الأدلة الجنائية في جرائم الابتزاز الالكتروني

دراسة تطبيقية مقارنة

الدكتور

محمـــود رجـــب فتـــح الله
دكتوراه القانون الجنائي
كلية الحقوق جامعة الاسكندرية

قال تعالى :

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

صدق الله العظيم

مقدمة:

من المسلم بـه، ان التطـور التكنولـوجى لتقنيـة المعلومـات والطفرات المتواصـلة فـي تطـوير الاجهـزة والبـرامج المعلوماتيـة وإعتمـاد قطاعـات عديـدة فـي المجتمـع علـى المعلومـات فـى شـتى

(*) القرآن الكريم – سورة الممتحنة، الآية 12 .

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 .

د. محمود رجب فتح الله

مقدمة البحث :

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 .

حيث بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلومات، حيث أصبحت المعلومة أهم ممتلكات الإنسان، اهتم بها، على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتقلت إلى ورق البردي، وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الأقراص الإلكترونية الممغنطة.

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

وبعد ان كانت الحياة الخاصة للإنسان تواجه الاعتداء باستراق السمع أو الصور الفوتوغرافية، صارت هذه الخصوصية تنتهك بواسطة اختراق البريد الالكتروني والحواسب الشخصية، وقواعد البيانات الخاصة بالتأمين الصحي والمستشفيات ومؤسسات الائتمان والتأمين الاجتماعي، وصولا الي ارتكاب جرائم الابتزاز الالكتروني.

ذلك ان الفضاء المعلوماتي المتعولم وضع اكثر من 200 دول في حالة اتصال دائم واصبحت شبكة الانترنت اليوم تشهد تعايشاً مستمرا في جميع المجالات العلمية والبحثية والاقتصادية، بل والسياسية والاجتماعية على السواء، وهو ما يقود الى ضرورة التعرض الى تحديات

جرائم الابتزاز الالكتروني، في ظل الاتجاه التشريعي المصرى الحديث في مواجهة هذه الجرائم من جهة، من جهة وتحديات تلك الجرائم العابرة للحدود الاقليمية من جهة اخرى.

حيث ان نتاج التطور في الجانبين من أدوات واختراعات وخدمات جديدة ظهرت في مختلف المجالات، ولقد نتج عن الثورة التكنولوجية تلك، ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التى نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

ثانياً: أهمية الدراسة:

تكمن أهمية دراسة هذا الموضوع لما يكتسبه من جدية وغموض، أمام انتشار ظاهرة جرائم الابتزاز الالكتروني، 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، رغم أن ملفات المتابعة القضائية لها تعد شبه معدومة، مما تطلب سن نصوص تشريعية لمكافحة هذه الجريمة وهو الحاصل في الآونة الاخيرة، والتي خرقت كل المبادئ والأسس القانونية، كما تكمن أهميته في اتساع مجاله وكلما تناولنا فكرة منه، بقي الكثير منه يحتاج لتوضيح لأنه موضوع جديد من جهة ويحتاج لإيجاد إجراءات جديدة لمتابعته من جهة أخرى.

ثانيا : 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 للقضاء عليها أو علي الأقل الحد منها، ومن ثم، كشف مواطن الخلل واقتراح سبل معالجتها.

حيث يقصد بالمعاملات الإلكترونية كل المعاملات التى تتم عبر تجهيزات إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً عن طريق الهاتف المحمول، وتتكون تلك المعاملات من عدد من المكونات الأساسية، وما يهمنا هنا طرح مكون أساسي فيها وهو الجزء الخاص بجرائم تلك المعاملات، أو بمعني أدق القواعد القانونية التي تحكم الأفعال التى تتم من خلال أجهزة الحواسب، أو عبر شبكة الانترنت، متي كان الغرض منها ابتزاز الآخرين.

حيث تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، وتعتبر ثورة الاتصالات هي المحرك الأساسي في التطورات الحادثة في الوقت الحالي.

رابعا : أهداف الدراسة :

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

حيث يقصد بالمعاملات الإلكترونية كل المعاملات التى تتم عبر تجهيزات إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً عن طريق الهاتف المحمول، وتتكون تلك المعاملات من عدد من المكونات الأساسية، وما يهمنا هنا طرح مكون أساسي فيها وهو الجزء الخاص بجرائم تلك المعاملات، أو بمعني أدق القواعد القانونية التي تحكم الأفعال التى تتم من خلال أجهزة الحواسب، أو عبر شبكة الانترنت، متي كان الغرض منها ابتزاز الآخرين.

حيث تعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، وتعتبر ثورة الاتصالات هي المحرك الأساسي في التطورات الحادثة في الوقت الحالي.

خامسا : منهج الدراسة:

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

سادسا : خطة الدراسة:

لمعالجة إشكالية البحث قمت بتقسيم الخطة إلي فصول خمس، نتطرف في الفصل الاول لماهية جرائم الابتزاز الالكتروني، علي ان يعرض الفصل الثاني لبيان انواع ومخاطر جرائم الابتزاز الالكتروني وصورها، بينما يخصص الفصل الثالث لعرض الطبيعة القانونية لجرائم الابتزاز الالكتروني، علي ان يتناول الفصل الرابع الأدلة الجنائية في جرائم الابتزاز الالكتروني، وأخيرا يختتم هذا المؤلف بالفصل الخامس والاخير، لعرض تطبيقات عملية لجرائم الابتزاز الالكتروني، وترتيبا على ذلك تكون معالجة هذا المؤلف وفقا للتالي:

تمهيد وتقسيم:

الفصل الاول: مفهوم جرائم الابتزاز الالكتروني.

- **المبحث الاول : تعريف جرائم الابتزاز الالكتروني وموضوعها.**
- **المطلب الأول : التعريف اللغوي والاصطلاحي لجرائم الابتزاز الالكتروني.**
- **الفرع الأول : المفهوم القانوني للمعلومات في جرائم الابتزاز الالكتروني.**

- الفرع الثاني : التعريف المقترح لجرائم الابتزاز الالكتروني.
  - المطلب الثاني : التعريف القانوني لجرائم الابتزاز الالكتروني.
- المبحث الثاني: اسباب جرائم الابتزاز الالكتروني وخصائصها.
  - المطلب الأول: أسباب جرائم الابتزاز الالكتروني.
  - المطلب الثاني: خصائص جرائم الابتزاز الالكتروني.
- الفرع الأول : سمات جرائم الابتزاز الالكتروني.
- الفرع الثاني : خصوصية مجرمي الابتزاز الالكتروني.

الفصل الثاني: انواع ومخاطر جرائم الابتزاز الالكتروني وصورها.

- المبحث الأول: أنواع جرائم الابتزاز الالكتروني.
- المبحث الثاني: مخاطر جرائم الابتزاز الالكتروني.
  - المطلب الاول: المخاطر الاجتماعية لجرائم الابتزاز الالكتروني.
  - المطلب الثاني: المخاطر الإقتصادية لجرائم الابتزاز الالكتروني.
  - المطلب الثالث: المخاطر الأمنية لجرائم الابتزاز الالكتروني.
- المبحث الثالث: صور جرائم الابتزاز الالكتروني.
- المبحث الرابع: واقع جرائم الابتزاز الالكتروني على المستوى الدولي والعربي.
  - المطلب الاول: واقع جرائم الابتزاز الالكتروني على المستوى الدولي.
  - المطلب الثاني: واقع جرائم الابتزاز الالكتروني في الوطن العربي.

الفصل الثالث: الطبيعة القانونية لجرائم الابتزاز الالكتروني.

- المبحث الأول: الطبيعة القانونية الخاصة لجرائم الابتزاز الالكتروني.
- المبحث الثاني: الشرعية الجنائية لجرائم الابتزاز الالكتروني.
  - المطلب الأولً: مبررات مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني.
  - المطلب الثانيً: نتائج مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني.
  - المطلب الثالث: الوضع التشريعي لجرائم الابتزاز الالكتروني في مصر.
- المبحث الثالث: دور القاضي الجنائي في ظل غياب النص العقابي لجرائم الابتزاز الالكتروني.
  - المطلب الأول: دور القاضي في مواجهة النقص التشريعي لمواجهة جرائم الابتزاز الالكتروني في التشريعات المقارنة.

- المطلب الثاني: التفسير القضائي للنص الجنائي التقليدي لتطبيقه علي جرائم الابتزاز الالكتروني.
- المطلب الثالث: التفسير القضائي للنص الجنائي بشأن جرائم الابتزاز الالكتروني.

- المبحث الرابع: تنازع الاختصاص بشأن جرائم الابتزاز الالكتروني.
- المطلب الأول: السمات الخاصة لجرائم الابتزاز الالكتروني.
- المطلب الثاني: نطاق جرائم الابتزاز الالكتروني.
- المطلب الثالث: قواعد الاختصاص في جرائم الابتزاز الالكتروني.
- المطلب الرابع: التحديات التي تواجه الجوانب الإجرائية في جرائم الابتزاز الالكتروني.

الفصل الرابع: الأدلة الجنائية 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 : الضخامة البالغة لكم البيانات المتعين فحصها.

- المبحث الثاني: طرق اثبات جرائم الابتزاز الالكتروني.
- المطلب الاول: وسائل إثبات جرائم الابتزاز الالكتروني.
- الفرع الاول : البريد الالكتروني.
- الفرع الثاني : التوقيع الالكترونى.
- الفرع الثالث : العقد الالكترونى.
- المطلب الثاني: الأدلة المعلوماتية في الدعوى الجنائية .

الفصل الخامس : تطبيقات عملية لجرائم الابتزاز الالكتروني

- الفصل الاول: حالات عملية لجرائم الابتزاز الالكتروني على المستوى على الدولى.
- الفصل الثاني: حالات عملية لجرائم الابتزاز الالكتروني على الصعيد العربي.

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

خاتمة البحث.

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

- **المبحث الاول:** تعريف جرائم الابتزاز الالكتروني وموضوعها.
- **المبحث الثاني:** اسباب جرائم الابتزاز الالكتروني وخصائصها.

1(راجع في ذلك: د.عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة 1988، الدار الجامعية، بيروت، ص 259 .

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.

المطلب الثاني : التعريف القانوني لجرائم الابتزاز الالكتروني.

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 الاضرار 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 1999 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 82-652 الصادر في 26 يوليو لسنة 1982، يعرف المعلومة على أنها صورة أو مستندات أو معطيات أو خطابات أيا كانت طبيعتها.

أما قانون البحرين رقم 83 لسنة 2002 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 2 لسنة 2002، 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، فتنقسم 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[2].

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 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.

) يعتبر مصطلح " البورصة "من المسميات التي تطلق على سوق الأوراق المالية ويعود هذا المصطلح إلى القرن 2(الخامس عشر الميلادي، حيث كان التجار القادمين من فلورنسا يجتمعون في فندق تملكه عائلة تسمى Van der ، يقع في مدينة بروج البلجيكية، والذي كان يؤمه التجار من كافة المناطق، وتطور التعامل فيه للدرجة bourse 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 1999، ص 23، 24، هامش رقم (1).

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 175 لسنة 2018 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 32 عقوبات، وذلك متي توافر الارتباط الذي لا يقبل التجزئة.

فنجد المادة 327 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 500 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 6 أشهر أو بغرامة لا تزيد على 200 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"[3].

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

) محكمة النقض المصرية : الطعن رقم 176 لسنة 26 مكتب فنى 7 صفحة رقم 758 بتاريخ 21-5-1956، اذ 3(قضي بأن " المقصود بالتهديد بإفشاء أمور أو نسبة أمور مخدشة بالشرف والمنصوص عليها بالفقرة الأولى من المادة 327 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 302 من قانون العقوبات، والتهديد فى هذا المعنى يشمل التبليغ عن جريمة سواء أكانت صحيحة وقعت بالفعل أو كانت مختلفة."، وكذا الطعن رقم 1425 لسنة 2 مجموعة عمر 2ع صفحة رقم 466 بتاريخ 22-2-1932، 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 1425 لسنة 2 مجموعة عمر 2ع صفحة رقم 466 بتاريخ 22-2-1932، 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."

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 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. [4]

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 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.

---

4) محكمة النقض المصرية : الطعن رقم الطعن رقم 2167 لسنة 46 مجموعة عمر 1ع صفحة رقم 357 بتاريخ 31-10-1929، اذ قضي بأن " لم تبين المادة 284 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 284 عقوبات ولو كان المهدد لا يقصد إلا الحصول على حقوق له عند من هدده.".

المطلب الثاني

التعريف القانوني لجرائم الابتزاز الالكتروني

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.

وعلي ذلك، الابتزاز الإلكتروني، هو الابتزاز الذي يتم باستخدام 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.

وترتيبا على ذلك، يلزم التعرض لأسباب جرائم الابتزاز الالكتروني في مطلب اول، على ان نتبع ذلك ببيان الخصائص المميزة لتلك الجرائم في المطلب الثاني، على الترتيب التالي:

- **المطلب الأول:** أسباب جرائم الابتزاز الالكتروني.
- **المطلب الثاني:** خصائص جرائم الابتزاز الالكتروني.

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.[5]

) وتتنوع الجرائم المعلوماتية على النحو التالي:5(

- إساءة استخدام الإنترنت.

حيث نتج عن ثورة الاتصالات وتكنولوجيا المعلومات العديد من التطبيقات، التي من شأنها التأثير بدرجة كبيرة على أوجه النشاط الاقتصادي[6] 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[7] 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 الحيوية والحاسب وهندسة الاتصالات

- 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

6) راجع في ذلك: د. عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة 1988، الدار الجامعية، بيروت، ص. 259 .

7) انظر: د. عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، المرجع السابق، ص. 264 .

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:

1- 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.

2- 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.

3- 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.

4- 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 24 ساعة.

5- اللا مادية وتضاؤل قيمة المكونات المادية:

حيث تتضاءلت قيم المكونات المادية في المنتجات الجديدة بصورة كبيرة، فبعد أن كانت هذه المكونات تصل إلى 30% من قيمة المنتج، فإنها قد وصلت إلى حوالي 10% ويُنتظر أن تصل إلى أقل من 2% 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) [8].

---

8) 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 1980، 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،

وأسباب جرائم الابتزاز الالكتروني، منها

1- ضعف الوازع الديني .

2- الفراغ الروحي أو العاطفي أو الوقتي 0

3- أصدقاء السوء 0

4- الاختلاط 0

5- ضعف الرقابة الأسرية وتقصيرها في توجيه الأبناء وعدم مراقبتهم والجهل ببعض الأمور والحرمان من المحبة والتودد والتعامل الحسن 0

6- التقنيات الحديثة مثل الإنترنت وبعض القنوات الفضائية والإعلام غير السوي، والبلاك بيري والجوال والهاتف وغيرها إذا ما أسيئ استخدامها 0

7- حب التجربة والتقليد من الجنسين مما يوقعه بشباك الابتزاز 0

8- روايات الحب والغرام 0

9- الحرية المطلقة المفتوحة بدون رقيب أو عتيد للجنسين 0

10- تأخر الزواج والمغالاة بالمهور 0

11- ضعف الشخصية لدى المجني عليه ، فيستغل الجاني هذا الضعف ويمارس عليه الضغط 0

12- ضعف العقوبة لمرتكبي جرائم الابتزاز 0

حيث يتم التصيّد والقيام بالابتزاز للأفراد، من خلال البريد الإلكتروني أو من خلال مواقع التواصل الاجتماعي كالفيس بوك أو التوتير أو الواتس اب، أو من خلال برامج التك توك وغيرها، فانتشار وكثرة ممارسة الابتزاز يكون مرتبط بلا شك بعدد مستخدمي وسائل ومواقع التواصل الاجتماعي.

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.

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:

1- 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.

2- 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 1% فقط، والذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى 15 % من النسبة السابقة.

3- ان أدلة الإدانة في جرائم الابتزاز الالكتروني، غير كافية إلا في حدود 20% 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.

4- 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.

5- 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.

6- **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.

7- **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.

8- **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 .

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:

1. **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.
2. **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.
3. **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(9)، 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 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(10).

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.

) راجع في ذلك: د. خالد سعد زغلول حلمى – مثلث قيادة الاقتصاد العالمى – دراسة قانونية اقتصادية– الكويت 9(– جامعة الكويت – سنة 2002 – صـ 3 ، 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.

(10) 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 1997، ص 220 – 221، وايضا : عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– الناشر : جامعة نايف العربية للعلوم الأمنية – 2008 م – صـ 46 وما بعدها، وايضا : محمد فتحى عيد، مرجع سابق، سنة 1990، ص 131.

4. **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[11] أو اعتراض العمليات المالية وتحويلا مسارها أو استخدام أرقام البطاقات بابتزاز اموالها.
5. **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 1989 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.

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

وفي الثالث من فبراير من عام 1990 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:

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

2- **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.

6. **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.
7. **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 للقضايا هو المتعارف عليه بالدولة المصرية[12].

8. **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.
9. **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 أن تتعاون الدول المتطورة وخاصة

---

12) انظر في ذلك: سلوى شعراوى جمعة، الدولة وتحديث الجهاز الادارى، رؤية للاصلاح، مركز دراسات واستشارات الادارة العامة، جامعة القاهرة، سنة 2004، صـ 3 – 8، وايضا : مونت بالمر، البيروقراطية المصرية، ترجمة : على ليلة، مركز الدراسات السياسية والاستراتيجية بالاهرام، القاهرة، سنة 1994، صـ 95 –96.

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

10. 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.
11. 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.
12. صعوبة المباحثة بالتعويض المدني بخصوص جرائم الابتزاز الالكتروني لكل تلك الاسباب المسبقة.

الفرع الثاني

خصوصية مجرمي الابتزاز الالكتروني

من المقرر ان 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 (25– 45) عاما، ويتميز هؤلاء بسمات عامة، يمكن النظر إليها من زاويتين:

1– 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.

2– 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.

1 – 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 عرضا لبعض 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.

2 – 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.

- 3 - 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[13][14].

) راجع في ذلك، د. هدى حامد قشقوش، "الجريمة المنظمة (القواعد الموضوعية والاجرائية والتعاون الدولي)، 13(الطبعة الثانية، الاسكندرية، منشأة المعارف، سنة 2006، ص 18، وايضا : محمد ابراهيم زيد، "الجريمة المنظمة

ويتمتع هؤلاء الجناة بصفات سيكولوجية أخرى غير متوفرة في الجناة العاديين، نذكر منها:

- أعمارهم تتراوح عادة بين 18 إلى 46 سنة والمتوسط العمري لهم 25 عاما.
- المعرفة والقدرة الفنية الهائلة.
- الحرص الشديد وخشية الضبط وافتضاح الأمر.
- ارتفاع مستوى الذكاء ومحاولة التخفي.

(تعريفها وانماطها وجوانبها التشريعية)"، ابحاث حلقة علمية حول الجريمة المنظمة واساليب مكافحتها، الرياض، اكاديمية نايف للعلوم الامنية، سنة 1999، ص 33

) انظر في ذلك: سناء خليل، الجريمة المنظمة عبر الوطنية والجهود الدولية والمشكلات القضائية، المجلة 14(الجنائية القومية، المجلد التاسع والثلاثون، العدد الثانى، يوليو 1996 ، ص 103، انظر : عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– مرجع سابق – ص 46 وما بعدها، وايضا : محمد فتحى عيد، السنوات الحرجة في تاريخ المخدرات، مرجع سابق، ص 131، وايضا : تقرير الهيئة الدولية لمراقبة المخدرات لسنة 2000 ، الغصون (50 – 56) ، ص 12 ، 13، مطبوعات الامم المتحدة، نيويورك، 2001، الوثيقة المنشور بتاريخ 21 فبراير 2001 ، وكذلك انظر: مجلة الحقوق الكويتية، مجلس النشر العلمى، Elincb 200Dرقم الكويت، 1998، العدد الثالث، ص 381 ، منشور دورة البحث الجنائى للضباط رقم (5) دراسات حول الجريمة الاقتصادية في دولة الامارات، معهد البحث الجنائى، شرطة دبى، دولة الامارات العربية المتحدة، سنة 1998، ص 98.

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).

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:

1. دفع مبالغ مادية.
2. القيام باعمال غير مشروعة.
3. القيام باعمال منافية للاخلاق.
4. الافصاح عن معلومات سرية مؤسسية او سياسية.
5. العمل مع العدو.

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.

- **المبحث الثاني:** مخاطر جرائم الابتزاز الالكتروني.
- **المبحث الثالث:** صور جرائم الابتزاز الالكتروني.
- **المبحث الرابع:** واقع جرائم الابتزاز الالكتروني على المستوى الدولي والعربي.

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:

1- 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.

2- جرائم استغلال الأطفال في المواد الإباحية:

والمقصود من هذا المصطلح هو ظهور الأطفال والقصر الذين تقل أعمارهم عن 18 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

تهمـة الاتجـار أو تـداول صـور أو أفـلام إباحيـة للأطفـال، وكـذلك المنظمـات الدوليـة بشـدة مثـل اليونسيف والشرطة الدولية "الإنتربول"[15].

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

3- جرائم المطاردة الالكترونية:

ويقصـد بهـا اسـتخدام الإنترنـت لتعقـب أو مطـاردة أي فـرد لغـرض الإحـراج العـام، 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.

4- 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 ببرنـامج أخر يسمى الحاضـن، ولا يمكن أن تنشأ الفيروسات من ذاتها ولكن يمكنها أن تنتقل من حاسب مصاب لآخر سليم.

وأهـم طـرق الانتقـال الآن هـي الشـبكة العنكبوتيـة (الإنترنـت) لكونهـا وسـيلة سـهلة لانتقـال 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.

5- برامج القرصنة:

ويقصـد بالقرصـنة هنـا الاسـتخدام أو/ و النسـخ غيـر المشـروع لـنظم التشـغيل أو/ ولبـرامج الحاسب الآلي المختلفة، وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت

---

15) انظر في ذلك: عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 2008/03/07، المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:3.

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.

6- 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[16].

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.

---

16) راجع في ذلك: على عدنان الفيل، المسؤولية الجزائية عن اساءة استخدام بطاقة الائتمان الالكترونية، الطبعة الاولى، المؤسسة الحديثة للكتاب، لبنان، سنة 2011، ص 17

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.

