموضوع لما يكتسبه من جدية وغموض، أمام انتشار ظاهرة جرائم الابتزاز الالكتروني للطفل، مقابل الاتجاه القانوني الحديث في التشريع الوطني بالموازاه لما تعرفه مقاهي الانترنت من إقبال واسع وإدمان شبابنا على شاشات الحاسب، وربط اغلب مصالحنا وإداراتنا بالشبكة المعلوماتية، مما يدفعنا للبحث عن الأسلوب الأمثل للتعامل مع هذه الظاهرة بسبب ما خلفته من حيرة لدى رجال القانون لعدم إمكانية تطبيق النصوص القانونية السارية بالنظر إلى عدم تناسبها مع طبيعة جرائم الابتزاز الالكتروني، التي تغزو مجتمعنا بمختلف فئاته.

ثالثا : اشكالية الدراسة:

بناء على ما تقدم، فإن الإشكالية التي أحرص علي طرحها ومعالجتها من خلال تسليط الضوء علي جرائم الابتزاز الالكتروني، من حيث ماهيتها وأركانها ومراحلها وخصائصها وسمات مرتكبيها، وما يمكن أن تخلفه من آثار سلبية، وطرق مكافحتها علي المستويين الوطني والدولي، ومن ثم، كشف مواطن الخلل واقتراح سبل معالجتها.

رابعا : أهداف الدراسة :

تستهدف الدراسة تحديد الأدلة الجنائية في جرائم الابتزاز الالكتروني الموجهة للطفل، في اطار عرض تطبيقات عملية لجرائم الابتزاز الالكتروني.

خامسا : منهج الدراسة:

يعتمد البحث الأسلوب النظري الاستقرائي في تناوله لمكافحة جرائم الابتزاز الالكتروني ، والتي تهاجم كل المبادئ والأسس القانونية.

سادسا : خطة الدراسة:

وبناء على ما تقدم، فإن الإشكالية التي أحرص علي طرحها ومعالجتها من خلال تسليط الضوء علي جرائم الابتزاز الالكتروني علي الطفل، من حيث ماهيتها وأركانها ومراحلها وخصائصها وسمات مرتكبيها، وما يمكن أن تخلفه من آثار سلبية، وطرق مكافحتها علي المستويين الوطني والدولي للقضاء عليها أو علي الأقل الحد منها، ومن ثم، كشف مواطن الخلل واقتراح سبل معالجتها.

- **الفصل الأول : مفهوم جرائم الابتزاز الالكتروني.**
- المبحث الأول : تعريف جرائم الابتزاز الالكتروني وموضوعها.
- المطلب الأول : التعريف اللغوي والاصطلاحي لجرائم الابتزاز الالكتروني.

- المطلب الثاني : التعريف القانوني لجرائم الابتزاز الالكتروني.
- المطلب الثاني : التعريف القانوني لجرائم الابتزازالالكتروني.
- المبحث الثاني : أسباب جرائم الابتزاز الالكتروني وخصائصها.
- المطلب الأول : أسباب جرائم الابتزاز الالكتروني.
- المطلب الثاني : خصائص جرائم الابتزاز الالكتروني.
- **الفصل الثاني : أنواع ومخاطر جرائم الابتزاز الالكتروني وصورها.**
- المبحث الأول : أنواع جرائم الابتزاز الالكتروني.
- المبحث الثاني : مخاطر جرائم الابتزاز الالكتروني.
- المطلب الأول : المخاطر الاجتماعية لجرائم الابتزاز الالكتروني.
- المطلب الثاني : المخاطر الاقتصادية لجرائم الابتزاز الالكتروني.
- المطلب الثالث : المخاطر الأمنية لجرائم الابتزاز الالكتروني.
- المبحث الثالث : صور جرائم الابتزاز الالكتروني.
- المبحث الرابع : واقع جرائم الابتزاز الالكتروني على المستوى الدولى والعربي.
- المطلب الأول : واقع جرائم الابتزاز الالكتروني على المستوى الدولي.
- المطلب الثاني : واقع جرائم الابتزاز الالكتروني في الوطن العربي.
- **الفصل الثالث : جرائم الابتزاز الالكتروني التي تستهدف الاطفال.**
- **الفصل الرابع : الادلة المعلوماتية في جرائم الابتزاز الالكتروني.**
- المبحث الاول : معوقات الاثبات الجنائي في جرائم الابتزاز الالكتروني.
- المطلب الاول : معوقات الوصول إلى الدليل في جرائم الابتزاز الالكتروني.
- المطلب الثاني : سهولة إخفاء الدليل او محوه في جرائم الابتزاز الالكتروني.
- المطلب الثالث : غياب الدليل المرئي في جرائم الابتزاز الالكتروني.
- المطلب الرابع : صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية.
- المطلب الخامس : مدى الضخامة البالغة لكم البيانات المتعين فحصها.
- **الفصل الخامس : تطبيقات عملية لجرائم الابتزاز الالكتروني ضد الطفل.**
- المبحث الاول : حالات عملية لجرائم الابتزاز الالكتروني على الصعيد العربي.

- المبحث الثاني : نماذج لبعض القضايا المتعلقة بجرائم الابتزاز الالكتروني في مصر.
- المطلب الاول : قضية ابتزاز الكتروني علي قاصرة.
- المطلب الثاني : قضية تهديد وابتزاز وتشهير معلوماتى.

التوصيـات

الفصل الأول

مفهوم جرائم الابتزاز الالكتروني

تمهيد وتقسيم:

من المقرر ان المعلوماتية، قد أسهمت بشكل كبير في تغيير مبادئ الفهم القانوني، خاصة في القانون الجنائي، نظرا لظهور قيم حديثة ذات طبيعة خاصة، محلها معلومات ومعطيات.

ومن ثم، أصبحت جريمة الابتزاز الالكتروني، من أخطر أنواع الجرائم التي أوجدتها المعلوماتية، ويعد هذا إهداراً حقيقياً ليس فقط لحقوق مبتكريها الخاصة، بل وأيضا مساسا خطيرا بحقوق المجتمع ككل، مما ينعكس سلبا على الاقتصاد الوطني[1] مع ما يمكن أن ينجم عنه من زعزعة للأمن الاجتماعي، ومثال ذلك التعديات على البرامج المعلوماتية التي يبدعها بعض المؤلفين، الامر الذي يدفع إلى تقدير الخسائر التي يمكن أن تمنى بها هذه الملكية الفكرية، حال تعرضها للعدوان المعلوماتي.

وعلى اثر هذا الواقع التقني، ظهرت مصطلحات عديدة دالة على الأفعال الجريمة المتصلة بالتقنية، بعضها دل على الأفعال المتصل على نحو خاص بالحوسبة، والبعض الاخر شمل بدلالته قطبي التقنية، وبعضها الثالث دل على عموم التقنية باعتبارها تحقق من اندماج وتألف بين ميادينها، ومع أتساع استخدام الانترنت برزت اصطلاحات جديدة تحاول التقارب مع هذه البيئة المجمعة للوسائط التقنية ولوسائل المعالجة وتبادل المعلومات.

ويقتضي بحث ماهية جرائم الابتزاز الالكتروني، استعراض التعريفات المختلفة للجريمة وموضوعها في مبحث أول ومن ثم اسباب تلك الجريمة

---

(١) راجع في ذلك: د.عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة ١٩٨٨، الدار الجامعية، بيروت، ص ٢٥٩ .

وسماتها وخصائصها وسمات مرتكبيها ودوافعهم في مبحث ثان، على الترتيب التالي.

المبحث الأول

تعريف جرائم الابتزاز الالكتروني وموضوعها

بصدد التطرق الى تعريف جرائم الابتزاز الالكتروني، يتضح أن لها نفس هيكل الجريمة العادية ولكن حين الخوض في التعريف، يظهر الفارق الضخم بين الجريمتين، فمن عالم واقعي الى عالم افتراضي أوجدته الثورة التكنولوجية، حينما ظهرت جرائم الابتزاز الالكتروني.

ويلاحظ تعدد التعريفات التي تناولت جرائم الابتزاز الالكتروني، ومرجع ذلك إلي الخلاف الذى أثير بشأن تعريف هذه الجريمة، ومن قبلها تعريف المعلومة ذاتها، فجرائم الابتزاز الالكتروني هي صنف جديد من الجرائم، ذلك أنه مع ظهور ثورة المعلومات والاتصالات ظهرت طائفة جديدة من المجرمين تناقلوا الجريمة من صورتها التقليدية إلى أخرى معلوماتية قد يصعب التعامل معها.

ولأن جرائم الابتزاز الالكتروني، هي من الظواهر الحديثة؛ ولارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات، فقد أحاط تعريف تلك الجرائم الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها، ولكن الفقه لم يجمع علي تعريف محدد لها، بل أن البعض ذهب إلى عدم وضع هذا التعريف تذرعا بأن هذا النوع من الإجرام ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني.

وترتيبا علي ذلك، يتعين عرض التعريف اللغوي والاصطلاحي لجرائم الابتزاز الالكتروني، في مطلب اول، علي ان يخصص المطلب الثاني لبيان التعريف القانوني لجرائم الابتزاز الالكتروني، علي الترتيب التالي.

المطلب الأول

التعريف اللغوي والاصطلاحي لجرائم الابتزاز الالكتروني

نظرا لما ترتب على الثورة المعلوماتية التي عرفتها المجتمعات الإنسانية من صدى كبيرا أدى إلى زعزعة الفهم التقليدي الذى ظل سائدا امدا طويلا من الزمن، ولم يكن الإجرام بمنأى عن هذه التحولات، بل حاول المجرمون أن يتلائموا مع الفهم الجديد، وابتدعوا أساليب ووسائل حديثة، تمكنت من تجاوز الأساليب التقليدية التي كانت معتادة لارتكاب الجرائم التقليدية، مما أدى إلى ظهور انماط جديدة كجرائم الابتزاز الالكتروني .

ذلك أن مفهوم جرائم الابتزاز الالكتروني، يحتاج إلى دراسة موضوعية لحصر نطاقه وتحديد طبيعة هذه الجريمة وخصائصها التي تميزها عن غيرها من الجرائم الأخرى مع بسط نظامها القانوني في مصر وغيرها من الأنظمة القانونية المقارنة.

حيث ان الفقه القانوني يتفادى غالبا التسرع إلى وضع تعريفات للظواهر القانونية الجديدة، لأنها تتميز بالتغير والتقلب وعدم الثبات، حتى لا يكون التعريف بمثابة مجازفة غير مأمونة العواقب، ومع ذلك نالت جرائم الابتزاز الالكتروني اهتماما كبيرا من جانب الفقه الجنائي الذي خصص لها تعريفات متعددة وانطلق في اطارها من زوايا مختلفة.

اذ عرف الابتزاز لغة، علي انه أخذ الشيء بجفاء وقهره وابتزه، سلبه ورمى به، ولم يرده، وعلي ذلك الابتزاز لغة، مأخوذ من البز، وهو السلب، ومنه قولهم عز بز، ومعناه غلب وسلب، وابتزت الشي استلبته وبزه يبزه بزا غلبه وغصبه.

ذلك ان الابتزاز من الناحية اللغوية؛ هو محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه المعنوي للضحية، وذلك بالتهديد بكشف أسرار أو معلومات خاصة.

والابتزاز بهذه الصورة يمتد ليشمل جميع القطاعات، فنجد ما يسمى بالابتزاز السياسي والابتزاز العاطفي والابتزاز الإلكتروني، وفقا للغرض محل الابتزاز .

ويعرف الابتزاز في الاصطلاح القانوني؛ بانه جريمة ترتكب ضد شخص لاجباره على تسليم المال او التوقيع على وثيقة بتهديد لكشف امر معين او لصق تهمة بارتكاب جريمة وتقاس بالدرجة التي يحصل عليها المستجيبون على الاداة المستخدمة .

فيعرف اصطلاحا بانه استخدام التهديد بالايذاء الجسدي او النفسي او الاضار بالسمعة والمكانة الاجتماعية بتلفيق الفضائح والصاق التهم، ونشر اسرار مما يجبر الشخص المبتز على دفع مكرها ، لمن يمارس الابتزاز عليه.

المطلب الثاني

التعريف القانوني لجرائم الابتزاز الالكتروني

لكى يمكن وضع تعريف محدد جامع مانع لجريمة الابتزاز الالكتروني، يجب مراعاة عدة اعتبارات مهمة منها:

- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.
- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.
- أن يحدد التعريف الدور الذي يقوم به جهاز الحاسب الآلي في إتمام النشاط الإجرامي.
- أن يفرق هذا التعريف بين الجريمة العادية وجريمة الابتزاز الالكتروني، وذلك عن طريق إيضاح الخصائص المميزة لجريمة الابتزاز الالكتروني.

وترتيبا على ذلك، يجب الوقوف على المفهوم القانوني للمعلومات، وهو ما نتعرض له أولا، وصولا إلى التعريف المقترح لجرائم الابتزاز الالكتروني.

الفرع الأول

المفهوم القانوني للمعلومات

من المسلم به أن المعلومات أصبحت في العصر الراهن سلعة تباع وتشترى ومصدر قوة اقتصادية وسياسية وعسكرية، نظرا لارتباطها بمختلف مجالات النشاط الإنساني ودورها الجوهري في كافة جوانب الحياة العصرية، وأمسي الوعي بأهميتها مظهرا لتقدم الأمم والشعوب.

وسوف نعرض هنا، لماهية المعلومة من حيث تعريفها ثم أنواعها والشروط اللازم توافرها فيها.

أ) تعريف المعلومة:

لم تعد المعلومات الآن مجرد نوع من الرفاهية والترف تتباهى بها الشعوب أو المنظمات، وإنما أصبحت ركيزة أساسية في تقدم وتطور المجتمع وتحقيق تقدمه المنشود، ولأجل ذلك وضع عدد غير قليل من التشريعات الوطنية المختلفة تعريفا للمعلومة، وهو ما سوف نعرض للعديد منها.

فقد عرف المشرع الامريكي، المعلومات في قانون المعاملات التجارية الإلكتروني لعام ١٩٩٩ بالغصن العاشرة من المادة الثانية بأنها تشمل البيانات والكلمات والصور والأصوات والوسائل وبرامج الحاسب الآلي والبرامج المضغوطة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.

ويلاحظ على التعريف السابق انه قد وسع من مفهوم المعلومة ووضع تقريبا كل ما يتعلق بها، بل أكثر من ذلك أنها تحتسب ما قد يظهر من تطور تكنولوجي جديد.

والمشرع الفرنسي ووفقا للقانون ٨٢-٦٥٢ الصادر في ٢٦ يوليو لسنة ١٩٨٢، يعرف المعلومة على أنها صورة أو مستندات أو معطيات أو خطابات أيا كانت طبيعتها.

أما قانون البحرين رقم ٨٣ لسنة ٢٠٠٢ بشأن المعاملات المعلوماتية، فقد عرف المعلومات بأنها البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسب الآلي والبرمجيات ويمكن أن تكون قواعد البيانات والكلام.

كما عرف قانون إمارة دبي بشأن المعاملات والتجارة المعلوماتية رقم ٢ لسنة ٢٠٠٢، المعلومات او المعلوماتية بأنها معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب إلى أو غيرها من قواعد البيانات.

ويتضح من ذلك، ان مجموعة التشريعات التي وضعت تعريفا واضحا للمعلومة والمعلومات كان أغلبها يدور حول الأشكال المختلفة للمعلومات وصورها التي تظهر فيها، سواء تعلق الأمر برموز أو صور أو بيانات.

وقد ذهب البعض إلى ضرورة التفرقة بين المعلومات والبيانات، فالبيانات تعبر عن مجموعة من الأرقام والرموز والحقائق التي لا علاقة بين بعضها البعض، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات.

ب) أنواع المعلومات:

تقسم المعلومات إلي ثلاث طوائف هي، المعلومات الاسمية والمعلومات المتعلقة بالمصنفات الفكرية والمعلومات المباحة.

أما الطائفة الأولي وهى المعلومات الاسمية، فتتقسم إلي مجموعتين هما:

- **المعلومات الموضوعية** وهى تلك المعلومات المرتبطة بشخص المخاطب بها، مثل اسمه وموطنه وحالته الاجتماعية، وهى معلومات لا يجوز الإطلاع عليها إلا بموافقة الشخص نفسه.
- **المعلومات الشخصية** ويقصد بها تلك المعلومات المنسوبة لآخر مما يستدعى إدلاء الغير برأيه الشخصي فيها، ومثالها المقالات الصحفية والملفات الإدارية للعاملين لدى جهة معينة.

وأما **الطائفة الثانية**، وهى المعلومات الخاصة بالمصنفات الفكرية، فهذه المصنفات محمية بموجب قوانين الملكية الفكرية مثل الاختراعات والابتكارات المختلفة والتسجيلات الفنية والمؤلفات الأدبية.

وأما **الطائفة الثالثة** وهى المعلومات المباحة، فيقصد بها تلك المعلومات التى تكون مباحة للجميع الحصول عليها، لأنها بدون مالك مثل تقارير البورصة والنشرات الجوية، وهذه المعلومات مباحة للكافة وغير محمية بأي من وسائل الحماية(١).

جـ) الشروط التي يجب توافرها في المعلومة محل الحماية:

هناك شروط عامة يتعين توافرها في المعلومة حتى تتمتع بالحماية القانونية وتتمثل هذه الشروط في الآتي:

أولا : أن يتوافر في المعلومة التحديد والابتكار.

ذلك ان المعلومة التي تفتقد لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فإذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة، وهذا يتطلب أن تكون محددة

---

(١) يعتبر مصطلح " البورصة "من المسميات التي تطلق على سوق الأوراق المالية ويعود هذا المصطلح إلى القرن الخامس عشر الميلادي، حيث كان التجار القادمين من فلورنسا يجتمعون في فندق تملكه عائلة تسمى Van der bourse ، يقع في مدينة بروج البلجيكية، والذي كان يؤمه التجار من كافة المناطق، وتطور التعامل فيه للدرجة التي أصبح معها التجار لم يصطحبوا معهم بضائعهم إلى الفندق، بل كانت تتم الارتباطات في شكل عقود=-=وتعهدات، ومن ثم استبدلت البضائع الحاضرة بالتزامات مستقبلية قائمة على ثقة متبادلة بين الطرفين، وأتى لفظ Bourse ليعبر عن المكان الذي يجتمع فيه التجار بشكل منتظم ودوري لإبرام الصفقات، راجع في ذلك، د. محسن أحمد الخضيري: كيف تتعلم البورصة، ايتراك للنشر والتوزيع، الطبعة الثانية ، سنة ١٩٩٩، ص ٢٣، ٢٤، هامش رقم (١).

تحديدا دقيقا، سيما في مجال الاعتداء على الأموال، فهذه الاعتداءات تتطلب أن يكون هناك شيء محددا ومبتكرا، أما الشيء الشائع فلا يتمتع بأي حماية قانونية.

ثانيا : أن يتوافر في المعلومة السرية والاستئثار.

اذ ان السرية صفة لازمة للمعلومة محل الحماية القانونية، ولا يتصور في جرائم الابتزاز الالكتروني وقوعها إذا انعدم هذا الوصف، وذلك لان المعلومة العامة الشائعة تكون بمنأى عن أي حيازة.

وتكتسب المعلومة وصفها، إما بالنظر إلى طبيعتها أو بالنظر إلى إرادة الشخص أو إلي الأمرين معا مثل الرقم السري (passwoard).

وترتيبا على ذلك، حتى تتمتع المعلومة بالحماية القانونية، فلابد أن يتوافر فيها الشرطان السابقان، فإذا فقدتهما أصبحت معلومة غير محمية، ولا يملكها أحد وغير قابلة لأن يستأثر بها أي شخص بل أصبحت عامة لكل من يريد استخدامها.

الفرع الثاني

التعريف المقترح لجرائم الابتزاز الالكتروني

علي الرغم من صدور قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ في مصر، إلا أن المشرع لم ينص فيه علي جريمة الابتزاز الالكتروني، سيما وتجريمه الدخول غير المشروع علي المواقع والصفحات والحصول علي البيانات الشخصية لمستخدمي الموقع والصفحات ومعالجتها إلكترونيا، وكذا الاعتداء علي الحياة الخاصة والقيم الاسرية.

ولعل خطة المشرع في الاغفال قد يكون لها ما يبررها، بذريعة أن نصوص قانون العقوبات الحالي كفيله بالعقاب علي الابتزاز الالكتروني، بل قد تتعدد الجرائم في حق المبتز، إذ يسند إليه احدي جرائم تقنية المعلومات بالإضافة إلي جريمة التهديد المنصوص عليها في قانون العقوبات وعندئذ، تطبق

عقوبة الجريمة الأشد طبقا للمادة ٣٢ عقوبات، وذلك متي توافر الارتباط الذي لا يقبل التجزئة.

فنجد المادة ٣٢٧ من قانون العقوبات المصري، تحمى المبتز بالنص على كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو الأشغال الشاقة المؤبدة أو المؤقتة أو بإفشاء أمور أو نسبة أمور مخدوشة بالشرف، وكان التهديد مصحوبا بطلب أو بتكليف بأمر يعاقب بالسجن، ويعاقب بالحبس إذا لم يكن التهديد مصحوبا بطلب أو بتكليف بأمر وكل من هدد غيره شفهيا بواسطة شخص أخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على ٥٠٠ جنيه سواء أكان التهديد مصحوبا بتكليف بأمر أم لا، كل تهديد سواء أكان بالكتابة أم شفهيا بواسطة شخص أخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مدة لا تزيد على ٦ أشهر أو بغرامة لا تزيد على ٢٠٠ جنيه.

إذن حتى يتم معاقبة المبتز، يجب أن يبتز أو يهدد ضحيته أما عن طريق الكتابة، ولا يكون التهديد مجرماً إذا كان شفاهة إلا إذا تم بواسطة شخص آخر أي أن المبتز حين يهدد ضحيته بنفسه، ولكن شفاهة فهو خارج إطار المحاسبة قانوناً ويمكن أن ينجو بفعلته.

ولعل المشرع المصري حين صاغ قانون مكافحة جرائم تقنية المعلومات، لم يكن يعي أن جريمة الابتزاز والتهديد باستخدام البيانات الشخصية للضحية أو صورها والمتحصلة باستخدام الإنترنت هي من جرائم تقنية المعلومات، لذا لا نجد أى إشارة ولو من بعيد حول جرائم الابتزاز الالكتروني.

وقد استقر قضاء النقض على أن "ركن التهديد في جريمة الحصول بالتهديد على مبلغ من النقود ليس له شكل خاص، فهو يتحقق بحصول التهديد كتابة أو شفاهه أو بشكل رمزي، وتتخذ الكتابة أي صورة كرسائل إلكترونية، بما يسمح بدخول وسائل التواصل الاجتماعي ضمن الركن المادي لجريمة التهديد

باعتبارها من جرائم القالب الحر التي لا تستلزم أن يحصل التهديد من خلال وسائل محددة حصريا أو شكل بعينه بل يكفي وقوع التهديد بأي وسيلة"[1].