ففي العالم الافتراضي 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 الاول:** المخاطر الاجتماعية لجرائم الابتزاز الالكتروني.
- **المطلب الثاني:** المخاطر الإقتصادية لجرائم الابتزاز الالكتروني.
- **المطلب الثالث:** المخاطر الأمنية لجرائم الابتزاز الالكتروني.

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[17].

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 18 في المائة من مجمل قضايا الإجرام المعلوماتي، بينما سجلت قضايا ابتزاز الأطفال جنسيا ما نسبته 14 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 27 في المائة، فيما سجلت قضايا استغلال الأطفال جنسيا ما نسبته 14 في المائة، بينما وصلت قضايا السب والتشهير وإساءة السمعة ما نسبته 13 في المائة، في حين سجلت قضايا الاختراقات المالية 12 في المائة، بينما وصلت نسبة الاختراق المعلوماتي بواسطة برامج خبيثة ما قدره 6 في المائة، فيما بلغت نسبة الخداع والاحتيال إلكترونيا 5 في المائة، كما وصلت نسبة التهديدات الإرهابية عبر المواقع 4 في المائة، بينما لم تتجاوز شكاوى الاتصالات المشبوهة ما نسبته 1 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.

---

17) راجع في ذلك: عبد الفتاح الجبالى، الاقتصاد المصرى من التثبيت الى النمو، مركز الدراسات السياسية والاستراتيجية بالاهرام ، القاهرة، سنة 2000، ص 20.

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. [18]

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[19].

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؟
- سرقة بطاقة الائتمان الخاصة به لابتزازه .[20]
- الابتزاز بالتهديد المباشر.
- عمليات الاحتيال بغرض الابتزاز.

---

18) مشار اليه في، د. خالد سعد زغلول حلمى – مرجع سابق – مطبعة الفجر الكويتية – الكويت – سنة 2001 –صـ 439 وما بعدها، وكذلك: د. خالد سعد زغلول حلمى – مرجع سابق – جامعة الكويت – سنة 2002 – صـ 3، وايضا: د. سوزى عدلى ناشد، مرجع سابق، دار المطبوعات الجامعية – طبعة 2011 – ص 78 وما بعدها.

19) راجف في ذلك: د.عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة 1988، الدار الجامعية، بيروت، ص. 259 .

20) راجع في ذلك: على عدنان الفيل، المسؤولية الجزائية عن اساءة استخدام بطاقة الائتمان الالكترونية، الطبعة الاولى، المؤسسة الحديثة للكتاب، لبنان، سنة 2011، ص 17

- الابتزاز عن طريق تحويل أو نقل حسابه المصرفي.
- الابتزاز بطريق نقل ملكية الأسهم[21] .
- ابتزاز زيادة الفواتير بطريق تحويل فواتير المجرم للضحية.

ثانيا: على مستوى معظم المنظمات والبنوك والشركات الربحية وغير الربحية والمؤسسات والجهات الحكومية وغير الحكومية[22]:

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: [23]

) السهم ما هو إلا شهادة تخول مالكها الحق في ملكية جزء من ممتلكات الشركة التي أصدرت هذا السهم، وهو 21(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 10 وما بعدها. هذا وتنص المادة (17) من قانون إنشاء سوق أبو ظبي للأوراق المالية على أن " يتم قبول وإدراج الأوراق المالية التالية للتداول في السوق : 1. أسهم وسندات والأذونات المالية التي تصدرها الشركات المساهمة العامة. 2 . الأسهم والسندات والأذونات المالية التي تصدرها الشركات المؤسسة خارج الإمارة والتي يقبل المجلس تداولها. 3 . الأسهم والسندات والأذونات المالية التي تصدرها الشركات والمؤسسات خارج الدولة والتي يقبل المجلس تداولها . 4 . سندات الدين التي يقبل المجلس تداولها . 5 . وحدات الصناديق الاستثمارية. 6 . السندات والأذونات الصادرة عن الحكومة المحلية أو الهيئات والمؤسسات العامة. 7 . أية أوراق أو أدوات مالية يقبل المجلس تداولها".

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

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

- 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: [24]

- 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: [25]

- 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.

---

24) راجع في ذلك: مركز التميز لأمن المعلومات، تصنيف الجرائم المعلوماتية تبعا لاستخدام الحاسب فيها http://coeia.edu.sa/index.

25) راجع في ذلك: http://ar.shvoong.com/humanities/1746290 .

- 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 550 مليون و735 مليون دولار أميركي سنويا. [26]

- كما أكد الخبراء أن معدل نسبة جرائم الابتزاز الالكتروني في العالم يصل إلى 57.6% حيث يكلف الاقتصاد العالمي ما يقارب (12.950) مليار دولار سنوياً، وإن نسبة معدل الهجمات الالكترونية في السعودية على سبيل المثال يقارب 45.8% لعام 2009، كما كانت نسبة الهجمات للحسابات البنكية للأفراد عام 2009، بلغت 40%، واختراق المواقع الالكترونية لعام 2009 بلغ 63%، ورسائل الاحتيال فيها لعام 2009م بلغت 43.7%.[27]
- كما كشفت السلطات الأمريكية عام 2009 أن عمليات قرصنة وسرقة طالت أكثر من 130 مليون بطاقة ائتمان وبطاقة سحب مصرفية.
- وأظهر تقرير نشرته "سيمانتك كوربوريشن" تزايداً مضطرداً في هجمات جرائم الابتزاز الالكتروني، حيث رصد 100 تهديد إلكتروني في الثانية خلال العام 2009.[28]
- 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 28 يوم كما تكلف في المتوسط 334 دولار.[29]

---

26) راجع في ذلك: مجلة المعلوماتية– الجريمة الالكترونية
http://infomag.news.sy/index.php?inc=issues/showarticle&issuenb=29&id=590 .

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

28) 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

29) 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 700 ألف انهيار نظام خلال تسعة شهور.[30]

وهذه الأرقام تشير لمدى تفشي جرائم الابتزاز الالكتروني وتهديدها الحقيقي والسلبي على الاقتصاد، والسبب في ذلك يعود إلى: [31]

- 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. [32]

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.[33]

المطلب الثالث

وايضا انظر: البوابة العربية للأخبار التقنية –الجرائم المعلوماتية تكبد دول الخليج خسائر تصل إلى 2.7 مليار درهم سنوياً

http://www.aitnews.com

30( ) انظر في ذلك: منتدى الإمارات الاقتصادي – غياب إدارات لمكافحة الجرائم المعلوماتية في 5 إمارات

http://www.uaeec.com

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

http://www.ulum.nl

32( ) انظر في ذلك: موقع المسائية الإخباري– حيث ان الجريمة الإلكترونية تكلف العالم 500 مليار جنيه خلال 2009

http://www.msaeya.com

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

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

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.
- 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.[34]

) راجع في ذلك: سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 34(سنة 2007، ص 83.

جـ – **الجـرائم الماسـة بـالأمن الفكـري:** اذ يبقـى الأمـن الفكـري مـن بـين أخطـر جـرائم الابتـزاز 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. [35]

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:

1) جرائم الإضرار بالبيانات:

يعتبر هذا الصنف من جرائم الابتزاز الالكتروني من أشدها خطورة وتأثيرا وأكثرها حدوثا وتحقيقاً 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

) انظر في ذلك: علي عدنان الفيل، الاجرام الالكترونى – دراسة مقارنة، منشورات زين الحقوقية، سنة 2011، 35(ص 123.

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.

أما بالنسبة إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات، فان تلك الأنشطة تتم بواسطة أفراد هواه أو محترفون يطلق عليهم المخترقون ذوى القبعات السوداء (Black Hat Hackers) الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات والمعلومات التي يقومون بالاستيلاء عليها أو بغرض الإضرار بالجهة صاحبة تلك الأنظمة لوجود كراهية شخصية أو قبلية أو سياسية أو دينية أو القيام بذلك لحساب احد المؤسسات المنافسة.

وخير مثال على ذلك، ما أعلنه مكتب التحقيقات الفيدرالية الأمريكي (FBI) في السادس والعشرون من سبتمبر عام 2002 من القبض على احد عملائها ويدعى ماريو كاستللو 36 عاما ومحاكمته بتهمة تخطى الحاجز الأمني المسموح له به والدخول على احد أجهزة المكتب ستة مرات بغرض الحصول على بعض الأموال بطريق الابتزاز.

فقد ورد بالتقرير السنوي الثامن لمكتب التحقيقات الفيدرالية الأميركي الصادر عام 2003 بعنوان جرائم الحاسب، أن أكثر خسائر المؤسسات بالولايات المتحدة الأمريكية تأتى من الاستيلاء على المعلومات، والتي تكبدتها خلال هذا العام خسائر تتجاوز السبعون مليون دولار أمريكي، ويأتي

في المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز الخمسة وستين ونصف مليون دولار هذا العام.

وقد يبلغ الامر الى تعطيل العمل والذي يطلق عليه الـ (Denial Of Service Attack) واختصاراً الـ (Dos) والذي يعتمد على إغراق أجهزة الخوادم بالاف أو ملايين طلبات الحصول على معلومات، الأمر الذي لا تحتمله قدرة المكونات المادية (Hardware) أو نظم قواعد البيانات والتطبيقات والبرامج الموجودة على تلك الخوادم، فتصاب بالشلل التام لعدم قدرتها على تلبية هذا الكم الهائل من الطلبات والتعامل معها، ويحتاج الأمر إلى آلاف الساعات الزمنية حتى يتمكن مديري النظم والشبكات من التعرف على مصادر الهجوم وعيوب النظم لديهم واستعادة العمل بصورة طبيعية، وبالطبع فان هذه الساعات التى يكون فيها نظام المعلومات متعطلاً، من شأنها ان تكبد المؤسسة الخسائر المادية الجسيمة، فضلا عن تعطيل مصالح المتعاملين مع تلك الأنظمة وفقدانهم الثقة في تلك المؤسسة وهروب العملاء منها إلى مؤسسات منافسة كلما أمكن ذلك.

ومما هو جدير بالذكر أن ثاني أكثر مواقع الانترنت شعبية وعدد زائرين هو الـ (Yahoo) الذى تعرض لهجوم من ذلك النوع في فبراير من عام 2000، الأمر الذي أدى لانقطاع خدمة الاتصال بالموقع لمدة تجاوزت الثلاث ساعات حتى استطاع المهندسون بالشركة من تحديد المناطق التى بدء منها الهجوم وتعاملوا معها بوضع فلاتر على جهاز الاتصال (Router) الموجود بالشركة لحجب تلك المناطق عن الاتصال بالخوادم الموجودة بالشركة وتعطيلها عن العمل.

كما ذكر أيضا تقرير لمكتب التحقيقات الفيدرالية الامريكية، التزايد السنوي للخسائر المادية للشركات الأمريكية من جرائم الابتزاز الالكتروني في الأعوام من 2000 إلى 2003 الذي اظهر جنوح اغلب الجرائم إلى الانخفاض في حجم الخسائر السنوية، ماعدا جريمة تعطيل العمل للأنظمة والذي تضاعف حجم الخسائر المادية الناجمة منها من حوالي 18 مليون دولار عام 2002 إلى ما يقارب ال 65 مليون دولار عام 2003.

2) 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 2001[36]، وتكرر الاختراق سنة 2017، 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.[37]

ومن صور الاعتداء الأخرى التى تمثل اعتداء على الملكية الفكرية للأسماء ما يحدث من اعتداءات على أسماء مواقع الانترنت (Domain Names) حيث أن القاعدة العالمية في تسجيل أسماء النطاقات، والتي تتم أيضا باستخدام بطاقات الائتمان من خلال شبكة الانترنت، هى أن التسجيل بالأسبقية وليس بالأحقية (First Come First Served)، الأمر الذي أحدث الكثير من المخالفات التى يتم تصعيدها إلى القضاء، وبتدخل من منظمة الايكان التى تقوم بتخصيص عناوين وأسماء المواقع على شبكة الانترنت (ICANN) (Internet Corporation for Assigned Names and Numbers) وذلك من اجل التنازل عن النطاق للجهة صاحبة الحق مع توقيع العقوبة أو الغرامة المناسبة .

كما يحدث أيضا في تسجيل النطاقات عبر الانترنت، والتى يتم تسجيلها لمدد تتراوح من عام إلى تسعة أعوام، أن لا تنتبه الجهة التى قامت بالتسجيل إلى انتهاء فترة تسجيل النطاق ووجوب التجديد حيث توجد شركات يطلق عليها صائدو النطاقات (Domain Hunters) تقوم بتجديد النطاق لها ومساومة الشركة الأصلية في التنازل عليه نظير ألاف الدولارات مستغلة اعتماد الشركة

---

36) جلسة مجلس ادارة البنك المركزى المصرى بتاريخ 2002/2/28 في شأن الضوابط الرقابية للعمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية، وايضا د/ شريف محمد غنام، مسؤولية البنك عن اخطاء الكومبيوتر في النقل الالكترونى للنقود، الطبعة الاولى، دار الجامعة الجديدة للنشر بالاسكندرية، سنة 2006، ص 101

37) راجع في ذلك: أحمد البرماوي، مقال تحت عنوان "اقتصاد مصر" منشور بتاريخ 2017/5/13، جريدة اخبار التحرير، تم الاطلاع عليه بتاريخ 2018/2/17.

على هذا الاسم ومعرفة العملاء به لمدد طويلة، هذا فضلا عن الحملات الدعائية له وكم المطبوعات الورقية التى أصدرتها الشركة وتحمل ذلك العنوان.

ايضا، من الجرائم الأخرى المتعلقة بأسماء النطاقات على شبكة الانترنت ما يعرف بإعادة التوجيه (Redirection) مثلما حدث لموقع شركة Nike في شهر يونيو عام 2000 حيث قامت جماعة من المحترفين بالدخول على موقع شركة تسجيل النطاقات الشهيرة والمعروفة باسم (Network Solutions) وتغيير بيانات النطاق لضعف إجراءات امن المعلومات بالشركة في ذلك الحين، وبذلك تم إعادة توجيه مستخدمي الانترنت إلى موقع لشركة انترنت في اسكوتلاندا.

أيضا، قامت إحدى الجماعات بعمل موقع على شبكة الانترنت تحت عنوان (http://www.gatt.org) مستخدمة شكل وتصميم الموقع الخاص بمنظمة التجارة العالمية (World Trade Organization) والذي يظهر كخامس نتيجة في اغلب محركات البحث عن الـ WTO ، وقد استخدمته للحصول على بيانات البريد الالكتروني وباقي بيانات مستخدمي الانترنت الذين كانوا في الأصل يرغبون في زيارة موقع منظمة التجارة العالمية، وهو ما ادى الى العديد من المشكلات مع المنظمة الدولية لحماية حقوق الملكية الفكرية (World Intellectual Property Organization) .

3) 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.

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:

1) 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.

وقد يلجأ البعض الى استخدام الحواسب الآلية وشبكة الانترنت في انتهاك حقوق الملكية الفكرية لبرامج الحاسب والمصنفات الفنية المسموعة والمرئية ونشرها وتداولها عبر شبكات الانترنت، فيما يعرف بالقرصنة، الأمر الذي يلحق الضرر المادي والمعنوي بالشخص أو الجهة مالكة تلك المواد، ولمكافحة قرصنة برامج الحاسب تقوم منظمة ال بى اس ايه (BSA) العالمية Business Software Alliance بتلقي تقارير وبلاغات انتهاكات برامج الحاسب، كما تقوم بإنشاء مكاتب لها حول العالم وتقوم بالتنسيق مع الحكومات لزيادة الوعى ومحاولة تقليل تلك الجرائم، من خلال السعي إلى اصدار قوانين لمعاقبة المخالفين، والتى اشارت في تقريرها السنوي، الصادر في الثامن من يونيو سنة 2003، إلى أن خسائر شركات البرمجيات وصلت إلى 13.1 مليار دولار امريكى في عام

2002 ، ويشير التقرير أيضا إلى أن أكثر دول العالم في نسخ البرامج والعمل بنسخ غير مرخصة هـى فيتنـام حيـث يصـل نسـبة النسـخ غيـر المرخصـة إلـى حـوالي 97 % مـن إجمـالي البـرامج المستخدمة، يليها دولـة الصين بنسبة 94% ثم اندونيسيا بنسبة 89%، ويشير التقرير إلى تحسن نسب القرصنة في مصر من 86 % عام 1994 إلى حوالي 52% عام 2002.

أما بالنسبة لاستخدام الحاسب لنسخ كافة المصنفات المسموعة والمرئية وتوزيعها بصورة غير مشروعة سواء من خلال الاسطوانات الممغنطة او من خلال مواقع الانترنت، فانها من الجرائم التى انتشرت انتشارا كبيرا في الآونة الأخيرة، وأيضا انتشرت برامج تبادل الملفات بين مستخدمي الانترنت التى يتم استخدامها في تبادل الاغانى والأفلام والبرامج غير المرخصة، أما في الولايات المتحدة فقد بدأت رابطة شركات الاسطوانات الامريكية معركتها ضد المواقع الالكترونية التي تقدم خدمات تبادل الملفات وتحميل الأغاني بالمجاني على أجهزة الكمبيوتر عام 1999 ، وذلك بعد انخفاض مبيعات الاسطوانات بنحو 31 % بسبب النقل والنسخ عبر الانترنت، وقد تحقق للرابطة بالفعل إغلاق احد اشهر مواقع بث الاغانى والذي يدعى Napster ومازالت العديد من القضايا مرفوعة من قبل الرابطة ضد شركات بث الاغانى أو خوادم التبادل بين المستخدمين، بل ووصل الأمر إلى اقامة العديد من القضايا على الأطفال والمراهقين مستخدمي تلك البرامج للاستماع والحفظ والتبادل للمصنفات.

ومن جرائم الابتزاز الالكتروني، التى تتم باستخدام الحواسب وشبكات المعلومات هى التخابر أو الاتصال بين أفراد منظمة أو نشاط يهدد امن واستقرار الدولة أو نشاط محرم قانونا مثل شبكات الدعارة والشذوذ التى باتت وسيلة الاتصال الرئيسية لها هى حجرات الدردشة (Chatting Rooms) المنتشرة عبر شبكة الانترنت وصولا الي التحصل علي مكاسب مالية من المجني عليهم بطريق الابتزاز.

ومن أمثلة جرائم الابتزاز الالكتروني، التي يمكن أن تهدد الأمن القومي ما حدث في عيد الميلاد في عام 2000 من قيام أربعة تلاميذ بريطانيين بإرسال بريد إلكتروني بعنوان تهنئة بمناسبة الأعياد إلي الرئيس الأمريكي السابق بيل كلينتون ويطالبوا فيها بمليون دولار أمريكي وإلا سيفجروا البيت الأبيض، وعلي الفور قام مكتب التحقيقات الفيدرالية FBI ومن خلال عمليات التتبع الالكتروني ومتابعة IP Address الخاص بالرسالة المرسلة، توصلوا للتلاميذ البريطانيين بالتعاون مع شرطة اسكوتلانديارد، وتم مجازاة هؤلاء الطلاب بحرمانهم من استخدام البريد الالكتروني من مدرستهم بعد التأكد أن الأمر لا يعدو أن يكون مزاح.

2) 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، فقد تم تحقيق ذلك عن طريق الاتصال المباشر من خلال شبكات المعلومات الخاصة غير المتاحة لمستخدمي الانترنت (Private Networks) التى كان لها بعض القيود المكانية للاتصال أو من خلال شبكة الانترنت من خلال تواجد واجهة لتلك التعاملات (Web Interface).

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[38]، الا انه ذو اثارا سلبية ضخمة فيما يتعلق بجرائم الابتزاز الالكتروني.

ذلك ان ذلك النوع من التعاملات قد أصبح أمرا واقعاً يتزايد الاعتماد عليه، خاصة بعد تنامى حجم الأعمال التى تتم من خلال التجارة الالكترونية (Electronic Commerce) وظهور الأسواق الالكترونية (Electronic Marketplace) لتسويق وبيع السلع والخدمات، وقد ظهر نتيجة ذلك ظهور خدمات كثيرة يمكن أن تؤدي من خلال الشبكة مثل الاشتراك في المنتديات الخاصة أو الاشتراك في مسابقات علي الشبكة أو لعب القمار أو ألعاب أخري نظير أجور محددة.

وللوقوف على ازدياد مثل هذا النوع من الدفع الالكتروني، ففي دولة مثل الولايات المتحدة الأمريكية، فانه يوجد بها حوالي 185 مليون بطاقة بنسبة 63 % من اجمالى عدد السكان.

أما بالنسبة للصين فان حجم التعاملات المالية باستخدام بطاقات الائتمان قد تعدى الـ 169 مليار دولار أمريكي في عام 2001.

---

38) راجع في ذلك: د. عبد العزيز عجمية، د. محمد اسماعيل، "التطوّر الاقتصادي في أوروبا والعالم العربي"، سنة 1988، الدار الجامعية، بيروت، ص. 259 .

وفي مصر، نجد ان هذه النسبة ترتفع كذلك، حيث ان حجم التعامل بالتجارة الالكترونية داخل وخارج مصر في ازدياد مستمر، ويعتمد على شراء خدمات مواقع المعلومات والكتب العلمية والترفيه.

وبالنظر الى جرائم الابتزاز الالكتروني حسب انتشارها، فقد أقرت وزارة العدل الأمريكية سنة 2000 احدى عشرة نوع من هذه الجرائم، وهي كالآتي:

- السطو على بيانات الحاسب بغية الابتزاز.
- الاتجار بكلمة السر لابتزاز مالكها.
- عمليات الهاكرز (القرصنة).[39]
- ابتزاز الأسرار التجارية باستخدام الحاسب.
- تزوير الماركات التجارية وابتزازها.
- تزوير العملة باستخدام الحاسب بغرض الابتزاز.
- الصور الجنسية بابتزاز الأطفال.
- الاحتيال بغرض الابتزاز عبر شبكة الانترنت.
- الإزعاج عن طريق شبكة الانترنت بغرض الابتزاز.
- تهديدات القنابل بواسطة الانترنت لغرض الابتزاز.
- الاتجار بالمتفجرات والأسلحة النارية[40] أو المخدرات[41] وغسل الأموال عبر شبكة الانترنت.[42]

---

39) راجع في ذلك: د. عبد القادر عودة، التشريع الجنائي الاسلامي مقارنا بالقانون الوضعى، دار الكتب، بيروت، سنة 2010، ص99.