ويكفي لتحقق القصد الجنائي في تلك الجريمة، أن يثبت للمحكمة أن "الجاني ارتكب التهديد وهو يدرك أثره من حيث إيقاع الرعب في نفس المجنى عليه، وأنه يريد تحقيق ذلك الأثر بما قد يترتب عليه من أن يذعن المجنى عليه راغماً إلى إجابة الطلب، وذلك بغض النظر عما إذا كان قد قصد إلى تنفيذ التهديد فعلاً، ومن غير حاجة إلى تعرف الأثر الفعلي الذى أحدثه التهديد في

---

(١) محكمة النقض المصرية : الطعن رقم ١٧٦ لسنة ٢٦ مكتب فنى ٧ صفحة رقم ٧٥٨ بتاريخ ٢١-٥-١٩٥٦، اذ قضي بأن " المقصود بالتهديد بإفشاء أمور أو نسبة أمور مخدشة بالشرف والمنصوص عليها بالفقرة الأولى من المادة ٣٢٧ من قانون العقوبات، هو إفشاء أمور أو نسبة أمور لو كانت صادقة لأوجبت عقاب من أسندت إليه أو أوجبت إحتقاره عند أهل وطنه، وهى الأمور التى أشير إليها فى جريمة القذف المنصوص عليها فى المادة ٣٠٢ من قانون العقوبات، والتهديد فى هذا المعنى يشمل التبليغ عن جريمة سواء أكانت صحيحة وقعت بالفعل أو كانت مختلفة."، وكذا الطعن رقم ١٤٢٥ لسنة ٢ مجموعة عمر ٢ع صفحة رقم ٤٦٦ بتاريخ ٢٢-٢-١٩٣٢، حيث قضي بأنه " يعتبر تهديداً بإفشاء أمور خادشة لشرف مصرف توجيه عبارات إلى بعض موظفى هذا المصرف فيها إشارة إلى حصول خسائر فى أعماله وإلى فضائح إرتكبتها إدارته، وإشارة إلى أن مديرين للمصارف فى البلاد الأجنبية قد أودعوا السجن وتلميح إلى أن مديرى هذا المصرف ليسوا خيراً من أولئك المديرين، إذ أن فى هذه العبارات أشد ما يمس سمعة البنك ويهز ثقة الجمهور فى كفايته لأن المصارف المالية بطبيعتها حساسة وقد تضار بأقل تعريض بسمعتها مهما كان شأن المهاجم ضئيلاً وحجيته واهية."، وكذا الطعن رقم ١٤٢٥ لسنة ٢ مجموعة عمر ٢ع صفحة رقم ٤٦٦ بتاريخ ٢٢-٢-١٩٣٢، اذ قضي بأن " ليس للمتهم أن يتذرع بأن نشره عبارات التهديد لا يعاقب عليه إذا هو مكن من إثبات وقائعها، ذلك لأن التهديد بإفشاء الأمور الخادشة للشرف بطريقة نشرها إنما هو جريمة مستقلة بذاتها تتم بمجرد صدور التهديد سواء أحصل الإفشاء بالنشر فعلاً أم لم يحصل."

نفس المجنى عليه، كما لا يعيب الحكم إغفال التحدث عن أثر التهديد في نفس المجنى عليه وما يقال من أن المتهم لم يكن جاداً فى تهديده. (١)

ولاختيار المصطلح الدقيق، يتعين أن يتم الدمج بين البعدين التقني والقانوني، فإذا عدنا للحقيقة الأولى المتصلة بنشأة وتطور تقنية المعلومات، نجد أن تقنية المعلومات تشمل مطلبين جرى بحكم التطور تقاربهما واندماجهما، الحوسبة والاتصال.

فالحوسبة تقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، اما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة .

وهذا ما دعا مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين إلى تبنى تعريف منضبط للجريمة المعلوماتية بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسبي أو شبكة حاسبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".

ونحن من جانبنا نتفق مع هذا التعريف، إذ أنه تعريف حاول الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجرائم المعلوماتية، وعلي رأسها جرائم الابتزاز الالكتروني، سواء التي قد تقع بواسطة النظام المعلوماتي أو داخل هذا

---

(١) محكمة النقض المصرية : الطعن رقم الطعن رقم ٢١٦٧ لسنة ٤٦ مجموعة عمر ١ع صفحة رقم ٣٥٧ بتاريخ ٣١-١٠-١٩٢٩، اذ قضي بأن " لم تبين المادة ٢٨٤ عقوبات نوع الطلب أو التكليف المصاحب للتهديد، بل جاءت بلفظيهما منكرين لتقع العقوبة على التهديد، سواء أكان الطلب قائماً على مال أم على شئ آخر، وسواء أكان التكليف خاصاً بعمل أم بإمتناع عن عمل، وسواء أكان الطلب أو التكليف غير شرعى فى ذاته أم لا، فالتهديد فإفشاء أمور مخدشة تهديداً مصحوباً بطلب تنطبق عليه الفقرة الأولى من المادة ٢٨٤ عقوبات ولو كان المهدد لا يقصد إلا الحصول على حقوق له عند من هدده.".

النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة إلكترونية.

فهذا التعريف لم يركز على فاعل الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجرائم المعلوماتية، بل إنه حاول عدم حصر الجرائم المعلوماتية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.

المطلب الثاني

التعريف القانوني لجرائم الابتزازالالكتروني

من المقرر ان الابتزاز هو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيء لتدمير الشخص المهدد، إن لم يقم الشخص المهدد بالاستجابة إلى بعض الطلبات.

وهذه المعلومات تكون عادة محرجة أو ذات طبيعة مدمرة اجتماعيًا او من شأنها ان تفضي الي نتائج ضارة، وهو بمعنى الاستبزاز فلا فارق بينهما.

وبالمعنى العام، الابتزاز هو عرض طلب أن يتوقف الشخص المهدد من عمل شيء مسموح به عادة، لذا فهو يختلف عن التهديد extortion ، الذي يحمل تهديدًا ينتهي بعمل غير قانوني أو عنف ضد الشخص إن لم يستجب للمطالب.

ويسمى البعض المال المدفوع نتيجة الابتزاز رشوة إسكات، مع للتحفظ علي استخدام هذا المصطلح، للتفاوت الصارخ ما بين اللفظين قانونا، وكان مصطلح ابتزاز أصلًا مقصورًا على جمع رسوم غير قانونية بوساطة موظف عام في اطار جريمة الغدر، ويعاقب على الابتزاز بالسجن، أو بالغرامة، أو بكلتيهما ويضاف في بعض البلدان الطرد من الوظيفة.

وعلـي ذلـك، الابتـزاز الإلكترونـي، هـو الابتـزاز الـذي يـتم باسـتخدام الإمكانيات التكنولوجية الحديثة ضد ضحايا أغلبهم من النساء لابتزازهم ماديا أو جنسيا او لاغراض آخري.

وعلى الرغم من انه بات معروفاً لدى أغلبية مستخدمي مواقع التواصل الإجتماعي ومستخدمي الهواتف الذكية من أن البيانات الشخصية والصور يمكن سرقتها أو استدراج الضحية للحصول على صور أو فيديوهات لاستخدامها فيما بعد لابتزاز الضحية، إلا انه حتى ألان لم تقم مصر بتشريع يمكن من حماية الضحية من الابتزاز الالكتروني.

وعلي ذلك، يقصد بالابتزاز، تلك العمليات التي من خلالها يتم تهديد وتعريض أشخاص مستهدفين للضرر، سواء كان ذلك بطريق نشر صور أو مواد فيليمية متعلقه بهم؛ وذلك مقابل مبلغ من المال أو استغلالهم ودفعهم للقيام بأعمال غير مشروعة أو غير قانونية.

وتعد جريمة الابتزاز الإلكتروني من الجرائم المستحدثة بفعل التقدم الكبير في تكنولوجيا المعلومات، مما جعل من العالم قرية صغيرة، وسهل الكثير من أمور الحياة، ولا يخفى ما لهذا التطور من فوائد في النواحي الاقتصادية والسياسية والاجتماعية والعلمية إلا أنه لم يخلو من مواطن خلل، فقد سهلت لظهور نوع من المرجمين يستخدمون هذه التقنيات لتنفيذ جرائمهم بواسطتها، وفي مقدمة تلك الجرائم تتجلي جرائم الابتزاز الالكتروني .

وترتيبا علي ما تقدم، يتضح ان جرائم الابتزاز الإلكتروني (Cyber extortion crime) هي أن يتعرّض نظامٌ حاسبيّ او موقعٌ إلكترونيّ ما لهجماتِ حرمانٍ من خدمات مُعيّنة؛ حيثُ يشنّ هذه الهجمات ويُكرّرها قراصنة محترفون، بهدفِ تحصيلِ مُقابلٍ ماديّ لوقف هذه الهجمات.

المبحث الثاني

أسباب جرائم الابتزاز الالكتروني وخصائصها

لجريمة الابتزاز متي وقعت الكترونية طبيعتها الخاصة، التي يجعلها تحتفظ باسبابا أيضا خاصة، تميزها عن جرائم الابتزاز التقليدية، فضلا عن اتسامها بخصائص مميزة، تختلف عن تلك التي تتصف بها الجرائم التقليدية ايضا، لكون جرائم الابتزاز الالكتروني تتميز بعدد من الخصائص التي تختلف تماما عن الخصائص التى تتمتع بها الجرائم التقليدية، كما أن الجانى المعلوماتي أو المجرم المعلوماتي يختلف أيضا وبالتبعية عن المجرم العادى.

المطلب الأول

أسباب جرائم الابتزاز الالكتروني

لاشك أن فئات مرتكبي جرائم الابتزاز الالكتروني تتميز عن مرتكبي الأفعال الإجرامية التقليدية، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع في ارتكاب الفعل غير المشروع.[١]

---

(١) وتتنوع الجرائم المعلوماتية على النحو التالي:

- إساءة استخدام الإنترنت.
- استخدام برامج حل وكشف كلمات المرور.
- نشر برامج حصان طروادة وغيرها من الفيروسات.
- هجمات المخربين.
- الهجمات الاختراقية.
- الانتهاكات الأمنية التي تتضمن حالات إساءة استخدام عن طريق الدخول غير المخول به على النظام : وتتبع غالبية الانتهاكات الأمنية من مصادر داخلية، مثال : مستخدمين من داخل المؤسسة يحاولون الوصول إلى بيانات سرية غير مخول لهم بالإطلاع عليها.

راجع في ذلك :

Dr. Linda volonino.cyber terrorism. Op. cit 12

حيث نتج عن ثورة الاتصالات وتكنولوجيا المعلومات العديد من التطبيقات، التي من شأنها التأثير بدرجة كبيرة على أوجه النشاط الاقتصادي[١] والاجتماعي، من بينها التجارة الإلكترونية (e-Commerce)، والحكومة الإلكترونية (e-Government)، والتعليم عن بعد (Distance-Learning)، والعمل عن بعد (Tele- Working).

وهكذا أصبح النظام الدولي للمعلومات يعتمد على نمط جديد للتطور والسيطرة والسلطة على المعرفة العلمية المتقدمة والاستخدام الأمثل للمعلومات المتدفقة بوتيرة سريعة، ويتصف هذا النمط بسيطرة المعلومات والمعرفة على مختلف مجالات الحياة وظهور دور صناعة المعلومات باعتبارها الركيزة الأساسية في بناء الاقتصاديات الوطنية[٢] وتميز الأنشطة المعرفية الفكرية والذهنية، لتكون في أكثر الأماكن تأثيراً وحساسية في منظمات الإنتاج والخدمات.

ويتميز النظام الدولي للمعلومات في كثير من الوجوه عن النظام الصناعي، فبينما كان النظام الصناعي يعتمد في مراحله الأولى على البخار والميكانيكا والفحم والحديد وعلى الرأسمالية، وقوة الدولة العسكرية المباشرة لتأمين المواد الخام وفتح السوق من خلال الاحتلال العسكري السافر، ثم صار يعتمد على طاقة الكهرباء والنفط والطاقة النووية وفن الإدارة الحديثة والشركات الوطنية المساهمة والأحلاف العسكرية لتأمين المواد الخام والأسواق، فإن النظام الدولي للمعلومات يعتمد أساساً على العقل البشرى والإلكترونيات الدقيقة والهندسة

---

(١) راجع في ذلك: د. عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة ١٩٨٨، الدار الجامعية، بيروت، ص. ٢٥٩ .

(٢) انظر: د. عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، المرجع السابق، ص. ٢٦٤ .

الحيوية والحاسب وهندسة الاتصالات والذكاء الإصطناعى وتوليد المعلومات لكل شئون الأفراد والمجتمعات الطبيعية، واختزان هذه المعلومات واستردادها وتوصيلها بسرعة متناهية، ويعتمد كذلك على تنامي دور الشركات العملاقة متعددة الجنسيات.

وعلى ذلك يرتكز النظام الجديد في عماده وقوته الأساسية على العقل، وبذلك فإنه يعتمد على طاقة متجددة لا تنضب، ومن ثم لن يكون هذا النظام حكراً أو احتكارا للمجتمعات كبيرة المساحة أو ضخمة السكان أو الغنية بمواردها الأولية.

فهو بذلك اصبح نظام يمكن لجميع شعوب العالم أن تشارك فيه، سواء أكانت كبيرة أم صغيرة، إذا ما أحسنت إعداد نفسها وأبنائها لذلك.

ويمكن الوقوف على عدد من الخصائص الهامة التي يتسم بها النظام الدولي للمعلومات، والذى يطلق عليه "العالم الإلكتروني الجديد" على النحو التالي:

١- التسارع:

ذلك ان وتيرة الحياة هى التغير المستمر والمتلاحق، وإذا كان التغير في فجر التاريخ بطيئاً فإنه حالياً يتسم بتزايد سرعته باستمرار، ويخلق بذلك فجوة تتزايد بين الدول المتقدمة والدول النامية، ومن أمثلة هذا التسارع تنامى معدلات المعاملات الإلكترونية العالمية عبر شبكة الإنترنت.

٢- التطور التكنولوجي:

اذ تتصف التكنولوجيا بان لها صفة مميزة طبيعة اقتحامية، بمعنى أنها تقتحم المجتمعات سواء كانت تحتاج إليها أو غير راغبة فيها، وذلك بما تقدمه من سلع وخدمات جديدة أو بما تولده من حاجات إلى سلع جديدة، وغالبا ما تكون التكنولوجيا الجديدة أكثر كفاءة في الأداء وأقل ثمناً أو أصغر وأخف وزناً وأكثر تقدماً وتعقيداً من سابقتها، كما أن التكنولوجيا والمعرفة الكامنة في إنتاجها تكون أكثر كثافة وتتطلب ارتفاعا متزايداً للقدرات البشرية وخاصة للعلماء

والمطورين والمهندسين، وتقوم على ما تتوصل إليه أنشطة الابحاث والتطوير التى تمثل أحد الركائز الأساسية للريادة في ذلك العالم الإلكتروني الجديد.

٣- اللا محدودية وانهيار الفواصل الجغرافية:

حيث ان النظام الدولي للمعلومات يقوم بتوفير الفرص للجميع للخروج إلى العالمية فوق كل الحدود وفوق كل الفواصل ويخلق ما يسمى فضاءاً لا متناهياً (Cyber Space) يتسابق فيه الجميع، ويعنى انهيار الفواصل الجغرافية، ذلك أن منتجاً صغيراً في قرية نائية في مصر، على سبيل المثال، يستطيع أن يعرض منتجاته أمام مشترى في كوريا أو الهند أو في أي مكان في العالم، واللا محدودية هنا تعنى أداء الأعمال عن بعد مع منافسة عالمية.

الأمر الذي يتطلب درجة تنافسية مرتفعة وأعلى مستوى من الجودة لتلك المنتجات، كذلك فهي تعنى قيام مجتمعاً تخيلياً (Virtual Society) يتعامل فيه الناس دون أن يلتقوا وجهاً لوجه. **٤- اللا زمنية والتنافس في الوقت:**

اذ يتصف النظام الدولي للمعلومات بالعمل في الزمن الحقيقي، حيث كل مواقع العمل والإنتاج والخدمات تعمل بلا توقف لتلبية احتياجات العملاء في جميع أنحاء العالم بالرغم من الفواصل الزمنية، فيما يعرف باستمرار العمل والإنتاج وتقديم الخدمة على مدار ٢٤ ساعة.

٥- اللا مادية وتضاؤل قيمة المكونات المادية:

حيث تتضاءلت قيم المكونات المادية في المنتجات الجديدة بصورة كبيرة، فبعد أن كانت هذه المكونات تصل إلى ٣٠٪ من قيمة المنتج، فإنها قد وصلت إلى حوالي ١٠٪ ويُنتظر أن تصل إلى أقل من ٢٪ مع تزايد قيمة المكون المعرفي والتكنولوجي، ويكمن تضاؤل قيمة المكونات المادية لعدة أسباب، أهمها:

- المواد الجديدة والمختلقة.
- تزايد قيمة المكون المعرفي في المنتج.
- تزايد قيمة وأهمية جودة المنتج وتكلفة تحقيق الجودة.

- ارتفاع تكلفة البحث والتطوير اللازمة لإنتاج المنتجات الجديدة، وعلى سبيل المثال الصناعات الدوائية والكيمائية.

هذا وتجدر الإشارة إلى أن انخفاض قيمة المكونات المادية، يهدد الدول التي تعتمد على المصادر الطبيعية كمصدر أساسي لتوليد الدخل، مما يزيد من أهمية الدول التى تمتاز بأن القيمة المضافة في منتجاتها هى المصدر الأساسي لإيراداتها (غنى الشمال وفقر الجنوب) [1].

وأسباب جرائم الابتزاز الالكتروني، منها

١- ضعف الوازع الديني .
٢- الفراغ الروحي أو العاطفي أو الوقتي ٠
٣- أصدقاء السوء ٠
٤- الاختلاط ٠
٥- ضعف الرقابة الأسرية وتقصيرها في توجيه الأبناء وعدم مراقبتهم والجهل ببعض الأمور والحرمان من المحبة والتودد والتعامل الحسن ٠
٦- التقنيات الحديثة مثل الإنترنت وبعض القنوات الفضائية والإعلام غير السوي، والبلاك بيري والجوال والهاتف وغيرها إذا ما أسيئ استخدامها ٠

---

(١) حد شمال/جنوب ويسمى أيضا خط برانت، هو خط وهمي يفصل الدول المتقدمة (دول الشمال) والدول الفقيرة والتي في طور النمو (دول الجنوب) وفي الحقيقة يشبه هذا الفصل الحد الموجود بين نصف الأرض الشمالي ونصف الأرض الجنوبي، ولكنه يمثل أساسا اللامساواة واللا عدالة في التنمية، وهذا الفصل مشكوك فيه ويتم نقده بشكل متزايد حيث لم يتم تغيير الخريطة ولم تتطور منذ سنة ١٩٨٠، في حين أن مؤشر التنمية البشرية لعدة دول من الجنوب قد تطور كثيرا وسبق مؤشر تنمية عدة دول من الشمال، مثلا مؤشر التنمية البشرية لكل من الأرجنتين، الإمارات العربية المتحدة، تشيلي، كوبا، كوستاريكا، المكسيك، ليبيا، قطر وفنزويلا يفوقون الأن مؤشر التنمية= =البشرية لرومانيا وألبانيا وأوكرانيا، كذلك البلدان الخمسة التي في طور النمو (روسيا، الصين، البرازيل، الهند، المكسيك) هم جميعا، باستثناء روسيا، يوجدون في الجزء الجنوبي، بينما هم في مرحلة نمو اقتصادي.

٧- حب التجربة والتقليد من الجنسين مما يوقعه بشباك الابتزاز ٠

٨- روايات الحب والغرام ٠

٩- الحرية المطلقة المفتوحة بدون رقيب أو عتيد للجنسين ٠

١٠- تأخر الزواج والمغالاة بالمهور ٠

١١- ضعف الشخصية لدى المجني عليه ، فيستغل الجاني هذا الضعف ويمارس عليه الضغط ٠

١٢- ضعف العقوبة لمرتكبي جرائم الابتزاز ٠

المطلب الثاني

خصائص جرائم الابتزاز الالكتروني

من المقرر ان ارتباط جرائم الابتزاز الالكتروني بجهاز الحاسب الآلي وشبكة الإنترنت أضفي عليها مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن جرائم الابتزاز التقليدية.

ذلك إن بلورة تصور واضح عن ماهية جرائم الابتزاز الالكتروني، يتطلب بالإضافة إلى بحث تعريفاتها وموضوعها، وتحديد سماتها التي تميزها عن جرائم الابتزاز التقليدية، وكذلك سمات المجرمين المعلوماتيين ودوافعهم إلى ارتكابها وهو ما سنتناوله فيما يأتي:

الفرع الأول

سمات جرائم الابتزاز الالكتروني

- أ) تتسم جرائم الابتزاز الالكتروني بصفات تميزها عن جرائم الابتزاز التقليدية، هي التالية:

١- تقع جريمة الابتزاز الالكتروني في بيئة المعالجة الآلية للبيانات، حيث يستلزم لقيامها التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي بغرض معالجتها الكترونياً، بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو

استرجاعها وطباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجريمة، ولابد من فهم الجاني لها أثناء ارتكابها في حالات الاختراق والقرصنة والولوج غير القانوني خلال تلك العمليات.

٢- ان إثبات تلك الجرائم تكتنفه الكثير من الصعوبات التي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثراً خارجياً، فلا يوجد جثث لقتلى أو أثاراً لدماء، وإذا اكتُشفت جريمة فلا يكون ذلك إلا بمحض الصدفة، والدليل على ذلك أنه لم يُكتشف منها إلا نسبة ١٪ فقط، والذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى ١٥ % من النسبة السابقة.

٣- ان أدلة الإدانة في جرائم الابتزاز الالكتروني، غير كافية إلا في حدود ٢٠٪ فقط، ويرجع ذلك إلى عدة عوامل تتمثل في عدم وجود أي أثر كتابي، إذ يتم نقل المعلومات بالنبضات المعلوماتية، كما أن الجاني يستطيع تدمير دليل الإدانة ضده في أقل من ثانية.

٤- إحجام الشركات والمؤسسات في مجتمع الأعمال عن الإبلاغ عما يُرتكب داخلها من جرائم الابتزاز الالكتروني، تجنباً للإساءة إلى السمعة واهتزاز الثقة فيها، وتكرارها مرات لاحقة من قبل آخرين.

٥- ان جرائم الابتزاز الالكتروني لا تعرف الحدود بين الدول والقارات، حيث أن القائم على النظام المعلوماتي في أي دولة يمكنه أن يرتكب فعل الابتزاز في أي مكان في العالم مضيفاً له طلب تحويل صفر أو بعض الأصفار لحسابه الخاص، بل يستطيع أي شخص أن يعرف كلمة السر لأي شبكة في العالم ويتصل بها ويغير ما بها من معلومات.

٦- **الرغبة في استقرار حركة التعامل** ومحاولة إخفاء أسلوب الجريمة حتى لا يتم تقليدها من جانب الآخرين، كل ذلك يدفع المجني عليه إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة أو الكشف عنها، حتى في حالة الضبط لا يتعاون مع جهات التحقيق خوفاً مما يترتب على ذلك من دعاية مضادة وضياع الثقة، متي كان المجني عليه في مثل هذه الحالات بنك أو مؤسسة مالية.

٧- **أسلوب ارتكاب جرائم الابتزاز الالكتروني:** حيث أن ذاتية جرائم الابتزاز الالكتروني، تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة، فإن جرائم الابتزاز الالكتروني، هي جرائم هادئة بطبيعتها(soft crime) لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسب الآلي بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة المكونة لتلك الجرائم.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية، مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة، كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، كل ذلك دون حاجة لسفك الدماء.

٨- **جرائم الابتزاز الالكتروني تتم عادة بتعاون أكثر من شخص:** حيث تتميز جرائم الابتزاز الالكتروني، بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالجهة المجني عليها، وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسب الآلي والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج جرائم الابتزاز الالكتروني، إلى حيز الوجود قد يكون اشتراكاً سلبياً وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكاً إيجابيا وهو غالباً كذلك يتمثل في مساعدة فنية أو مادية.

- ب) وتتميز جرائم الابتزاز الالكتروني بالخصائص التالية:

١. **سرعة التنفيذ:** حيث لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكبير، وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل الجريمة باركانها المادية

والمعنوية من مكان إلى آخر، وهذا لا يعني إنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

٢. **التنفيذ عن بعد:** اذ لا تتطلب اغلب جرائم الابتزاز الالكتروني، وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل، سواء كان من خلال الدخول للشبكة المعنية أو اعتراض معلومات هامة أو تخريب.

٣. **إخفاء آثار الجريمة:** حيث أن جرائم الابتزاز الالكتروني التي تقع على الحاسب الآلي أو بواسطته هي جرائم مخفية، إلا انه يمكن أن تلاحظ آثارها، والتخمين بوقوعها، مما يترتب عليه صعوبة اكتشاف جرائم الابتزاز الالكتروني.

وحيث تتميز جرائم الابتزاز الالكتروني، بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم
قليلة إذا قورنت بما يتم اكتشافه من جرائم الابتزاز التقليدية.

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف جرائم الابتزاز الالكتروني إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، إذ أن تلك الجرائم عابرة للدول، وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة، يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم.

فجرائم الابتزاز الالكتروني في أكثر صورها، خفية قد لا يلاحظها المجني عليه توا، أو لا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات المعلوماتية التي تسجل البيانات عن طريقها، أمراً ليس عسيراً في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالباً لدى مرتكبها.

كما أن المجني عليه، يلعب دوراً رئيسياً في صعوبة اكتشاف وقوع جرائم الابتزاز الالكتورني، حيث تحرص أكثر الجهات التي تتعرض أنظمتها

المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية، دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وزعزعة الثقة في كفاءتها.

ويرى البعض أن للمجني عليه دوراً مثيراً للريبة في بعض الأحيان، فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل تعرضه لجريمة الابتزاز الالكتروني أمراً مرتفعاً بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي، ويترتب على ذلك نتيجة أخرى تميز جرائم الابتزاز الالكتروني، هي إمكانية الحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم، إذ يعتمد ذلك أساساً على تطوير نظم الأمن الخاصة بأنظمة الحاسبات وشبكاتها.

وفي الواقع، إن إحجام المجني عليه عن الإبلاغ عن وقوع جرائم الابتزاز الالكتروني، يبدو أكثر وضوحاً في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة(١)، حيث تخشى مجالس إداراتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها، إلى زعزعة الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من جرائم الابتزاز الالكتروني لا يتم الكشف أو التبليغ عنه، فإن

---

(١) راجع في ذلك: د. خالد سعد زغلول حلمى – مثلث قيادة الاقتصاد العالمى – دراسة قانونية اقتصادية– الكويت – جامعة الكويت – سنة ٢٠٠٢ – صـ ٣ ، حيث يرى ان اتباع قاعدة الذهب من شانه تحقيق العديد من الفوائد للدولة التى تلتزم بها ، من اهمها ثبات سعر الصرف بين الدول المختلفة، فضلا عن عن انها تعمل على تصحيح موازين المدفوعات بطريقة الية، دون حاجة الى تدخل من السلطات المختصة بالدولة.

ذلك يؤثر سلباً في السياسة التي يمكن أن توضع لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي(١).

وإلى جانب ذلك، فإن المجني عليه يتردد أحياناً في الإبلاغ عن جرائم الابتزاز الالكتروني، خوفاً من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين كما أن الإعلان عن هذه الجرائم يؤدي أحياناً إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه.

٤. **الجاذبية:** نظرا لما تمثله سوق الحاسب الآلي والإنترنت من ثروة كبيرة للمجرمين أو الأجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وابتزاز المعلومات وبيعها أو ابتزاز البنوك[٢] أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات بابتزاز اموالها.

---

(1) John Madinger, Sydney A. Zal: Money laundering: aguide for criminal investigators, CRC press Boca Raton, London, New York, Washington D.C 1999.

مشار اليه كذلك: د. حمدي عبد العظيم: غسل الأموال في مصر والعالم، الجريمة البيضاء، أبعادها، آثارها، كيفية معالجتها، الطبعة الأولى، القاهرة، سنة ١٩٩٧، ص ٢٢٠ – ٢٢١، وايضا : عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– الناشر : جامعة نايف العربية للعلوم الأمنية – ٢٠٠٨ م – صـ ٤٦ وما بعدها، وايضا : محمد فتحى عيد، مرجع سابق، سنة ١٩٩٠، ص ١٣١.

(2) see : chehire and fifoot , the law of contract, London , 1964 , p.457.

٥. **عابرة للدول:** ذلك إن جرائم الابتزاز الالكتروني متعدية الحدود أو جريمة عابرة للدول لان المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحدود.

فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحواسب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة الواحدة في آن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل من الإمكان ارتكاب جريمة عن طريق حاسب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

وهذه الطبيعة التي تتميز بها جرائم الابتزاز الالكتروني، كونها جريمة عابرة للحدود خلقت العديد من المشكلات حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

وكانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الايدز) من القضايا التي أثارت الاهتمام بالنظر إلى البعد الدولي لجرائم الابتزاز الالكتروني، وتتلخص وقائع هذه القضية التي حدثت عام ١٩٨٩ في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأخذ البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس حصان طروادة، إذ كان يترتب على تشغيله تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس.

وفي الثالث من فبراير من عام ١٩٩٠ تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية، ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

- **الأولى:** أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة ابتزاز الكتروني.
- **الثانية:** أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث (فيروس).

ونتيجة لهذه الطبيعة الخاصة لجريمة الابتزاز الالكتروني، ونظراً للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها، ازداد الاتجاه إلى التعاون الدولي من أجل التصدي لهذه الجرائم، وهذا التعاون الدولي يتمثل في المعاهدات والاتفاقيات الدولية التي تعمل على توفير إطار من التنسيق بين الدول الأعضاء، الأمر الذي يكفل الإيقاع بمجرمي الابتزاز الالكتروني وتقديمهم للمحاكمة.

وتتمثل أهم المشكلات المتعلقة بالتعاون الدولي حول جرائم الابتزاز الالكتروني، في أنه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة، بالإضافة إلى أن نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع الأدلة عنها للإدانة فيها يشكل عائقاً كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم.

وبالتالي من أجل التصدي لجرائم الابتزاز الالكتروني، لابد أن تعمل الدول في اتجاهين:

١- **الأول:** اتجاه داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة جرائم الابتزاز الالكتروني.

٢- **الثاني:** اتجاه دولي عن طريق عقد اتفاقيات الدولية، حتى لا يستفيد مجرمو الابتزاز الالكتروني من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم، حيث أن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، وأصبحت ساحتها العالم أجمع.

ففي ظل مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث أن أغلب جرائم الابتزاز الالكتروني، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى، وقد يكون الضرر المترتب عن الجريمة ليس واقعا على المجني عليه داخل إقليم دولة الجاني، وتتعارض هنا الثقافات المتلقية لها، خاصة إذا كانت تتعارض في الدين والعرف والاجتماعي والنظام الأخلاقي والسياسي للدولة.

٦. **جرائم ناعمة:** حيث تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح، إلا أن جرائم الابتزاز الالكتروني تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، فنقل بيانات من حاسب إلى أخر أو السلب الإلكتروني بغية ابتزاز أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن.

٧. **صعوبة إثباتها:** تتميز جرائم الابتزاز الالكتروني عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي من بصمات، أو تخريب، أو شواهد مادية أخرى، وسهولة محو الدليل أو تدميره في زمن في منتهى القصر، ويضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

ويضاف إلى الصعوبات التي تكتنف اكتشاف جرائم الابتزاز الالكتروني، انه حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها، فإن إثباتها أمر يحيط به كذلك الكثير من الصعوبات الأخرى.

ذلك ان جرائم الابتزاز الالكتروني تتم في بيئة غير تقليدية، إذ تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسب الآلي والإنترنت، مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تمر عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كلياً من قبل الفاعل أمراً في غاية السهولة.

ففي إحدى القضايا الشهيرة، التي شهدتها ألمانيا قام أحد الجناة بإدخال نظام الحاسب الآلي تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا تم اختراقه من قبل الغير.

وتجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح غالباً في إثبات جرائم الابتزاز الالكتروني، نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثاراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في جرائم الابتزاز الالكتروني، يتضاءل دوره في الإفصاح عن الحقائق المفضية للأدلة المطلوبة، وذلك لسببين:

- **الأول:** إن جرائم الابتزاز الالكتروني لا تخلف آثاراً مادية كشأن الجرائم التقليدية.
- **الثاني:** إن كثيراً من الأشخاص يدخلون إلى مسرح الجريمة خلال الفترة من زمن وقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي فترة طويلة نسبياً، الأمر الذي يعطي مجالاً للجاني أو للآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية

إن وجدت، الأمر الذي يورث الشك في الدلالة القانونية لتلك الأدلة المستقاة من المعاينة في جرائم الابتزاز الالكتروني.

بالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء يشكل عائقاً أساسياً أمام إثبات جرائم الابتزاز الالكتروني.

ذلك أن هذا النوع من الجرائم يحتاج إلى الكثير من تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسب الآلي والإنترنت، ونتيجة لنقص الخبرة والتدريب كثيراً ما تخفق أجهزة الشرطة في تقدير أهمية جرائم الابتزاز الالكتروني، فلا تبذل لكشف غموضها وضبط مرتكبيها جهوداً تتناسب وهذه الأهمية، بل إن المحقق قد يدمر الدليل بمحوه محتويات الاسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة، وخاصة في مصر، حيث أن النمط اليدوي من القضايا هو المتعارف عليه بالدولة المصرية(١).

٨. **التلوث الثقافي:** لا يتوقف تأثير جرائم الابتزاز الالكتروني عند الأثر المادي الناجم عنها، وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمنغلقة، اذ غالبا ما يكون محل تلك الجرائم أمور شائنة تتعلق بالشرف والحريات.

٩. **عالمية الجريمة والنظام العدلي:** نظرا لارتباط المجتمع الدولي إلكترونيا، فقد أصبح مجتمعنا تخيليا، مما أدى إلى أن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب جرائم الابتزاز الالكتروني من كل مكان، مما يتطلب

---

(١) انظر في ذلك: سلوى شعراوى جمعة، الدولة وتحديث الجهاز الادارى، رؤية للاصلاح، مركز دراسات واستشارات الادارة العامة، جامعة القاهرة، سنة ٢٠٠٤، صـ ٣ – ٨، وايضا : مونت بالمر، البيروقراطية المصرية، ترجمة : على ليلة، مركز الدراسات السياسية والاستراتيجية بالاهرام، القاهرة، سنة ١٩٩٤، صـ ٩٥ –٩٦.

أن تتعاون الدول المتطورة وخاصة الصناعية مع الدول النامية من أجل سن تشريعات جديدة لمكافحة جرائم الابتزاز الالكتروني وأن تكون تلك القوانين ذات صبغة عالمية.

١٠. لا يبادر الكثير من المجني عليهم إلى الإبلاغ عن جرائم الابتزاز الالكتروني، إما لتأخر اكتشاف الضحية لوقائعها وإما خشيته من التشهير، لذا نجد أن معظم جرائم الابتزاز الالكتروني يتم اكتشاف الجاني فيها بالمصادفة، بل وبعد وقت طويل من ارتكابها، فضلا عن أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة، والعدد الذي تم اكتشافه هو رقم خطير، يمثل فجوة كبيرة ما بين جرائم الابتزاز الالكتروني التي لم يتم اكتشافها وتلك التي ظلت في طي السهو أو الكتمان.

١١. تعتمد هذه الجرائم على قمة الذكاء في ارتكابها، ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، إذ يصعب عليه متابعة جرائم الابتزاز الالكتروني والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض، وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، ولذلك فان الوصول للحقيقة بشأنها تستوجب الاستعانة بخبرة فنية عالية المستوى.

١٢. صعوبة المباحثة بالتعويض المدني بخصوص جرائم الابتزاز الالكتروني لكل تلك الاسباب المسبقة.

الفرع الثاني

خصوصية مجرمي الابتزاز الالكتروني

المجرم الذي يقترف جرائم الابتزاز الالكتروني، الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية فهو هناك المجرم التقليدي.

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة لجرائم الابتزاز الالكتروني، فهي

جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسب الآلي والتعامل مع شبكة الإنترنت.

فعلى سبيل المثال، إن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.

- أ) حيث إن مرتكبي جرائم الحاسب الآلي عموماً، ينتمون وفقا للدراسات المسحية إلى فئة عمرية تتراوح بين (٢٥- ٤٥) عاما، ويتميز هؤلاء بسمات عامة، يمكن النظر إليها من زاويتين:

١- الصفات الشخصية والتخصص والكفاءة:

ذلك أن الصفة الجامعة بين محترفي جرائم الابتزاز الالكتروني، هى تمتعهم بقدرة عالية من الذكاء، وإلمام جيد بالتقنية العالية، واكتسابهم معرفة عملية وعلمية، وانتمائهم إلى التخصصات المتصلة بالحاسب الآلي من الناحية الوظيفية، وهذه السمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء.

كما أن مرتكبي هذا النوع من الجرائم المعالجة الآلية للمعلومات يتميزون في غالب الأحيان بأنهم أفراد ذوي مكانة في المجتمع، فغالباً ما يكون هؤلاء من أصحاب الوظائف الحيوية في مقار عملهم، سواء في بيئة القطاع الخاص كالشركات والمؤسسات والمنشات الاقتصادية والمصارف الخاصة، أو في القطاع العام وأجهزته من وزارات وهيئات حكومية أخرى.

٢- من حيث الجوانب السيكولوجية:

إن الدراسة السيكولوجية للمجرمين المعلوماتيين في جرائم الابتزاز الالكتروني، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية وبلا مشروعية الأفعال التي يقترفونها، وكذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الشر والخير متداخلة لدى هذه الفئة، وتغيب في داخلهم مشاعر الإحساس بالذنب، وهذه المشاعر في الحقيقة تبدو متعارضة.

كما يصاب هذا النوع من المجرمين بصفة عامة الشعور بالخشية من اكتشافهم وافتضاح أمرهم، ولكن هذه الرهبة والخشية مرجعها انتماؤهم في الأعم الأغلب إلى فئة اجتماعية متعلمة ومثقفة.

- ب) لم يكن لارتباط جرائم الابتزاز الالكتروني بالحاسب الآلي أثره على تمييز تلك الجرائم عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره في تمييز المجرم المعلوماتي عن غيره من المجرمين العاديين، الذين جنحوا إلى السلوك الاجرامي النمطي، وهذا ما سوف نعرض له موضحين أهم سمات المجرم المعلوماتي ثم خصائصه المميزة وأخيرا لأنماط هذا المجرم وذلك على النحو التالي.

١ – السمات المميزة للمجرم المعلوماتي:

يمكن القول بان هناك مجموعة من السمات التي يتميز بها المجرم المعلوماتي، والتي يساعد التعرف عليها على مواجهة هذا النمط الجديد من المجرمين، ويعد الأستاذ (parker) واحد من أهم الباحثين الذين اهتموا بجرائم التقنيات بصفة عامة والمجرم المعلوماتي بصفة خاصة، ويرى (parker) أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة، إلا انه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه.

وفيما يلي بعض السمات العديدة للمجرم المعلوماتي والتي في الغالب تميزه عن غيره من المجرمين العاديين:

أولا: المجرم المعلوماتي هو مجرم متخصص:

حيث اتضح من العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الابتزاز الالكتروني، أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يبين أن المجرم الذي يرتكب الإجرام المعلوماتي هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

ثانيا: المجرم المعلوماتي هو مجرم عائد إلى الإجرام.

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الحاسب الآلي، انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويعزى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.

ثالثا: المجرم المعلوماتي هو مجرم محترف.

حيث يتمتع المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الحاسب الآلي، الأمر يقتضى الكثير من الدقة والتخصص والاحتراف في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسب الآلي كما هو في حالة البنوك والمؤسسات العسكرية.

رابعا: المجرم المعلوماتي هو مجرم غير عنيف.

المجرم المعلوماتي من المجرمين الذين لا يلجأون إلى العنف إطلاقا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام الحيلة والذكاء، فهو لا يلجا إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.

يضاف إلى ذلك، أن المجرم المعلوماتي مجرم ذكى، يتمتع بالتكيف الاجتماعي، أي غير عدوانى فهو لا يناصب أحد العداء، وأيضا يتمتع بالمهارة والمعرفة وأحيانا كثيرة على درجة عالية من الثقافة.

٢ – خصائص المجرم المعلوماتي:

يتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين التقليدين، وهى:

أولا: المهارة: يتطلب تنفيذ جرائم الابتزاز الالكتروني، قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في المجال التكنولوجي، أو بمجرد التفاعل الاجتماعي مع الآخرين، وتلك ليست قاعدة في أن يكون المجرم المعلوماتي على هذا القدر

من العلم، حيث يشير الواقع العملي أن جانبا من انجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

ثانيا: المعرفة: وهى من أهم الخصائص، حيث تميز خصيصه المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يكون تصورا كاملا لجريمته، ويرجع ذلك إلى أن المسرح الذي تمارس فيه جرائم الابتزاز الالكتروني هو نظام الحاسب الأولى، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة.

ثالثا: الوسيلة: ويراد بها الإمكانيات التي يحتاجها المجرم المعلوماتي لإتمام جريمته، وهذه الوسائل قد تكون في غالب الأحيان وسائل بسيطة وسهلة الحصول عليها، خاصة إذا كان النظام الذي يعمل به الحاسب الآلي من الأنظمة الشائعة، أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر كبير من الصعوبة.

رابعا: السلطة: يقصد بالسلطة هنا، الحقوق والمزايا التي قد يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فكثيرا من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وصولا الي ابتزاز مالكها.

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات، وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، وتلك السلطة قد تكون مشروعة، ومن الممكن أن تكون غير مشروعة، كما في حالة اختلاس شفرة الدخول الخاصة بشخص آخر.

خامسا: الباعث: وهو تلك الرغبة في تحقيق الربح المادي أو المعنوي بطريقة غير مشروعة وهي الابتزاز، ويظل الربح المادي هو الباعث الأول وراء ارتكاب جرائم الابتزاز الالكتروني، ويرى البعض أيضا ما يخالف ذلك في أن الربح المادي لا يعد هو الباعث في أغلب القضايا على ارتكاب جرائم الابتزاز

الالكتروني، وإنما هناك أمور عديدة أخرى، قد تكون جنسية او تحقيق مكسب آخر.

لكن الأرجح تكون هي الباعث، مع احتمال توافر بواعث أخرى مثل الرضوخ لطلب ما، وأيضا التحصل علي مطالب ادبية او سياسية او اقتصادية.

- ٣ - الأنماط المختلفة للمجرم المعلوماتي:

يمكن تقسيم مجرمي المعلوماتية (Cybr Criminals) إلي مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال إلي وجود عدد من الأنماط المختلفة لمجرمي المعلومات، نرصدها فيما يلي:

الطائفة الأولي (Pranksters): وتضم تلك الطائفة، الأشخاص الذين يرتكبون جرائم الابتزاز الالكتروني بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ومن أمثلة هذه الطائفة صغار مجرمي المعلوماتية.

الطائفة الثانية (Hackers): وتضم تلك الطائفة، الأشخاص الذين يستهدفوا من الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها، بهدف كسر الحواجز الأمنية المقامة لهذا الغرض، وذلك بهدف اكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

الطائفة الثالثة (Malicious Hackers): وهى طائفة أشخاص هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مالية ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

الطائفة الرابعة (Personal Problem Solvers): وهى الطائفة الأكثر شيوعا من مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم الابتزاز الالكتروني بحيث يترتب عليها في كثير من الأحيان خسائر كبيرة تلحق بالمجني عليه، ويكون الباعث في هذه الجريمة إيجاد حلول لمشكلات مادية تواجه الجاني لا يستطيع حلها بالطرق العادية.

الطائفة الخامسة (Career Criminals): وهى طائفة مجرمي المعلوماتية الذين يهدفون من وراء نشاطهم الإجرامي تحقيق ربح مادي بطريق غير مشروع، ويقترب المجرم المعلوماتي من هذه الطائفة في سماته إلى المجرم التقليدي.

ومن جانب آخر، أكدت بعض الدراسات والأبحاث العلمية على أن فئات مجرمي أو جناة جرائم الابتزاز الالكتروني، تنحدر من:

- مستخدمو الحاسب بالمنازل.
- الموظفون الساخطون على منظماتهم.
- المتسللون ومنهم الهواة أو العابثون بقصد التسلية.
- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويعبثون أو يتلفون النظام أو يختلسون محتوياته وتقع أغلب جرائم الانترنت حاليا تحت هذه الفئة بتقسيمها.
- العاملون في الجريمة المنظمة[١][٢].

---

(١) راجع في ذلك، د. هدى حامد قشقوش، "الجريمة المنظمة (القواعد الموضوعية والاجرائية والتعاون الدولي)، الطبعة الثانية، الاسكندرية، منشأة المعارف، سنة ٢٠٠٦، ص ١٨، وايضا : محمد ابراهيم زيد، "الجريمة المنظمة (تعريفها وانماطها وجوانبها التشريعية)"، ابحاث حلقة علمية حول الجريمة المنظمة واساليب مكافحتها، الرياض، اكاديمية نايف للعلوم الامنية، سنة ١٩٩٩، ص ٣٣

(٢) انظر في ذلك: سناء خليل، الجريمة المنظمة عبر الوطنية والجهود الدولية والمشكلات القضائية، المجلة الجنائية القومية، المجلد التاسع والثلاثون، العدد الثانى، يوليو ١٩٩٦ ، ص ١٠٣، انظر : عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– مرجع سابق – ص ٤٦ وما بعدها، وايضا : محمد فتحى عيد، السنوات الحرجة في تاريخ المخدرات، مرجع سابق، ص ١٣١، وايضا : تقرير الهيئة الدولية لمراقبة المخدرات لسنة ٢٠٠٠ ، الغصون (٥٠ – ٥٦) ، ص ١٢ ، ١٣، مطبوعات الامم المتحدة، نيويورك، ٢٠٠١، الوثيقة رقمElincb 200D المنشور بتاريخ ٢١ فبراير ٢٠٠١ ، وكذلك انظر: مجلة الحقوق الكويتية، مجلس النشر العلمى، الكويت، ١٩٩٨، العدد الثالث، ص ٣٨١ ، منشور دورة البحث الجنائى للضباط رقم (٥) دراسات حول الجريمة الاقتصادية في دولة الامارات، معهد البحث الجنائى، شرطة دبى، دولة الامارات العربية المتحدة، سنة ١٩٩٨، ص ٩٨.