40) مشار اليه في: على عبدالهادى،"الاموال القذرة وغسيل الاموال جريمة عقد التسعينات، مجلة الحكمة، العدد 19، السنة الرابعة، بغداد، دار الحكمة، سنة 2001، ص 80 وما بعدها.

41) راجع في ذلك: اتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع للمخدرات والمؤثرات العقلية لسنة 1988، منصوص في المادة (3) منها على غسل الاموال المستمدة من الاتجار في المخدرات، وسارت على ذات النمط الاتفاقية العربية لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية لسنة 1994، وقد تضمنت احكاما خاصة بغسل الاموال ومصادرتها، وايضا: عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– الناشر : جامعة نايف العربية للعلوم الأمنية – 2008 م – صـ 46 وما بعدها، وايضا : محمد فتحى عيد، مرجع سابق ، ص 131.

وهناك تصنيف آخر لمكتب التحقيقات الفدرالي الأمريكي FBI ، حيث يصنفها الى:

- اقتحام شبكات الهواتف العامة أو الرسمية.
- اقتحام المواقع الرسمية.
- انتهاك سرية بعض المواقع.
- التجسس[43].
- البرامج المسروقة.

وقد ذهب البعض من الفقه الى أيراد خمس من أنواع جرائم الابتزاز الالكتروني هي:

- الاختراق غير المسموح به بغرض الابتزاز.
- إتلاف المعلومات والبرامج بغية الابتزاز.
- تعطيل نظام الكمبيوتر وتخريب شبكة الاتصالات بغرض الابتزاز.
- اختراق الغير مسموح به للمعلومات داخل نظام و خارجه بغرض الابتزاز.
- التجسس على الحاسب للابتزاز.

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 الاول:** واقع جرائم الابتزاز الالكتروني على المستوى الدولي.
- **المطلب الثاني:** واقع جرائم الابتزاز الالكتروني في الوطن العربي.

المطلب الأول

---

42) راجع في ذلك: د. عبد الفتاح حجازي: مكافحة جرائم الكمبيوتر والانترنت، دراسة معمقة في القانون المعلوماتي، ط1، دار الفكر الجامعي، الإسكندرية، سنة 2006. الصفحة 7 وما بعدها.

43) انظر في ذلك: د. داود حسن طاهر، نظم المعلومات، أكاديمية نايف الأمنية، الرياض –1420 هـ – صفحة 95 وما بعدها.

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[44]

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 555 مليون مستخدم سنويا، وأكثر من 1.5 مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات.

ومن أكثر أنواع تلك الجرائم؛ ابتزاز هويات وعددها 224 مليون سرقة، وأظهرت الدراسة أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ بينت أن أكثر من 600 ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن التكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ 100 مليار دولار، بعدما كانت في حدود 63.1 مليار دولار سنة 2011

ومن المتوقع أن تتجاوز 120 مليار دولار بحلول سنة 2017[45]، وحسب تقرير نشرته شركة مشروعات الأمن المعلوماتي (CYBERSECURITY VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته 1 تريليون دولار خلال الفترة التي تمتد من 2017 إلى غاية 2021 على منتجات وخدمات الأمن المعلوماتي لمكافحة جرائم الابتزاز الالكتروني، وفي هذا الإطار فقد سجل فتح حوالي مليون وظيفة خاصة بالأمن المعلوماتي خلال سنة 2016، ومن المتوقع أن يكون هناك عجز بحوالي 1.5 مليون وظيفة خلال عام 2019. [46]

---

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

http://www.aljazeera.net

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

http://digital.argaam.com.

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

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. (47)

ومن المتوقع أن تكبد جرائم الابتزاز الالكتروني الاقتصاد العالمي حوالي 6 تريليون دولار بحلول سنة 2021 وهي ضعف الخسائر المسجلة سنة 2015 والمقدرة بحوالي 3 تريليون دولار، 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 2015 و 2016 العديد من حوادث الاختراق والقرصنة لغرض الابتزاز، ولعل أهمها ما يلي:

1- في سبتمبر من سنة 2016، 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 500 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.

2- لقد واجه مستخدمو الإنترنت حول العالم يوم 2016/10/21، 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 ترجمة عنوان الموقع إلى عنوان IP، وأبرز المواقع الرئيسية التي تعرضت للسقوط هي Spotify, Etsy Github, Twitter, Amazon.[48]

.

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

(48) انظر في ذلك: تحت عنوان "الانترنت ينهار.. والطائر الأزرق يكف عن التغريد"، مقال منشور بتاريخ 2016/10/22، على موقع تاريخ الاطلاع 11/ 2/2017:

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

3- 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. (49)

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(50) أو الإرهابيين أو حتى الدول المعادية.

ذلك أن الأرباح الضخمة غير المشروعة التي تحققها تلك الجرائم تجاوزت أرباح تجارة المخدرات(51)، كما أن جرائم الابتزاز الالكتروني أصبحت اليوم واقعاً لا ينكر في مصر، بوقوع نحو ثلاثون مليون شخص من سكان الدولة ضحايا جرائم الابتزاز الالكتروني خلال سنة 2015. (52)

---

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

http://www.skynewsarabia.com.

(50) راجع في ذلك: د. هدى حامد قشقوش، مرجع سابق، منشأة المعارف، سنة 2006، ص 18، وايضا : محمد ابراهيم زيد، "الجريمة المنظمة (تعريفها وانماطها وجوانبها التشريعية)"، ابحاث حلقة علمية حول الجريمة المنظمة واساليب مكافحتها، الرياض، اكاديمية نايف للعلوم الامنية، سنة 1999، ص 33

(51) انظر في هذا الصدد:

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

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

وفي شأن الافيون : يبلغ انتاج العالم من الافيون 4000 طن متري، يمكن ان يترتب على تنقيتها انتاج 400 طن مترى تقريبا من الهيروين، وينتج الافيون اساسا في منطقتين هما الهلال الذهبي في جنوب شرق اسيا، في افغانستان هناك كميات صغيرة تنتج في لبنان Laosوايران وباكستان، وكذلك في المثلث الذهبي تايلاند وبورما ولاوس

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 2015 إلى 160 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.[53]

وحسب تقارير دولية مستقلة، فإن الإمارات سجلت أفضل أداء في صد الهجمات الإلكترونية في منطقة الشرق الأوسط خلال النصف الأول من سنة 2016، في الوقت الذي أكدت هيئة تنظيم الاتصالات على فعالية منظومة الحماية الإلكترونية في الدولة.[54]

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 2000، الغصون (50 – 56) ، ص 12 ، 13، مطبوعات الامم المتحدة، نيويورك، سنة 2001، الوثيقة رقم المنشور بتاريخ 21 فبراير 2001 ، وكذلك انظر : مجلة الحقوق الكويتية، مجلس النشر العلمى، Elincb 200D الكويت، 1998، العدد الثالث، ص 381 ، منشور دورة البحث الجنائى للضباط رقم (5) دراسات حول الجريمة الاقتصادية في دولة الامارات، معهد البحث الجنائى، شرطة دبى، دولة الامارات العربية المتحدة، سنة 1998، ص 98.

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)

52(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..

53(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.

54(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..

ومنذ عام 2014، ارتفعت معدلات جرائم الابتزاز الالكتروني في لبنان، مما وضع المعنيين في المصارف والمؤسسات المالية والأجهزة الأمنية أمام سباق مع القراصنة القادرين على تطوير أدواتهم وتنظيماتهم بموازاة تطور وسائل المكافحة، حيث بلغ عدد عمليات القرصنة الإلكترونية التي تعرضت لها المصارف اللبنانية حصراً منذ عام 2011 حتى الفصل الثالث من سنة 2016، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان، 233 عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو 26 مليوناً ونصف مليون دولار، من ضمنها 15 مليون دولار بين عامي 2015 و2016 طالت القطاع 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.[55]

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 500 جريمة ابتزاز الكتروني في الجزائر خلال سنة 2016، علما أن هذا يخص عدد الحالات التي قامت بعملية التبليغ فقط[56]

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

) حيث تم الاستيلاء على 26.5 مليون دولار، من مصارف لبنان التى تعرّضت لـ7 أنواع من الهجمات 55(الإلكترونية .

http://ghadinews.net/Newsdet..

(56) 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: مرجع سابق، ص 220 – 221، وايضا: عادل حسن السيد – طبيعة عمليات غسل الاموال وعلاقتها بأنتشار المخدرات– الناشر : جامعة نايف العربية للعلوم الأمنية – 2008 م – صـ 46 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 1990، ص 131.

الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة 385 جريمة معلوماتية من قبل الفرق المتخصصة في مكافحة الجريمة المعلوماتية التابعة للأمن الوطني، إلى جانب تسجيل 57 قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية.[57]

57(انظر في ذلك: تحت عنوان "أزيد من 500 جريمة إلكترونية في الجزائر سنة 2016"، مقال منشور على الموقع الالكتروني لجريدة الفجر

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

الفصل الثالث

الطبيعة القانونية لجرائم الابتزاز الالكتروني

تمهيد وتقسيم:

مما لا شك فيه ان دراسة الجرائم بشكل عام، وجرائم الابتزاز الالكتروني بشكل خاص، تدخل في نطاق دراسة القسم الخاص لقانون العقوبات، ذلك القسم المختص بدراسة كل جريمة على حدة، ومتناولاً عناصرها الأساسية والعقوبة المقررة لها.[58]

بيد ان جرائم الابتزاز الالكتروني تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي بالنظر إلى طبيعتها المعلوماتية الخاصة[59]، وبالنظر كذلك الى ان معظم هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها ام في تجهيزها أم بإدخالها إلى الحاسب المرتبط بشبكة المعلومات، ولغرض الحصول على معلومات معينة.

كما قد ترتكب هذه الجرائم في مجال معالجة الكلمات أو معالجة النصوص، وهذا النوع الاخير من الجرائم لا يعدو ان يكون طريقة أوتوماتيكية، تمكن المستخدم من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانية التصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة.[60]

فجميع تلك العمليات هي ذات صلة بجرائم الابتزاز الالكتروني، وعليه لابد للجاني من استيعابها، فضلاً عن ان الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الاعتداء او تستخدم وسيلةً له، وبالنظر لهذه الجرائم من طبيعة خاصة هي قدرة شبكة المعلومات الفريدة على نقل وتبادل معلومات ذات طابع شخصي وعام في أن واحد، كالاعتداء على الخصوصية، والحكمة من ذلك توسع بنوك المعلومات بأنواعها، علاوة على توسع الأفراد وسعيهم الى ربط حواسبهم بالشبكة المذكورة، مما يطرح تساؤلاً حول طبيعة الخدمات والتطبيقات في هذه الشبكة، ليتسنى معرفة ماهية النصوص والقوانين التي يجب تطبيقها على خدمات نشر المواقع

---

58) انظر في ذلك: د. محمد زكي أبو عامر، ود. علي عبد القادر القهوجي، قانون العقوبات – القسم الخاص، بدون مكان وسنة نشر، ص9 وما بعدها.

59) انظر في ذلك: د. هدى حامد قشقوش، جرائم المعلوماتية الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، سنة 1992م، ص18.

60) انظر في ذلك: د. هدى حامد قشقوش، المصدر السابق، ص16.

وتبادل المعلومات فيها بشكل عام، وبشكل خاص معرفة النظام القانوني للمسؤولية التي يفترض تطبيقها على الاشخاص المسؤولين عن هذا النشر او التبادل.[61]

وبشكل مغاير، هل يمكن وصف الخدمات والتطبيقات في شبكة المعلومات بأنها داخلة ضمن احكام خدمات البريد او التخابر الخاص، ام انها تدخل ضمن مفهوم الصحافة والمطبوعات او الوسائل السمعية والبصرية او المؤسسات التلفزيونية والاذاعية[62]، ام هل انه في كل الاحوال يجب اعتبار شبكة المعلومات فضاءاً جديداً للمعلومات، لا علاقة له بعلم البريد والاتصالات الخاصة، ولا بعلم الصحافة، او الوسائل السمعية والبث الاذاعي والتلفزيوني، ومن ثم تكون القواعد والمبادئ العامة حول المسؤولية واجبة التطبيق على الخدمات والتطبيقات فيها.[63]

ذلك ان البحث عن النظام القانوني الملائم لطبيعة جرائم الابتزاز الالكتروني، يهدف بشكل اساسي الى معرفة ماهية النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها، فضلاً عن معرفة النظام القانوني للمسؤولية، الذي يفترض تطبيقه على الاشخاص المسؤولين عن هذا النشر، وخصوصا لتأرجح واختلاف موقف الدول بهذا الشان، وبناءاً على ما تقدم تتضح الطبيعة القانونية الخاصة لهذه الجرائم من خلال المجال الذي يمكن ان ترتكب فيه، ومن جانب اخر المحل الذي يقع عليه الاعتداء المذكور.

ويرى جانب من الفقه القانوني[64] ان التطور السريع في مجال المعلوماتية قد يفسح المجال لاقتناء وسائل الكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة، تتمثل بالاعتداء على حق الخصوصية والحرية الشخصية[65]، ولا شك في ان الاجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية لبيانات وادخال المعلومات ونقلها، ومن ثم يجب ضمه إلى

---

61) انظر في ذلك: د. طوني ميشال عيسى، التنظيم القانوني لشبكة الانترنت، طبعة اولى، دار صادر للمنشورات الحقوقية، بيروت، سنة 2001م، ص 373.

62) انظر في ذلك: د. جميل عبد الباقي الصغير، المواجهة الجنائية لقرصنة البرامج التلفزيونية المدفوعة، دار النهضة العربية، القاهرة، سنة 2001م، ص 11 وما بعدها.

63) انظر في ذلك: د. طوني ميشال عيسى، مصدر سابق، ص 388 وما بعدها.

(64) David Johnston Electronic Privacy, OP. Cit, P (70).

65) انظر في ذلك: د. مبدر الويس، اثر التطور التكنولوجي على الحريات العامة، منشاة المعارف، الإسكندرية، سنة 1983م، ص 46 وما بعدها.

نطاق القانون الجنائي، على الرغم من ان معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي، أو لما يحويه من فراغ او نقص تشريعي في هذا المجال.[66]

ومن جانب أخر، تتخذ هذه الجرائم طبيعة خاصة من حيث تكييفها القانوني، اذ لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، فالنصوص التقليدية وضعت وفقاً لمعايير معينة كالمنقول المادي، بينما مفهوم الحقوق الشخصية في شبكة المعلومات هو الذي يرد على نتاج الفكر البشري، وهو يتعلق بشخص المرء وأمواله وممتلكاته.

كما أن تطبيق النصوص التقليدية على جرائم الابتزاز الالكتروني يثير مشكلات عديدة في مقدمتها مسألة الإثبات[67] كالحصول على اثر مادي، اذ يمكن للجاني محو أدلة الإدانة وتدميرها في وقت وجيز، وخاصة في حالة تفتيش الشبكات او عمليات اعتراض الاتصال، فقد تكون البيانات التي يجري البحث عنها مشفرة، ولا يعرف شفرة الدخول إلا احد العاملين على الشبكة، ومن هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة[68]

ومما يزيد من صعوبة الأمر ملاحقة جناة جرائم الابتزاز الالكتروني، الذين يقيمون في دولة أخرى لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه، وفي ضوء تلك الاعتبارات يمكن الجزم بان هذه الجرائم تتمتع بطبيعة قانونية شديدة الخصوصية.

وترتيبا على ذلك، تعد جرائم الابتزاز الالكتروني، جرائم ذات طبيعة خاصة وخصائص فريدة، لا تتوافر في الجرائم التقليدية، سواء من حيث أسلوب وطرق ارتكابها، أو شخص مرتكبيها، فنتناول في هذا الفصل الطبيعة القانونية الخاصة لجرائم الابتزاز الالكتروني في مبحث أول، على أن نعرض للشرعية الجنائية لجرائم الابتزاز الالكتروني في مبحث ثان، ونستتبع ذلك ببيان دور القاضي الجنائي في ظل غياب النص العقابي لجرائم الابتزاز الالكتروني في مبحث ثالث، على يختتم هذا الفصل بمعالجة تنازع الاختصاص بشأن جرائم الابتزاز الالكتروني في مبحث رابع وأخير، وذلك على الترتيب التالي:

- **المبحث الأول:** الطبيعة القانونية الخاصة لجرائم الابتزاز الالكتروني.

---

66) انظر في ذلك: د. عبد الستار الكبيسي، المسؤولية الجنائية الناشئة عن استعمال الحاسب، سلسلة المائدة الحرة من ندوة القانون والحاسب، بيت الحكمة، سنة 1999م، ص127.

67) انظر في ذلك: د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، سنة 2001م، ص 4.

68) انظر في ذلك: د. هلالي عبد اللاه احمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، طبعة اولى، دار النهضة العربية، القاهرة، سنة 1997م، ص66.

- **المبحث الثاني:** الشرعية الجنائية لجرائم الابتزاز الالكتروني.
- **المبحث الثالث:** دور القاضي الجنائي في ظل غياب النص العقابي لجرائم الابتزاز الالكتروني.
- **المبحث الرابع:** تنازع الاختصاص بشأن جرائم الابتزاز الالكتروني.

المبحث الأول
الطبيعة القانونية الخاصة لجرائم الابتزاز الالكتروني

تمهيد وتقسيم:

تكمن الطبيعة الخاصة لجرائم الابتزاز الالكتروني في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى إرتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسبهم بالشبكة، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات، سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات، ولغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال أو معالجة النصوص، وصعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة.

بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشكلات عديدة في مقدمتها مسألة الإثبات، ومتابعة مرتكبيها، وعلى ضوء تلك الاعتبارات يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[69]

حيث صاحب التطور التكنولوجي والتقني الحادث تطور في كل مجالات الحياة، في اتجاه إيجابي أو في الاتجاه المعاكس السلبي، ومما ترتب على ذلك التطور، تمتع الإنسان بقسط وافر من الرفاهية وتيسير معاملاته في شتى الميادين، هذا في الاتجاه الايجابي، أما في الاتجاه السلبي فأن ذلك التطور صاحبه تطور خطير في نوعية الجرائم، إذ ظهرت جرائم الابتزاز الالكتروني، والوسائل المستخدمة فيها، كما صاحب ذلك تطورا في نوعية المجرم الذى يرتكب تلك الجرائم.

69) انظر في ذلك: د. محمد زكي أبوعامر، وعلي عبد القادر القهوجي، قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة، سنة 1993، ص9.

ويمكن القول إن العقود الأخيرة من القرن المنصرم وبداية القرن الحالى شهدت ثورة في مجال التكنولوجيا والاتصالات، مما أدى لظهور أجيال جديدة من وسائل الاتصال عن بعد، والتي أعادت صياغة شكل العالم فأصبح العالم قرية صغيرة لا تعرف الحدود، وبالطبع تم الاستفادة من هذه التكنولوجيا في مختلف القطاعات الحياتية في الدولة، وعلى جميع المستويات، خاصة بعد تطور نظم المعلومات وربطها بالأقمار الصناعية، وبالطبع تعقدت الجريمة وتنوعت أساليب ارتكابها، مستفيدة من هذا التطور التقني المذهل، فظهر ما يعرف بجرائم الابتزاز الالكتروني التي أخذت أبعادا جديدة بداية من ثمانينات القرن الماضي، حيث كانت بدايات انتشار الحاسب الآلي وتطبيقاته بشكل عام، لحقه انتشار شبكة الإنترنت في بداية التسعينيات من ذات القرن، وهذه الأخيرة التي برزت كأسرع وأقوى وسائل اتصال حديثة في العالم اليوم.

كما أدى التطور المتلاحق للإنترنت وانتشار أجيال جديدة وأنواع مختلفة من أجهزة الحاسب الآلي إلى مضاعفة المخاطر والاعتداءات على الحريات الشخصية والملكية الخاصة، بل وعلى مصالح الدولة ذاتها.

مما حدا ببعض الدول أن تقر اتفاقيات تقرر تجريم بعض الأفعال الحادثة عبر الوسائل الالكترونية أو بواسطتها، ومنها اتفاقية بودابست لعام 2001، والقانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، والذي تم اقراره من قبل وزراء العدل العرب في اجتماعهم المشترك في الفترة من 12-2003/5/22، غير أننا لم نر له أثرا فعليا علي أغلب التشريعات الجنائية في الدول العربية وبصفة خاصة مصر الا في الآونة الاخيرة، فلا يوجد بها حتى الآن تشريع جنائي خاص بجرائم الابتزاز الالكتروني يقدم الحلول الناجعة لكافة المشكلات القانونية الناجمة عنها على الرغم من وجود بعض النصوص القانونية التى تحتويها قوانين تنظم موضوعات مختلفة تناولت بعض صور التجريم المعلوماتي، منها قانون الأحوال المدنية المصري رقم 143 لسنة 1994، وقانون حماية الملكية الفكرية رقم 82 لسنة 2002، وقانون تنظيم الاتصالات 10 لسنة 2003، وقانون التوقيع الالكتروني 15 لسنة 2004، وقانون الطفل المعدل في 2008.

إلا أن هذه القوانين لم تغط كافة صور التجريم المعلوماتي، وهو ما كان له أثره السيئ علي المجتمع بسبب عدم توفير الحماية القانونية لأفراده خصوصا في ظل وجود مبدأ دستوري يحكم التجريم في مصر وهو مبدأ الشرعية الجنائية والذي ورد النص عليه في المادة 95 من الدستور المصري الحالي الصادر في عام 2014، والتى جرى نصها على أن "العقوبة شخصية، ولا جريمة

ولا عقوبة إلا بناء على قانون، ولا توقع عقوبة إلا بحكم قضائي ولا عقاب إلا على الأفعال اللاحقة لتاريخ نفاذ القانون" [70]

فمع وجود ذلك النص الدستوري وغياب النص التشريعي العقابي يصبح القاضي الجنائي في حيرة من أمره، خصوصا عندما يعرض عليه فعل يشكل جريمة من جرائم الابتزاز الالكتروني، التي لا يجد لها نصا صريحا يجرمها في قانون العقوبات، فكيف السبيل إلى الحكم القويم ؟ هل يحكم بالبراءة إعمالا لمبدأ شرعية التجريم؟ أم يحاول إنزال حكم القانون في الجرائم التقليدية علي تلك الجريمة أخذا بالتفسير القضائي الواسع للنصوص القانونية؟ ذاك ما تحاول هذه الدراسة الإجابة عنه من خلال تحديد هذه المعضلة القانونية الواقعية.