الفصل الثاني

أنواع ومخاطر جرائم الابتزاز الالكتروني وصورها

لما كانت جرائم الابتزاز الالكتروني؛ تشير عموماً إلى أي ممارسات غير مشروعة أو نشاط إجرامي يتضمن حاسب أو شبكة إلكترونية أو أي نوع من أجهزة الاتصال بحيث يكون الحاسب أو شبكة الاتصال وغيرها المذكور سابقا المصدر أو الهدف أو مكان الجريمة، بغية ابتزاز المجني عليه في تلك الجرائم.

وعلى ذلك، جرى مفهوم جرائم الابتزاز الالكتروني على نطاق واسع كأي مخالفة ترتكب ضد أفراد أو جماعات بدافع إجرامي، كجريمة تتعلق بالبنية التحتية لتكنولوجيا المعلومات يكون مستهدفها ابتزاز ما، بما في ذلك الوصول غير المشروع أو غير المصرح به للبيانات أو المعلومات، والاعتراض غير القانوني للبيانات عن طريق نقلها من و إلى أي جهاز حاسب، وإدخال بيانات خاطئة أو تغيير البيانات الموجودة والعبث بها كحذفها أو إتلافها، وإساءة استخدام الأجهزة والتزوير كسرقة الهوية، وأخيرا الاحتيال الالكتروني، في اطار عملية تهديد بنشر صور او فيديو او معلومات شخصية وحساسة اذا لم ترضخ الضحية لطلبات المبتز، ومعظم الطلبات تتلخص في التالي:

١. دفع مبالغ مادية.
٢. القيام باعمال غير مشروعة.
٣. القيام باعمال منافية للاخلاق.
٤. الافصاح عن معلومات سرية مؤسسية او سياسية.
٥. العمل مع العدو.

DUNCAN. Alfod. Anti- mony laundering regulations: Aburden on financial institutions, volume 19 north Carolina jounal of international and commercial regulations, p.p 441 – 442 (summer 1994).

ولا شك ان أنماط جرائم الابتزاز الالكتروني، كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها وهذا راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها.

وعلى ذلك، نتناول في المبحث الأول أنواع جرائم الابتزاز الالكتروني، ثم نتبع ذلك ببيان مخاطر جرائم الابتزاز الالكتروني في مبحث ثان، على ان يخصص المبحث الثالث صور جرائم الابتزاز الالكتروني، وأخيرا يختتم هذا الفصل بالعرض لواقع جرائم الابتزاز الالكتروني على المستوى الدولي والعربي، من خلال المبحث الرابع والاخير، على الترتيب التالي.

المبحث الأول

أنواع جرائم الابتزاز الالكتروني

من المقرر ان جرائم الابتزاز الالكتروني، لها انواع عديدة لا تندرج تحت حصر، فهى تتعدد وتتطور بمقدار التطور التكنولوجى ذاته، ويمكن ايراد عدد من الانواع لتلك الجرائم على النحو التالي:

١- **جرائم القرصنة الالكترونية:** يشير مفهوم القرصنة الإلكترونية إلى أي ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيا، وذلك من خلال قراصنة الكتابة أو أستخدام برامج الحاسب الجاهزة، ويختلف سبب القرصنة من واقعة إلى أخرى، فبعضها يكون بهدف مهاجمة جهاز الحاسب لابتزاز مالكه، أو لتحقيق مكاسب مالية شخصية مثل ابتزاز معلومات بطاقات الائتمان، وتحويل الأموال من حسابات مصرفية مختلفة إلى حساب المقرصن الخاص أو أي حسابات أخرى.

وبالإضافة إلى ذلك يعتمد بعض القراصنة على ابتزاز الشركات العالمية وتهديدها بنشر المعلومات الخاصة بها والسرية في حال عدم قيامهم بدفع أو تحويل المبلغ المالي المطلوب.

يضاف الى ذلك، ان هناك من يقوم بإستهداف المواقع الحكومية الهامة للحصول على الشهرة من خلال التغطية الصحفية الاعلامية.

٢- جرائم استغلال الأطفال في المواد الإباحية: والمقصود من هذا المصطلح هو ظهور الأطفال والقصر الذين تقل أعمارهم عن ١٨ عاما في صور أو أفلام أو مشاهد ذات طبيعة إباحية أو مضمون جنسي، بما فيها مشاهد أو صور للاعتداء الجنسي على الأطفال وهي جريمة منفردة قائمة بذاتها، يعاقب عليها قانونا في أغلب دول العالم، وتتعامل أغلب دول العالم بحسم وجدية مع هذا النوع من الجرائم على كل من تثبت عليه تهمة الاتجار أو تداول صور أو أفلام إباحية للأطفال، وكذلك المنظمات الدولية بشدة مثل اليونسيف والشرطة الدولية "الإنتربول"(١).

وتوجد تجارة عبر شبكة الإنترنت تختص بهذا النوع من الاستغلال الجنسي للأطفال تشمل صورا وأفلام تظهر أطفالا أو قصر يجرى استغلالهم جنسيا.

٣- جرائم المطاردة الالكترونية: ويقصد بها استخدام الإنترنت لتعقب أو مطاردة أي فرد لغرض الإحراج العام، أو المضايقات الشخصية، أو الابتزاز المالي وغيرها من الأمور بسلوك تهديدي، ويقوم المضايقون بجمع المعلومات الشخصية عن الضحية مثل إسمه، ومعلومات عن عائلته، وأرقام هواتفه، ومكان الاقامة ومكان العمل وما الى ذلك عن طريق مواقع الشبكات الاجتماعية والمدونات وغرف المحادثة وغيرها من المواقع.

---

(١) انظر في ذلك: عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ ٢٠٠٨/٠٣/٠٧، المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:٣.

٤- **جرائم الفيروسات وطريقة نشرها:** ذلك ان الفيروسات بصفة عامة، هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بمواقع او أجهزة أخرى، أو السيطرة عليها أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة، ويتصف فيروس الحاسب بأنه برنامج قادر على التناسخ والانتشار، حيث يربط الفيروس نفسه ببرنامج أخر يسمى الحاضن، ولا يمكن أن تنشأ الفيروسات من ذاتها ولكن يمكنها أن تنتقل من حاسب مصاب لآخر سليم.

وأهم طرق الانتقال الآن هي الشبكة العنكبوتية (الإنترنت) لكونها وسيلة سهلة لانتقال الفيروسات من جهاز لآخر، ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات، وكذلك عن طريق وسائط التخزين مثل ذاكرة الفلاش والأقراص الضوئية والمرنة سابقا ويأتي أيضا ضمن رسائل البريد الإلكتروني.

٥- **برامج القرصنة:** ويقصد بالقرصنة هنا الاستخدام أو/ و النسخ غير المشروع لنظم التشغيل أو/ ولبرامج الحاسب الآلي المختلفة، وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور القرصنة واتسعت وأصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي، ومن هنا وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها ووجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز بمرتبات عالية لتكون مهمتهم منع محاولة اختراق أنظمتها المختلفة والعثور على أماكن الضعف فيها، واقتراح سبل للوقاية اللازمة من الأضرار التي يتسبب فيها قراصنة الحاسب، ففي هذه الحالة بدأت صورة الهاكر في كسب الكثير من الايجابيات إلا أن المسمى الأساسي يظل واحدا.

٦- **جرائم الإحتيال باستخدام بطاقات الإئتمان عبر الإنترنت:** حيث يهدف احتيال الإنترنت في العادة إلى الاحتيال على المستخدمين عن طريق سلب أموالهم، إما بابتزاز أرقام بطاقات ائتمانهم أو بجعلهم يرسلون حوالات مالية

أو شيكات، ويهدف بذلك لغرض شخصي كالشراء عبر الإنترنت أو دفعهم إلى الكشف عن معلومات شخصية بغرض التجسس أو انتحال الشخصية أو الحصول على معلومات حسابهم في مركز حساس، ويمكن تعريف احتيال بطاقات الإئتمان بشكل عام على أنه خداع الشخص وسرقة معلوماته عن طريق الاستخدام غير المصرح وغير المشروع به لبيانات البطاقة الإئتمانية(١).

المبحث الثاني

مخاطر جرائم الابتزاز الالكتروني

من المقرر انه، وفي فترة زمنية وجيزة صارت شبكة الانترنت الأداة الأهم في حياة معظم الأشخاص، فبعد أن كان مقصورة علي الجانب العسكري أصبحت جزءا لا يتجزأ من التعاملات اليومية، وعلى اثر ذلك ظهرت جرائم الابتزاز الالكتروني، حينما يستخدم المجرم جهاز الحاسب الآلي كأداة رئيسية لتنفيذ جريمته، وقد انتشرت هذه الجرائم بشكل مخيف وينبأ بالخطر بسبب خصائصها التي تميزها عن الجريمة التقليدية، لكونها تنتقي ضحايا يتعرضون لتعطيل وتدمير مخازن المعلومات الخاصة بهم وابتزاز أموالهم بطريق التهديد، كل ذلك وبشكل متكرر يؤثر بشكل سيئ على الاقتصاد، ونتيجة لذلك سنت الدول قوانين وطرق للحد من هذه جرائم الابتزاز الالكتروني.

حيث ان انتشار جرائم الابتزاز الالكتروني، قد يؤدي الى خلل عام قد يهدد المجتمع كله في اقتصاده وسيادته وأمنه الوطني، اذ تتسبب جرائم الابتزاز الالكتروني أيضا بالتفكك الأسري والخلافات بين الافراد بسبب التشهير أو إشاعة الأخبار الكاذبة وسرقة الملفات الخاصة بالأفراد ونشرها في الانترنت ووسائل الاتصالات وغيرها العديد من التأثيرات السلبية التي تهدد أمن المجتمع وسلامته.

---

(١) راجع في ذلك: على عدنان الفيل، المسؤولية الجزائية عن اساءة استخدام بطاقة الائتمان الالكترونية، الطبعة الاولى، المؤسسة الحديثة للكتاب، لبنان، سنة ٢٠١١، ص ١٧

ففي العالم الافتراضى وهو عالم الانترنت يحاول المخترقون والجواسيس والإرهابيون والعابثون، الاستفادة قدر الإمكان من توسع استخدام الانترنت، وذلك بنشر فيروساتهم المدمرة لتعطيل أجهزة وقطاعات حكومية وإيقاف الخوادم والحاسبات عن العمل أو تجميد الشبكة بكاملها، وقد يقومون باختراق الأنظمة ومسح البيانات والقيام بالسرقات الإلكترونية وانتحال الشخصية والابتزاز ونشر إشاعات عبر الانترنت، وبالطبعً هذا النوع من جرائم الابتزاز الالكتروني له تأثيرات كبيرة ويسبب تقلبات خطيرة من الناحية الاقتصادية في حال عدم التصدي لها.

وعلى ذلك نعرض في المطلب الاول للمخاطر الاجتماعية لجرائم الابتزاز الالكتروني، على ان يتناول المطلب الثاني المخاطر الإقتصادية لجرائم الابتزاز الالكتروني، ويخصص المطلب الثالث والاخير للمخاطر الأمنية لجرائم الابتزاز الالكتروني، على الترتيب التالي.

المطلب الأول

المخاطر الاجتماعية لجرائم الابتزاز الالكتروني

وهي أهم أنواع المخاطر التى تترتب على ارتكاب جرائم الابتزاز الالكتروني على اطلاقها، لأنها تمس الشخص والعرض، مثل إساءة السمعة وانتهاك الحرية الشخصية والجرائم المخلة بالآداب العامة وجرائم السلوك العام، ولقد تزايدت هذه الجرائم مع انتشار المواقع الاجتماعية مثل الفيس بوك وتويتر، والمنتديات الحوارية وغيرها، وهذه المواقع إذا لم تستغل للفائدة والتزيد من العلم والثقافة والتواصل الصحى والسوي، فستكون لها آثار اجتماعية خطيرة على مستوى الفرد والأسرة والمجتمع[١].

---

(١) راجع في ذلك: عبد الفتاح الجبالى، الاقتصاد المصرى من التثبيت الى النمو، مركز الدراسات السياسية والاستراتيجية بالاهرام ، القاهرة، سنة ٢٠٠٠، ص ٢٠.

وتعد من اشهر جرائم الابتزاز الالكتروني التى لها بالغ التأثير والخطورة من الناحية الاجتماعية، جريمة الابتزاز التى تقع على الاناث، ذلك ان إحصائيات الحالات الاجتماعية للمبتزات او المجنى عليهن في جرائم الابتزاز المعلوماتي، تصل الى ارقام مخيفة، حيث تتصدر الفتيات اللاتي لم يتزوجن بنسبة ٥٨٪ ثم المتزوجات بنسبة ٢٦٪ ثم المطلقات بنسبة ٨٪ ثم المخطوبات بنسبة ٧٪ ثم الأرامل بنسبة ١٪.

حيث بلغت قضايا التهديد والابتزاز عن طريق الشبكة العنكوبتية "الإنترنت" عالميا ما نسبته ١٨ في المائة من مجمل قضايا الإجرام المعلوماتي، بينما سجلت قضايا ابتزاز الأطفال جنسيا ما نسبته ١٤ في المائة من مجمل جرائم الابتزاز الالكتروني.

كما تشير التقارير الى ان قضايا اختراق البريد الإلكتروني بهدف الابتزاز، تصدرت مجمل قضايا الإجرام المعلوماتي بما نسبته ٢٧ في المائة، فيما سجلت قضايا استغلال الأطفال جنسيا ما نسبته ١٤ في المائة، بينما وصلت قضايا السب والتشهير وإساءة السمعة ما نسبته ١٣ في المائة، في حين سجلت قضايا الاختراقات المالية ١٢ في المائة، بينما وصلت نسبة الاختراق المعلوماتي بواسطة برامج خبيثة ما قدره ٦ في المائة، فيما بلغت نسبة الخداع والاحتيال إلكترونيا ٥ في المائة، كما وصلت نسبة التهديدات الإرهابية عبر المواقع ٤ في المائة، بينما لم تتجاوز شكاوى الاتصالات المشبوهة ما نسبته ١ في المائة.

ايضا تزايدت حالات الاحتيال الإلكتروني من خلال عمليات البيع والشراء عبر الإنترنت والشركات الوهمية، وكذلك من إعلانات الوظائف، والانسياق وراء الإعلانات التجارية والانجراف وراء الفرص التجارية الزائفة، مما يؤدى الى الوقوع تحت طائلة النصب والاحتيال.

حيث ان الانسياق وراء إعلانات الوظائف، والتي تطلب إرسال البيانات الشخصية وصورة لجواز السفر والخبرات والمعلومات التفصيلية بحجة استكمال

إجراءات الوظيفة، ثم يقع المتجاوبون معها والمتقدمون لها ضحية للابتزاز المالي أو عمليات الاستغلال والاستخدام المشبوه.

المطلب الثاني

المخاطر الاقتصادية لجرائم الابتزاز الالكتروني

لما كان الاقتصاد عصب الحياة، فان المخاطر الاقتصادية لجرائم الابتزاز الالكتروني لا تقل عن مخاطر الجرائم الاجتماعية، حيث أنها تهدد الاقتصاد وتستخدم عدة جرائم منها التزييف والتزوير وجرائم ابتزاز البنوك والمصارف.

ومع تزايد نسبة جرائم الابتزاز الالكتروني وتنوع طرقها، لا شك أنها تلحق خسائر مادية كبيرة وفادحة، أكثر مما تسببه الجرائم التقليدية ليس فقط على مستوى الفرد بل تتعداه إلى مستوى المنظمات والجهات والمؤسسات، وهذا بالطبع يؤثر بشكل سلبى على الاقتصاد في عمومه، وكافة قطاعاته(١).

ذلك ان جرائم الابتزاز الالكتروني تمثل هجوما شرسا من أشخاص أو مجموعات أو منظمات محترفة هدفها الرئيسي تحقيق ربح مادي، بالإضافة إلى أهداف أخرى وذلك بالاستفادة من توسع استخدام الكمبيوتر والانترنت ويمكن إجمالهم في مستويين هما:

أولاً: على مستوى الفرد: حيث أصبح الفرد ينجز تعاملاته ويدير أعماله وابحاثه ويتواصل مع العالم الخارجي بواسطة استخدام الانترنت، ومن جرائم الابتزاز الالكتروني التي قد يتعرض لها الفرد والتي تؤثر على الجانب المادي لديه:

- سرقة الهوية الشخصية وصولا الي ابتزاز مالكها وصاحبها؟

---

(١) راجف في ذلك: د.عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة ١٩٨٨، الدار الجامعية، بيروت، ص. ٢٥٩ .

- سرقة بطاقة الائتمان الخاصة به لابتزازه .[١]
- الابتزاز بالتهديد المباشر.
- عمليات الاحتيال بغرض الابتزاز.
- الابتزاز عن طريق تحويل أو نقل حسابه المصرفي.
- الابتزاز بطريق نقل ملكية الأسهم[٢] .
- ابتزاز زيادة الفواتير بطريق تحويل فواتير المجرم للضحية.

---

(١) راجع في ذلك: على عدنان الفيل، المسؤولية الجزائية عن اساءة استخدام بطاقة الائتمان الالكترونية، الطبعة الاولى، المؤسسة الحديثة للكتاب، لبنان، سنة ٢٠١١، ص ١٧

(٢) السهم ما هو إلا شهادة تخول مالكها الحق في ملكية جزء من ممتلكات الشركة التي أصدرت هذا السهم، وهو قابل للتداول والانتقال من مكان لآخر، وليس له تاريخ استحقاق، ومسئولية حامله محدودة بقيمة السهم، ولا يحق له المباحثة بالأرباح إلا إذا قررت الإدارة توزيعها، وتنتقل حقوق المساهم الحائز للسهم إلى مالك السهم الجديد، أما السندات، فهي عبارة عن جزء من قرض تصدره شركة مقترضة أو دولة أو هيئة، ويتم طرحه للاكتتاب فيه من جانب المقترض على المقترضين، وهو بمثابة تعهد بسداد مبلغ معين في تاريخ معين بمعدل فائدة محدد، وتتأثر قيمة السندات السوقية مثلها مثل قيمة الأسهم بما يطرأ على المركز المالي للشركة التي أصدرتها، أما الصكوك، فتتخذ العديد من الأنواع، فمنها صكوك الادخار، وصكوك التمويل، وصكوك الاستثمار، وصكوك الإقراض، وجميعها قابلة للتداول، وقابلة للخصم، وقابلة للبيع والشراء لمزيد من التفصيل راجع، د . محسن أحمد الخضيري: المرجع السابق، ص ١٠ وما بعدها. هذا وتنص المادة (١٧) من قانون إنشاء سوق أبو ظبي للأوراق المالية على أن " يتم قبول وإدراج الأوراق المالية التالية للتداول في السوق : ١. أسهم وسندات والأذونات المالية التي تصدرها الشركات المساهمة العامة. ٢ . الأسهم والسندات والأذونات المالية التي تصدرها الشركات المؤسسة خارج الإمارة والتي يقبل المجلس تداولها. ٣ . الأسهم والسندات والأذونات المالية التي تصدرها الشركات والمؤسسات خارج الدولة والتي يقبل المجلس تداولها . ٤ . سندات الدين التي يقبل المجلس تداولها . ٥ . وحدات الصناديق الاستثمارية. ٦ . السندات والأذونات الصادرة عن الحكومة المحلية أو الهيئات والمؤسسات العامة. ٧ . أية أوراق أو أدوات مالية يقبل المجلس تداولها".

ثانيا: على مستوى معظم المنظمات والبنوك والشركات الربحية وغير الربحية والمؤسسات والجهات الحكومية وغير الحكومية[١]:

حيث أصبحت تلك الهيئات والمؤسسات والجهات تدار الكترونيا وتتواجد على الشبكة الالكترونية لفتح قنوات تواصل جديدة مع الناس والإعلان عن آخر أخبارها وتسهيل التواصل معها والتفاعل مع ما تقدمه من خدمات وعروض، كل هذا دون الحاجة إلى الذهاب إليها، فقط عن طريق الشبكة الإلكترونية، بهدف استقطاب شريحة أكبر من الناس وزيادة أرباحها.

ومن جرائم الابتزاز الالكتروني التي قد تتعرض لها الشركات والتي تؤثر على الجانب المادي لديها: [٢]

- الإطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها بالابتزاز.
- العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها بغرض الابتزاز.
- ابتزاز الأموال بواسطة تحويل حسابات مصرفية الخاصة بالشركة.
- الغش في المعاملات الالكترونية كالتغيير في المبيعات بغرض الابتزاز.
- عمليات الاحتيال بالابتزاز.
- التهديد والابتزاز المباشر.
- اختراق الموقع الإلكتروني الخاص بالشركة بغرض الابتزاز.

ومن جرائم الابتزاز الالكتروني التي قد تتعرض لها البنوك والتي تؤثر على الجانب المادي لديها: [١]

---

(1) see : chehire and fifoot , the law of contract, London , 1964 , p.457.

(٢) انظر في ذلك: موقع تقنية المعلومات والاتصالات – جرائم المعلومات.
http://ict.sd/index.php?option=com_content&task=view&id=12&Itemid=26

- السطو الإلكتروني بغرض الابتزاز.
- العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها بغرض الابتزاز.
- تعطيل النظام لغرض الابتزاز.
- الابتزاز عن طريق نقل ملكية الأسهم.
- اختراق الموقع الإلكتروني الخاص بالبنك بغرض الابتزاز.

ومن جرائم الابتزاز الالكتروني التي قد تتعرض لها المنظمات والمؤسسات والتي تؤثر على الجانب المادي لديهما: [٢]

- الإطلاع على معلومات سرية والاستفادة منها بغرض الابتزاز.
- العبث بمخازن المعلومات الخاصة بالمنظمة أو المؤسسة بحذفها أو تعديلها أو تعطيل الوصول إليها لاستهداف ابتزازها.
- ابتزاز الأموال بواسطة تحويل حسابات مصرفية الخاصة بالمنظمة أو المؤسسة.
- عمليات الاحتيال بغرض الابتزاز.
- الابتزاز بالتهديد المباشر .
- اختراق الموقع الإلكتروني الخاص بالمنظمة أو المؤسسة بغرض الابتزاز.

ويشار إلى أن جرائم الابتزاز الالكتروني قد تسببت بخسارة دول مجلس التعاون الخليجي بين ٥٥٠ مليون و٧٣٥ مليون دولار أميركي سنويا. [٣]

---

(١) راجع في ذلك: مركز التميز لأمن المعلومات، تصنيف الجرائم المعلوماتية تبعا لاستخدام الحاسب فيها

http://coeia.edu.sa/index.

(٢) راجع في ذلك:

.http://ar.shvoong.com/humanities/1746290

(٣) راجع في ذلك: مجلة المعلوماتية– الجريمة الالكترونية

http://infomag.news.sy/index.php?inc=issues/showarticle&issuenb=29&id=5.90

- كما أكد الخبراء أن معدل نسبة جرائم الابتزاز الالكتروني في العالم يصل إلى ٥٧.٦٪ حيث يكلف الاقتصاد العالمي ما يقارب (١٢.٩٥٠) مليار دولار سنوياً، وإن نسبة معدل الهجمات الالكترونية في السعودية على سبيل المثال يقارب ٤٥.٨٪ لعام ٢٠٠٩، كما كانت نسبة الهجمات للحسابات البنكية للأفراد عام ٢٠٠٩، بلغت ٤٠٪، واختراق المواقع الالكترونية لعام ٢٠٠٩ بلغ ٦٣٪، ورسائل الاحتيال فيها لعام ٢٠٠٩م بلغت ٤٣.٧٪.(١)
- كما كشفت السلطات الأمريكية عام ٢٠٠٩ أن عمليات قرصنة وسرقة طالت أكثر من ١٣٠ مليون بطاقة ائتمان وبطاقة سحب مصرفية.
- وأظهر تقرير نشرته "سيمانتك كوربوريشن" تزايداً مضطرداً في هجمات جرائم الابتزاز الالكتروني، حيث رصد ١٠٠ تهديد إلكتروني في الثانية خلال العام ٢٠٠٩.(٢)
- وفي دراسة أجرتها شركة نورتن الرائدة في تطوير الحلول البرمجية الأمنية أن ثلثي مستخدمي الانترنت حول العالم تعرضوا لجريمة ابتزاز الكتروني على الأقل مرة واحدة وقد تمثلت في هجمات فيروسية وتجسسية واحتيالية لسرقة بطاقات الائتمان وسرقة الهوية أو البيانات المصرفية والشخصية الحساسة، كما أشارت الدراسة إلى أن عملية إزالة الآثار المترتبة من جرائم الابتزاز الالكتروني تستغرق في المتوسط ٢٨ يوم كما تكلف في المتوسط ٣٣٤ دولار.(٣)

---

(١) راجع في ذلك: منتديات الخريف – الجريمة الالكترونية
.http://www.5reeef.com/vb/t62711.html

(٢) انظر في ذلك: جريدة الرياض – الجريمة الالكترونية.
http://www.alriyadh.com
وايضا انظر: العربية دوت نت–السعودية والإمارات في صدارة ضحايا الجرائم المعلوماتية
http://www.alarabiya.net

(٣) راجع في ذلك: تقرير تحت عنوان الوباء الصامت
http://www.menafn.com

- وفي دراسة أجرتها شركة تريند مايكرو المشهورة بمحاربة الفيروسات أشارت إلى أن السعودية والإمارات تتصدر المركز الأول والثاني على مستوى دول المجلس التعاوني الخليجي، وفي السعودية فقط حصل ٧٠٠ ألف انهيار نظام خلال تسعة شهور.[١]

وهذه الأرقام تشير لمدى تفشي جرائم الابتزاز الالكتروني وتهديدها الحقيقي والسلبي على الاقتصاد، والسبب في ذلك يعود إلى: [٢]

- جهل الناس بأنواع جرائم الابتزاز الالكتروني وطرق استدراج الضحايا.
- ثقة الناس ببعض الأشخاص والمواقع والرسائل الإلكترونية دون التأكد من المصداقية.
- تنوع طرق جرائم الابتزاز الالكتروني وتعدد أساليبها مع تقدم الزمن وتطور التقنية الحديثة.
- عدم حرص المستخدم على وضع برامج حماية ضد الفيروسات والتجسس .
- عدم تحديث أنظمة الحماية المستخدمة.
- وجود نقص وضعف في التشريعات والقوانين الخاصة بهذا النوع من الجرائم مما أسهم في تمادي المجرمين. [١]

وايضا انظر: البوابة العربية للأخبار التقنية –الجرائم المعلوماتية تكبد دول الخليج خسائر تصل إلى ٢.٧ مليار درهم سنوياً

http://www.aitnews.com

(١) انظر في ذلك: منتدى الإمارات الاقتصادي – غياب إدارات لمكافحة الجرائم المعلوماتية في ٥ إمارات

http://www.uaeec.com

(٢) انظر في ذلك: مجلة العلوم الإنسانية –تعزيز الأمن القومي من خلال الاستخدام الأمثل لتقنية المعلومات

http://www.ulum.nl

وبسبب الكم الهائل من الخسائر ووجود توقعات قوية بتزايد نسبة جرائم الابتزاز الالكتروني، وتطور طرقها وتعدد مجالاتها وتفاقم حجم أضرارها، أدركت الدول ضرورة التحرك ومواجهة جرائم الابتزاز الالكتروني بقوة، فنادت بسن عقوبات رادعة على مرتكبيها وشجعت على تكوين منظمة لمكافحة جرائم الابتزاز الالكتروني.(٢)

المطلب الثالث

المخاطر الأمنية لجرائم الابتزاز الالكتروني

حيث ان من أخطر أشكال جرائم الابتزاز الالكتروني، هي الاختراقات التي تكون جزءاً من جهد منظم لإرهابيين معلوماتيين أو وكالات مخابرات أجنبية أو أي إختراقات تهدف إلى إستغلال الثغرات الأمنية المحتملة، بشكل عام كل جريمة من هدفها زعزعة المصالح العامة والإقتصاد والأمن الوطني.

ومن جرائم الابتزاز الالكتروني التي قد تتعرض لها الجهات والأجهزة الحكومية بهدف توليد الاضطراب ومحاولة لزعزعة الأمن والاستقرار وتحميل الدولة خسائر مالية :

- الوصول إلى المعلومات سرية والإطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم المعلوماتي في ابتزاز مطالبه.
- دعم الإرهاب والأفكار المتطرفة ونشر الإشاعات.
- تعطيل وتخريب الخوادم الموفرة للمعلومات.

---

(١) انظر في ذلك: موقع المسائية الإخباري– حيث ان الجريمة الإلكترونية تكلف العالم ٥٠٠ مليار جنيه خلال ٢٠٠٩

http://www.msaeya.com

(٢) انظر في ذلك: تقرير تحت عنوان "جرائم الحاسب والانترنت .. تحدّ خطير يواجه التجارة الإلكترونية"

http://www.jo1jo.com/vb/showthread.

- تعطيل أنظمة القطاعات الحكومية والحيوية.
- تعطيل الانترنت بالكامل.
- الابتزاز المباشر للأموال.

والجرائم الواقعة على أمن الدولة: من أهم جرائم الابتزاز الالكتروني التي تهدد أمن الدول ومجتمعاتها ما يلي:

أ- **الجماعات الإرهابية:** حيث استغلت الكثير من الجماعات المتطرفة الطبيعة الاتصالية للانترنت من أجل بث معتقداتها وأفكارها، بل تجاوز الأمر مداه إلى ممارسات تهدد أمن الدولة المعتدى عليها.

ب- **الجريمة المنظمة:** حيث استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الاتصال والانترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ العمليات الإجرامية بيسر وسهولة.(١)

جـ - **الجرائم الماسة بالأمن الفكري:** اذ يبقى الأمن الفكري من بين أخطر جرائم الابتزاز الالكتروني، حيث يعطي الانترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية، والأمراض الفكرية وهو ما يسهل خلق الفوضى.

د- **جريمة التجسس الالكتروني:** حيث سهلت شبكة الانترنت الأعمال التجسسية بشكل كبير، اذ يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عملية التجسس في عصر المعلوماتية ثلاث أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي. (٢)

---

(١) راجع في ذلك: سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، سنة ٢٠٠٧، ص ٨٣.

(٢) انظر في ذلك: علي عدنان الفيل، الاجرام الالكترونى – دراسة مقارنة، منشورات زين الحقوقية، سنة ٢٠١١، ص ١٢٣.

المبحث الثالث

صور جرائم الابتزاز الالكتروني

كسائر الجرائم، فان جرائم الابتزاز الالكتروني لها صور، تختلف تلك الصور باختلاف طبيعة الحق الذي يكون محلا لها، وعلى ذلك نعرض لمختلف صور جرائم الابتزاز الالكتروني بحسب الحق التي تقوم بالاعتداء عليه، ويمكن تقسيمها إلى:

أولا الجرائم التي تتم ضد الحواسب الآلية ونظم المعلومات:

١) جرائم الإضرار بالبيانات:

يعتبر هذا الصنف من جرائم الابتزاز الالكتروني من أشدها خطورة وتأثيرا وأكثرها حدوثا وتحقيقاُ للخسائر للإفراد والمؤسسات، ويشمل هذا المطلب كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة الكترونية (Digital Form) على الحواسب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها، وصولا الي التحصل علي مطالب ابتزازية.

وأبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها، ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوى القبعات البيضاء (White Hat Hackers) الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت، مستغلين بعض الثغرات في تلك النظم، ومخترقين بذلك كل سياسات وإجراءات امن المعلومات التي يقوم بها مديري تلك الأنظمة والشبكات (System And Network Administrators) وكما ذكر عدم ارتباط ذلك النشاط بالشبكات، فاختراق الأمن الفيزيقي للاماكن التي يوجد بها أجهزة الحاسب التي تحتوى على بيانات هامة بالرغم من وجود إجراءات أمنية لمنع الوصول إليها، وبمعنى أخر وصول

شخص غير مصرح له وإمكانية دخوله إلى حجرة الحواسب المركزية بالمؤسسة ثم خروجه دون إحداث أي أضرار، فانه يعتبر خرقا لسياسة وإجراءات امن المعلومات بتلك المؤسسة.

ويتم استخدام الشبكات وبصفة خاصة شبكة الانترنت في الدخول على قواعد البيانات أو مواقع الانترنت والحصول على معلومات غير مسموح بها أو إمكانية السيطرة التامة على تلك الأنظمة بالرغم من وجود إجراءات حماية متعددة الدرجات من الحوائط النارية وأنظمة كشف ومنع الاختراق بالإضافة لآليات تشفير البيانات وكلمات السر المعقدة وبتخطي كل تلك الحواجز والدخول على أنظمة المعلومات ثم الخروج دون إحداث أي تغيير أو إتلاف بها، فانه ابسط أنواع الاختراق الذي يعطى الإشارة الحمراء لمديري النظم وأمن المعلومات بان سياساتهم وإجراءاتهم التنفيذية لأمن المعلومات بحاجة إلى التعديل والتغيير، وانه يتعين عليهم البدء مرة أخرى في عمل اختبار وتحليل للتهديدات ونقاط الضعف الموجودة بأنظمتهم (Risk Assessment) لإعادة بناء النظام الأمني مرة أخرى، وأيضا العمل على إجراء ذلك الاختبار بصورة دورية لمواكبة الأساليب الجديدة في الاختراق استهدافا للابتزاز.

٢) جرائم الاعتداء على الأشخاص:

والمقصود بالاعتداء هنا هو السب والقذف والتشهير وبث أفكار وأخبار من شانها الإضرار الادبى أو المعنوي بالشخص أو الجهة المقصودة، عملية تهديد بنشر صور او فيديو او معلومات شخصية وحساسة اذا لم ترضخ الضحية لطلبات المبتز.

وتتعدد طرق الاعتداء بداية من الدخول على الموقع الشخصي للشخص المشهر به وتغيير محتوياته، والذى يندرج تحت الجرائم التى تتم ضد الحواسب والشبكات أو عمل موقع أخر يتم نشر أخبار ومعلومات غير صحيحة، والذي يندرج تحت الجرائم باستخدام الحواسب الآلية والشبكات والذى غالبا ما يتم من خلال إحدى مواقع الاستضافة المجانية لصفحات الانترنت والتى أصبح عددها

بالآلاف في كافة الدول المتصلة بالانترنت والتى تسمى بالـ (Free Web Hosting Services) .

ومن أشهر تلك الوقائع، ما حدث لموقع البنك المركزي المصري على شبكة الانترنت سنة ٢٠٠١[١]، وتكرر الاختراق سنة ٢٠١٧، حيث قام المهاجمين بالدخول بصورة غير مشروعة على جهاز الخادم الذي يتم بث الموقع منه مستغلا إحدى نقاط الضعف فيه، وقام بتغيير الصفحة الرئيسية للموقع، الأمر الذي أحدث بلبلة في أوساط المتعاملين مع البنك خوفا من أن يكون الاعتداء قد امتد إلى المعاملات البنكية الأخرى.[٢]

٣) جرائم تطوير ونشر الفيروسات:

كانت البداية لتطوير فيروسات الحاسب في منتصف الثمانينات من القرن الماضي في باكستان على ايدى اثنين من المتخصصين العاملين في مجال الحواسب الآلية.

واستمرت الفيروسات في التطور والانتشار حتى بات يظهر ما يقارب مئتان فيروس جديد شهريا، والتي تعددت خصائصها وأضرارها، فالبعض ينشط في تاريخ معين والبعض الأخر يأتي ملتصقا بملفات عادية، وعند تشغيلها فان الفيروس ينشط ويبدأ في العمل الذي يختلف من فيروس لأخر بين أن يقوم بإتلاف الملفات الموجودة على القرص الصلب أو إتلاف القرص الصلب ذاته أو إرسال الملفات الهامة بالبريد الالكتروني ونشرها عبر شبكة الانترنت.

---

(١) جلسة مجلس ادارة البنك المركزى المصرى بتاريخ ٢٠٠٢/٢/٢٨ في شأن الضوابط الرقابية للعمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية، وايضا د/ شريف محمد غنام، مسؤولية البنك عن اخطاء الكومبيوتر في النقل الالكتروني للنقود، الطبعة الاولى، دار الجامعة الجديدة للنشر بالاسكندرية، سنة ٢٠٠٦، ص ١٠١

(٢) راجع في ذلك: أحمد البرماوي، مقال تحت عنوان "اقتصاد مصر" منشور بتاريخ ٢٠١٧/٥/١٣، جريدة اخبار التحرير، تم الاطلاع عليه بتاريخ ٢٠١٨/٢/١٧.

www.tahrirnews.com

وقد ظهرت مؤخرا نسخ مطورة من الفيروسات، تسمى الديدان التى لديها القدرة على العمل والانتشار من حاسب لأخر من خلال شبكات المعلومات بسرعة رهيبة، وتقوم بتعطيل عمل الخوادم المركزية والإقلال من كفاءة وسرعة شبكات المعلومات أو إصابتها بالشلل التام.

وهناك نوع أخر والذي يدعى حصان طروادة (Trojan Horse) يقوم بالتخفي داخل الملفات العادية ويحدث ثغرة أمنية في الجهاز المصاب تمكن المخترقين من الدخول بسهولة على ذلك الجهاز والعبث بمحتوياته، ونقل أو محو ما هو هام منها أو استخدام هوية هذا الجهاز في الهجوم على أجهزة أخرى فيما يعرف بالـ Leapfrog attack والذي يتم من خلال الحصول على عنوان الانترنت الخاص بجهاز الضحية، ومنه يتم الهجوم على أجهزة أخرى (IP Spoofing).

ويلاحظ الكم الضخم من الخسائر الناجمة سنويا عن ذلك النوع من جرائم الابتزاز الالكتروني، ومثال ذلك ان فيروس مثل (WS32.SOBIG) قد كبد الولايات المتحدة أكثر من خمسين مليون دولار امريكى خسائر من توقف العمل وفقد الملفات.

ثانيا الجرائم التى تتم باستخدام الحواسب الآلية ونظم المعلومات:

١) جرائم الاعتداء والتشهير والأضرار بالمصالح الخاصة والعامة:

ومنها الاعتداء والتشهير بالأنظمة السياسية والدينية والمستمرة، ولعل اشهر تلك الوقائع قيام بعض الهواة بوضع بعض البيانات في شكل سور من القران الكريم وبدءوا في الإعلان عنها من خلال إحدى مواقع البث المجاني الشهيرة، وهو موقع شركة Yahoo وعنوانه (http://www.yahoo.com) الأمر الذي استدعى الأزهر الشريف والمجلس الاعلي للشئون الإسلامية والكثير من الجهات الإسلامية الأخرى في شتى بقاع الأرض إلى مخاطبة المسئولين عن الموقع، وتم بالفعل إزالة تلك الصفحات ووضع اعتذار بدلاً منها.

أما ما يندرج منها تحت بند الجرائم التى تتم باستخدام الحواسب الآلية، هو ما يشابه التشهير بالأشخاص المعنويين أو الحقيقيين من بث أفكار ومعلومات وأحيانا أخبار وفضائح ملفقة من خلال بناء مواقع على شبكة الانترنت تتضمن كافة البيانات والمعلومات الشخصية مع العديد من الأخبار والموضوعات التى من شأنها ان تسبب الإضرار الادبى والمعنوي والمادي بالشخص أو الجهة المقصودة.

٢) جرائم الاعتداء علي الأموال:

حيث ترتب على التجاء المؤسسات المصرفية والمالية الى تكنولوجيا المعلومات والاتصالات والتحول التدريجي في كافة أنحاء العالم نحو ما يطلق عليه البنوك والمصارف والمؤسسات المالية الالكترونية، فقد شهد هذا التطور ظهور عدد كبير من جرائم الابتزاز الالكتروني.

فعلى مستوى البنوك والمؤسسات المالية، فقد تم ميكنة نظم الإدارة والمحاسبة وربط المطالب المختلفة لتلك المؤسسات بعضها ببعض من خلال شبكات المعلومات لضمان سهولة ويسر إدارة العمليات المالية داخلها، وفي تعامل تلك المؤسسات مع العملاء عن بعد.

كما تم أيضا دخول بطاقات الائتمان والدفع الالكتروني(Credit Cards) بأنواعها المختلفة لتسهيل المعاملات والتوجه للتقليل من التعاملات بالنقد المباشر في إطار التحول إلى المجتمع اللا نقدى (Cash-less Society) وبالرغم من فوائد وأهمية مثل هذا النوع من التعامل المالي وآثاره الايجابية على كفاءة البنوك في القيام بدورها وأيضا آثاره على الاقتصاد ككل[١]، الا انه ذو اثارا سلبية ضخمة فيما يتعلق بجرائم الابتزاز الالكتروني.

---

(١) راجع في ذلك: د. عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة ١٩٨٨، الدار الجامعية، بيروت، ص. ٢٥٩ .

المبحث الرابع

واقع جرائم الابتزاز الالكتروني على المستوى الدولى والعربي

من المقرر ان جرائم الابتزاز الالكتروني، لها واقع واحصائيات في ارتكابها، سواء على المستوى الدولى او العربي، تشير الى الخطر المحدق بالمجتمعات من جراء ازدياد معدلات تلك الجرائم، والاثار التى تترتب عليه.

وعليه نعرض في مطلب اول لواقع جرائم الابتزاز الالكتروني على المستوى الدولى، على ان يخصص المطلب الثاني واقع جرائم الابتزاز الالكتروني في الوطن العربي، على الترتيب التالي.

المطلب الأول

واقع جرائم الابتزاز الالكتروني على المستوى الدولي

بالنظر إلى شيوع استخدام الحاسب أواخر سبعينات القرن الماضي برزت ظاهرة القرصنة الإلكترونية، وسرعان ما تحول السلوك الذي بدا في بدايته انحرافا لمراهقين شغوفين بالتكنولوجيا، إلى حربا تشن بين الدول، وهي تهدد منشئات حيوية كالمفاعلات النووية ومحطات الكهرباء، كما تدمر المخزونات النقدية لبنوك ودول وتهتك أسرارا لا يراد لها الخروج إلى العلن[١]

وقد كشفت أرقام وبيانات عالمية، عن تزايد جرائم الابتزاز الالكتروني في مختلف أنحاء العالم، مع التوسع المتزايد لاستخدام الانترنت والأجهزة الذكية، وأظهرت دراسة لموقع "أرقام ديجتال" أن عدد ضحايا الهجمات وجرائم الابتزاز الالكتروني، يبلغ ٥٥٥ مليون مستخدم سنويا، وأكثر من ١.٥ مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات.

---

(١) انظر في ذلك: تحت عنوان "القرصنة الالكترونية سلاح العصر الرقمي"، مقال منشور على موقع قناة الجزيرة الالكتروني

http://www.aljazeera.net

ومن أكثر أنواع تلك الجرائم؛ ابتزاز هويات وعددها ٢٢٤ مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ بينت أن أكثر من ٦٠٠ ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن التكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ ١٠٠ مليار دولار، بعدما كانت في حدود ٦٣.١ مليار دولار سنة ٢٠١١

ومن المتوقع أن تتجاوز ١٢٠ مليار دولار بحلول سنة ٢٠١٧[١]، وحسب تقرير نشرته شركة مشروعات الأمن المعلوماتي (CYBERSECURITY VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته ١ تريليون دولار خلال الفترة التي تمتد من ٢٠١٧ إلى غاية ٢٠٢١ على منتجات وخدمات الأمن المعلوماتي لمكافحة جرائم الابتزاز الالكتروني، وفي هذا الإطار فقد سجل فتح حوالي مليون وظيفة خاصة بالأمن المعلوماتي خلال سنة ٢٠١٦، ومن المتوقع أن يكون هناك عجز بحوالي ١.٥ مليون وظيفة خلال عام ٢٠١٩. [٢]

أما بالنسبة للدوافع الأساسية للإجرام في جرائم الابتزاز الالكتروني، فقد تباينت ما بين جرائم من اجل الابتزاز، ودافع التجسس المعلوماتي، والحرب الالكترونية أو الاختراق من أجل قضية ما. [٣]

---

(١) راجع في ذلك: إحصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال

.http://digital.argaam.com

(2) cyber security economy predictions 2017-2021, cybersecurity ventures 2016.

.

(3) http://digital.argaam.com/article/detail/112326.

ومن المتوقع أن تكبد جرائم الابتزاز الالكتروني الاقتصاد العالمي حوالي ٦ تريليون دولار بحلول سنة ٢٠٢١ وهي ضعف الخسائر المسجلة سنة ٢٠١٥ والمقدرة بحوالي ٣ تريليون دولار[١]، وأكثر الخسائر تحدث إما بسبب فقدان بيانات ومعلومات هامة أو نتيجة لتكلفة صيانة عمليات الاختراق أو بسبب احتيال وابتزاز أموال من الشركات.

ولقد وقعت خلال عامى ٢٠١٥ و ٢٠١٦ العديد من حوادث الاختراق والقرصنة لغرض الابتزاز، ولعل أهمها ما يلي:

١- في سبتمبر من سنة ٢٠١٦، كشفت شركة ياهوو (yahoo) عن أكبر عمليات قرصنة وسرقة لقاعدة بيانات مستخدميها، وتعتبر هذه العملية من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل القراصنة على بيانات أكثر من ٥٠٠ مليون مستخدم، وفي ديسمبر من نفس السنة تعرضت الشركة نفسها، لصدمة أخرى، حيث أعلنت بأن بيانات أكثر من مليار مستخدم قد تم الاستيلاء عليها وأصبحت معروضة للبيع، منها كلمات السر وأسئلة الأمان وأرقام هواتف وتواريخ ميلاد، ويلاحظ ان هذه الحوادث خفضت من أسهم الشركة الأمريكية اقتصاديا وإعلامياً بشكل ملحوظ.

٢- لقد واجه مستخدمو الإنترنت حول العالم يوم ٢٠١٦/١٠/٢١، صعوبات في دخول المواقع الالكترونية الرئيسية، وهذه المشكلة تسببت في سقوط أهم مواقع العالم، مع تردد أنباء عن أن سبب المشكلة هجمات إلكترونية، وبحسب موقع Business Insider، فقد تعرضت أهم مواقع العالم لهجوم الحرمان من الخدمة (DDOS) والذي يعتبر أكثر الهجمات الإلكترونية شيوعاً في عالم الإنترنت، والذي يستهدف DNS، وهي أهم غصن في منظومة الانترنت، إذ تعمل على

(1) cyber security economy predictions 2017-2021, Op. Cit.
http://digital.argaam.com/article/detail/112326

ترجمة عنوان الموقع إلى عنوان IP، وأبرز المواقع الرئيسية التي تعرضت للسقوط هي Spotify, Etsy Github, Twitter, Amazon.[١]

٣- كشف محققون عما يعتقدون أنه أكبر جريمة ابتزاز الكتروني في التاريخ، توصل خلالها قراصنة روس من الاستيلاء علي العديد من بنوك دول العالم، شملت اهم المصارف في اليابان والصين والولايات المتحدة، مروراً بمصارف في الدول الأوروبية، ما يصل إلى مليار دولار، وهي العملية التي وصفت بأنها ثورة في عالم جرائم الابتزاز الالكتروني، وهذه الجريمة تشكل علامة فارقة على بداية مرحلة جديدة في ثورة النشاط الإجرامي المعلوماتي، حيث سرق المستخدمون الأموال مباشرة من البنوك ويتجنبون المستخدمين العاديين. [٢]

المطلب الثاني

واقع جرائم الابتزاز الالكتروني في الوطن العربي

لقد أصبحت الهجمات الإلكترونية مصدر تهديدا حقيقيا لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على ابتزاو أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة[٣] أو الإرهابيين أو حتى الدول المعادية.