وحيث أسهم دخول التقنيات الحديثة في مجال الاتصالات وتكنولوجيا المعلومات وشبكة الإنترنت إلى إفراز أنماط مستحدثة من الجرائم لم يكن للبشرية سابق عهد بها، وتتميز هذه النوعية من الجرائم بأنها معقدة في طرق ارتكابها، ووسائل كشفها، كما أنها ذات طابع دولي، لذلك أصبحت تمثل خطرا داهما يؤرق دول العالم بأسره[71]

وفي هذا المبحث يتناول التعرف على بعض جوانب جرائم الابتزاز الالكتروني، من حيث طبيعتها الخاصة، وغير ذلك من الأمور التي تساعد على الفهم المبسط لجرائم الابتزاز الالكتروني.

ولتحديد الطبيعة الخاصة لجرائم الابتزاز الالكتروني أهميتها الجلية للوقوف على كنهها، فضلاً عن كونه الوسيلة التي تكشف عن موضوعات الدراسة وجوانبها، ولهذه الأهمية التي يحظى بها التعريف ظلّ الفقهاء والمفكرون لا يتفقون حول تعريف واحد وثابت لأي موضوع، وذلك لاختلاف وجهات النظر واختلاف الزاوية التي يتخذها كل فَقيه معيارا وأساسا لتعريفه، ونستطيع أن نقابل اتجاهين رئيسيين في هذا المجال، محاولة للوقوف على الطبيعة القانونية لجرائم الابتزاز الالكتروني.

– يهتم الاتجاه الأول بالناحية العضوية أو الشكلية.

---

70) راجع في ذلك: د. السعيد مصطفي السعيد – الاحكام العامة في قانون العقوبات – دار المعارف – الطبعة الرابعة، سنة 1962 – ص 50.

71) انظر في ذلك: عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 2008/03/07، المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:3.

– بينمـا يهـتم الاتجـاه الثـاني بالناحيـة الموضـوعية أو الوظيفيـة، فعـرّف فريـق الجريمـة المعلوماتيـة[72] (cyber crime) بأنهـا "الاعتداء غير القانوني الذي يرتكب بواسطة المعلومات الحاسبية بغرض تحقيق الربح"[73]، كمـا عرفت بأنهـا" كـل فعـل إجرامـي متعمـد أيـا كانـت صـلته بالمعلومات ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل"[74] وعرفت أيضا بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابها من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"[75]، بينما عرفها فريق آخر بأنها "كل جريمة تتم في محيط أجهزة الحاسب" أو هي" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[76]، كما تعرف أيضا بأنها "كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".[77]

ولتحديد الطبيعة الخاصة لجرائم الابتزاز الالكتروني، نوضح بعض خصائص تلك الجرائم، والتي تميزها عن غيرها من جرائم الابتزاز التقليدية هي:

1- حيث انها ترتكب بواسطة شبكة الإنترنت، أي تستخدم شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها؛ إذ تعد شبكة الإنترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات بكافة أنواعها والأشخاص وغيرها، والتي غالبا ما تكون الضحية فيها.

2- كما أن مرتكب الجريمة مجرم ذو خبرة في استخدام الحاسب الآلي والإنترنت، حيث ان جرائم الابتزاز الالكتروني لا تعرف الحدود المكانية ولا الحدود الزمنية، لأنها ترتكب عبر

---

72) بأنه هو نطاق ذو دلالة علي شبكة الإنترنت يحدد بأن الكلمة التي ستلي هذا النطاق لها cyber) يقصد بنطاق cyber terrorism والنقود cyber المقهى الالكتروني، والإرهاب الالكتروني cyber cafe علاقة بشبكة الإنترنت مثل cyber cash الالكترونية هي الجرائم التي لها علاقة بالحاسب وشبكة الإنترنت.راجع في cyber crime ومن هنا ذلك: د. مصطفي محمد موسي: التحقيق الجنائي في الجرائم المعلوماتية، ط1، دن، سنة 2008، ص111.

73) انظر في ذلك: هلال بن محمد بن حارب البوسعيدى: الحماية القانونية والفنية لقواعد المعلومات المحوسبة" دراسة قانونية وفنية مقارنة"، دار النهضة العربية، سنة 2009، ص15، وما بعدها.

74) راجع في ذلك:

D.B Parker,combattre la crimipin alite informatique,1985,p18.

75) انظر في ذلك: د. نائلة عادل محمد فريد قورة: جرائم المعلوماتية الاقتصادية" دراسة نظرية وتطبيقية"، دار النهضة العربية، سنة 2003-2004، ص21.

76) انظر في ذلك: د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، سنة 2009، ص74.76

77) راجع في ذلك: د. مصطفي محمد موسي، مرجع سابق، ص77.112

شبكة الإنترنت، لا تحدها حدود جغرافية كحدود دولة بعينها، فالعالم كله يمكن أن يكون مسرحا لارتكاب الجريمة، كما لا يحدها زمان معين رغم الاختلاف في التوقيتات بين الدول.

3- أيضا تلك الجرائم تتسم بالخطورة البالغة، وذلك من نواحٍ عدة، فمن ناحية الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية، ومن ناحية ثانية نجدها ترتكب من فئات إجرامية متعددة تجعل من الصعب معرفة الفاعل، ومن ناحية أخيرة تنطوي على سلوكيات وافعال وتصرفات غير معتادة او مألوفة.

4- كما ان هناك صعوبة التحري والتحقيق في هذه الجرائم ومن ثم محاكمة مرتكبها، فهناك صعوبة في ملاحقة مرتكب هذه الجرائم، ولو تم التوصل إليه فمن السهل إتلاف الأدلة من قبل الجناة، كما أن هذه الجرائم لا تحدها حدود، فهي جرائم عابرة للحدود مما يثير تحديات ومعوقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

5- فضلا عن ذلك، فان الدافع لارتكاب جرائم الابتزاز الالكتروني يختلف عن دافع الجرائم التقليدية، فالبعض يرتكب جرائم الابتزاز الالكتروني لرغبته في الحصول على المعلومات الجديدة، مثل القراصنة، أو للاستيلاء على المعلومات الموجودة على جهاز الحاسب أو حذفها أو تدميرها أو إلغائها نهائيا، وقد يكون الدافع الرغبة في قهر النظام الالكتروني بغرض تحقيق شهرة وإثبات التفوق العلمي لديه، وهى تكون بين الشباب، وقد تكون لاستهداف بعض الأشخاص والجهات.[78]

6- أيضا إن سمات المجرم المعلوماتي تختلف عن صفات المجرم التقليدي، حيث يتميز المجرم المعلوماتي، بعدد من السمات والخصائص التي تجعله مختلفا عن المجرم التقليدي والتي منها:

- أ – **انه مجرم ذكي:** حيث يعتبر الذكاء من أهم صفات المجرم المعلوماتي لأنه يتطلب منه الإلمام التام بتقنية بتكنولوجيا المعلومات والقدرة على تعديل وتغيير برامج الحاسب الآلي.

---

78) راجع في ذلك: د. مصطفي محمد موسي، مرجع سابق، ص134، 135، وايضا راجع: د. حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم المعلوماتية دراسة مقارنة، دار النهضة العربية، سنة 2009، ص53، وما بعدها، وكذلك راجع: د. رامى متولي القاضي: مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، ط1، سنة 2011، ص52، وما بعدها.

- **ب – كما انه مجرم محترف:** اذ يتصف مرتكب جرائم الابتزاز الالكتروني بأنه على درجة عالية من الخبرة والمهارة في استخدام الحاسب الآلي، والتكنولوجيا الحديثة.
- **جـ – كذلك هو مجرم غير عنيف:** حيث ينتمي إجرام الابتزاز المعلوماتي في غالبه الأعم إلى إجرام الحيلة، وهذا النوع من الإجرام لا يستلزم مقدارا من العنف للقيام به.
- **د – ايضا هو مجرم متكيف اجتماعيا:** فلا يضع المجرم المعلوماتي نفسه في حالة عدوانية مع المجتمع الذي يحيط به، بل إن ذكاءه يدفعه للتكيف مع المجتمع، وكلما ازداد تكيفه وتوافقه مع المجتمع كلما ازدادت خطورته الإجرامية.
- **و– كما يتميز بالميل إلى ارتكاب الجرائم:** اذ يتميز مرتكب جرائم الابتزاز اللكتروني بالنزعة الإجرامية والميل إلى ارتكاب الجرائم.
- **هـ – ومن صفاته الميل إلى التقليد:** لان أغلب جرائم الابتزاز الالكتروني تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه مما يؤدي لارتكابه للجريمة.[79]

7- **وفي إطار تصنيف جرائم الابتزاز الالكتروني:** تتعدد صور جرائم الابتزاز الالكتروني، إلا أنها تتفق جميعها في الوسيلة المستخدمة لارتكابها وهي الأجهزة التقنية الحديثة من حاسبات آلية وخلافها، وكلها تتم عبر شبكة الإنترنت، وقد عددت اتفاقية بودابست المتعلقة بالإجرام الكوني او الإجرام المعلوماتي، والموقعة من الإتحاد الأوروبي في 11/23/ 2001، وصور الجرائم المعلوماتية التي عددتها الاتفاقية هي الصور الممثلة للإجرام المعلوماتي المرتكب حاليا، وتتمثل في الآتي: [80]

أولاً: الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية: وقد عددت اتفاقية بودابست، صور هذه الجرائم في الآتي:

- أ – الولوج غير القانونى : وهو يعني الدخول غير المشروع لنظام معلوماتي مملوك للغير "القرصنة" والتي قد تكون بهدف إتلاف أو تدمير النظام المعلوماتي للغير أو الحصول

---

79) راجع في ذلك: د. أيمن عبد الحفيظ: الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دن، سنة 2005، ص13، وما بعدها، وايضا راجع: د. رامى متولي القاضي، مرجع سابق، ص54، وما بعدها.

وكذلك راجع:

Cohen Frederick: Protection and security on the information super high way,Wiley&sons,Inc,1995,p66.ets.

80) انظر في ذلك: د. هلال عبد الله أحمد: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية علي ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية، سنة 2002، ص67، وما بعدها.

علي معلومات وبيانات سرية مملوكة للغير أو التدخل بتغيير البيانات المخزنة في النظام المعلوماتي المملوك للغير، وهو ما يطلق عليه الغش أو التزوير المعلوماتي.

- ب – الاعتراض غير القانونى: وهى جريمة انتهاك الحق في الخصوصية والتى تحدث عندما يتم اعتراض المراسلات الالكترونية والاتصالات الالكترونية الخاصة بالغير، وهذه الجريمة تتعلق بكافة أشكال النقل الالكتروني للبيانات سواء عن طريق التليفون أو الفاكس أو البريد الالكتروني أو غير ذلك من الوسائل التقنية الحديثة.
- جـ – الاعتداء علي سلامة البيانات: وتتمثل في الاعتداء عمدا على البيانات والبرامج الخاصة بجهاز الحاسب الآلي المملوك للغير بهدف تعطيل الجهاز أو محو وطمس بيانات الحاسب الآلي.
- د – الاعتداء على سلامة النظام: وهي تتمثل في الأفعال التي تحمل اعتداء على حسن تشغيل نظام الحاسب الآلي بشكل جسيم مما يؤدي لتوقف النظام عن العمل مثل الإعتداء من خلال استخدام الفيروسات.
- و– إساءة استخدام أجهزة الحاسب: أي كل فعل مجرم قانونا يتم من خلال استخدام الحاسب الآلي.

ثانيا: جرائم الابتزاز الالكتروني المتصلة بالحاسب وتتمثل في الآتي:

- أ – **الاحتيال المعلوماتي أو التزوير والغش المعلوماتيين:** ويقصد به الخداع أو الغش المعلوماتي الذي يقوم علي التلاعب في نظم المعالجة الآلية للمعلومات بهدف الحصول دون وجه حق علي خدمات أو أموال أو أصول معينة، ويقوم الجاني في هذه الجريمة باستخدام التقنيات الحديثة بغية التلاعب في البيانات المصرفية ونتائج الميزانيات والمستحقات المالية، فيتم تحويل تلك الأموال في ثوانٍ معدودة من حساب إلى آخر، وتتمثل خطورة هذا الفعل الإجرامي في كونه يتم عبر الحدود الإقليمية لأكثر من دولة وفي ثوان معدودة، وهو ما يجعله بالغ الأثر السلبي على الاقتصاد القومي، إذ من الممكن أن يؤدي ارتكاب مثل هذه الجريمة إلى إفلاس شركات أو بنوك كبرى في الدولة.[81]
- **ب – الجرائم المتصلة بمحتوى الحاسب الآلي:** وهي تتعلق بجرائم إنتاج ونشر المواد الإباحية الخاصة بالأطفال وبيع الأطفال والاتجار فيهم والترويج لدعارة الأطفال.

---

81) انظر في ذلك: أ. محمد محمد شتات: فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، سنة 2001، ص79، وما بعدها.

- **جـ – الجرائم المتصلة بالاعتداءات الواقعة علي الملكية الفكرية والحقوق المجاورة:** وهي تعد من جرائم الابتزاز الالكتروني الأكثر شيوعا وانتشارا وتستهدف الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية، وذلك نظرا للسهولة التي يمكن من خلالها عمل نسخ غير مصرح بها عن طريق التكنولوجية الرقمية، مما يضر بالحقوق المالية للمالكين والمنتجين.

أما **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات** فلم تقم بعمل تصنيف مشابه للاتفاقية السابقة، بل قامت بسرد للجرائم المعلوماتية، علي سبيل المثال مثل جرائم استخدام وسائل المعلومات، وجرائم الاحتيال والإباحية، وجرائم الاستغلال الجنسي، وحرمة الاعتداء علي الحياة الخاصة، وما يتعلق بالإرهاب والجريمة المنظمة.[82]

وهناك من الفقه من صنف جرائم الابتزاز الالكتروني تحت نوعين من الجرائم على حسب الأداة المستخدمة في ارتكابها: [83]

- **النوع الأول:web crime computer** : وهو يتعلق بجرائم الشبكة العالمية التي تستخدم الحاسب وشبكاته كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيال وتشويه السمعة والسب والقذف، وفي هذا النوع من الجرائم يكون الحاسب الآلي محتفظا بأدلة رقمية تساعد في كشف الفاعل.
- **النوع الثاني: crime computer**: وهو يتعلق بالجرائم التي يكون الحاسب فيها محلا للفعل الإجرامي ذاته كالأفعال الإجرامية الواقعة على مكونات الحاسب المادية، أو المكونات المعنوية soft ware أو قاعدة البيانات date bases أو المعلومات التي قد تكون علي الحاسب من خلال الحصول غير المشروع عليها ونشرها" انتهاك الملكية الفكرية"، أو من خلال تسجيل مواد إباحية عليه.

وهناك جانب أخر من الفقه قسم جرائم الابتزاز الالكتروني، إلى جرائم تقليدية: ترتكب عن طريق استخدام الحاسب الآلي وهي جرائم الإتلاف والتصنت إلى غير ذلك من الجرائم، وجرائم مستحدثة مثل جرائم التجسس والقرصنة، وبعضهم قسم جرائم الابتزاز الالكتروني حسب المصلحة المحمية بالقانون إلى جرائم الابتزاز الالكتروني التي تمثل الاعتداء على الأشخاص، وجرائم الابتزاز الالكتروني التي تمثل اعتداء على الأموال، وجرائم الابتزاز الالكتروني التي تمثل اعتداء على

) انظر في ذلك: د. رامى متولي القاضي، مرجع سابق، ص82.29(

) انظر في ذلك: د. مصطفي محمد موسي، مرجع سابق، ص83.112(

البيانات، وجرائم الابتزاز الالكتروني التي تمثل اعتداء على الآداب العامة وحقوق الملكية الفكرية، وجرائم الابتزاز الالكتروني ذات الصلة بالإجرام المنظم والجرائم السياسية.[84]

ومما سبق تقديمه من تقسيمات وتصنيفات عدة، يتضح أنه لكي يدخل الفعل في إطار جرائم الابتزاز الالكتروني يجب أن يقوم جهاز الحاسب الآلي في الجريمة بدور على قدر من الأهمية.

ويقصد بجهاز الحاسب الآلي في هذا المقام المكونات المنطقية للحاسب الآلي من معلومات وبرامج وكذلك جميع المكونات الأخرى التي تساعد في عملية المعالجة الآلية للمعلومات، ويكمن هذا الدور في كون النظام قد ساعد وسهل في ارتكاب الفعل على نحو كبير، ويختلف دور الحاسب الآلي في جرائم الابتزاز الالكتروني من جريمة لأخرى.[85]

المبحث الثاني

الشرعية الجنائية لجرائم الابتزاز الالكتروني

تمهيد وتقسيم:

لا شك في أن التجريم والعقاب يعد من أخطر الأمور التشريعية التي تتصل بحقوق المواطنين وحرياتهم، وذلك بسبب خطورة الآثار والنتائج التي تترتب عليه، ولذلك فإن النصوص التشريعية التي تصدر به، يتعين أن تصدر دائما وفقاً لمبدأ الشرعية الجنائية[86]، الذي نتولى إلقاء الضوء عليه في إطار جرائم الابتزاز الالكتروني.

ولما كانت الدولة هي القاسم المشترك بين القانون الدستوري والقانون الجنائي، فالدستور ينظم نشاط الدولة من الناحية السياسية، والقانون الجنائي ينظم نشاطها من الناحية الجنائية من خلال تنظيم علاقة الفرد بالدولة، وعلاقة الأفراد بعضهم مع بعض.

ومن مظاهر هذه الصلة، ما تتضمنه الدساتير من نصوص ذات صبغة جنائية بدافع الرغبة في فرض حماية الدستور وإسباغه بطابع القدسية عليها لتعلقها بحقوق الأفراد وحرياتهم، فالعلاقة وثيقة بين القانون الدستوري والقانون الجنائي، ذلك أن مبادئ الدستور تسهم في تحديد مضمون القانون الجنائي ذاته بحيث يتوقف تحديد الجرائم على تطوير المبادئ الدستورية أكثر من اعتماده

---

84) راجع في تفاصيل هذا التقسيم د. رامى متولي القاضي، مرجع سابق، ص31، وما بعدها.

85) انظر في ذلك: د. نائلة عادل محمد فريد قورة، مرجع سابق، ص25.

86) انظر في ذلك: د. محمود علي أحمد مدنى: دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التى يقوم عليها النظام القانونى المصري " دراسة مقارنة" رسالة دكتوراه، حقوق حلوان، سنة 2015، ص349.

على تطوير القيم والمصالح الاجتماعية، وفي ضوء ذلك يؤدي القانون الجنائي وظيفته في الدولة في إطار الشرعية الدستورية على النحو الذي يحدده الدستور[87]

وقد قام القانون الجنائي على عدد من المبادئ الدستورية، والتي يعد أهمها هو "مبدأ الشرعية الجنائية"[88]، الذي يمثل حجر الزاوية والاساس للنظام الجنائي بأسره، فمنه وحوله تدور كافة المبادئ التي تحكم القواعد الجنائية موضوعية كانت أو إجرائية[89]، ويقصد به بصفة عامة" أن التشريع هو المصدر الأساسي للتجريم والعقاب، وأن السلطة التشريعية هي وحدها المختصة بتحديد الجرائم والعقوبات دون السلطتين القضائية والتنفيذية، وأن القاضي مهمته تطبيق النصوص التي وضعها المشرع".[90]

ويرجع تاريخ هذا المبدأ في القانون الوضعي إلى تاريخ الفصل بين سلطات الدولة، إذ قبل ذلك كان للملك منفردا سلطة تجريم الأفعال بمطلق إرادته[91]، ثم انتقل الأمر في القرون الوسطى للقضاة، فكان القضاة يملكون سلطة تحكمية في تجريم الأفعال والعقاب عليها دون نص في القانون، حتى نص على ذلك المبدأ بداية من صدور ميثاق هنري الأول في انجلترا، ثم دستور كلاريندون، وأكد عليه العهد الأعظم، وجاءت الثورة الفرنسية لتؤكد عليه في المادة الثانية من إعلان حقوق الإنسان والمواطن الصادر عام 1789، ثم جاء الإعلان العالمي لحقوق الإنسان الصادر عام 1948

---

87) انظر في ذلك: د. خالد عبد الله الشافي: المبادىء الجنائية الدستورية في النظام الأساسي للحكم في المملكة العربية السعودية دراسة مقارنة، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، سنة 2010، ص58، 59.

88) راجع في ذلك: د. عمر سالم: شرح قانون العقوبات المصري، دار النهضة العربية، سنة 2010، ص30.88

89) انظر في ذلك: د. عبد العظيم مرسي وزير: شرح قانون العقوبات، دار النهضة العربية، دت، ص33.=

راجع أيضا: BECCARIA: Traité des délits et des peines. Nouvelle Traduction jrançaise, Introduction de ANCEL et STEFANI ,Paris, Cujas 1966,p.67.

90) انظر في ذلك: د. حسنى الجندى: شرح قانون العقوبات، دن، سنة 1999، ص76، وايضا راجع: د. هدى حامد قشقوش، مرجع سابق، ص30.

91) ويرجع تاريخ الفصل بين السلطات في آوروبا إلي العصور الوسطى حيث كان ملوكها يتمتعون بصلاحيات واسعة ويحكمون حكما مطلقا، ووصل الاستبداد ذروته في عهد الأمير : لويس الرابع عشر الذي قال مقولته الشهيرة " أنا الدولة"، وكرد فعل لتلك السلطة المطلقة التى يتمتع بها الملوك نادى الكثير من المفكرين في آوروبا بمبدأ الفصل بين السلطات، منهم لوك وجان جاك روسو وغيرهم، راجع في ذلك د. خالد عبد الله الشافي، مرجع سابق، ص102.

ليؤكد عليه[92]، وتضمنته الاتفاقية الأوروبية لحقوق الإنسان الصادرة عام 1950، وكذلك العهد الدولي للحقوق المدنية والسياسية لعام1966[93].