---

(١) انظر في ذلك: تحت عنوان "الانترنت ينهار.. والطائر الأزرق يكف عن التغريد"، مقال منشور بتاريخ ٢٠١٦/١٠/٢٢، على موقع تاريخ الاطلاع ١١/ ٢٠١٧/٢:

.http://bab.com/Node/275623

(٢) انظر في ذلك: تحت عنوان "أكبر سرقة بالتاريخ.. متسللون سرقوا مليار دولار"، مقال منشور على موقع " عربية NEWS SKY".

.http://www.skynewsarabia.com

(٣) راجع في ذلك: د. هدى حامد قشقوش، مرجع سابق، منشأة المعارف، سنة ٢٠٠٦، ص ١٨، وايضا : محمد ابراهيم زيد، **"الجريمة المنظمة (تعريفها وانماطها وجوانبها التشريعية)"**، ابحاث حلقة علمية حول الجريمة المنظمة واساليب مكافحتها، الرياض، اكاديمية نايف للعلوم الامنية، سنة ١٩٩٩، ص ٣٣

ذلك أن الأرباح الضخمة غير المشروعة التي تحققها تلك الجرائم تجاوزت أرباح تجارة المخدرات[1]، كما أن جرائم الابتزاز الالكتروني أصبحت

---

(١) انظر في هذا الصدد:

Arlacci, P (1988) Mafia Business,
Verso, Oxford

Kehoe, M. (1996) the Threat of Money Laundering " unpublished paper, Department of Economics, Trinity College D, the University of Dublin, Dublin. Ireland وانظر كذلك

وفي شأن الافيون : يبلغ انتاج العالم من الافيون ٤٠٠٠ طن متري، يمكن ان يترتب على تنقيتها انتاج ٤٠٠ طن متري تقريبا من الهيروين، وينتج الافيون اساسا في منطقتين هما الهلال الذهبي في جنوب شرق اسيا، في افغانستان وايران وباكستان، وكذلك في المثلث الذهبي تايلاند وبورما ولاوس Laos هناك كميات صغيرة تنتج في لبنان والمكسيك، ويلاحظ ان هناك اتجاها لتنويع انتاج المخدرات في امريكا اللاتينية من خلال استبدال بعض انتاج الكوكايين والماريجوانا بالافيون (Davies and Saltmarsh 1994 ، وايضا : تقرير الهيئة الدولية لمراقبة المخدرات لسنة ٢٠٠٠، الغصون (٥٠ – ٥٦) ، ص ١٢ ، ١٣، مطبوعات الامم المتحدة، نيويورك، سنة ٢٠٠١، الوثيقة رقم Elincb 200D المنشور بتاريخ ٢١ فبراير ٢٠٠١ ، وكذلك انظر : مجلة الحقوق الكويتية، مجلس النشر العلمي، الكويت، ١٩٩٨، العدد الثالث، ص ٣٨١ ، منشور دورة البحث الجنائي للضباط رقم (٥) دراسات حول الجريمة الاقتصادية في دولة الامارات، معهد البحث الجنائي، شرطة دبي، دولة الامارات العربية المتحدة، سنة ١٩٩٨، ص ٩٨.

DUNCAN. Alfod. Anti- mony laundering regulations: Aburden on financial institutions, volume 19 north Carolina jounal of international and commercial regulations, p.p 441 – 442 (summer 1994)

اليوم واقعاً لا ينكر في مصر، بوقوع نحو ثلاثون مليون شخص من سكان الدولة ضحايا جرائم الابتزاز الالكتروني خلال سنة ٢٠١٥. [١]

وكشف موقع «جوبال ريسك إنسايتس» أن المملكة العربية السعودية هي البلد الأكثر استهدافا بالهجمات الإلكترونية في الشرق الأوسط، وأن إيران كذلك أكثر من يستهدفها إلكترونيا».

وقد نوه ذلك التقرير إلى أن الهجمات الإلكترونية على المملكة السعودية وصلت عام ٢٠١٥ إلى ١٦٠ ألف محاولة هجوم يوميا، ويشير نفس التقرير إلى أن الإمكانيات الرقمية والالكترونية الكبيرة للسعودية تجعلها هدفا مميزا للهجمات الالكترونية حيث تمتلك المملكة أكبر عدد من المشتركين في خدمة الإنترنت في العالم العربي.[٢]

وحسب تقارير دولية مستقلة، فإن الإمارات سجلت أفضل أداء في صد الهجمات الإلكترونية في منطقة الشرق الأوسط خلال النصف الأول من سنة ٢٠١٦، في الوقت الذي أكدت هيئة تنظيم الاتصالات على فعالية منظومة الحماية الإلكترونية في الدولة.[٣]

ومنذ عام ٢٠١٤، ارتفعت معدلات جرائم الابتزاز الالكتروني في لبنان، مما وضع المعنيين في المصارف والمؤسسات المالية والأجهزة الأمنية أمام سباق

---

(١) انظر في ذلك: تحت عنوان "الجرائم المعلوماتية.. أرباح تفوق ما تجنيه تجارة المخدرات"، مقال منشور على الموقع الالكتروني لجريدة الاتحاد

.http://www.alittihad.ae/details.

(٢) انظر في ذلك: محمد خالد، تحت عنوان "السعودية الأكثر تعرضا للهجمات الإلكترونية في الشرق الأوسط"، مقال منشور على موقع الخليج الجديد.

.http://thenewkhalij.org/ar/node/43159

(٣) انظر في ذلك: يوسف العربي، تحت عنوان "الهجمات الإلكترونية تزداد شراسة على الإمارات ومنظومة حماية متكاملة في المواجهة"، مقال منشور على الموقع الالكتروني لجريدة الاتحاد

.http://www.alittihad.ae/details.

مـع القراصـنة القـادرين علـى تطـوير أدواتهـم وتنظيمـاتهم بمـوازاة تطـور وسـائل المكافحـة، حيـث بلـغ عـدد عمليـات القرصـنة الإلكترونيـة التـي تعرضـت لهـا المصارف اللبنانية حصراً منذ عام ٢٠١١ حتى الفصل الثالث من سنة ٢٠١٦، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان، ٢٣٣ عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو ٢٦ مليوناً ونصف مليون دولار، مـن ضـمنها ١٥ مليـون دولار بـين عـامي ٢٠١٥ و٢٠١٦ طالـت القطـاع المصرفي بشكل مباشر، وفق تقرير مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية بلبنان، وتعكس هذه الأرقام الحد الأدنى، إذ إن القيمة الفعلية للغنائم وعدد العمليات الإلكترونية، باعتراف هيئة التحقيق ومكتب مكافحة الجرائم المعلوماتية، أكبر بالتأكيد، لأن هناك حالات لم يتم الإبلاغ عنها إما بدافع الحفاظ على السمعة أو يقيناً باستحالة استعادة تلك الأموال.[١]

ولم تسلم دولة الجزائر كغيرها من الدول، من جرائم الابتزاز الالكتروني، حيث لم تسلم مواقع التواصل الاجتماعي وفضاء تبادل المعلومات، من عملية السطو على الصور والبيانات الشخصية، واستعمالها كوسيلة للابتزاز والمساومة والتشهير، فضلا عن استغلال بيانات الحسابات الشخصية، وقد تم تسجيل أكثر من ٥٠٠ جريمة ابتزاز الكتروني في الجزائر خلال سنة ٢٠١٦، علما أن هذا يخص عدد الحالات التي قامت بعملية التبليغ فقط[٢]

---

(١) حيث تم الاستيلاء على ٢٦.٥ مليون دولار، من مصارف لبنان التى تعرّضت لـ٧ أنواع من الهجمات الإلكترونية .

.http://ghadinews.net/Newsdet

(2) John Madinger, Sydney A. Zal: Money laundering: aguide for criminal investigators, CRC press Boca Raton, London, New York, Washington D.C 1999.

والواقع أن الأغلب يرفض إيداع شكوى لاعتبارات اجتماعية وثقافية، وهو الأمر الذي جعل مصالح الدرك الوطني بالجزائر تتجند لحماية مستعملي الانترنت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة ٣٨٥ جريمة معلوماتية من قبل الفرق المتخصصة في مكافحة الجريمة المعلوماتية التابعة للأمن الوطني، إلى جانب تسجيل ٥٧ قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية.(١)

مشار اليه كذلك: د. حمدي عبد العظيم: مرجع سابق، ص ٢٢٠ – ٢٢١، وايضا: عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– الناشر : جامعة نايف العربية للعلوم الأمنية – ٢٠٠٨ م – صـ ٤٦ وما بعدها، وايضا : محمد فتحى عيد، السنوات الحرجة في تاريخ المخدرات، نذر الخطر وعلامات التفاؤل، مركز ابحاث مكافحة المخدرات بوزارة الداخلية، الرياض، الطبعة الاولى، سنة ١٩٩٠، ص ١٣١.

(١) انظر في ذلك: تحت عنوان "أزيد من ٥٠٠ جريمة إلكترونية في الجزائر سنة ٢٠١٦"، مقال منشور على الموقع الالكتروني لجريدة الفجر

.http://www.al-fadjr.com

الفصل الثالث

جرائم الابتزاز الالكتروني التي تستهدف الاطفال

من المقرر ان الطفل هو الخلية الاساسية لاى مجتمع، مما يستلزم حمايته، وحفظ كافة حقوقه وحرياته بموجب نصوص قانونية صارمة، ذلك ان الاطفال والمراهقين اصبحوا في الاونة الاخيرة ضحايا لجرائم الابتزاز الالكتروني بشكل ملحوظ، ويكون ذلك في الغالب الاعم بسبب ثقتهم بالاخرين وبسبب غياب التوجيه او الرقابة في كثير من الاحوال، ولانه لا تتوفر لديهم الخبرة والدراية الكافية لتقدير المخاطر .

وابرز انماط جرائم الابتزاز الالكتروني التي تستهدف الاطفال عبر الانترنت تتمثل بما يلي:

١- اقحام الاطفال باتصالات عبر الخط يكون غرضها أنشطة جنسية Sexual acts.

٢- استخدام الانترنت لترويج وانتاج وتوزيع مواد دعارة الاطفال Child pornography.

٣- استخدام الانترنت لاجبار الشباب والاطفال على ممارسة افعال الدعارة وتشجيعهم لتبادلها.

٤- اقحام الاطفال في أنشطة سياحية تستهدف اغراض جنسية، كالسفر للمشاركة في أنشطة غير اخلاقية سواء لكسب مادي او لتحقيق منافع شخصية.

٥- تنسيق وتنظيم الأنشطة الجنسية الواقعية او الاتصالات الجنسية، باستخدام البريد الالكتروني او التليفون او انتقال الشخص فعلا الى مكان مادي لاجراء هذه الأنشطة الجنسية.

٦- توزيع المواد الجنسية غير المطلوبة اصلا، حيث انه وبمجرد الاتصال بالانترنت او فتح البريد الالكتروني او الدخول على بعض المواقع المشروعة، تظهر مواد جنسية وصور اباحية دون ان يكون الشخص قد طلبها.

٧- أنشطة الابتزاز وتشويه السمعة والتهديد الموجهة للشباب والاطفال عبر الرسائل الالكترونية سواء أكانت تتصل باغراض جنسية او اجرامية او غيرها.

ذلك ان حجم مشكلة المواد الاباحية بوجه عام، والمواد والأنشطة الجنسية المتصلة بالاطفال والقصر بوجه خاص، يتزايد بشكل غير عادي، ووفقا لتقديرات حديثة فان واحدا من كل خمسة شباب قد توصل مع احد مواقع المواد الجنسية على الانترنت، وان واحدا من كل ثلاثة وثلاثين شاب تلقى عرضا لأنشطة جنسية بشكل او بأخر، وان كل واحد من اربعة شباب وصلته مواد جنسية غير مطلوبة، وان كل واحد من سبعة عشر شاب تلقى تهديدات او ابتزازات او غيرها من المواد المسيئة، وذلك كله خلال عام ٢٠٠٠ وفقا للدراسة التي اجراها مكتب ضحايا الجريمة التابع لوزارة العدل الامريكية.

الفصل الرابع

الادلة المعلوماتية في جرائم الابتزاز الالكتروني

ما لا شك فيه مساهمة شبكة المعلومات الدولية "الإنترنت" في تعزيز الثورة المعلوماتية، وذلك بانتقال المعلومات وعدم احتكارها وانتشارها بأسرع وقت ممكن متى تعلق الأمر بخبر أو نبأ أو معلومة، كما اصبحت هذه الشبكة فضاء متاح للجميع فيمكن لأي فرد أن يلج إلى هذه الشبكة في أي وقت ومن أي مكان دون حاجة لأذن مسبق من حكومة أو دولة، بل ويستطيع أن يخاطب المجتمعات الأخرى وأن يعبر عن رأيه ويتواصل مع الآخرين دون الخوف من أن يتم مصادرة أرائه وأفكاره.

فالإنترنت اصبح فضاء معلوماتى لا يمكن السيطرة عليه عملياً أو إستحواذه أو إحتكاره، ويمكن لكل شخص طبيعي أو معنوي من خلال هذا الفضاء، أن يزاول أي نشاط يريد سواء كان هذا النشاط تجاري، او فكري، او ثقافي او إجتماعي، أو سياسي أو غير ذلك من نشاطات أخرى.

وأمام هذه الحرية المتاحة في العالم الإفتراضي ونظراً لسهولة الاتصال والولوج للشبكة الإنترنت وإنتشار مستخدميها في مختلف أنحاء العالم، فإنها أفرزت لنا العديد من النشطاء الذين لم يجيدوا التعامل معها بشكل صالح وخيَر وإستغلوها للقيام ببعض الأفعال غير المشروعة قانوناً والمنافية للدين والأخلاق وللطبيعة البشرية أحياناً .

فلقد أفرزت شبكة الإنترنت أنماطا خاصة من السلوك الإجرامي المستحدث الذي لم نألفه في أنماط الجرائم المتعارف عليها والتي تصدت لها بعض التشريعات ووضعت لها القوانين والعقوبات، فجريمة التحويل الإلكتروني

غير المشروع للأموال[١] وسرقة المعلومات وتدمير المواقع والإرهاب عبر الإنترنت وجرائم التجسس على المعلومات والأشخاص والجنس وترويج الأفكار الهدامة بإستخدام الإنترنت كوسيلة للإشهار, وكلها تصب في قالب الجرائم المستحدثة، وقد تفنن مستحدثي هذه الجرائم في تنوع الأساليب المبتكرة للتنفيذ هذه الجرائم استغلال لمعرفتهم وقدراتهم في هذا المجال من أجل القيام بنشاطاتهم غير المشروعة[٢] .

ومن اهم الأمثلة لتلك الجرائم، سرقة معلومات الحاسب وقرصنة البرامج وسرقة خدمات الحاسب وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الحاسب وتزوير البريد الإلكتروني أو الوثائق والسجلات والهوية.

وايضا جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب وتملك وإدارة مشروع مقامرة على الانترنت وتسهيل إدارة مشروعات القمار على الإنترنت وتشجيع المقامرة عبر الانترنت واستخدام الانترنت لترويج الكحول ومواد الإدمان للقصر والحيازة غير المشروعة للمعلومات وإفشاء كلمة سر الغير وإساءة استخدام المعلومات وخلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات وغيرها من الجرائم المعلوماتية.

---

(1) Electronic cash (EC): the Funds or value is stored on an electronic device as the personal computer of the consumer which is loaded using specialized software0 EC is used to make small payments through a transfer of value to the merchants electronic device

(٢) راجع في ذلك: د. محمد مدحت عزمى، المعاملات التجارية الالكترونية، الاسس القانونية والتطبيقات، الطبعة الاولى، مركز الاسكندرية للكتاب، مصر، سنة ٢٠٠٩، ص ٣٥٤، وايضا : د. احمد سفر، العمل المصرفي الالكترونى في البلدان العربية، الطبعة الاولى، المؤسسة الحديثة للكتاب، لبنان، سنة ٢٠٠٦، ص ٢١٩

المبحث الاول

معوقات الاثبات الجنائي في جرائم الابتزاز الالكتروني

يطلق فقهاء القانون الجنائى على الشخص الذى يقترف جرائم الابتزاز الالكتروني مصطلح المجرم المعلوماتي، تمييزا له عن المجرم التقليدى وهو الشخص الذى لدية مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي، والقادر على إستخدام هذا التكتيك المحترف لإختراق الكود السرى لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق إستخدام الحاسب نفسه.

فالمجرم المعلوماتي اذن، ليس شخص عادى وانما هو شخص محترف له اوصافه وسماته الخاصة التى تميزه عن المجرم التقليدى، وهو شخص يتميز بالذكاء الشديد والخبرة الفائقة في مجال الحاسب الآلي والانترنت، وهذه السمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء، ولم يجد المجرم المعلوماتي رادعه، نظرا لصعوبة الاثبات الجنائي في هذا النوع من الجرائم, خصوصا ان ادلة الاثبات يصعب الوصول اليها.

ذلك إن هذا المجرم متخصص له قدرة فائقة علي المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمة المرور أو الشفرات, وهو كذلك مجرم عائد للجريمة دائما يوظف مهاراته بصورة سلبية في كيفية عمل الحواسب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات, وهو مجرم محترف يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء علي حقوق الملكية الفكرية، وغيرها من الجرائم مقابل المال, وهو مجرم ذكي يمتلك مهارات تؤهله بتعديل وتطوير الأنظمة الأمنية.

وجدير بالذكر، مدي الصعوبات التي تكتنف ملاحقة السلطات لهذا المجرم وتتبع أعماله الإجرامية، ومما يزيد من صعوبة هذه الملاحقة ايضا هو ان هذا المجرم لا يلج النظام المعلوماتي الذى سيرتكب عليه جريمته باسمه الحقيقى

او بمعلومات صحيحة، بل دائما يدخل باسم مستعار ومعلومات غير صحيحة، كما انه يرتكب الجريمة عن بعد مما يصعب أكثر من ملاحقته، بل انه يمكن ان يرتكب الجريمة من دولة على نظام معلوماتى موجود في دولة اخرى.

كما ان المجرم المعلوماتي ليس نوع واحد واهدافهم ليست واحدة، فمنهم صغار السن الذين قد لا يقدرون خطورة ما يقومون به، وهناك المجرم المعلوماتي الذى يتعمد اختراق الانظمة المختلفة لتحقيق اهداف خاصة اهداف سياسية او اقتصادية او ممارسة جرائم عبر الانترنت، كالقراصنة المرتزقة الذين يستخدمون من قبل أفراد أو حكومات لاقتحام برامج ونظم حواسب محددة لتدميرها او سرقة ما فيها او تشويهها مقابل مبالغ مالية.

ومن هنا، نجد ان بعض الاجهزة الحكومية في دول مختلفة تستعين بهم لتحقيق مصالح خاصة بها، وبالتالي هؤلاء القراصنة يجدوا الحماية من الاجهزة الحكومية، وبالتالي فان ملاحقتهم ليست بالأمر اليسير، لاننا نكون امام مجرم يتمتع بالذكاء الفائق والخبرة الكبيرة في مجال الحاسب الآلي، ويسخر كل ذلك لارتكاب جرائم الابتزاز الالكتروني مما يجعل ملاحقته أمر غاية في الصعوبة.

ويزيد من هذه الصعوبة انه يرتكب جرائمه عن بعد، ويكون بعيد عن مسرح الجريمة الذى تنعدم علية الادلة تماما، بالاضافة الى قدرة هذا المجرم على محو كل دليل او اثر يمكن ان يدل عليه مما يجعل ملاحقته امر صعب للغاية .

الا انه يمكن التخفيف من هذه الصعوبات، بالتعاون الفعال بين الدول المختلفة لمحاولة السيطرة على هذه الجرائم التى انتشرت بصورة كبيرة، ويطور المجرم المعلوماتي فيها من اساليب ارتكابه للجريمة، بالاضافة الى انشاء جهاز لتعقب مجرمى المعلوماتية يعمل على مستوى كل الدول ويحقق التعاون الايجابى بين الدول[1].

---

(١) انظر في ذلك: حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء الجنائى الوطنى، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، سنة ٢٠٠٠ ، ص ٢٥

فالاثبات الجنائى هنا، هو اقامة الدليل على وقوع الجريمة ونسبتها الى المتهم، وذلك وفق الطرق التى حددها القانون، والاثبات في مجال جرائم الابتزاز الالكتروني، ينطبق عليه المفهوم العام للاثبات، وهو بذلك يواجه العديد من الصعوبات التى تتعلق بصعوبة الحصول على دليل، واذا تم الحصول على دليل نجد ان هناك عقبات اخرى تقف وراء الاستفادة من هذا الدليل، وهو ما نعرض له من خلال المطلب الاول، على ان يخصص المطلب الثاني لمدى سهولة إخفاء الدليل او محوه، وفي المطلب الثالث نوضح غياب الدليل المرئي، ويعرض المطلب الرابع لصعوبة فهم الدليل المتحصل من الوسائل الإلكترونية، اما المطلب الخامس والاخير فيختتم ببيان الضخامة البالغة لكم البيانات المتعين فحصها، وذلك على الترتيب التالي:

المطلب الاول

معوقات الوصول إلى الدليل في جرائم الابتزاز الالكتروني

من المقرر ان الجناة في جرائم الابتزاز الالكتروني من المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو الاستثارة، وإنما هم يخططون لما يفعلون ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط، ولذلك نجد انهم وهم يرتكبون جرائم الابتزاز الالكتروني يحيطون انفسهم بتدابير أمنية واقية، تزيد من صعوبات كشف سترهم.

ومثال لذلك، نجد أنهم قد يستخدمون التشفير وكلمات السر التي تمكنهم من اخفاء الإدلة التي قد تكون قائمة ضدهم، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم ان يفهم مقصودها، وقد يقوم هؤلاء ايضا

وايضا : عبدالرؤوف مهدى، التعاون القضائى كاحد موجبات الاختصاص الوطنى، مؤتمر القانون الدولي الانسانى بين الاتفاقيات الدولية والتشريعات الجنائية المصرفية، ورقة عمل مقدمة الى المؤتمر الحادى عشر للجمعية المصرية للقانون الجنائى في الفترة من ٢٠ – ٢١ مايو ٢٠٠٣ ، ص ١٠.

بتشفير التعليمات بإستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها في قمة الصعوبة.

وكما أن هؤلاء الجناة قد يستخدمون الوسائل الإلكترونية المختلفة، لإعاقة الوصول إليهم، فقد يستخدمون البريد الإلكتروني في إصدار تكليفاتهم بإرتكاب جرائم القتل والاغتيالات والتخريب دون ان يتمكن أحد من تحديد اماكنهم أو تسجيل هذه التكليفات على النحو الذي كان يحدث في الاتصالات السلكية واللاسلكية.