ومن هنا يعد هذا المبدأ من المبادئ الدستورية ذات الطابع العالمي، ويرجع الفضل في ظهوره للنور إلى الفقيه الإيطالي "شيزاري دي بكاريا" صاحب الكتاب الشهير "الجرائم والعقوبات" الذي أصدره في سنة 1764، وقد جاء فيه أن" القوانين وحدها هي التي تحدد العقوبات التي تقابل الجرائم، ولا يستطيع القاضي أن يوقع سواها".[94]

ويعد مبدأ شرعية الجرائم والعقوبات أحد تطبيقات فكرة الأمن القانوني، فيجب العمل علي استجلاء حقيقته وفحواه ودلالته وماهيته ومداه والضوابط التي تقيده، ووضع الضوابط الصحيحة لتفويض السلطة التنفيذية في بعض جوانب التجريم والعقاب، وعليه لا يجوز توقيع عقوبة إلا بناء على حكم قضائي، ومفهوم الجريمة له تحديد جامع مانع من الناحية القانونية، كما يجب وضع الضوابط التي بموجب تباشر الرقابة على دستورية النص الجنائي.[95]

ذلك ان استقرار مبدأ شرعية الجرائم والعقوبات في مفاهيم الدول المتحضرة، دعا إلى توكيده، ومن ثم وجد صداه في العديد من المواثيق الدولية، من أهمها الغصن 11 من الإعلان العالمي

---

92) الإعلان العالمي لحقوق الإنسان – اعتمد ونشر على الملأ بموجب قرار الجمعية العامة للأمم المتحدة 217 –المؤرخ في 10 ديسمبر 1948.

93) اعتمد العهد الدولي الخاص بالحقوق المدنية والسياسية وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف (د–21) المؤرخ في 16 ديسمبر1966 ، تاريخ بدء النفاذ : 23 مارس 1976، وفقا لأحكام المادة 49.

94) راجع في ذلك: د. أحمد فتحى سرور: القانون الجنائي الدستورى، دار الشروق، ط2، سنة 2002، ص31، وايضا راجع: د. هدى حامد قشقوش: شرح قانون العقوبات، دار النهضة العربية، سنة 2010، ص30، 31.
وكذلك راجع:
J.P.Delms saint hilair: un probleme qui évolue, le principe de la léqali –té en matiére d'attante á la liberté de l'ass.inter.de droit penal-bordeaux 1984.p12.etss.

95) راجع في تفاصيل ذلك: دور المحكمة الدستورية في إرساء مبدأ الشرعية الجنائية، مشار اليه في د. محمود علي أحمد مدنى، مرجع سابق، ص348، وما بعدها.

لحقوق الإنسان، والغصن الأولي من المادة 15 من العهد الدولي للحقوق المدنية والسياسية[96]، وأيضا المادة 7 من الاتفاقية الأوروبية لحماية حقوق الإنسان كما تردد في العديد من الدساتير، "فغدا أصلا ثابتا وضمانة ضد التحكم، فلا يؤثم القاضي أفعالاً ينتقيها ولا يقرر عقوباتها وفق اختياره، إشباعا لنزوة أو انفلاتا عن الحق والعدل، وصار التأثيم بالتالي – وبعد زوال السلطة المنفردة – عائدا إلى المشرع وحده[97]، إذ يقرر للجرائم التي يحدثها عقوباتها التي يجرمها، ويفسر هذا المبدأ بأن القيم الجوهرية التي يصدر القانون الجنائي لحمايتها، لا يمكن بلورتها إلا من خلال السلطة التشريعية التي انتخبها المواطنون لتمثيلهم، وأن تعبيرها عن إرادتهم يقتضي أن تكون بيد سلطة التقرير في شأن تحديد الأفعال التي لا يجوز تأثيمها وعقوبتها لضمان مشروعيته، ومن ثم كان المبدأ لازما لتمكين المواطنين من الاتصال بتلك القيم التي يقوم عليها بنيان مجتمعهم، بما يوحد بينهم ويكفل تماسكهم اجتماعيا فلا يزدرونها".[98]

ولأن" السياسة الجنائية الرشيدة يتعين أن تقوم علي عناصر متجانسة، فإن قامت علي عناصر متنافرة، نجم عن ذلك افتقاد الصلة بين النصوص ومراميها، بحيث لا تكون مؤدية إلى تحقيق الغاية المقصودة منها لانعدام الرابطة المنطقية بينهما، إيمانا بأن الأصل في النصوص التشريعية – في الدولة القانونية – هو ارتباطها عقلا بأهدافها، باعتبار أن أي تنظيم تشريعي ليس مقصودا لذاته، وإنما هو مجرد وسيلة لتحقيق تلك الأهداف.

ومن ثم يتعين دائما استظهار ما إذا كان النص المطعون عليه يلتزم إطار منطقيا للدائرة التي يعمل فيها، كافلا تناغم الأغراض التي يستهدفها أو متناقضا مع مقاصده أو مجاوزا لها مناهضا – بالتالي لمبدأ خضوع الدولة للقانون".[99]

---

96) اعتمد العهد الدولي الخاص بالحقوق المدنية والسياسية وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف (د–21) المؤرخ في 16 ديسمبر 1966 ، تاريخ بدء النفاذ : 23 مارس 1976، وفقا لأحكام المادة 49.

97) راجع في ذلك: د. عبد الأحد جمال الدين – النظرية العامة للجريمة – طبعة 1995– 1996 – ص 141.

98) راجع في ذلك: حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري جلسة 1997/2/22.

99) راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 114 لسنة 21 قضاء دستوري جلسة 2001/6/2.

كما ان" العدالة الجنائية في جوهر ملامحها، هي التي يتعين ضمانها من خلال قواعد محددة تحديدا دقيقاً، ومنصفا، يتقرر على صونها ما إذا كان المتهم مدانا أو بريئا، ويفترض ذلك توازنا بين مصلحة الجماعة في استقرار أمنها، ومصلحة المتهم هي ألا تفرض عليه عقوبة ليس لها من صلة بفعل أتاه، أو تفتقر هذه الصلة إلى دليل يؤكدها، ولا يجوز النزول عنها أو التفريط فيها". (100)

وعلى ذلك، بأن" النطاق الحقيقي لمبدأ شرعية الجرائم والعقوبات، إنما يتحدد علي ضوء ضمانتين تكفلان الأغراض التي توخاها:

- **أولهما:** أن تصاغ النصوص العقابية بطريقة واضحة محددة لا خفاء فيها أو غموض، فلا تكون هذه النصوص شباكاً أو شراكاً يلقيها المشرع متصيدا باتساعها أو بخفائها من يقعون تحتها أو يخطئون مواقعها، وهي بعد ضمان غايتها أن يكون المخاطبون بالنصوص العقابية على بينة من حقيقتها، فلا يكون سلوكهم مجافٍ لها بل متسقا معها .

وثانيهما: ومفترضها أن المرحلة الزمنية التى تقع بين دخول القانون الجنائي حيز التنفيذ وإلغاء هذا القانون، إنما تمثل تلك الفترة التى كان يحيا خلالها، فلا يطبق على أفعال أتاها جناتها قبل نفاذه، بل يتعين أن يكون هذا القانون سابقا عليها فلا يكون رجعيا".[101]

وترتيبا على ذلك كله، لا يجوز إعمال نصوص عقابية يسيء تطبيقها إلى مركز قائم لمتهم، ولا تفسيرها بما يخرجها عن معناها أو مقاصدها، ولا مد نطاق التجريم – وبطريق القياس– إلى أفعال لم يؤثمها القاضي من بينها ما يكون أكثر ضمانا للحرية الشخصية في إطار علاقة منطقية يقيمها بين هذه النصوص وإرادة المشرع، سواء في ذلك تلك التي أعلنتها، أو التي يمكن افتراضها عقلاً".[102]

وعلى ذلك، يجب لزاما بيان مبررات مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني في المطلب الأول، ثم نعرض لنتائج مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني في المطلب

---

(100) راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 49 لسنة 17 قضاء دستوري جلسة 15/6/1996.

(101) راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري جلسة 22/2/1997.

(102) راجع حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري جلسة 22/2/1997، وايض، حكم المحكمة الدستورية العليا المصرية في القضية رقم 58 لسنة 18 قضاء دستوري جلسة 5/7/1997.

الثاني، على ان يختتم هذا المبحث ببيان الوضع التشريعي لجرائم الابتزاز الالكتروني في مصر في المطلب الثالث والاخير، وذلك على الترتيب التالي:

- **المطلب الأولً:** مبررات مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني.
- **المطلب الثانيً:** نتائج مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني.
- **المطلب الثالث:** الوضع التشريعي لجرائم الابتزاز الالكتروني في مصر.

المطلب الأولً

مبررات مبدأ الشرعية الجنائية لجرائم الابتزاز الالكتروني

من المقرر ان هناك عدة مبررات ونتائج طرحها الفقه للتأكيد على أهمية وضرورات مبدأ الشرعية الجنائية للجريمة بصفة عامة، ولجرائم الابتزاز الالكتروني بصفة خاصة، ويمكن حصرها في الآتي:

أولا : تحقيق مبدأ العدالة:

ذلك ان احترام الذات الإنسانية، يتطلب حصر الأفعال غير المشروعة الكترونيا ومعلوماتيا حصرا مانعا جامعا في صورة جرائم الابتزاز الالكتروني، وأن تتحدد تحديدا دقيقا العقوبات التى عن طريقها يواجه الشارع هذه الجرائم وأن يتم إعلام المجتمع جميعا بهذه الجرائم والعقوبات.

ثانيا : تحقيق مبدأ الفصل بين السلطات:

ذلك ان هناك سلطة ممثلة من الشعب تتولى وضع نصوص التجريم والعقاب بالنسبة لجرائم الابتزاز الالكتروني، وهناك سلطة قضائية تتولى تطبيق هذه النصوص، ثم هناك سلطة تنفيذية تتولى تنفيذ ما يصدر عن السلطة القضائية من أحكام في هذا الشأن.

ثالثا: تحقيق مبدأ الردع والزجر العقابي:

ويتحقق ذلك عن طريق إعلام المخاطبين بالقانون بنصوص التجريم والعقاب المقررة لجرائم الابتزاز الالكتروني ومضمونها والعقوبات المقررة لها، مما يؤدي إلي إحجامهم عن إرتكاب الجريمة خشية القضاء بموجب احكاما قضائية عليهم بهذه العقوبة، كما يؤدي باقتناع مرتكب جرائم الابتزاز الالكتروني بالعقوبة المطبقة عليه.

رابعا : تحقيق مبدأ المساواه في العقاب:

حيث ان النصوص الخاصة بالتجريم والعقاب لجرائم الابتزاز الالكتروني يجب ان تصاغ بشكل عام ومجرد بحيث تطبق على الكافة، بل وعلى جميع الوقائع دون تمييز، وهذا يؤدى إلى

تحقيق المساواة بين الأفراد أمام القانون فلا يختلف تطبيق القانون على حسب الوضع الاجتماعي أو صفة الجاني.[103]

المطلب الثاني

نتائج مبدأ الشرعية الجنائية لجرائم

الابتزاز الالكتروني

تظهر وتتجلى نتائج مبدأ الشرعية الجنائية، من انه لا جريمة ولا عقوبة الا بناءا على نص قانوني[104]، من جوانب عدة، سواء بالنسبة إلى المشرع الجنائي الذي يختص بسن القوانين والتشريعات المنظمة[105]، أو بالنسبة إلى القاضي الذي يتولى تطبيق تلك القوانين، او بالنسبة إلى السلطة التنفيذية التي يعهد إليها بمهمة تنفيذ ما يصدر من أحكام قضائية.

أولا: بالنسبة للمشرع:

حيث تختص السلطة التشريعية وحدها بمهمة التشريع الجنائي لجرائم الابتزاز الالكتروني، وتلتزم عند وضعها للنصوص الجنائية ألا تتعسف في استعمال حقها في التجريم، بحيث لا يجرم المشرع إلا الأفعال الالكترونية التي تمثل اعتداء على المصالح الأساسية للأمة، وإن كان من الصعب تحديد المصالح الأساسية للأمة التي يقوم عليها بنيان المجتمع، إلا أنه يكفي في هذا السياق ألا يقوم المشرع الجنائي بحماية مصالح لا تشكل قيمة لدى المجتمع أو لدى أغلب أفراده.[106]

كما يلتزم المشرع بالنص على عدم سريان نصوص تجريم جرائم الابتزاز الالكتروني على الوقائع الحادثة قبل صدور نصوص التجريم، بل يقتصر سريانها على المستقبل وهو ما يمكن أن يعبر عنه بمبدأ عدم رجعية النصوص الجنائية لجرائم الابتزاز الالكتروني، كما يجب على المشرع

---

103) راجع في ذلك: د. إبراهيم حامد طنطاوى، د. علي محمود حمودة: شرح الأحكام العامة لقانون العقوبات الجزء الأول النظرية العامة للجريمة، دار النهضة العربية، سنة 2008، ص17، 18.

104) راجع في ذلك: د. السعيد مصطفي السعيد – الاحكام العامة في قانون العقوبات – دار المعارف – الطبعة الرابعة – سنة 1962 – ص 50.

105) راجع في ذلك: د. عبد الأحد جمال الدين – النظرية العامة للجريمة – طبعة 1995– 1996 – ص 141.

106) راجع في ذلك: د. عمر سالم، مرجع سابق، ص35، 36.

الجنائي التزام الوضوح التام في النصوص الجنائية[107]، فلا يجوز أن يلجأ عند إقراره لنصوص التجريم المعلوماتي إلى أسلوب "النماذج المفتوحة" باستخدام عبارات غامضة أو تحمل عدة أوجه.[108]

- ثانيا: بالنسبة للقاضي:

حيث يلتزم القاضي بتطبيق النص الجنائي المتعلق بجرائم الابتزاز الالكتروني، دون تعديل بالإضافة أو بالحذف سواء بالنسبة لشق التجريم أو العقاب، فيجب عليه ابتداءا أن يحدد ما إذا كانت الواقعة تندرج تحت أحد النماذج الإجرامية التي قررها المشرع أم لا، فإذا لم يثبت ذلك وجب الحكم ببراءة المتهم، أما إذا كانت الواقعة مجرمة وجب عليه أن يضع لها التكييف القانوني السليم.

- ثالثا: بالنسبة للسلطة التنفيذية:

حيث تلتزم الجهات القائمة على التنفيذ العقابي بتنفيذ الحكم بذات الأوضاع التي نص عليها القانون، وبالتالي فإن الإدارة لا تستطيع أن تنفذ عقوبة لم يقض بها حكم قضائي أو أن تحل نفسها محل القضاء في تطبيق العقوبة، أو أن تظل تنفذ العقوبة على خلاف مقتضى الحكم القضائي.[109]

المبحث الثالث

دور القاضي الجنائي في ظل غياب النص العقابي لجرائم الابتزاز الالكتروني في التشريعات المقارنة

تمهيد وتقسيم:

نظرا لعدم وجود نظام قانوني متكامل خاص بجرائم الابتزاز الالكتروني في غالبية التشريعات المقارنة، يوضح ويصف بدقة جرائم الابتزاز الالكتروني، محددا أنواع هذه الجرائم والأشكال التي تتخذها، والركن المادي والمعنوي للجريمة بنصوص تتسم بالتحديد مع السماح بأن يدرج تحتها كل ما هو جديد في عالم جرائم الابتزاز الالكتروني، مع تحديد دقيق للعقوبة بحديها الأعلى والأدنى كعقوبة أصلية وغيرها من العقوبات التكميلية والتبعية، وبما لا يخل بمبدأ الشرعية الجنائية كمبدأ دستوري

---

(107) راجع في ذلك: د.هدى حامد قشقوش، مرجع سابق، ص35، 36.

(108) انظر في ذلك:

BERNA RDINI(R.),Droit Pénal general, Paris,2003, No193, p171.

(109) راجع في ذلك: د. عمر سالم، مرجع سابق، ص39، وما بعدها.

حاكم في كافة التشريعات المقارنة، حيث أن جرائم الابتزاز الالكتروني تتطور بشكل مذهل نظرا لتطور الأجهزة الالكترونية، مما يوجد شبه استحالة في مواكبة ذلك التطور بتشريعات تجرمها.

وهنا تكمن صعوبة وضع تشريع جامع لكل صور جرائم الابتزاز الالكتروني، مانعا أمام المشرع مرة أخرى من التدخل لتعديل التشريع بإضافة أشكال جديدة للتجريم[110].

وفي ظل غياب التشريع سيجد القاضي نفسه مضطرا للحكم بالبراءة على مرتكبي وقائع الكترونية عبر جرائم الابتزاز الالكتروني، سواء ضد الدولة أو ضد مواطنيها، وذلك تطبيقا لمبدأ المشروعية، وعندئذ ستتفشي جرائم الابتزاز الالكتروني وتدمر مصالح كثيرة سواء للدولة أو لمواطنيها.

والسؤال المطروح هنا: هل يسكت القاضي عن ذلك وينتظر السلطة التشريعية، أم يجتهد حماية للمصلحة العليا للبلاد؟

ترتيبا على ذلك، يتعين أن نتناول دور القاضي في مواجهة النقص التشريعي لمواجهة جرائم الابتزاز الالكتروني في التشريعات المقارنة، في المطلب الأول، ثم التعرض الى التفسير القضائي للنص الجنائي التقليدي لتطبيقه علي جرائم الابتزاز الالكتروني في المطلب الثاني، على ان يتناول المطلب الثالث التفسير القضائي للنص الجنائي بشأن جرائم الابتزاز الالكتروني، وذلك على الترتيب التالي :

- **المطلب الأول:** دور القاضي في مواجهة النقص التشريعي لمواجهة جرائم الابتزاز الالكتروني في التشريعات المقارنة.
- **المطلب الثاني:** التفسير القضائي للنص الجنائي التقليدي لتطبيقه علي جرائم الابتزاز الالكتروني.
- **المطلب الثالث:** التفسير القضائي للنص الجنائي بشأن جرائم الابتزاز الالكتروني.

المطلب الأول

دور القاضي في مواجهة النقص التشريعي لمواجهة جرائم الابتزاز الالكتروني في التشريع المقارن

) راجع في ذلك: د. عبد الأحد جمال الدين – النظرية العامة للجريمة – طبعة 1995– 1996 – ص 110(141.

ازاء النقص التشريعي لجرائم الابتزاز الالكتروني، وبالنظر الى الفراغ التشريعي لعدم تنظيم تلك النوعية من الجرائم، ليس أمام القاضي الآن إلا أن يطبق النصوص القانونية التقليدية الواردة في قانون العقوبات أو أية قوانين خاصة أخرى معمولا بها على بعض جرائم الابتزاز الالكتروني في حالة عدم تعارضها مع هذه النصوص وإمكانية تطبيقها عليها، وذلك حتى لا يفلت الجناة من العدالة، وهو ما قد يمس مبدأ شرعية الجرائم خصوصا في جرائم الابتزاز الالكتروني التي تأبى طبيعتها الخضوع للنصوص التقليدية[111]، وقد انقسم الفقه في هذا الصدد ما بين مؤيد لفكرة تطبيق النص التقليدي على جريمة الابتزاز الالكتروني ومعارض لذلك.

وجدير بالذكر هنا انه جرى الاعتماد علي ما انتهت إليه محكمتي النقض المصرية والفرنسية في أحكامها عندما ظهرت جريمة سرقة التيار الكهربائي باعتبارها تقع على مال غير ملموس مع عدم وجود نصوص قانونية تجرمها فقام القضاء بتطبيق نصوص السرقة التقليدية، واعتبرت محكمتا النقض أن التيار يمر في أسلاك وتوصيلات ذات كيان مادي، وبالتالي يمكن اختلاسه وانطباق نص السرقة عليه، وكذلك سرقة المكالمات التليفونية وإن لم يكن ماديا وملموسا ولكنه رغم ذلك قابل للحيازة والانتقال.[112]

وعلى الصعيد المقابل، فيرى البعض من الفقه، أن القضاء في الحالتين السابقتين قد توسعا في تطبيق النصوص القانونية وفي تفسيرهما لمعنى الاختلاس المكون لجريمة السرقة، وهو ما لا يمكن تصوره بالنسبة للجرائم المستحدثة ومنها جرائم الابتزاز الالكتروني، لأن السرقة تفترض انتقال الحيازة من مالكها إلي السارق وهو ما لم يحدث في الحالة محل البحث، بل ينحصر في أغلب

---

111) وهو ما يعد أحد أوجه النقد التى وجهت لمبدأ الشرعية الجنائية، حيث قيل من قبل بعض الفقه أن هذا المبدأ يقف عقبة في سبيل تطور المجتمع ورقيه، لأن المشرع عندما يضع نصوص التجريم والعقاب فإنما يضعها لكي تحمى المصالح والحقوق التى تكون قائمة وقت التشريع وإذا كانت هذه المصالح بحكم طبيعتها قابلة للتطور قد يكون هذا التطور عن أفعال تمثل خطرا عليها، مما يؤدي إلي عدم خضوع الكثير من الأفعال الضارة بمصالح المجتمع للعقاب لعدم وجود نص يجرمها ويعاقب عليها، ولعل ذلك ما يجعل المشرع يستخدم عند وضعه لنصوص التجريم والعقاب عبارات ذات أفكار قانونية عامة بحيث يمكن عن طريق تفسيرها التفسير السليم تحقيق التوازن بين المحافظة علي مبدأ الشرعية وبين الحاجة إلي تمكين القاضي من حماية المجتمع إزاء الأفعال الضارة التى تهدد مصالحه، راجع في ذلك: د. إبراهيم حامد طنطاوى، وايضا راجع: د. علي محمود حمودة، مرجع سابق، ص21.

112) راجع في ذلك: أ. شمسان ناجى صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت – دراسة مقارنة، دار النهضة العربية، سنة 2009، ص47، وما بعدها.

الأحوال في الحصول على منفعة الشيء فقط دون أصله الذي يبقي في حيازة صاحبه، ولا صعوبة في القول بأننا هنا بصدد سرقة منفعة، والتي تحتاج إلى نص خاص صريح.

وهو ما يتضح من رفض القضاء، تطبيق نصوص السرقة على من يتناول طعاما أو شرابا في محل معد لذلك ثم يمتنع دون مبرر عن دفع الثمن أو يفر دون الوفاء به، وذلك لتحقق التسليم النافي للاختلاس من جانب صاحب العمل.

الأمر الذي اقتضي من المشرع بأن يتدخل للنص على تجريم الفعل في المادة (324 مكرر) من قانون العقوبات المصري، وكذلك بالنسبة لمن يستولي على سيارة مملوكة للغير دون نية تملكها، فلم يستطع القضاء تطبيق نص السرقة على الفعل، نظرا لأن الفاعل وإن كان قد استولى على حيازة المال بغير رضا صاحبه إلا أن نية التملك لم تكن متوافرة لديه، وقد تدخل المشرع مؤخرا لتجريم ذلك الفعل بالمادة (323) مكرر من قانون العقوبات المصري، وغير ذلك الكثير[113]

وهو ما دعا اغلب المشرعين في عدد من الدول بالتدخل، وإصدار قانون يتعلق بالجرائم المعلوماتية، منهم المشرع الأمريكي الذي أصدر قانونه عام 1986، أما المشرع الفرنسي فقد أدمج فصلا في قانون العقوبات الفرنسي يتحدث عن بعض الجرائم المعلوماتية وذلك في 1994/3/1، وفي بلجيكا صدر قانون مكافحة الإجرام المعلوماتي في 2001/2/3، أما الاتحاد الأوروبي فقد حرص على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات وذلك في اتفاقية بودابست الموقعة في 2001/11/23 المتعلقة بالإجرام الكوني "الجرائم المعلوماتية".[114]

المطلب الثاني

التفسير القضائي للنص الجنائي التقليدي لتطبيقه

علي جرائم الابتزاز الالكتروني

بالنظر الى عدم وجود قانون موضوعي ينظم الإجرام المعلوماتي في بعض التشريعات المقارنة، فليس أمام القاضي في تلك البلاد إلا تفسير النص الجنائي "التفسير القضائي للنص الجنائي" في معرض الفصل في دعوى معينة للتعرف على قصد المشرع بغية التوصل إلى تطبيق النص على الواقعة المطروحة أمامه أو عدم تطبيقه.[115]

أولا: مفهوم التفسير القضائي للنصوص الجنائية:

) راجع في ذلك: د. عبد العظيم مرسي وزير، مرجع سابق، ص35، 113.36(

) راجع في ذلك: أ. شمسان ناجى صالح الخيلي، مرجع سابق، ص56، وما بعدها. 114(

) راجع في ذلك: د. عبد العظيم مرسي وزير، مرجع سابق، ص115.54(

اختلف الفقهاء في إعطاء تعريف موحد للتفسير بحسب اختلاف نظرة كل واحد منهم له، فهناك من نظر إليه نظرة موضوعية وبالتالي غلب على تعريفه الطابع الموضوعي، ومنهم من عرفه على أساس الهدف منه أو الغاية، وهناك من عرفه من منطلق لغوي بحت، ومنهم من ركز على الوظائف التي يؤديها التفسير، ومنهم من ربط بين أكثر من عامل من هذه العوامل لإعطاء تعريف للتفسير.

وبصفة عامة، يقصد بالتفسير القضائي "عملية ذهنية تهدف إلى تحديد المعنى الذي يقصده واضع القانون من ألفاظ القاعدة القانونية لجعلها صالحة التطبيق على وقائع الحياة"[116]، كما عرّف أيضاً بأنه" إعطاء المعنى الحقيقي للنصوص الغامضة سواء أكان هذا الغموض ناتجاً عن نقص موجود في النصوص إما بسبب عدم التناسب والتناسق بين الألفاظ أو لكونها ألفاظاً غريبة، أم ناتجاً عن خلل في البناء المنطقي أو في العبارات المستعملة، نتيجة لطابع أو أسلوب اللغة المستخدم، أو نتيجة للأخطاء المطبعية"، هذا وقد عرّف أيضاً بأنه " البحث والتحري بهدف إيجاد المعنى الصحيح للقاعدة القانونية لتطبيقها بعد ذلك على الحالة الواقعية، أو الاستدلال على الحكم القانوني وعلى الحالة النموذجية التي وضع لها هذا الحكم من واقع الألفاظ التي عبر بها المشرع عن ذلك"[117]، وكذلك عرّف بأنه" بيان المعنى المقصود للمشرع من المادة القانونية الواردة في هذا القانون فكل مادة قانونية أوردها المشرع قصد بها معنى، والتفسير هو بيان لذلك المعنى المقصود للمشرع، وتفسير النص لا يكون إلا بعد فهمه، فالفهم عملية عقلية يتوصل من خلالها إلي التفسير". [118]

ثانيا: الطبيعة القانونية للتفسير القضائي للنصوص الجنائية:

حيث يتنازع الكشف عن طبيعة التفسير في هذا الصدد، مذهبان:

- **المذهب التقليدي:** والذي يذهب إلى أن التفسير يقف عند معرفة القاضي لإرادة المشرع التي يعبر عنها في القاعدة القانونية دون أن يخرج عن هذه الإرادة لتكملة أي نقص قد يبدو فيها.

---

116) راجع في ذلك: د. حسنى الجندي، شرح قانون العقوبات، دن، سنة 1999، ص 96.

117) انظر في ذلك: أ. عثامنية لخميسي: التفسير في المادة الجزائية وأثره علي حركة التشريع، مجلة العلوم الإنسانية، جامعة محمد خضيرة بسكره، العدد السابع، فبراير 2005، ص3، بحث متاح علي شبكة الإنترنت علي موقع:
http://www.webreview.dz/IMG/pdf/20_L_explication_en_matiere_penale_Aathamnia2.pdf

118) راجع في ذلك: د. عبد المهدى "محمد سعيد" أحمد العجلونى: قواعد تفسير النصوص وتطبيقاتها في الاجتهاد القضائي الأردني دراسة أصولية مقارنة، رسالة دكتوراه، كلية الدراسات العليا، الجامعة الأردنية، سنة 2005، ص58.

- **المذهب الواقعي:** الذي يذهب إلى أن المشرع عندما يضع القواعد القانونية إنما يضعها بصورة عامة مجردة، ويترك للقاضي سلطة تحديد هذه العمومية لكي يتمكن من تطبيق هذه القواعد على الواقعة المجردة والمحددة التي يفصل فيها، لذلك يذهب هذا المذهب إلى أن التفسير لا يعنى مجرد الوصول إلى إرادة المشرع، وإنما هو عملية قد تكمل النقص الذي قد يصيب بعض القواعد الجنائية، فالقاضي يجب أن يتمتع بدور إيجابي في فهم النص أثناء تطبيقه بحيث يستطيع أن يكمل أوجه النقص في النص الذي يطبقه دون أن يرقي ذلك إلى تكملته بإنشاء قاعدة عقابية جديدة، لأنه لو فعل يكون بفعله هذا هادما لمبدأ شرعية الجرائم والعقوبات.[119]

ثالثا: وسائل القاضي الجنائي في تفسير النص العقابي:

تتعدد وسائل التفسير التي يمكن للقاضي استخدامها في فهم مدلول النص الجنائي المطلوب تطبيقه على الوقائع المعروضة عليه ليطبقه تطبيقا سليما، وهذه الوسائل تتمثل في الآتي:

1) **التفسير واللغوي للنص الجنائي:** وذلك من خلال فهم القاضي لمدلول المصطلح أو التعبير المستخدم من المشرع في نص التجريم والعقاب وفقا لمعناه اللغوي، ولعل هذا التفسير هو ما ينبغي على المفسر أن يلجأ إليه كأول خطوة من خطوات التفسير، والعملية الفنية لهذا التفسير اللغوي تعتمد علي الوصول إلى معاني ألفاظ النص القانوني وتحديد مدلولاته اللغوية، وفي الحالات التي يعطي فيها المشرع بعض ألفاظ النص مدلولا اصطلاحيا خاصا، فيجب على المفسر هنا أن يبحث في اللغة القانونية عن هذا المدلول.
2) **التفسير المنطقي للنص الجنائي:** ويسمي البعض هذه الطريقة بطريقة التفسير الغائي باعتبارها تهدف إلى البحث عن الغاية من وضع النص، وهي تستعمل للوصول إلى تلك الغاية.

ويعتمد هذا النوع من التفسير على البحث عن مقصود الشارع من الألفاظ والعبارات التي يستخدمها في نصوص التجريم والعقاب، ولذلك فإنه لا يقف عند عبارات ومعاني النص القانوني محل التفسير، وإنما يمكن للمفسر أن يستعين في عمله هذا بالمصادر التاريخية للنص، وإجراء مقارنة بين النص الذي يفسره بغيره من النصوص.

كما يمكن كذلك الرجوع إلى الأعمال التحضيرية التي ولد من خلالها هذا النص، سواء أكانت مذكرات إيضاحية أم مناقشات برلمانية، أو محاضر لجان تشريعية أسهمت في وضعه،

) انظر في ذلك: د. إبراهيم حامد طنطاوى، د. علي محمود حمودة، مرجع سابق، ص33، 34، وايضا راجع: 119(أ. عثامنية لخميسي، مرجع سابق، ص8، وما بعدها.

وكذلك المصالح والاعتبارات الاجتماعية والسياسية والاقتصادية والأخلاقية التي دعت إليه وهو ما يطلق عليه "بروح التشريع"، وروح التشريع تعني تحديد معنى النص إذ يفسر التشريع على ضوء الغاية منه أو حكمته.

وههنا تظهر بجلاء، اهمية إدراك الحكمة التشريعية من النص، فتعرف المصالح التي يراد من خلاله حمايتها، والمساوئ التي يهدف إلى قطع السبيل عليها، والغاية السياسية والاجتماعية والاقتصادية والأخلاقية التي يرمي إلى تحقيقها، ولعل أهم طريقة يمكن أن يتم بها هذا النوع من التفسير تلك التي تتعلق بالوصول إلى علة النص.

فالمشرع يضع النص ليحقق من ورائه علة معينة، كحماية الحقوق والمصالح التي تقدر جدارتها بالحماية الجنائية، ولذلك فإنه إذا تمكن القاضي من تحديد الحق الذي يريد المشرع حمايته من وراء نص التجريم والعقاب، استطاع تحديد أركان الجريمة التي يراد بالعقاب على ارتكابها حماية هذا الحق.[120]

رابعا: أهمية التفسير القضائي للنصوص الجنائية:

وترجع أهمية التفسير القضائي للنصوص الجنائية إلى سببين جوهريين:

- **السبب الأول:** أن وضوح القاعدة أو النص من عدمه هو أمر نسبي يختلف من شخص لآخر، فما يكون واضحا بالنسبة لشخص قد لا يكون كذلك بالنسبة لآخر.
- **السبب الثاني:** أن المعنى الظاهر من القاعدة ليس بالضرورة هو المعنى الذي يرمى إليه النص، وإن الاكتفاء أحيانا بالمعنى الظاهر يؤدي إلى الفهم الخاطئ له[121]، والقاضي في هذه الحالة عندما يفسر القانون لا يعطى رأيه الشخصي ولكنه يبحث عن المعنى الحقيقي للقانون، وعن قيمته الموضوعية كما أرادها المشرع التي ضمنها النص والتي ليست مبدأ جامداً محكوم بالوقائع الاجتماعية المتوافرة وقت وضع النص، بل هي إرادة متغيرة تتطور بتطور هذه الوقائع الاجتماعية طالما أنها تراعى المصلحة الاجتماعية المحمية بالنص، ذلك أن هذه المصلحة تبلور إرادة المشرع، وتحدد تبعا لها نطاق تطبيق نصوصه، فلم يصنع القانون من أجل اليوم فقط بل إنه صنع من أجل المستقبل، وإرادة القانون بهذا المعنى تترك للتفسير مهمة تحديد معنى النصوص القانونية المجردة في ضوء التحولات والتغيرات الاجتماعية، وبتطبيق ذلك المنهج نجد أنه يقدم الحلول الصحيحة، خاصة عندما يعبر القانون

) راجع في ذلك: د. إبراهيم حامد طنطاوى، د. علي محمود حمودة، مرجع سابق، ص35، 120.36(

) راجع في ذلك: د. حسنى الجندى، مرجع سابق، ص 121.96(

عن فكرة متحركة متطورة بحسب طبيعتها مثل النظام العام أو الأدب العامة، وكذلك الشأن لمواجهة الاختراعات العلمية التي تصلح محلا أو أداة للجريمة مثل الطاقة الكهربائية كمحل للسرقة والراديو والتليفزيون كوسيلة للعلانية في جرائم النشر.[122]

خامسا: أنواع التفسير القضائي للنص الجنائي:

هناك ثلاثة أنواع من التفسير القضائي للنص الجنائي:

- **النوع الأول وهو تفسير مقرر:** يقصد به أن يصل القاضي إلى فهم النص القانوني من مدلوله الظاهر.
- **والنوع الثاني وهو تفسير ضيق:** ويقصد به أن النص العقابي يفيد في ظاهره أكثر مما أراده منه المشرع فيقيد القاضي الظاهر.
- **والنوع الثالث وهو تفسير موسع:** وهو الذي يهمنا في الحالة محل الدراسة، وذلك عندما تكون عبارات النص تفيد في ظاهرها أقل مما أراده الشارع، فيلزم للمفسر أن يوسع هذا الظاهر ويمد تطبيقه إلى ما أريد به في حقيقة الأمر، وبغير ذلك التفسير يصبح القانون عاجزا عن مواجهة الظروف الجديدة، بل أنه يصبح عاجزا عن حماية المجتمع في الظروف التي وضع فيها، نظرا لأنه يصعب إن لم يتعذر بالفعل أن يجري المشرع حصرا أو إشارة إلى كل الحالات الضارة بالمجتمع.[123]

سادسا: الضوابط القانونية المفروضة علي القاضي الجنائي عند تصديه لتفسير النص العقابي:

هناك عدد من الضوابط تحكم عمل القاضي الجنائي عند تفسيره للنصوص العقابية والتي تتمثل في:

1) يجب علي القاضي الجنائي عند تفسيره للنص العقابي التزام جانب الدقة وعدم تحميل عبارات النص فوق ما تحتمل، فيما يسمى "التفسير المنضبط للنصوص العقابية" فلا يجوز له في حالة إذا كانت عبارات النص واضحة أن يبحث عن علة التجريم، ليوسع من نطاق التطبيق، والتفسير المنضبط لقانون العقوبات لا يحول بالطبع دون محاولة تطويع النصوص لتحيط بالمعطيات التكنولوجية الحديثة وخاصة في مجال ثورة المعلومات، ولكن

---

(122) راجع في ذلك: د. أحمد فتحى سرور، مرجع سابق، ص95، وما بعدها.

(123) راجع في ذلك: د. عبد العظيم مرسي وزير، مرجع سابق، ص58، وما بعدها، د. حسنى الجندى، مرجع سابق، ص98.

على القاضي إذا اتضح أن الأمر قد تجاوز حدود التفسير المنضبط إلى حد خلق جرائم جديدة، وجب عليه الحكم بالبراءة تاركا الأمر لتدخل تشريعي.

2) يلتزم القاضي بإستخدام قاعدة "الاستغراق" وهى تعني أن هناك نصين في التشريع العقابي كل منهما يعاقب على جريمة مستقلة عن الأخرى، ثم يصدر نص عقابي ثالث تالٍ لهما يجعل إحدى الجريمتين المجرمتين بالنصين العقابين السابقين له ظرفا مشددا للأخرى.

3) ففي هذه الحالة يتعين على القاضي استبعاد نصي الجريمتين ويطبق النص الثالث المستغرق لهما والذي يضم الجريمتين في جريمة واحدة مشددة.[124]

ولا يجوز للقاضى أن يستخدم القياس لتفسير النص العقابي، والقياس في مجال التجريم يعني "إلحاق فعل مباح بفعل مجرم لاشتراكهما في علة التجريم"، أي استكمال ما يشوب القانون من نقص عن طريق إيجاد الحل لمسألة لم ينظمها القانون وذلك عن طريق استعارة الحل الذي قرره القانون لمسألة مماثلة.

فالقياس بالتالي ليس وسيلة لاستخلاص إرادة القانون في إطار الصيغة التي استعملها، بل إنه يفترض أن القانون لم ينظم المسألة محل البحث ولم يقدم لها مباشرة الحل الواجب التطبيق[125]،

---

124) راجع في ذلك: د. حسنى الجندى، مرجع سابق، ص99، د. عمر سالم، مرجع سابق، ص63، وما بعدها، ومثال لذلك المادة 318 من قانون العقوبات، حيث جاء نصها" يعاقب علي جريمة انتهاك ملك الغير في المادة 370 من ذات القانون، ثم جاء نص المادة 317 لينص علي السرقة من محل مسكون باعتبارها سرقة مشددة، وفي هذه الحالة يكون نص المادة 317 قد استغرق نصي المادتين 318، 370 ويلزم تطبيقه.

125) راجع في ذلك: د. أحمد فتحى سرور، مرجع سابق، ص101، وما بعدها، د. عمر سالم، مرجع سابق، ص59. وان الاجتهاد القضائي يبنى كقاعدة عامة مبدأ التفسير الضيق للنصوص العقابية الموضوعية، وهناك العديد من الأحكام القضائية التي أكدت هذا التوجه بالنص على أن النصوص الجنائية تفسر تفسيرا صارما والقضاة لا يستطيعوا في هذا المجال التفسير الواسع أو المنطقي، والقانون الجنائي الفرنسي الجديد لسنة 1994 أكد هذا الاجتهاد بالمادة 111/4 التى تنص على "القانون الجنائي يفسر تفسيرا صارماً"، إلا انه من الناحية التطبيقية عرف مبدأ التفسير الصارم للنصوص الجنائية صعوبات تختلف باختلاف طبيعة النص فيما إذا كان النص واضحاً أو غامضاً، أما التفسير في القواعد الشكلية على خلاف القواعد الموضوعية يعطي مجال أوسع للقضاة لاعتماد طريقة التفسير المنطقي من منطلق أن البعض يرى أن مبدأ الشرعية يشمل فقط الجرائم والعقوبات ولا يشمل النصوص الإجرائية التي تحكم سير الدعوى العمومية وعليه فان القضاة لا يجب أن يتقيدوا في تفسير النصوص الإجرائية بالطريقة الضيقة أو الصارمة وإنما يمكنهم اعتماد أسلوب المنطق في التفسير أي اعتماد التفسير الواسع شريطة أن لا يؤدي هذا التفسير للنصوص الإجرائية إلى الأضرار بالمتهمين، راجع في ذلك: أ. عثامنية لخميسي، مرجع سابق، ص13، وما بعدها.

والسماح للقاضي بذلك يحوّل القاضي إلى مشرّع يقوم بخلق قاعدة عقابية جديدة لم ينص عليها المشرع الفعلي ولم يفرد لها نصا مكتوبا مما يؤدي إلى هدم مبدأ شرعية الجرائم والعقاب.

وعليه فالقياس محظور في المجال الجنائي سواء كان كليا أو جزئيا، علما بأن صورة القياس الكلي هي انعدام النص، أما القياس الجزئي فصورته أن يكون النص الجنائي ناقصا في تحديد أركان الجريمة أو تعيين العقوبة، فلا يملك القاضي الجنائي أن يكمل هذا النقص عن طريق القياس علي نص آخر.[126]

والتفسير الذي يقوم به قضاة المحاكم غير ملزم لهم إذا ما عرضت عليهم واقعة جديدة تستلزم تطبيق النص، وبالتالي غير ملزم لغيره من القضاة لأنه اجتهاد في فهم معنى نصوص التجريم والعقاب، وقد يختلف هذا الاجتهاد من قاض إلى آخر وفقا لاختلاف ملكات هذا الاجتهاد، أي ما ينعم به الله على البعض من حسن الفهم ونفاذ البصيرة، بل أن هذا التفسير لا يلزم غيره من القضاء،[127]

وقد قرر القانون الفرنسي رقم 2001- 539 والصادر في 25 يوليو 2001 للقاضي الجنائي حق اللجوء إلى محكمة النقض لتحديد معنى نص وجد صعوبة في تفسيره، وفي حالة اتجاه القاضي ذلك، فإنه يلتزم بإخطاره طرفي الدعوى بهذه النية ويوقف نظر الدعوى الى حين وصول رد محكمة النقض، والذي يجب أن يصل خلال ثلاثة أشهر من تاريخ استلام الطلب.

وعلى الرغم من هذا التنظيم القانوني لطلب التفسير في فرنسا وكونه صادرا من محكمة النقض إلا أنه لا يلزم القاضي الجنائي في فرنسا فله أن يخرج عليه.[128]

المطلب الثالث

التفسير القضائي للنص الجنائي بشأن جرائم الابتزاز الالكتروني في التشريعات المقارنة

---

126) راجع في ذلك: د. عبد العظيم مرسي وزير، مرجع سابق، ص63، وما بعدها، وايضا راجع: د. حسنى الجندى، مرجع سابق، ص100، وكذلك راجع: د. إبراهيم حامد طنطاوى، د. علي محمود حمودة، مرجع سابق، ص38، وما بعدها.

127) راجع في ذلك: د. إبراهيم حامد طنطاوى، د. علي محمود حمودة، مرجع سابق، ص35، وايضا راجع: د. عمر سالم، مرجع سابق، ص52، 53.