كذلك فإن مرتكبي جرائم الابتزاز الالكتروني يصعب ملاحقتهم لإستحالة تحديد هويتهم، سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها، لأنهم في الغالب يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة، ليس عن طريق ابواب حاسباتهم الآلية، وانما عن طريق مقاهي الإنترنت.

أيضا من الملاحظ، أن ملاحقة جرائم الابتزاز الالكتروني، قد تتعلق ببيانات تكون مخزنة في داخل دولة اجنبية بواسطة شبكة الاتصال عن بعد، ولذلك فإنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة الذي تحرص عليه كل دولة.

المطلب الثاني

سهولة إخفاء الدليل او محوه في جرائم الابتزاز الالكتروني

من المقرر ايضا ان الجناة الذين يستخدمون الوسائل الإلكترونية في إرتكاب جرائمهم، يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية، ولذلك فإنهم يتمكنون من اخفاء الافعال غير المشروعة التي يقومون بها اثناء تشغيلهم لهذه الوسائل الإلكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها.

كما أن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الإلكترونية، ويكون امرها حكرا عليهم، كالتجسس على ملفات البيانات المختزنة، والوقوف على ما بها من أسرار.

كما أنهم قد ينسخون هذه الملفات ويتحصلون على نسخ منها بقصد استعمالها تحقيقا لمصالحهم الخاصة، كذلك فإنه قد يقومون بإختراق قواعد البيانات والتغيير في محتوياتها تحقيقا لمآرب خاصة، وقد يخربون الانظمة تخريبا منطقيا بحيث يمكن تمويهه، كما لو كان مصدره خطأ في البرنامج للمعلومات، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون ان يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل.

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية، أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه ان يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده.

المطلب الثالث

غياب الدليل المرئي في جرائم الابتزاز الالكتروني

يجدر القول بان جرائم الابتزاز الالكتروني التي تقع على العمليات الإلكترونية المختلفة، كالتي تقع على عمليات التجارة الإلكترونية، أو على العمليات الإلكترونية للأعمال المصرفية، أو على أعمال الحكومة الإلكترونية، قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية، كجرائم الاختلاس أو الاستيلاء أو الغش أو التزوير أو الإتلاف، فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة.

ويلاحظ وجود شك قائم في ان إثبات الأمور المادية التي تترك آثارا ملحوظة يكون سهلا ميسورا، بعكس إثبات الأمور المعنوية فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، حيث أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية.

فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكتروني، يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة.

ومثال ذلك، نجد أن التجسس المعلوماتي بنسخ الملفات وسرقة وقت الآلة يصعب على الشركات التي تكون الضحية لمثل هذه الافعال اكتشاف امرها وملاحقة الجناة عنها.

والنظر الى هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية الحاسبات، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة، فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة، ولكن في محيط الإلكترونيات فالامر مختلف، فالمتحري أو المحقق لا يستطيع اي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية(١).

---

(١) انظر في ذلك: د. ابراهيم بن عوض العتيبى، استخدام التقنية في التحقيقات الامنية، مقال منشور بمجلة التقنية والامن، مجلة كلية الملك خالد العسكرية، العدد ٨٠ ، سنة ٢٠٠٥ ، ص ٧.

المطلب الرابع

صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية

لا شك في ان طبيعة الدليل تنعكس عليه، فالدليل الفني قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، بعكس الدليل القولي فإن الكثير ممن يتصلون به يسهل عليهم فهم مضمونه وإدراك حقيقته.

وإذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الإلكترونية، قد يتحصل من عمليات فنية معقدة عن طريق التلاعب في نبضات وذبذبات الكترونية وعمليات أخرى غير مرئية، فإن الوصول إليه وفهم مضمونه قد يكون في غاية الصعوبة.

فالطبيعة غير المادية للبيانات المخزنة بالحاسب الآلي، والطبيعة المعنوية لوسائل نقل هذه البيانات تثير مشكلات عديدة في الإثبات الجنائي، ومثال ذلك أن إثبات التدليس والذي قد يقع على نظام المعالجة الآلية للمعلومات يتطلب تمكين مأمور الضبط القضائي أو سلطة التحقيق من جميع المعطيات الضرورية التي تساعد على إجراء التحريات والتحقق من صحتها للتأكد عما إذا كانت هناك جريمة قد وقعت أم لا.

ومثل هذا الامر يتطلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا التدليس وقد يستعصى هذا الأمر فهما على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة التي من خلال ثناياها قد يتولد الدليل المتحصل من الوسائل الإلكترونية.

كذلك فإن الكثير من العمليات الآلية للبيانات التي قد يقوم بها الحاسب الآلي بطريقة آلية دون الحاجة أو اجراء تعديلات في برامجه أو القيام بالتلاعب في البيانات المخزنة، وبالنظر إلى أن طبيعة هذه العمليات يصعب ان تخلف وراءها آثار مادية ملموسة تكشف عنها والمخزنة في برنامج الحاسب، قد يكون من السهل إختراقها وإرتكاب جرائم تزوير واستيلاء تقع عليها عن طريق إدخال

بيانات غير معتمدة في نظام الحاسب، فإن ذلك يزيد من صعوبة عمل المحققين الذين يعملون في حقل الجرائم التي تتمخض عن هذه العمليات الإلكترونية.

فقد يستعصى عليهم فهم الأدلة المتحصلة عن هذه الوسائل، بسبب تعقيدها وصعوبة الإهتداء إلى مرتكبي الجرائم الواقعة في سياق مثل هذه العمليات أيضا، فإن فهم الدليل الموصل إلى اثبات الجرائم التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية قد يزداد صعوبة، في تلك الحالات التي يتصل فيها الحاسب الآلي بشبكة الإتصالات العالمية.

ففي مثل هذه الحالات؛ فإن فهم مثل هذا الدليل يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار افضل السبل لضبطه، بالنظر إلى أهمية الخبرة في ازالة غموض الجرائم التي تقع بالوسائل الإلكترونية، فإن ذلك يكشف لنا عن الاهمية المتزايدة لتدريب الخبراء القضائيين على تقنيات الحاسبات الآلية لتمكينهم من القيام بمهامهم في المسائل الإلكترونية الدقيقة وإعداد تقاريرهم الفنية فيها والتي تكون ذات اهمية بالنسبة لقضاء الحكم الذي غالبا ما يتخذ منها سندا يرتكن إليه في المسائل الفنية البحتة.

ولا يغيب عن الذهن إن فهم الأدلة الفنية التي تتحصل من الوسائل الإلكترونية يتطلب أيضا تدريب جهات الضبط القضائي والتحقيق والقضاء على فهم طبيعة المعطيات التي تقع عليها جرائم الابتزاز الالكتروني، والعمل على المامهم بمكونات الحاسب الآلية وكيفية عملها ومعرفة اللغة التي تتعامل بها، والتي تعتمد على المختصرات.

خاصة، وان الجرائم التي تقع بإستخدام الوسائل الإلكترونية في الغالب ما تعتمد على رموز تكون معروفة عند اهل العلم والخبرة ولقد جاء في توصيات المجلس الأوروبي الصادر في سنتي ١٩٨٥ و ١٩٩٥ بما يفيد ضرورة استحداث دوائر جديدة تضطلع بمواجهة جرائم الابتزاز الالكتروني وتزويدها بالموظفين

الأكفاء ذوي الخبرة والدراية العلمية بالاضافة إلى توفير الاجهزة والمعدات التقنية اللازمة لذلك.

المطلب الخامس

مدى الضخامة البالغة لكم البيانات المتعين فحصها

مما لا شك فيه ان الكم الهائل للبيانات التى يجرى في الانظمة المعلوماتية تداولها، يمثل احد واهم الصعوبات التى تعوق تحقيق الجرائم التى تقع عليها او بواسطتها، وأية ذلك ان طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الاهمية يتطلب مئات الالاف من الصفحات التى لا تثبت شيء على الاطلاق.

وفي مواجهة هذه الصعوبة يسلك المحقق غير المتدرب احد طريقين اما حجز البيانات الالكترونية بقدر يفوق القدرة البشرية على مراجعتها او التغاضى عن هذه البيانات كلية بأمل الحصول على اعتراف من المتهم، والواقع اننا يمكن مواجهة ذلك بطريقتين اخرتين ايسر في التطبيق وهما:

- اما الاستعانة بالخبرة الفنية لتحديد ما يجب البحث عنه دون سواه للاطلاع عليه وضبطه.
- او الاستعانة بما تتيحه نظم المعالجة الالية للبيانات من اساليب للتدقيق والفحص المنظم او المنهجى ونظم ووسائل الاختبار والمراجعة، بالاضافة الى اساليب الفحص المنصب بوجه خاص على الحالة او الواقعة محل البحث

وبالاضافة الى كل هذه العقبات، نجد ان هناك عقبة اخيرة تتصل بنقص خبرة الشرطة وجهات الادعاء والقضاء حيث يتطلب كشف جرائم الابتزاز الالكتروني والاهتداء الى مرتكبيها وملاحقتهم قضائيا استراتيجيات تحقيق وتدريب ومهارات خاصة تسمح بفهم ومواجهة تقنيات الحاسب الالكترونى المتطورة واساليب التلاعب المعلوماتي المعقدة التى تستخدم عادة في ارتكاب هذه الجرائم.

لذلك وجدت سلطات البحث الجنائى والتحقيق نفسها غير قادرة على التعامل بالوسائل التقليدية مع هذه النوعية من الجرائم ولنقص الخبرة والتدريب كثيرا ما تخفق اجهزة الشرطة في تقدير اهمية جرائم الابتزاز الالكتروني، فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب مع هذه الاهمية.

ولهذا كثيرا ما تفشل سلطات البحث الجنائي وجهات التحقيق في جمع أدلة جرائم نظم المعلومات مثل مخرجات الحاسب وقوائم التشغيل، بل ان المحقق نتيجة نقص خبرته في الحاسب الآلي قد يدمر الدليل بمحوه الاسطوانة الصلبة عن خطأ او اهمال او التعامل بخشونة مع الاقراص المرنة(١).

ومن الامثلة الواضحة على ان نقص خبرة جهات البحث في جرائم الابتزاز الالكتروني، قد يؤدى الى الاضرار بالدليل، ما حدث في الولايات المتحدة الامريكية حيث طلبت الشرطة من شركة تعرضت للقرصنة التوقف عن تشغيل اجهزتها الالية لتمكن من وضعها تحت المراقبة بهدف كشف الفاعل، وكان من نتيجة ذلك ان تسببت الشرطة من غير قصد في اتلاف ما كان تم تسليمه لها من برامج وملفات.

---

(١) انظر في ذلك: د. ابراهيم بن عوض العتيبى، استخدام التقنية في التحقيقات الامنية، مقال منشور بمجلة التقنية والامن، مجلة كلية الملك خالد العسكرية، العدد ٨٠ ، سنة ٢٠٠٥ ، ص ٧.

الفصل الخامس

تطبيقات عملية لجرائم الابتزاز الالكتروني ضد الطفل

مع المقرر ان استخدام الحاسب الآلي في أواخر سبعينات القرن الماضي، ترتب عليه انتشار ظاهرة القرصنة الإلكترونية، وسرعان ما تحول السلوك الذي بدا في بدايته انحرافا لمراهقين شغوفين بالتكنولوجيا، الى حرب شنيعة بين الدول، وهي تهدد كافة المنشئات الحيوية كالمفاعلات النووية ومحطات الكهرباء كما تدمر المخزون النقدي لبنوك ودول وتهتك أسرارا دولية ومجتمعية، وكشفت أرقام وبيانات عالمية، تزايد الجرائم المعلوماتية في مختلف أنحاء العالم، مع التوسع المتزايد لاستخدام الانترنت والأجهزة الذكية.

وأظهرت الدراسات أن عدد ضحايا هجمات الابتزاز الالكتروني، يبلغ ٥٥٥ مليون مستخدم سنويا، وأكثر من ١.٥ مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات، وأكثر أنواع الجرائم سرقة هويات وابتزاز اصحابها، وعددها ٢٢٤ مليون سرقة.

ويلاحظ أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ أن أكثر من ٦٠٠ ألف حساب فيسبوك يتم اختراقها بغرض الابتزاز يوميا، وأن التكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ ١٠٠ مليار دولار، بعدما كانت في حدود ٦٣,١ مليار دولار سنة ٢٠١١، وانها تجاوزت ١٢٠ مليار دولار بحلول سنة ٢٠١٧.

وحسب تقرير نشرته شركة مشروعات الأمن المعلوماتي (CYBERSECURITY VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته ١ تريليون دولار خلال الفترة التي تمتد من ٢٠١٧ الى غاية ٢٠٢١ على منتجات وخدمات الأمن المعلوماتي لمكافحة تلك الجرائم.

وفي هذا الإطار فقد سجل هذا التقرير فتح حوالي مليون وظيفة خاصة بالأمن المعلوماتي خلال سنة ٢٠١٦، ومن المتوقع أن يكون هناك عجز بحوالي ١.٥ مليون وظيفة خلال عام ٢٠١٩.

أما بالنسبة للدوافع الأساسية للإجرام المعلوماتي فقد تباينت ما بين جرائم من اجل الابتزاز، او بدافع التجسس المعلوماتي، او الحرب الالكترونية أو الاختراق من أجل قضية ما.

ومن المتوقع أن تكبد جرائم الابتزاز الالكتروني الاقتصاد العالمي حوالي ٦ تريليون دولار بحلول سنة ٢٠٢١ وهي ضعف الخسائر المسجلة سنة ٢٠١٥ والمقدرة بحوالي ٣ تريليون دولار، وأكثر الخسائر تحدث إما بسبب فقدان بيانات ومعلومات هامة أو نتيجة لتكلفة صيانة عمليات الاختراق أو بسبب احتيال وسرقة أموال من الشركات.

وحيث ان جرائم الابتزاز الالكتروني لها تطبيقاتها العملية بحالات ملموسة على الصعيد الدولى، مما يتعين تناولها من خلال المبحث الاول، لحالات عملية لجرائم الابتزاز الالكتروني على الصعيد العربي، واخيرا نتناول نماذج خاصة لبعض القضايا المتعلقة بجرائم الابتزاز الالكتروني في مصر من خلال المبحث الثاني.

المبحث الاول

حالات عملية لجرائم الابتزاز الالكتروني على الصعيد العربي

لقد أصبحت الهجمات الإلكترونية مصدر تهديد حقيقي لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار أمن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية.

وكشف موقع «جوبال ريسك إنسايتس» أن المملكة العربية السعودية هي البلد الأكثر استهدافا بهجمات الابتزاز الإلكتروني في الشرق الأوسط، وأن إيران أكثر من يستهدفها إلكترونيا، ونوه التقرير إلى أن هجمات الابتزاز الإلكتروني على المملكة العربية السعودية، وصلت عام ٢٠١٥ إلى ١٦٠ ألف محاولة هجوم يوميا، ويشير نفس التقرير إلى أن الإمكانيات الرقمية والالكترونية الكبيرة للسعودية تجعلها هدفا مميزا للهجمات الالكترونية حيث تمتلك المملكة أكبر عدد من المشتركين في خدمة الإنترنت في العالم العربي.

وحسب تقارير دولية مستقلة، فإن الإمارات سجلت أفضل أداء في صد الهجمات الإلكترونية في منطقة الشرق الأوسط خلال النصف الأول من سنة ٢٠١٦، في الوقت الذي أكدت هيئة تنظيم الاتصالات على فعالية منظومة الحماية الإلكترونية في الدولة[١].

وفي لبنان، ارتفعت معدلات جرائم الابتزاز الالكتروني منذ عام ٢٠١٤، مما وضع المعنيين في المصارف والمؤسسات المالية والأجهزة الأمنية أمام سباق مع القراصنة القادرين على تطوير أدواتهم وتكتيكاتهم بموازاة تطور وسائل المكافحة، حيث بلغ عدد عمليات القرصنة الإلكترونية التي تعرضت لها

---

(١) راجع في ذلك: د. علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، ايتراك للطباعة والنشر والتوزيع، الطبعة الاولى، مصر، سنة ٢٠٠٠، ص ١٩٧.

المصارف اللبنانية حصراً منذ عام ٢٠١١ حتى الفصل الثالث من سنة ٢٠١٦، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان، الى نحو ٢٣٣ عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو ٢٦ مليوناً ونصف مليون دولار، من ضمنها ١٥ مليون دولار بين عامي ٢٠١٥ و٢٠١٦ طالت القطاع المصرفي بشكل مباشر، وفق تقرير مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية.

وتعكس هذه الأرقام الحد الأدنى، إذ إن القيمة الفعلية للغنائم وعدد العمليات الإلكترونية، باعتراف هيئة التحقيق ومكتب مكافحة الجرائم المعلوماتية، أكبر بالتأكيد، لأن هناك حالات لم يتم الإبلاغ عنها إما بدافع الحفاظ على السمعة أو يقيناً باستحالة استعادة تلك الأموال.

والجزائر كغيرها من الدول لم تسلم هي الأخرى من جرائم الابتزاز الالكتروني، حيث لم تسلم مواقع التواصل الاجتماعي وفضاءات تبادل المعلومات، من عملية السطو على الصور والبيانات الشخصية، واستعمالها كوسيلة للابتزاز والمساومة والتشهير، فضلا عن استغلال بيانات الحسابات الشخصية بالإضافة إلى الاعتداء على أنظمة المعلومات، فقد تم تسجيل أكثر من ٥٠٠ جريمة إلكترونية في الجزائر خلال سنة ٢٠١٦، علما أن هذا يخص عدد الحالات التي قامت بعملية التبليغ فقط.

ويلاحظ أن البعض يرفض إيداع شكوى لاعتبارات اجتماعية وثقافية، وهو الأمر الذي جعل الهيئات الوطنية تتجند لحماية مستعملي الانترنت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة ٣٨٥ جريمة معلوماتية من قبل الفرق المتخصصة في مكافحة الجريمة المعلوماتية التابعة للأمن الداخلي، إلى جانب تسجيل ٥٧ قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية.

المبحث الثاني

نماذج لبعض القضايا المتعلقة بجرائم الابتزاز الالكتروني في مصر

نعرض في هذا الفصل لمجموعة نماذج خاصة من القضايا العملية المتعلقة بجرائم الابتزاز الالكتروني، والتى وقعت في مصر.

حيث يتناول المطلب الاول قضية ابتزاز الكتروني علي قاصرة، ويخصص المطلب الثاني لوقائع قضية تهديد وابتزاز وتشهير الكتروني وهى قضية شهيرة جرت وقائعها في المجتمع المصرى، وقضى فيها بحكم قضائى نهائي بواسطة القضاء المصرى، نعرض لما قضي فيها من حكم قضائي واسبابه وحيثياته ومنطوقه، وذلك على النحو التالي:

المطلب الاول

قضية ابتزاز الكتروني علي قاصرة

أولا: وقائع القضية:

حيث ورد بلاغ من **مواطن** بمحافظة الاسماعيلية بصفه ولي طبيعي علي ابنته القاصرة التي لم تتجاوز ١٢ سنة، بتضرره من قيام المتهم (....) معه علي موقع التواصل الاجتماعي (فيس بوك) من الحسابين الالكترونيين (... ، ...) علي حسابه الالكتروني المسمي (...) مرسلا اليه صورا ومقاطع فيديو اباحية للمجني عليها " **نجلته** " طالبا منه ارسال مبالغ مالية بواسطة كروت شحن شركة فودافون مصر مقابل عدم نشرها، فأذعن لأمره وارسال اليه المبالغ المالية (...)، ولطلبه مبالغ اخري اضافية، ولرفضه، ارسل مقاطع الفيديو والصور الاباحية الي اصدقائه علي مواقع التواصل الاجتماعي (فيس بوك).

الأمر الذي أدي الي تقديم بلاغه ضد صاحب الصفحة المرسل منها تلك المقاطع والصور الاباحية لنجلته.

ثانيا: التحريات عن الواقعة:

بإجراء التحريات والفحص وجمع المعلومات تبين أن بتتبع الحسابين الالكترونيين (... ، ...) تبين ان الحساب الاول يستخدم من هاتف محمول متصل بشريحة تليفون رقم (...) محل استخدام المتهم، والحساب الثاني متصل بالهاتف الارضي رقم (...) وان الهاتف الاخير مسجل باسم والد المتهم.

ثالثا : اجراءات التحقيق:

بالعرض علي النيابة العامة أمرت بالضبط والإحضار للمتهم، وتفتيش المسكن وجهاز الحاسب الخاص بالمتهم، وبضبطه ومواجهته اعترف بارتكابه للواقعة، وبالانتقال الي مسكنه تم ضبط الهاتف المحمول خاصته، وبداخله الشريحة رقم (...) وكذا ضبط الراوتر المتصل بالخط المذكور، وقيد المحضر برقم قضائي، وقدم للمحاكمة.

رابعا: نتائج التحقيق:

قضت النيابة بحبس المتهم لمدة أربعة أيام، وعرضه علي قاضي المعارضات فقرر استمرار حبس المتهم احتياطيا، حتي صدر بشأنها امر احالة الي محكمة جنايات الاسماعيلية لمعاقبة المتهم طبقا لأمر الاحالة وقائمة أدلة الثبوت المرفقين مع استمرار حبس المتهم احتياطيا علي ذمة المحاكمة الجنائية، وقد تضمن امر الاحالة المذكور الآتي :

بعد مطالعة الاوراق وما تم فيها من تحقيقات.

تتهم النيابة العامة :

السيد / ..... السن ١٩ سنة – طالب – مقيم .....

لانـه فـي يـوم ٢٠١٩/٦/٢٤ بـدائرة مركـز شـرطة ثـاني – محافظـة الاسماعيلية.

- **أولا** : هتك عرض المجني عليها الطفلة / ..... – والتي لم تبلغ من العمر ثمانية عشر سنة ميلادية – بالقوة، بأن هددها بنشر صورها علي الانترنت ان لم ترسل اليه صورا لها عارية، فاكرهها بذلك علي خلع ملابسها واظهار عورتها، وذلك علي النحو المبين بالتحقيقات.
- **ثانيا** : اعتدي علي حرمة الحياه الخاصة للمجني عليها سالفة الذكر، بان نقل بهاتفه الخلوي صور لها في مكان خاص موقع التواصل الاجتماعي (الانستجرام) علي النحو المبين بالاوراق .
- **ثالثا** : استعمل المستندات المتحصل عليها من الاتهام الثاني بان ارسلها لوالد المجني عليها / .....، وذلك علي النحو المبين بالاوراق .
- **رابعا** : هدد بافشاء المستندات المتحصل عليها بالطرق المبينة بالاتهامات السابقة، وذلك من أجل حمل المجني عليهما باداء المجني عليها الاولي عمل (ارسال صور ومقاطع فيديو اكثر عريا) والمجني عليه الثاني (ارسال مبالغ مالية) علي النحو المبين بالتحقيقات.
- **خامسا** : أنشا حسابات الكترونية علي الشبكة المعلوماتية لمواقع التواصل الاجتماعي (الفيس بوك – انستجرام) باسم (.... – .... – ....) بهدف ارتكاب جريمة معاقب عليها قانونا .
- **سادسا** : اعتدي علي القيم الاسرية بالمجتمع المصري، وانتهك حرمة الحياه الخاصة للمجني عليهما / .... ، .... ، بان نشر عبر الحسابات الالكترونية للمجني عليهما سالفي الذكر بموقعي التواصل الاجتماعي (الفيس بوك – انستجرام) صورا عارية للمجني عليها الاولي بمكان خاص وبأوضاع جنسية

مختلفة، مما ينتهك خصوصيتها وحرمة حياتها الخاصة وقيم المجتمع المصري وبدون رضاء صحيح منها.