128) راجع:

DRADEL(J.),Droit penal général ,CuJus,2002-2003,No181,p.175

من الملاحظ ان اغلب التشريعات المقارنة تقوم بإسناد مهمة التفسير القضائي للنصوص الى المحكمة العليا بها، كمحكمة النقض في فرنسا، والمحكمة الدستورية العليا في مصر[129]، على ان اختصاصها بالتفسير مشروط بشرطين هما:

- **الأول:** أن تكون للنص التشريعي المراد تفسيره أهمية جوهرية –لا ثانوية أو عرضية– تتحدد بالنظر إلى طبيعة الحقوق التي ينظمها ووزن المصالح المرتبطة بها.
- **والثاني:** أن يكون هذا النص – فوق أهميته– قد آثار عند تطبيقه خلافا حول مضمونه، بحيث تتباين معه الآثار القانونية التي يرتبها فيما بين المخاطبين بأحكامه، بما يخل عملا بعمومية القاعدة القانونية الصادرة في شأنهم والمتماثلة مراكزهم القانونية بالنسبة إليها، ويهدر بالتالي المساواه بينهم في مجال تطبيقها، وتفسير المحكمة الدستورية، وهكذا يندمج بالنص المطلوب تفسيره ويصبح جزءا لا يتجزأ منه، وبالتالي يصبح التفسير نافذا من تاريخ صدور النص القانوني.[130]

---

(129) حيث ورد نص الدستور المصري الصادر عام 2014 في المادة 192 منه علي أن" تتولى المحكمة الدستورية العليا دون غيرها الرقابة القضائية على دستورية القوانين، واللوائح، وتفسير النصوص التشريعية، والفصل في المنازعات المتعلقة بشئون أعضائها، وفي تنازع الاختصاص بين جهات القضاء، والهيئات ذات الاختصاص القضائي، والفصل في النزاع الذي يقوم بشأن تنفيذ حكمين نهائيين متناقضين صادر أحدهما من أية جهة من جهات القضاء، أو هيئة ذات اختصاص قضائى، والآخر من جهة أخرى منها، والمنازعات المتعلقة بتنفيذ أحكامها، والقرارات الصادرة منها. ويعين القانون الاختصاصات الأخرى للمحكمة، وينظم الإجراءات التى تتبع أمامها"، وقد نصت المادة 26 من قانون المحكمة الدستورية العليا رقم 48 لسنة 1979 بأن" تتولي المحكمة الدستورية العليا تفسير نصوص القوانين الصادرة من السلطة التشريعية والقرارات بقوانين الصادرة من رئيس الجمهورية وفقا لأحكام الدستور وذلك إذا أثارت خلافا في التطبيق وكان لها من الأهمية ما يقتضي توحيد تفسيرها"، وقد نصت المادة 33 من ذات القانون علي أنه" يقدم طلب التفسير من وزير العدل بناء علي طلب رئيس مجلس الوزراء أو رئيس مجلس الشعب أو المجلس الأعلى للهيئات القضائية، ويجب أن يبين في طلب التفسير النص التشريعي المطلوب تفسيره وما أثاره من خلاف في التطبيق ومدى أهميته التي تستدعى تفسيره تحقيقا لوحدة تطبيقه"، وقد نصت المادة 49 من ذات القانون علي أن يصبح هذا التفسير ملزما لجميع سلطات الدولة وللكافة بعد نشره في الجريدة الرسمية".

(130) راجع في ذلك: د. أحمد فتحى سرور، مرجع سابق، ص97، وما بعدها.

إلا أن هذا الاختصاص لا يصادر حق جهات القضاء الأخرى جميعا في تفسير القوانين وإنزال تفسيرها على الواقعة المعروضة عليها ما دام لم يصدر بشأن النص المطروح أمامها تفسير ملزم، سواء من السلطة التشريعية أم من المحكمة المختصة بالتفسير". [131]

وفي النهاية نري أنه يجب على القاضي الجنائي الذي يتصدى للحكم في جرائم الابتزاز الالكتروني، في محاولة منه لتفسير النصوص العقابية التقليدية بما يساعد في إدراج هذه الجرائم تحت عباءة تلك النصوص أن يكون على علم واسع بالتقنيات الحديثة وأنظمة المعلومات.

وإذ تناولت الدراسة جرائم الابتزاز الالكتروني من منظور المبدأ الدستوري المستقر في كل الدول المتحضرة وهو مبدأ الشرعية الجنائية، الذي يقرر أنه لا جريمة ولا عقوبة إلا بنص[132]، ونظرا لحداثة عهد جرائم الابتزاز الالكتروني على مستوى العالم وسرعة تطورها لسرعة تطور التقنيات المستخدمة فيها، والتي تتم عبرها، واجهت بعض الدول المتقدمة ذلك بتشريعات تحدد الجرائم بركنيها المادي والمعنوي والعقوبة، وهي الدول التي ظهرت التكنولوجيا الحديثة المستخدمة في تلك الجرائم في كنفها، وتحت سمعها وبصرها، أما أغلب الدول التى استوردت تلك التكنولوجيا، فلا زالت تتخبط في طريقها، فلم تضع تشريعا جامعا شاملا ينص على كافة صور جرائم الابتزاز الالكتروني الحالية، كما سيسمح في المستقبل بإدراج أي صور جديدة تظهر تحت مظلته، مما يثير التساؤل في تلك الدول: كيف سيتاح لها التعامل مع مرتكب جرائم الابتزاز الالكتروني في ظل غياب النص العقابي الذي يعاقبه صراحة عليها في ظل ما يقتضيه تطبيق المبدأ الدستوري الخاص بالشرعية الجنائية؟

ونرى أنه ليس أمام القاضي سوى إجابتان لهذا التساؤل، إجابة سهلة تكفيه العناء والبحث، وتتمثل في القضاء ببراءة المتهم في جرائم الابتزاز الالكتروني لعدم وجود النص العقابي الذي يجرم فعله، وهذه الإجابة بالطبع سيكون لها أسوء الأثر على المجتمع لأنها بسلبيتها ستساعد على انتشار جرائم الابتزاز الالكتروني في المجتمع كالنار في الهشيم، أما الإجابة الثانية فهي تعني الذهاب بمحض اختياره للعناء والبحث عن حل قضائي لمواجهة المجرم المعلوماتي ومحاكمته وذلك عن طريق محاولة تفسير النصوص التقليدية، بما يسمح له بإدراج الفعل الإجرامي المرتكب من المجرم

---

131) راجع قرار المحكمة الدستورية العليا المصرية في طلب التفسير رقم 1 لسنة 2 قضائية الصادر بتاريخ 1981/1/17.

132) انظر في ذلك: د. السعيد مصطفي السعيد – الاحكام العامة في قانون العقوبات – دار المعارف – الطبعة الرابعة، سنة 1962 – ص 50.

المعلوماتي تحت سلطانها، وهو ما يساعد مؤقتا في مواجهة تلك الجرائم، حتى صدور تشريع ينظم هذه النوعية من الجرائم.

ونري من جانبنا هذا الحل الأخير لكونه الحل المتاح حاليا ولكون تاريخ القضاء الجنائي قد قام بفعل ذلك مسبقا عندما ظهرت جرائم لم ينص عليها قانون العقوبات، حتى تنبه المشرع ونظمها بقوانين مستقلة مثل جرائم سرقة التيار الكهربائى، وجرائم دخول المطاعم للأكل والشراب دون سداد الثمن، وغير ذلك من الجرائم، إلا أنه على القاضي أن يتدخل بالتفسير طبقا للضوابط المقررة من الفقه لذلك، حتى لا يتحول من قاضي إلى مشرع، فيجمع بين سلطتين تم الفصل بينهما حماية للحريات الفردية.

كما يجب علي الجهاز القضائي في الدولة أن ينظم دورات تدريبية للقضاة بصفة دورية منتظمة تساعدهم في فهم التقنيات الحديثة وكيفية استخدامها في ارتكاب الجرائم، مع استحداث دوائر جنائية متخصصة في هذه النوعية من الجرائم، مما يساهم في بناء مبادىء قضائية تسهم في مواجهة هذه الجرائم.

وعلي ذلك، يتمثل الكيان القانوني لجريمة الابتزاز، من ركنين، اولهما مادي، وثانيهما معنوي علي الترتيب[133].

) محكمة النقض المصرية : الطعن رقم 2624 لسنة 32 مكتب فنى 13 صفحة رقم 780 بتاريخ 26-11-133(1962، اذ قضي بأن " إذا كان الحكم المطعون فيه قد أثبت فى حق الطاعن أنه تمكن خلسة من إلتقاط صور للمجنى عليه وهو فى وضع مناف للأداب، ثم قابله بعد ذلك وهدده بنشر هذه الصور للتشهير به، وإن لم يدفع له مبلغ مائتى جنيه، فإن هذا يعد بياناً كافياً على أن الطاعن قد إرتكب الجريمة مع علمه بأنه يغتصب مالاً لا حق له فيه قانوناً مستوخياً فى ذلك تعطيل إرادة المجنى عليه بطريق التهديد بالتشهير به بما من شأنه ترويع المجنى عليه بحيث يحمله على تسليم المال الذى طلبه منه، وهو ما تتوافر به كافة العناصر القانونية للجريمة المسندة إليه."، وكذا الطعن رقم 22 لسنة 8 مجموعة عمر 4ع صفحة رقم 115 بتاريخ 13-12-1937، حيث قضي بأن " يشترط لتطبيق المادة 283 من قانون العقوبات أن يقع من الجانى على المجنى عليه تهديد أى فعل من شأنه إكراهه بطريق التخويف والوعيد، وأن يكون التهديد بقصد الحصول بدون حق على مال أو شئ آخر، فمجرد إمتناع المتهم عن دفع ثمن ما تناوله فى مقهى من المشروب دون أن يبدو منه بأية طريقة أى تخويف أو وعيد لا يمكن عده جريمة فى حكم هذه المادة، إذ ان التهديد لا يتوافر بمجرد شعور المجنى عليه فى داخلية نفسه بالرهبة أو الخوف من المتهم لبطشه وسطوته وما إشتهر عنه من التعدى على الأنفس."، وايضا في ذات المعني الطعن رقم 235 لسنة 8 مجموعة عمر 4ع صفحة رقم 159 بتاريخ 14-3-1938، اذ قضي بأن " إذا كانت الجريمة تقوم على ركنين وإنهدم أحدهما فلا يلتفت لوجه الطعن المنصب على ركنها الآخر، فإذا إتهم شخص بأنه هدد آخر للحصول على مال، وثبت أن

أولا : الركن المادي لجريمة الابتزاز :

قد يكون الابتزاز الذي ينفذه الجاني ضد المجني عليه يقوم على أساس التهديد الذي يبعث الخوف في نفس المجني عليه من الاضرار به، او باي شخص يهمه الخوف الذي يدفع المجني عليه الى ان ينفذ ما يريده الجاني على ان يكون هذا التهديد يمثل جريمة بالاعتداء على النفس او المال او العرض او افضاء اسرار تهم المجني عليه او يضر به افشائها، اما التهديد بإمر ليس جريمة فلا يعد تهديد يعاقب عليه والتهديد قد يكون بطريقة مباشره من الجاني للمجني عليه، وقد يكون بواسطة شخص اخر مرسل من الجاني او بواسطة أي شيء اخر[134].

المال الذى حصل عليه هو من حقه فقد إنتفت جريمة التهديد، ولم يبق محل للبحث فى صحة ما أثبته الحكم من أن المتهم إستعمل طرقاً غير مشروعة للغرض الذى رمى إليه."

) محكمة النقض المصرية : الطعن رقم 1921 لسنة 11 مجموعة عمر 5ع صفحة رقم 564 بتاريخ 27–134(10–1941، اذ قضي بأن " من يهدد بالتبليغ عن جريمة لم تقع عليه شخصياً ويحصل بذلك على مبلغ من المال مقابل سكوته عن التبليغ يعد مغتصباً لهذا المال عن طريق التهديد الذى وقع منه، وبناء على ذلك إذا كانت الواقعة الثابتة بالحكم هى أن المتهم هدد أحد من يقبلون المراهنة خفية على سباق الخيل بأن تبليغ البوليس عنه لضبطه ما لم يدفع له مبلغاً من المال، وحصل منه فعلاً على مبلغ، فطبقت المحكمة عليه المادة 326 من قانون العقوبات فإنها لا تكون قد أخطأت."، وكذا الطعن رقم 109 لسنة 12 مجموعة عمر 5ع صفحة رقم 597 بتاريخ 15–12– 1941، اذ قضي بأن " يكفى فى التهديد المذكور فى المادة 326ع أن يكون من شأنه تخويف المجنى عليه وحمله على تسليم ماله الذى طلب منه، ولا أهمية للطريقة التى إستعملها الجانى للوصول إلى غرضه متى كانت فى ذاتها كافية للتأثير فى المجنى عليه إلى ذلك الحد، وكان الجانى لا يقصد منها إلا الحصول على مال لا حق له فيه."، وايضا الطعن رقم 351 لسنة 15 مجموعة عمر 6ع صفحة رقم 679 بتاريخ 2–4–1945، اذ قضي بأن " إذا كانت الواقعة الثابتة بالحكم هى أن المتهم إتصل بالمجنى عليه، لا مباشرة بل بالواسطة طالباً إليه أن يعطيه مالاً فى مقابل أن يكف عنه أذاه فلم يقبل المجنى عليه بادىء الأمر، ولكن الوسيط أقنعه بضرورة دفع شىء إليه ليأمن من شره، فقدم المجنى عليه بلاغاً للجهات المختصة ذكر فيه ما وقع من المتهم وتخوفه منه، وطلب سماع شهوده، فما كان من البوليس بعد أن سمع أقوال المجنى عليه والوسيط الذى أقره على أقواله إلا أن وضع خطة إنتهت بضبط المتهم بعد أن أخذ من المجنى عليه خمسة جنيهات – فهذه الواقعة تتكون منها جريمة الشروع فى التهديد بقصد الحصول على مال من المجنى عليه، ما دام التهديد الذى صدر عن المتهم من شأنه فى ذاته أن يخوف المجنى عليه ويحمله على تسليم ماله الذى طلب إليه تسليمه، ولو كان تسليم المال لم يتم أصلاً، وإذا كان الواقع أن الضبط قد حصل بعد أن أخذ المتهم من المجنى عليه المال، فإن المجادلة فى رابطة السببية بين أخذ المال وبين التهديد، على أساس أن التسليم إنما كان تنفيذاً للخطة التى رسمها البوليس ولم يكن بناء على التهديد، لا يكون لها محل ما دامت الإدانة لم تؤسس إلا على مجرد الشروع."

ثانيا : الركن المعنوي لجريمة الابتزاز :

لتوفر جريمة الابتزاز، يجب توفر القصد الجنائي لدى الجاني والوسيط لأنها من الجرائم المقصودة التي يكفي لارتكابها ان يقوم الجاني بارتكاب الفعل بإرادته وعلمه لإحداث النتيجة المعاقب عليها، أي ثبوت القصد الاجرامي لدى الجاني في احداث الخوف في نفس الشخص المجني عليه، ولا عبره بالدافع لارتكاب الجريمة سواء أراد تحقيق محصلة له او لغيره او كان يهدف للانتقام او أي هدف اخر[135]

) محكمة النقض المصرية : الطعن رقم 133 لسنة 12 مجموعة عمر 5ع صفحة رقم 601 بتاريخ 15-12-135(1941، اذ قضي بأن " يكفى لتوافر ركن القصد الجنائى فى جريمة الحصول على مال بطريق التهديد أن يكون الجانى، وهو يقارف فعلته، عالماً بأنه يغتصب مالاً لا حق له فيه، ولا عبرة بعد ذلك بالبواعث التى دفعت الجانى إلى إرتكاب الجريمة، فهو يستحق العقاب ولو كان لم يرتكبها إلا لمجرد الرغبة فى الإنتقام والثأر لنفسه للإهانة التى لحقته من المجنى عليه."، وكذا الطعن رقم 24 لسنة 46 مجموعة عمر 1ع صفحة رقم 97 بتاريخ 3-1-1929، اذ قضي بأن " إن أركان جريمة الحصول بالتهديد على مبلغ من النقود هى : " 1 " الحصول على مبلغ من النقود أو أى شئ آخر ، و " 2 " أن يكون هذا الحصول بغير حق ، و " 3 " أن يكون التهديد هو الوسيلة إليه، وهذه الجريمة هى من جرائم القصد، ويكفى لتوفر ركن القصد الجنائى فيها أن يكون الجانى عند إرتكاب الفعل عالماً أنه مقبل على إغتصاب مال أو متاع لا حق له فيه، وبما أن التهديد ركن من أركانها المادية، فإذا حصل هذا التهديد للغرض المتقدم والمتهم مضطلع بنية الإجرام لكن حال دون وصوله إلى مبتغاه أمر خارج عن إرادته، فهناك يكون فعله شروعاً قانونياً معاقباً عليه بالفقرة الثانية من المادة 283ع، فإذا رفض طبيب الترخيص فى دفن جثة متوفى قبل تشريحها إلا إذا حصل على نقود وهو يعلم أنه لا حق له فيها، وهدد بتشريح الجثة إن لم تدفع له النقود، وخاب أثر فعله لسبب خارج عن إرادته، فإن فعله هذا لا يعتبر شروعاً فى إرتشاء بل يعتبر شروعاً فى الحصول بالتهديد على مبلغ من النقود، وتنطبق عليه المادة 283 فقرة ثانية عقوبات، ولو أن فيه ما قد يؤذن بأنه من قبيل الشروع فى النصب على إعتبار أن الترخيص بالدفن بلا تشريح ليس فى يده بل هو برأى النيابة، إلا أنه متى لوحظ أن الواقع هو أن للطبيب دخلاً عظيماً فى تصرف النيابة من جهة الأمر بالتشريح وعدمه يعلم أن الواقعة فى مثل هذه الصورة أقرب إلى الجريمة المنصوص عنها بالمادة 283 منها إلى جريمة النصب."، وايضا الطعن رقم 4684 لسنة 58 مكتب فنى 40 صفحة رقم 819 بتاريخ 2-11-1989، اذ قضي بأن " لما كان مناط تحقق جريمة المادة 326 من قانون العقوبات أن يصدر من الجانى على المجنى عليه أى فعل بقصد تخويفه أو ترويعه بما يحمله على أن يسلم بغير حق، مبلغاً من المال أو أى شئ آخر، وكان تقدير توافر أركان هذه الجريمة من الموضوع الذى يستقل به قاضيه بلا رقابة عليه من محكمة النقض ما دام تقديره سائغاً مستنداً إلى أدلة مقبولة فى العقل والمنطق، وكان الحكم المطعون فيه قد خلص للأسباب السائغة التى أوردها إلى تبرئة المطعون ضده الأول من تهمة الشروع فى الحصول على مال بطريق التهديد تأسيساً على إنتفاء صدور أى تهديد أو ترويع منه على المبلغ، فإن ما تثيره الطاعنة من جدل فى هذا الخصوص يكون غير مقبول."

ويفرق البعض بين التهديد المطلق أي الذي يعدم الإرادة إعداماً كلياً، وبين التهديد النسبي.

اذ ترتكز نظرية التهديد المعنوي في تحديدها لمفهوم الاكراه، على تأثيره في إرادة الأفراد، باعتبار أن المشرع حينما يجرم إنما يبتغي حماية الحرية المعنوية للأفراد المتمثلة في حرية الإرادة.

وبذلك فإن التهديد يتحقق بأية وسيلة يكون من شأنها التأثير أو الضغط أو الإكراه على إرادة الغير، وطبقاً لهذه النظرية يتحدد العنف في تنازع أو صراع بين إرادتين، ومحاولة تغليب إرادة الجاني على إرادة المجني عليه.

فالتهديد طبقاً لهذه النظرية، ينصرف إلى كل سلوك يؤدي إلى الضغط على الإرادة، وعليه فإن التهديد يشمل كافة المؤثرات التي من شأنها تحقيق ضغط إرادي، وذلك مثل القوى الجسدية والطبيعية والنفسية. (136)

---

(1) محكمة النقض المصرية : الطعن رقم 1160 لسنة 49 مكتب فنى 30 صفحة رقم 939 بتاريخ 13-12-1979، حيث قضت بانه "لما كان الحكم المطعون فيه قد دان الطاعن طبقاً للفقرة الأولى من المادة 137 مكرر " أ " من قانون العقوبات وهى لا تستلزم لإنطباقها إحداث إصابات بالموظف المعتدى عليه، بل يكفى إستعمال القوة أو العنف أو التهديد، ومن ثم فلا على المحكمة إن هى لم تورد سبب إصابة كل من المجنى عليهم، ولا مصلحة للطاعن فى النعى على الحكم فى هذا الصدد، لأن المحكمة لا تلتزم فى أصول الإستدلال بالتحدث فى حكمها إلا عن الأدلة ذات الأثر فى تكوين عقيدتها، ومن ثم يكون هذا النعى غير سديد."، وايضا الطعن رقم 701 لسنة 56 مكتب فنى 37 صفحة رقم 663 بتاريخ 1-10-1986، بان قضت بانه " لما كان الحكم وقد دان الطاعنين طبقاً للفقرة الأولى من المادة 137 مكرر"أ" من قانون العقوبات، وهى لا تستلزم إحداث إصابات بالموظف المعتدى عليه، بل يكفى إستعمال القوة أو العنف أو التهديد، ومن ثم فلا على المحكمة إن هى لم تورد فى حكمها سبب إصابة المجنى عليها، ولا مصلحة للطاعنين فى النعى على الحكم فى هذا الصدد، ما دام أن الحكم قد إثبت - على ما سلف بيانه - واقعة التعدى بالضرب على المجنى عليه الثانى، وهى ضرب من ضروب القوة أو العنف المؤثم فى صورة الدعوى، يستوى فى ذلك أن يحدث أيهما إصابات أم لا"، وكذلك الطعن رقم 701 لسنة 56 مكتب فنى 37 صفحة رقم 663 بتاريخ 1-10-1986، بان قضت بان " لما كان الركن المادى فى الجريمة المنصوص عليها فى المادة 137 مكرراً "أ" من قانون العقوبات يتحقق بما يصدر عن الجانى من أعمال القوة أو العنف أو التهديد قبل الموظف العام، أياً كانت درجة القوة أو العنف أو التهديد، قبل الموظف العام، أياً كانت درجة القوة أو العنف أو التهديد، يستوى فى ذلك أن تترك القوة أو العنف أثراً أم لا وكان ما صدر من الطاعن الأول من إعتراض على توقيع الحجز ثم إنتزاعه أوراق الحجز من المحضر المكلف بالتنفيذ، ثم الشروع فى تمزيقها مع توجيه الشتائم والسباب المقذع إليه، يتضمن معنى القوة أو العنف أو بالقليل التهديد بالإيذاء إذا ما إستمر المذكور فى إداء عمله، وهو ما يتحقق به الركن المادى فى الجريمة فإن النعى عليه فى هذا الشأن يكون على غير أساس. لما كان ذلك، وكان من المقرر أن الركن الأدبى فى الجناية بادية الذكر لا يتحقق إلا إذا توافرت لدى الجانى نية خاصة بالإضافة إلى القصد الجنائى العام، تتمثل فى

ومؤدى هذه الصور جميعها أن يقوم الجاني بتوجيه تهديد إلى شخص ما، وتتحلل هذه الصور إلى ثلاثة عناصر، أطراف التهديد؛ ومضمونه؛ ومحله.