- **سابعا** : أرسل بكثافة عدد من الرسائل الالكترونية للمجني عليهما سالفي الذكر تنتهك خصوصيتهما تتضمن الموضوع محل الاتهام السابق وذلك بدون رضائهما.
- **ثامنا** : حصل بالتهديد الواقع علي المجني عليه / ..... (والد المجني عليها الاولي) مبلغا من النقود (....) مقابل عدم نشر صور (نجلته) علي الانترنت.
- **تاسعا** : تعمد ازعاج ومضايقة المجني عليهما سالفي الذكر باساءة استعمال اجهزة الاتصالات موقع التواصل الاجتماعي (الفيس بوك – الانستجرام) علي النحو المبين بالتحقيقات .

وبناء عليه يكون المتهم قد ارتكب الجناية المؤثمة بالمواد أرقام ٢٦٨ ، ٣٠٩ مكرر ا بند (أ ، ب) ، ٤ ، ٣٠٩ مكرر (١) / ١ – ٢ – ٤ ، ٣٢٦ من قانون العقوبات والمادتين ٢٥ ، ٢٧ من القانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بمكافحة جرائم تقنية المعلومات، والمادة ٢/٧٦ من القانون رقم ١٠ لسنة ٢٠٠٣ ، والمادتين ١/٢ ، ١١٦ مكرر / ١ من القانون رقم ١٢ لسنة ١٩٩٦ بشأن قانون الطفل المعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨ .

خامسا : حكم المحكمة:

انتهت المحاكمة بصدور حكم قضائي تضمن معاقبة المتهم بالسجن المشدد لمدة ست سنوات والقضاء بالدعوى المدنية والزام المتهم بالمصاريف الجنائية واتعاب المحاماه.

المطلب الثاني

القضية الثانية وهى تهديد وابتزاز وتشهير معلوماتى

وهنا نتناول تفصيلا وقائع قضية تهديد وابتزاز وتشهير معلوماتى وهى قضية شهيرة جرت وقائعها في المجتمع المصرى، وقضى فيها بحكم قضائى نهائي بواسطة القضاء المصرى، نعرض لما ورد فيها من وقائع واحداث، وما قضي فيها من حكم قضائي واسبابه وحيثياته ومنطوقه، وذلك على النحو التالي:

- باسم الشعب
- محكمة جنايات الجيزة
- المشكلة علنا برئاسة السيد المستشار/ مصطفي أبو طالب رئيس المحكمة وبحضور السيدين المستشارين/عبد الناصر محمد ، ومجدي عبد المجيد المستشارين بمحكمة استئناف القاهرة .
- والسيدين / احمد حمزة ، ومحمد سمير وكيلا النيابة .
- والسيد / محمد عبد العزيز أمين سر المحكمة .
- أصدرت الحكم الآتي:
- في قضية النيابة العامة رقم ٦٨٥٤ سنة ٢٠٠٣ الحوامدية (رقم ٣٢٦١ سنة ٢٠٠٣ كلى).
- ضد المتهم (--) حاضر .

حضر المتهم ومعه الدفاع من المحامين والموكلين بالدفاع عن المتهم، حيث اتهمت النيابة العامة المتهم المذكور، لأنه في يوم غضون الفترة من ٢٠٠٣/١٠/١٩م إلى ٢٠٠٣/١٠/٢٢م بدائرة قسم الحوامدية محافظة الجيزة .

١- هدد المدعوة/ --- كتابة بنسبة أمور مخدشة بالشرف لها، وكان ذلك مصحوبا بطلب بأن بعث إليها برسائل عبر شبكة المعلومات العالمية (الانترنت) مهددا إياها بوضع صورتها الحقيقية على صور جنسية مخلة ونشرها عبر تلك الشبكة

طالبا منها مبالغ نقدية (خمسة آلاف دولار امريكى)، وان تباشر الجنس معه لقاء عدم قيامه بتنفيذ تهديده لها على النحو المبين بالتحقيقات.

٢- شرع في الحصول من المذكورة على مبلغ من النقود (خمسة آلاف دولار امريكى) بأن هددها بارتكاب الجريمة موضوع التهمة الأولى، وأوقف اثر جريمته لسبب لا دخل لإرادته فيه وهو إلقاء القبض عليه .

٣- قذف في حق المذكورة بان اسند إليها بواسطة الكتابة أمرا لو كان صادقا لأوجب عقابها بالعقوبات المقررة قانونا، واحتقارها عند أهل وطنها في عرضها (وهو قيامها بممارسة الجنس مع الغير بدون تمييز وبمقابل مادي) وذلك على النحو المبين بالأوراق.

وقد أحيل المتهم إلى هذه المحكمة لمحاكمته طبقا للقيد والوصف الواردين بأمر الإحالة. وبجلسة اليوم سمعت الدعوى على الوجه المبين بمحضر الجلسة المحكمة

بعد الإطلاع على الأوراق وتلاوة أمر الإحالة وسماع طلبات النيابة العامة والمرافعة الشفوية والمداولة قانونا.

بما أن الوقائع كما استقرت في يقين المحكمة، واطمأن إليه وجدانها تتحصل في أن المتهم (--) والذى يعمل طبيبا بمستشفي القصر العيني كان قد التحق بالمركز الثقافي البريطاني لتحسين دراسته ولغته الإنجليزية, وتعرف على المجني عليها المذكورة، والتي تعمل محاسبة بأحد البنوك الأجنبية في مصر من بين الدارسين بهذه الدورة المحدودة العدد، فتعارفا وتبادل كل منها مع الأخر رقم تليفونه المحمول وبريد كل منهما الالكتروني على شبكة الانترنت، حتى انقضت الدورة التعليمية المذكورة، وفي الفترة من ٢٠٠٣/١٠/١٩م وحتى ٢٠٠٣/١٠/٢٢م استغل المتهم معرفته بأرقام التليفون المحمول والبريد الالكتروني للمجني عليها وقام بإرسال رسائل مكتوبة إليها يطلب منها أن يعاشرها جنسيا وان تدفع له مبلغ خمسة آلاف دولار وإلا أقام لها موقعا باسمها على شبكة الانترنت يتضمن الاساءة إليها، ولما لم تستجب لطلبه بإقامة علاقة

جنسية معها، ولم تجد الضمان الكافي لعدم تكرار فعله إذا ما دفعت إليه مبلغ مالي، فقد أقدم على تنفيذ تهديده وأقام باسمها موقعا على شبكة الانترنت يتضمن دعوى كاذبة منسوبة إليها أنها تقدم جسدها لمن يرغب لقاء جعل مادي، واثبت رقم هاتفها المحمول كوسيلة اتصال بها على الموقع الذي أقامه لها، وبالفعل تلقت المجني عليها عدة مكالمات على هاتفها المحمول يطلب منها المتحدثون إليها إقامة علاقة جنسية معها مقررين لها أن لها موقعا على شبكة الانترنت ثبت بها اسمها ورقم تليفونها تتضمن تلك الدعوى، فقامت المجني عليها بإبلاغ الشرطة ودلت تحريات المقدم/ xxxxx الضابط بإدارة مكافحة جرائم الحاسبات بمعاونة فنية من العقيد مهندس/ xxxxxx رئيس قسم المساعدات الفنية بالإدارة ذاتها على أن هناك موقعا على شبكة الانترنت يحمل رقم xxxxxx يتضمن البيانات الشخصية للمجني عليها، وعبارات خطية تفيد رغبتها في إقامة علاقة جنسية مع من يرغب، وان مستخدم هذا الرقم ينتحل شخصية المجني عليها في مخاطبة الآخرين عبر شبكة الانترنت، وانه يستخدم حاسبا آليا مرتبط بالخط التليفوني رقم xxxxxx والمسجل بالهيئة القومية للاتصالات باسم المتهم د. xxxxxx المقيم بقرية الشيخ عثمان دائرة قسم الحوامدية محافظة الجيزة، فاستأذن اولهما النيابة العامة بضبط المتهم وتفتيش مسكنه ونفاذا لذلك الأذن فقد انتقل إلى مسكن المتهم بالعنوان سالف الذكر وقام بتفتيشه فعثر على جهاز حاسب آلي متصل بالخط التليفوني رقم xxxxxx يختص المتهم بمفرده باستعماله والذى ثبت بفحصه فنيا وجود آثار ودلائل للرقم التسجيلي لبرنامج ICQ (الاى سى كيو) تم حذفها بمعرفة المتهم، إلا انه أمكن التوصل له وهو رقم xxxxxx وهو رقم الموقع الذي اصطنعه المتهم باسم المجني عليها، كما ثبت من فحص الجهاز فنيا وجود صورة للمجني عليها مدونة باسمها، ووجود آثار ودلائل للرسائل التى أرسلت من جهاز الحاسب الآلي المضبوط لدى المتهم، من الرقم التسجيلي لبرنامج الاى سى كيو xxxxxx على التليفون

المحمول الخاص بالمجني عليها ووجود آثار للمحادثة التى تمت بين المتهم والمجني عليها على ذات البرنامج.

وبما أن الواقعة على النحو سالف البيان قد قام الدليل على صحتها، وصحة إسنادها إلى المتهم، مما شهد به كل من xxxxxx المجني عليها المذكورة والمقدم/ xxxxxx والعقيد/ xxxxxx، وما ثبت بالتقرير الفني الذي قدمه الشاهد الأخير، ومما ثبت من الإطلاع على تفريغ الرسائل الالكترونية المرسلة من المتهم إلى المجني عليها على الحاسب الآلي الخاص بها، وعلى تليفونها المحمول، وكذلك الرسائل المرسلة لها من الغير.

- وبعد الإطلاع على المواد سالفة الذكر
- حكمت المحكمة حضوريا بمعاقبة المتهم xxxxxx بالحبس مع الشغل لمدة سنة واحدة عما اسند إليه.
- صدر الحكم ، وتلي علنا بجلسة يوم الأحد الموافق ١٨/١/٢٠٠٤م.

التوصيـــات

أولاً : التوصيات المتعلقة بآليات التدخل التشريعى والسياسى:

- الإسراع في إقرار التشريعات المتعلقة بالمعاملات الإلكترونية وبيانات التعريف الشخصية الالكترونية.
- اعتبار المال المعلوماتي المعنوى على قدم المساواه في الحماية الجنائية مع الأموال المادية مع الاعتراف بإمكان إتلاف هذا المال، والتقرير له بذات عقوبة إتلاف المال المادى.
- اعتبار الوقاية عاملاً أساسياً في مواجهة جرائم الابتزاز الالكتروني، وهي تتحقّق من خلال اعتماد تدابير إحترازية مناسبة والإستمرار في مراجعتها وتطويرها.
- التأكد من أن السياسات الحكومية والتشريعات المنظمة تحقق التوازن بين الحاجة إلى جميع المعاملات وتطوير المحتوى والخدمات الرقمية في مصر وزيادة وتعزيز المحتوى العربي من جهة وتوفير الحماية وضمان أمن المعلومات وحماية البيانات الشخصية والحد من جرائم الابتزاز الالكتروني.
- تحديث دوري للقوانين لتتلاءم مع التكنولوجيات الجديدة، وعلى سبيل المثال، إن القوانين التي تنظم عمليات مزودي خدمات الإنترنت تحتاج إلى تنظيم تحديث بشكل يتناسب والتطور التكنولوجى.
- تشديد العقوبة وزيادة مدة الحبس او السجن إذا كان المعتدى عليه / عليها شخص قاصر بسبب الإعاقة أو بسبب صغر السن لعدم إتمام الثامنة عشر من العمر.
- **ثانيا: على المستوى الدولى والعربي:**

يجب أن تسعي الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة جرائم الابتزاز الالكتروني، مع تشجيع قيام إتحادات عربية تهتم بالتصدي لجرائم الابتزاز الالكتروني وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، وخاصة إنشاء شرطة عربية تهتم بمكافحة جرائم الابتزاز الالكتروني، وحتى يتحقق ذلك، يجب

أن يتم التنسيق بين دول مجلس التعاون الخليجي بشأن مكافحة جرائم الابتزاز الالكتروني.

- إنشاء قسم جديد بكليات الحقوق على مستوى كافة الجامعات العربية لدراسة اوجه الحماية القانونية للمعلوماتية أو تحت مسمى آخر قانون المعلوماتية والانترنت أو قانون الحاسب الآلي والانترنت.
- إنشاء مجموعات عمل ميدانية عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.
- تزويد البلدان النامية الموارد والتقنيات اللازمة لمعالجة جرائم الابتزاز الالكتروني ومكافحتها.
- التطوير المستمر للتعاون بين الدول، ولاسيما أنه لا يوجد إجماع بين هذه الدول بشأن تعريف جرائم الابتزاز الالكتروني وتحديدها بصورة دقيقة، ذلك إن عدم تعريف هذه الجرائم بطريقة موحدة سوف يعقد الجهود المبذولة من قبل المكلفين بتطبيق القانون لمكافحة جرائم الابتزاز الالكتروني.
- تطوير وتوطيد علاقة مصرمع جهات انفاذ القانون الخارجية، والمنظمات والمؤسسات الدولية كافة المعنية بمواجهة جرائم الابتزاز الالكتروني والإلتزام بالقوانين الدوليّة في هذا المجال
- التعاون فيما بين كافة الدول العربية، لاعتماد معيار موحّد لمكافحة جرائم الفضاء المعلوماتي لمنع المجرمين من استغلال البلدان التي لديها قوانين أقل صرامة لأنهم يميلون إلى ارتكاب جرائم الابتزاز الالكتروني في البلدان ذات القوانين الأقل تشددًا، حيث يجد المجرم أنه من الأسهل ارتكاب جرائم الابتزاز الالكتروني في هذه البلدان.
- تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة جرائم الابتزاز الالكتروني، وخاصة الإنتربول، وفي هذ المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الابتزاز الالكتروني وخاصة

المعاهدة الدولية لمكافحة جرائم الابتزاز الالكتروني والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

ثالثا : فيما يتعلق بجهات انفاذ القانون والمحققين والقضاة:

- استحداث إدارات أمنية خاصة تعنى بمكافحة جرائم الابتزاز الالكتروني، وتزويدها بالكوادر المؤهلة في الشق الأمني والتقني للاهتمام بجمع المعلومات وإجراء التحريات والتواصل مع الجهات المماثلة لها في الدول الأخرى، مع تأهيل وتدريب سلطات المكافحة تدريباً وافياً لمواكبة التغير السريع في مجالات التقنية المعاصرة، لكي تتوافر لدى هذه السلطات القدرة على المكافحة الفعالة وتتواكب بقدراتها وكفاءتها مع ما يسعى إلى تحقيقه أطراف الجريمة المنظمة.
- الاستعانة بالمختصين والخبراء القادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والمحققين مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أفضل صورة.
- إنشاء مختبر للادلة الجنائية لجرائم الابتزاز الالكتروني (Digital Forensic Lab) وهو مختبر جنائي مشترك بالتعاون مع اتحاد المصارف، بغية اجراء التحقيقات المطلوبة والحصول على الأدلة، وتحليل الفيروسات، والحد من انتشارها محليا ودوليا واجراء الأبحاث العلمية في هذا المجال، والإهتمام بمكافحة جرائم الابتزاز الالكتروني والتصدي لها، نظرا لما تشكله من تهديد لسمعة المصرف فضلا عن الخسائر التي قد تنتج عن هذه الجرائم.

رابعا : فيما يتعلق بدور الجامعات والمؤسسات التربوية المتنوعة:

- تشجيع الباحثين بالدعم المعنوي، والمادي، لإجراء المزيد من البحوث والدراسات حول جرائم الابتزاز الالكتروني المستحدثة.
- تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة جرائم الابتزاز الالكترونيوالحد من آثارها.

- تطوير التعاون التقني بين الجهتين في مجالات البحث العملي والدراسات الفنية للتحذير من المخاطر الناجمة عن جرائم الابتزاز الالكتروني التي تحدث في القطاع المصرفي وتجنب الوقوع ضحيتها.
- العمل على إدخال مادة " جرائم الابتزاز الالكتروني" في مناهج التدريس لطلبة كلية الشرطة، كمادة مستقلة عن نظم التشغيل، وذلك حتى يستطيع الدارسون التعرف على هذه الجرائم والإلمام بها وكذا تعميم دراستها لطلاب كليات الحقوق بكافة الجامعات بالجمهورية.
- حث الجامعات والمراكز البحثية العربية للبحث والدراسة في جرائم الابتزاز الالكتروني، ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة جرائم الابتزاز الالكتروني.

المراجع والمصادر

أولاً: المراجع العربية:

- القرآن الكريم.
- الحديث الشريف.

أ) المراجع والمؤلفات العامة:

- إبراهيم حامد طنطاوى، علي محمود حمودة: شرح الأحكام العامة لقانون العقوبات – الجزء الأول النظرية العامة للجريمة، دار النهضة العربية، سنة ٢٠٠٨.
- أحمد الخمليشي، شرح قانون المسطرة الجنائية، الجزء الأول، مطبعة المعارف الجديدة – الرباط، الطبعة الخامسة، سنة ١٩٩٩ .
- احمد شوقى عمر ابوخطوة، شرح الاحكام العامة لقانون العقوبات لدولة الامارات العربية المتحدة، الجزء الاول، مطابع البيان التجارية، دبى، الطبعة الاولى، سنة ١٩٨٩
- أحمد فتحى سرور: القانون الجنائي الدستورى، دار الشروق، الطبعة الثانية، سنة ٢٠٠٢.
- أحمد فتحى سرور، الوسيط في قانون العقوبات، القسم العام، الطبعة السادسة، مطبعة جامعة القاهرة، سنة ١٩٩٦
- أحمد فتحي سرور، الوسيط في قانون العقوبات، الطبعة الخامسة، دار النهضة العربية، القاهرة، سنة ١٩٨٨.

ب) المراجع والمؤلفات المتخصصة:

- أسامة أبو الحجاج – دليلك الشخصي الى الأنترنت – دار نهضة مصر – القاهرة – سنة ١٩٩٨.
- امال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري . الطبعة الثانية، دار هومة للنشر، سنة ٢٠٠٧.
- أيمن عبد الحفيظ: الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، بدون دار نشر، سنة ٢٠٠٥.

- جعفر حسن جاسم الطائي: جرائم تكنولوجيا المعلومات، دار البداية، ليبيا، ٢٠٠٧.
- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، سنة ١٩٩٨م.
- حسنين عبيد: التعاون الدولي في مكافحة الجريمة، دار النهضة العربية، الإسكندرية، سنة ٢٠٠١.
- حسنين عبيد: الجريمة الدولية – دراسة تحليلية وتطبيقية، دار النهضة العربية، الإسكندرية، سنة ١٩٨٩.
- حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، دار النهضة العربية، سنة ٢٠٠٩.
- خالد المختار واسماعيل ببكر محمد، التحقيق الجنائئ في جرائم الحاسوب – دراسة سيكولوجية – اساليبه القانونية– ادواته العلمية – دار عزة للنشر والتوزيع، السودان، سنة ٢٠١٠م.
- خالد محمد كدفور المهيري: جرائم الكمبيوتر والانترنت والتجارة الالكترونية، دار العزيز للطباعة والنشر، دبي ، سنة ٢٠٠٥.
- خالد ممدوح ابراهيم : امن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، سنة ٢٠٠٨.
- خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، سنة ٢٠٠٩.
- رامى متولي القاضي: مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، ط١، سنة ٢٠١١.

ملخص البحث

من المسلم به، ان التطور التكنولوجى لتقنية المعلومات والطفرات المتواصلة في تطوير الاجهزة والبرامج المعلوماتية وإعتماد قطاعات عديدة في المجتمع على المعلومات فى شتى المجالات، فقد إتسعت دائرة إستخدام الحاسبات الآلية فى الاونة الاخيرة بشكل متسارع، وأصبحت كافة أجهزة الدولة والمؤسسات العامة والخاصة تستخدمها فى إدارة شئونها.

لذا فقد أصبح واجباً، على كافة الجهات المختصة بالدولة، أن تحمى هذا الكيان المعلوماتى الجديد وتوفر له وسائل تأمينية تتفق وطبيعته والجانب القانوني، وفى سبيل تحقيق ذلك تقوم إدارة البحث الجنائى بمواجهة جرائم الابتزاز الالكتروني، وذلك بإستخدام تقنيات أمنية فائقة التطور للتوصل لمرتكبى هذه الجرائم .

ذلك أن عملية التوصل للجناة فى جرائم الابتزاز الالكتروني، هى عملية ذات مزيج من أعمال البحث الجنائي التقليدية من جمع تحريات وأدلة، بالاضافة إلى الجوانب الفنية المطلوبة للتوافق مع طبيعة جرائم الابتزاز الالكتروني.

وحيث تتميز جرائم الابتزاز الالكتروني، بأنها جريمة لا أثر لها بعد ارتكابها، كما يصعب الاحتفاظ الفنى بآثارها إن وجدت.

كما انها تحتاج لخبرة فنية ويصعب على المحقق التقليدي التعامل معها، ويسهل نظرياً ارتكاب هذا النوع من الجريمة كما يسهل إخفاء معالم الجريمة، ويصعب تتبع مرتكبيها ويلعب البعد الزمنى من اختلاف المواقيت بين الدول، والبعد المكانى وهو إمكانية تنفيذ الجريمة عن بعد، فضلا عن البعد القانوني وهى تلك الاشكاليات القانونية فى شأن القانون المطبق على الواقعة، فجميع تلك الابعاد تلعب دوراً هاماً فى تشتيت جهود التحرى والتنسيق الدولى لتعقب هذه الجرائم.

ولما كانت هذه الجرائم غامضة يصعب إثباتها والتحقيق فيها، كان لازما التعرض للقواعد الموضوعية والاجرائية لجرائم الابتزاز الالكتروني، محاولة منا للحد لم يكن للقضاء علي جرائم الابتزاز الالكتروني .

It is renowned that the technological development of information technology and the continuous booms in the development of information devices and programs and the reliance of many sectors in society on information in various fields, the use of computers has recently expanded rapidly, and all state agencies and public and private institutions use them in managing their affairs .

Therefore, it has become a duty, for all the competent authorities in the state, to protect this new information entity and provide it with insurance means consistent with its nature and the legal aspect.

This is because the process of reaching the perpetrators of electronic extortion crimes is a process with a mixture of traditional criminal investigations from collecting investigations and evidence, in addition to the technical aspects required to comply with the nature of electronic extortion crimes.

And where the crimes of electronic blackmail are characterized as a crime that has no effect after its commission, and it is difficult to keep the technical traces, if any.

It also requires technical expertise, and it is difficult for a traditional investigator to deal with it, and it is theoretically easy to commit this type of crime, as it is easy to hide the features of the crime, and it is difficult to track its perpetrators. These are the legal problems regarding the law applicable to the incident. All of these dimensions play an important role in dispersing international investigation and coordination efforts to track down these crimes.

Since these crimes are vague and difficult to prove and investigate, it was necessary to expose the objective and procedural rules of the crimes of electronic extortion, an attempt by us to limit was not to eliminate the crimes of electronic extortion.