أما بالنسبة لأطراف التهديد، فهما الجاني والمجني عليه، أي المُهدِد والمُهَدد.

أما مضمونه، فينصرف إلى الوعيد باستخدام ما هدد به، كنشر امر مخل او ما يماثله.

اما محله، فهو المادة غير المشروعة، التي يهدد الجاني بها، حتي يتحصل علي بغيته من الابتزاز.

المبحث الرابع

تنازع الاختصاص في جرائم الابتزاز الالكتروني

نظرا للطبيعة الخاصة التي تتسم بها جرائم الابتزاز الالكتروني، فقد أفرزت تحديات واضحة للقوانين التي وضعت لمكافحة تلك الجرائم، ذلك أنها غيرت من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية، وما ينتج عن ذلك من مشكلة في تفسير النصوص القانونية وحظر القياس في المواد الجنائية واصطدامها بمبدأ الشرعية الجنائية.

وهذه القيود من شأنها أن تساهم في إفلات الكثير من المجرمين من العقاب من جهة، ومن جهة أخرى تطرح إشكاليات عند تطبيق النصوص، خاصة في المسائل المتعلقة بالاختصاص.

إنتواء الحصول من الموظف المعتدى عليه على نتيجة معينة، هى أن يؤدى عملاً لا يحل له أن يؤديه، أى أن يستجيب لرغبة المعتدى، فيمتنع عن أداء عمل مكلف به، قد أطلق الشارع حكم هذه المادة لينال بالعقاب كل من يستعمل القوة أو العنف أو التهديد مع الموظف العام أو المكلف بخدمة عامة، متى كانت غايته من الإعتداء أو التهديد حمل الموظف أو المكلف بالخدمة العامة على قضاء أمر غير حق أو إجتناب أداء عمله المكلف به، يستوى فى ذلك أن يقع الإعتداء أو التهديد أثناء قيام الموظف بعمله لمنعه من المضى فى تنفيذه، أو فى غير حالة قيامة به لمنعه من أدائه فى المستقبل، وكان الحكم المطعون فيه قد إستظهر فى مدوناته – على ما سلف البيان – إستظهاراً سليماً وسائغاً من ظروف الواقعة وملابساتها أن نية الطاعنين مما وقع منهما من أعمال مادية، قد إنصرفت إلى منع المحضر والخفير النظامى المصاحب له من أداء عمل من أعمال وظيفتهما، هو تنفيذ أولهما توقيع الحجز التحفظى على منقولات والد الطاعن الثانى وقريب الأول، ومنع الثانى من مساعدته فى أداء عمله وتمكينه منه، فإن الحكم يكون قد أثبت قيام الركن الأدبى للجناية التى دان الطاعنين بها، ويضحى منعى الطاعنين بعدم توافر الركن الأدبى، مجرد جدل فى تقدير الدليل وفى سلطة محكمة الموضوع فى وزن عناصر الدعوى وإستنباط معتقدها، وهو ما لا يجوز أثارته أمام محكمة النقض."

ومع زيادة انتشار شبكة الانترنت وتوسع استخدامها في مجال المعاملات التجارية ودخول جميع فئات المجتمع إلى قائمة المستخدمين، بدأت تظهر جرائم ذات طبيعة خاصة على هذه الشبكة وازداد عددها وتعددت صورها وأشكالها وهى جرائم الابتزاز الالكتروني.

ولعل التطور المستمر للانترنت وما تتميز به من سرعة في إعداد ونقل وتحزين المعلومات وما تتوفر عليه من السرية التامة جعلها بيئة ملائمة للإجرام بعيدا عن أعين الجهات الأمنية، وما زاد الأمر سهولة وجود فراغ تشريعي على المستوى الداخلي والدولي[137].

ومما زاد الأمر تعقيدا أن هذه الجرائم المستحدثة سريعة الحدوث، وفي العديد من الدول باعتبارها جريمة عابرة للحدود، وما تطرحه هذه الجرائم من مشكلات قانونية خصوصا في مجال الاختصاص من حيث الجهات المخول لها متابعة المجرم، أو من خلال المحكمة المختصة فقد ترتكب الجريمة في دولة وتكون آثارها في دولة أخرى، وقد يكون الجاني يحمل جنسية دولة أخرى وتكون أدلة الجريمة موجودة في دولة أخرى وخارج النطاق الإقليمي لجهة التحقيق، فكيف يتم جمع الأدلة وضبطها وما هو القانون الواجب التطبيق، وهذا ما يحتم ضرورة البحث عن الاختصاص في جرائم الابتزاز الالكتروني العابرة للحدود على المستوى الداخلي، وكذا على المستوى الدولي من خلال التعاون الاتفاقي والقضائي[138] للحد من هذه الظاهرة الإجرامية الخطيرة[139].

وعلى هذا الأساس يتعين في هذا المقام، أن نبين أحكام الاختصاص في جرائم الابتزاز الالكتروني، وذلك بالتطرق إلى السمات الخاصة لجرائم الابتزاز الالكتروني فيما يتعلق بقواعد الاختصاص بها في مطلب أول، على يتناول المطلب الثاني تحديد نطاق جرائم الابتزاز الالكتروني،

---

137) راجع في ذلك: عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 2008/03/07، المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:3.

138) راجع في ذلك: د. علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، ايتراك للطباعة والنشر والتوزيع، الطبعة الاولى، مصر، سنة 2000 ، ص 197.

139) انظر في ذلك: حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء الجنائى الوطنى، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، سنة 2000 ، ص 25 ، 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 20 – 21 مايو 2003 ، ص 10.

ثم يخصص المطلب الثالث لقواعد الاختصاص في جرائم الابتزاز الالكتروني، يتبع ذلك المطلب الرابع للوقوف على التحديات التي تواجه الجوانب الإجرائية في جرائم الابتزاز الالكتروني، وأخيرا نوضح أوجه التعاون الدولي في مجال مكافحة جرائم الابتزاز الالكتروني في مطلب خامس وأخير، على الترتيب التالي .

- **المطلب الأول:** السمات الخاصة لجرائم الابتزاز الالكتروني.
- **المطلب الثاني:** نطاق جرائم الابتزاز الالكتروني.
- **المطلب الثالث:** قواعد الاختصاص في جرائم الابتزاز الالكتروني.
- **المطلب الرابع:** التحديات التي تواجه الجوانب الإجرائية في جرائم الابتزاز الالكتروني.
- **المطلب الخامس:** التعاون الدولي في مجال مكافحة جرائم الابتزاز الالكتروني.

المطلب الأول

السمات الخاصة لجرائم الابتزاز الالكتروني

حيث تتميز جريمة الابتزاز الالكتروني بجملة من الخصائص التي تميزها عن الجريمة التقليدية ومن أهمها:

1- جريمة الابتزاز الالكتروني عابرة للحدود:

ذلك أنه غالبا ما يكون لهذه الجرائم طابع عالمي، لأن كل الدول مرتبطة وفي حالة اتصال دائم (ON LINE)، وعليه فان جريمة الابتزاز الالكتروني لا تعرف حدودا وبذلك أصبح مسرح جرائم الابتزاز الالكتروني عالميا.[140]

وهذا ما يطرح العديد من الإشكاليات القانونية، خصوصا أثناء عدم تواجد الجاني في مسرح الجريمة، وكذا التباعد الزماني والمكاني بين السلوك الإجرامي والمتمثل في جهاز الحاسب والنتيجة الإجرامية التي تمثل قاعدة البيانات والمعطيات محل الاعتداء بالنسبة إليها.

ولا شك ان هذا الأمر يثير إشكالية التعارض مع السيادة الوطنية مما يزيد من تعقيدات الموضوع، وذلك من خلال صعوبة اللجوء إلى عمل دولي مشترك للحد من هذه الجرائم، مما يستوجب الاعتماد على التشريعات الوطنية لكل دولة[141].

---

140) راجع في ذلك: عبد الله حسين على محمود: سرقة المعلومات المتخزينة في الحاسب الآلي، دار النهضة العربية، الإسكندرية، سنة 2002، ص351.

والحقيقة أن هذه الجرائم صورة صادقة من صور العولمة[142] وذلك باعتبار العالم قرية كبيرة، حيث يمكن ارتكاب الجرائم عن بعد، وقد يتعدد المكان إلى أكثر من دولة بل أكثر من قارة وهذا من شأنه أن يطرح إشكالية القانون الواجب التطبيق.

2- صعوبة إثبات جريمة الابتزاز الالكتروني:

مما يميز هذه الجريمة أنها تتصف بالخفاء وعدم وجود أثار مادية يمكن متابعتها مما يجعلها صعبة الاكتشاف، وعليه فمن الصعب تحديد مكان وقوعها وترجع أسباب ذلك إلى:

- إنها جريمة لا تترك أثار مادية بعد ارتكابها، وغالبا ما يتم اكتشاف الجاني فيها مؤخرا، وبعد وقت طويل من حدوثها.
- صعوبة الاحتفاظ بالدليل الفني على ارتكاب الجريمة[143]، وذلك لان الجاني يستطيع في ظرف وجيز جدا أن يمحو أو يحرف أو يغير أو يتلف البيانات والمعلومات وجميع المعطيات الموجودة في قاعدة البيانات، وعلى هذا الأساس كان للمصادفة دور كبير في اكتشافها.
- تحتاج هذه الجرائم إلى خبرة فنية وتقنية عالية، وذلك من خلال معرفة تقنيات الحاسب ونظم المعلومات، سواء في مجال جمع الأدلة والتحقيق أو المتابعة القضائية.

لذلك فإن رجال الضبطية القضائية غير قادرين على التعامل مع هذه الفئة من الجرائم بالطرق التقليدية، بالإضافة إلى صعوبة تتبع مسار العمليات الكترونيا خصوصا إذا كانت عابرة للقارات.

- إن هذه الجرائم تعتمد على الخداع في ارتكابها والتضليل، مما يساعد على عدم التعرف على الفاعل الحقيقي، والشيء الملاحظ هو أن المؤسسات والبنوك خصوصا تحجم عن الإبلاغ

---

141) انظر في ذلك: عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 2008/03/07، المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:3.

142) انظر في ذلك: عمر محمد خير الحاج، العادل العاجب: العولمة وآثارها في تطور الجريمة، مجلة الأمن والقانون، كلية شرطة دبي، السنة العاشرة، العدد الأول، شوال 1422هـ – يناير 2002 م ص 29.

(143) John Eaton & jermy smithers, A managers Guide to information Technology, London, Philip Allan,1982,p263.

وهذا تجنبا للإساءة إلى السمعة والخوف من اهتزاز ثقة العملاء فيها، بالإضافة إلى إخفاء أسلوب ارتكاب الجريمة خوفا من تكرارها مما يزيد من فرص إفلات الجاني من العقاب.[144]

- تعتمد معظم جرائم الابتزاز الالكتروني على الذكاء، ولهذا تسمى جرائم الذكاء، وهي ليست بالضرورة من الجريمة المنظمة، فغالبا ما ترتكب بصفة فردية، واهم دوافعها الطمع والجشع والانتقام وأحيانا بدافع إثبات الذات.

وعلى هذا الأساس نقول أن الإجرام المعلوماتي هو إجرام الأذكياء الذي يعتمد على مهارات فنية وتقنية وإلمام بنظم المعلوماتية بالمقارنة مع الإجرام التقليدي الذي يعتمد على العنف.[145]

3- عدم وجود مفهوم محدد ومشترك لجريمة الابتزاز الالكتروني:

يرجع ذلك بالأساس إلى اختلاف النظم القانونية في دول العالم، ويظهر هذا جليا من خلال اختلاف الفكر القانوني حول حماية المعلومات، فهناك من يرى بأن المعلومات ذات طبيعة خاصة، ولا يطبق عليها الشرط المادي الضروري لتعريف الجريمة، ويرى البعض الآخر أن المعلومات تأخذ قيمة مالية ومادية بصفتها حقا خاصا ينسب لشخص محدد .

ومما يزيد الأمر تعقيدا هو مبدأ الشرعية الجنائية باعتباره أمرا نسبيا من دولة إلى أخرى، وأحيانا في نفس الدولة الواحدة.

ولهذا يجب أن تتحرك الدول على محورين، من أجل مكافحة جريمة الابتزاز الالكتروني:

- **أولا:** على المستوى الداخلي، وهذا من خلال وضع قوانين تتماشى وطبيعة هذه الجرائم المستحدثة، وإقامة هيئات وطنية مستقلة تشرف على المراقبة والعمل على الوقاية من هذه جرائم الابتزاز الالكتروني .
- **ثانيا:** على المستوى الدولي، وهذا من خلال وضع اتفاقيات دولية وإقليمية وتفعيل دور المنظمات غير الحكومية من أجل مكافحة هذه الجرائم المستحدثة، والعمل على سد الفراغات

) راجع في ذلك: خالد ممدوح ابراهيم : امن الجرائم المعلوماتية، الدار الجامعية، الإسكندرية، سنة 2008، 144(ص47.

) راجع في ذلك: جعفر حسن جاسم الطائي: جرائم تكنولوجيا المعلومات، دار البداية، ليبيا، سنة 2007، 145(ص144.

التشـريعية حتـى لا يسـتفيد المجرمـون مـن عجـز التشـريعات الداخليـة وغيـاب النصـوص الدولية.[146]

4- وقوع الجريمة أثناء المعالجة الآلية للبيانات:

وتعتبر هذه الخصيصة ضرورية يجب توافرها لقيام جريمة الابتزاز الالكتروني، وفي أي مرحلة من المراحل سواء أكانت في مرحلة إدخال البيانات أو أثناء معالجتها أو أثناء خروج المعلومات والمعطيات أو حتى بعد تخزينها، وهذه الصور أخذ بها المشرع الفرنسي في قانون العقوبات المعدل لسنة 1994 ولا مانع في الاسترشاد بها عند وضع قانون خاص بجرائم الابتزاز الالكتروني.[147]

5- جريمة الابتزاز الالكتروني جريمة مستحدثة:

ذلك إن التقدم العلمي والتكنولوجي في ظل العولمة تجاوز قدرات الدولة الرقابية وإمكانياتها بل وأضعف قدرتها على تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وسلامتها. [148]

وعلى هذا الأساس، بادرت الدول إلى وضع تشريعات خاصة تعمل على الوقاية ومكافحة هذه الجريمة المستحدثة وسعت إلى عقد اتفاقيات دولية في هذا المجال[149].

غير أنه بالنظر لطبيعة وخصائص جرائم الابتزاز الالكتروني، نجدها تثير العديد من الإشكاليات القانونية خصوصا في مجال الاختصاص القضائي والقانون الواجب التطبيق[150]، لذلك

---

146) راجع في ذلك: خالد محمد كدفور المهيري: جرائم المعلوماتية والانترنت والتجارة الالكترونية، دار العزيز للطباعة والنشر، دبي، سنة 2005، ص135

147) انظر في ذلك: نائلة عادل محمد فريد: جرائم المعلوماتية والجريمة الاقتصادية،منشورات الحلبي الحقوقية، لبنان، سنة 2005، ص55.

148) راجع في ذلك: نبيلة هروال: الجوانب الإجرائية لجرائم المعلوماتية في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، سنة 2006، ص35.

149) انظر في ذلك: عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 2008/03/07، المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:3.

150) راجع في ذلك: حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء الجنائى الوطنى، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، سنة 2000 ، ص 25 ، وايضا : عبدالرؤوف مهدى،

سنحاول إيجاد رؤية توافقية تعمل على الحد من هذه الجرائم من خلال ملاحقة ومتابعة الجناة وعدم تهربهم من العقاب هذا من جهة، ومن وجهة أخرى حماية الحقوق الشخصية للأفراد وضمان حرياتهم الأساسية من سرية المعلومات وحرية الاتصال، مما يعد مكافحة جادة تجاه جرائم الابتزاز الالكتروني.

المطلب الثاني

نطاق جرائم الابتزاز الالكتروني

تتميز جريمة الابتزاز الالكتروني بأنها لا تقتصر على النظام المعلوماتي لدولة واحدة، وإنما تمتد إلى دول عديدة وفي قارات مختلفة، وعلى هذا الأساس ثار جدل فقهي حول نطاق جريمة الابتزاز الالكتروني، فهل تعد جريمة دولية أم جريمة عالمية، وسنحاول شرح ذلك على النحو التالي:

1- الجريمة الدولية[151]:

تعرف الجريمة في القانون الدولي على انها عدوان على مصلحة يحميها القانون الدولي الجنائي، أو هي كل تصرف غير مشروع يعاقب عليه القانون الدولي لانطوائه على اعتداء على العلاقات الإنسانية في الجماعة الدولية.

غير إن فقهاء القانون الجنائي الدولي اضافوا طائفة أخرى من الجرائم بالنظر إلى وسيلتها وليس لطبيعتها ومن أمثلة ذلك جريمة خطف الطائرات والقرصنة.[152]

2- الجريمة العالمية:

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 20 – 21 مايو 2003 ، ص 10.

) عبد الجواد الرايسي: التكوين المستمر للقضاة : عرض حول جرائم الأموال المنعقدة بتاريخ 2008/03/07، 151(المملكة المغربية وزارة العدل، المعهد العالي للقضاء، مديرية تكوين الملحقين القضائيين والقضاة، قسم التكوين المستمر، ص:3.

) حسنين عبيد: الجريمة الدولية دراسة تحليلية وتطبيقية،دار النهضة العربية، الإسكندرية، 1989، ص152.10(

ويقصد بها مجموعة القوانين الجنائية الوطنية مجتمعة، وبمعنى أخر أن يطبق قانون العقوبات على كل مجرم يقبض عليه في إقليم الدولة، أيا كانت الدولة التي ارتكب فيها الفعل الإجرامي، وأيا كانت جنسية الجاني وهذا ما يعبر عنه بعالمية القاعدة الجنائية.

ويرى جانب كبير من الفقه أن جريمة الابتزاز الالكتروني، هي جريمة عالمية وهذا بالنظر لطبيعتها والوسائل المستعملة فيها والنتائج المترتبة عنها، مما يستوجب وضع تشريعات تعمل على تجريم جميع السلوكيات الإجرامية من جهة، والسعي لزيادة التعاون الدولي في المجالين الاتفاقي والقضائي[153] وهذا في سبيل تطويق هذه الظاهرة الإجرامية الخطيرة. [154]

المطلب الثالث

قواعد الاختصاص في جرائم الابتزاز الالكتروني

يقصد بالاختصاص هو السلطة التي يقرها القانون للقضاء في أن ينظر في دعاوى من نوع معين.[155]

وبالنظر لطبيعة وخصائص جرائم الابتزاز الالكتروني، فليس لها مقر ثابت أو دولة معينة، بل تنتشر في كل دول العالم، وليست لها أية هيئة أو جهة تشرف عليها ومسؤولة عنها، مما يترتب عن ذلك عدم وجود قانون جنائي محدد أو موحد يحكم الجريمة، بل بالعكس هناك العديد من القوانين الجنائية بتعدد الدول والأنظمة القانونية، وذلك يرجع أساسا لارتباط القانون الجنائي بالسيادة الوطنية.

) حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء الجنائى الوطنى، 153(رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، سنة 2000 ، ص 25 ، 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 20 – 21 مايو 2003 ، ص 10.

) راجع في ذلك: د. جلال ثروت، شرح قانون العقوبات القسم العام، منشاة المعارف، الإسكندرية، سنة 1989، 154(ص104، وايضا راجع: د. مأمون محمد سلامة، شرح قانون العقوبات القسم العام، الطبعة الثالثة، دار النهضة العربية، الإسكندرية، سنة 2002، ص80.

) راجع في ذلك: د. محمود نجيب حسني، شرح قانون الإجراءات الجزائية، دار النهضة العربية، سنة 2002، 155(ص723.

ومن هنا تكمن الإشكالية في أن بعض السلوكيات والأفعال مجرمة في بعض الدول ومباحة في دول أخرى، وفي أغلب الدول لا توجد نصوص تنظم هذه السلوكيات، والسؤال المطروح إلى أي مدى يمكن تطبيق القانون الوطني على جرائم الابتزاز الالكتروني العابرة للحدود ؟

ذلك أن القاعدة العامة المطبقة في أغلب الدول هي مبدأ الإقليمية، بمعنى أن القانون الجنائي يطيق على كافة الجرائم التي تقع على ارض الدولة بغض النظر عن جنسية فاعلها أو مرتكبها، ومع هذا فإن تطور الإجرام وتوسعه إلى دول العالم تطلب وجود اتفاقيات دولية لتسليم المجرمين[156]، غير أن غالبية الدول لا تسلم رعاياها وفقا لمبدأ السيادة من جهة[157]، ومن جهة أخرى التعارض مع مبدأ أساسي في القانون الجنائي وهو عدم جواز محاكمة لشخص عن فعل واحد أكثر من مرة [158].

وعلى هذا الأساس يجب وضع ملامح نظام قانوني يسمح بمتابعة وملاحقة مرتكبي جرائم الابتزاز الالكتروني، دون المساس بحقوق وحريات الأفراد التي تقرها المواثيق الدولية، ووجوب احترام مبدأ الشرعية دون إعطاء فرصة للجناة من الإفلات من المتابعة الجنائية وتوقيع العقوبة المناسبة عليهم مما يحقق الأمن والاستقرار للمجتمع، وعليه يجب البحث على معيار يتلائم وطبيعة جرائم الابتزاز الالكتروني.

---

156) انظر في ذلك: توصيات مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين لسنة 1995م – منشورات الأمم المتحدة، ص 120. وايضا راجع في ذلك: د. عبدالعظيم مرسى وزير، المبادئ العامة لتسليم المجرمين في ضوء المجهودات الفقهية والمعاهدات الدولية، المؤتمر العلمى السنوى الثالث، كلية الحقوق، جامعة المنصورة، تحت عنوان المواجهة التشريعية لظاهرة الارهاب على الصعيدين الوطنى والدولي، القاهرة ، بتاريخ 21 – 22 ابريل 1998، ص 127 وما بعدها، وايضا: عبدالفتاح محمد سراج، النظرية العامة لتسليم المجرمين، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، مصر، سنة 1999، ص 57.

157) انظر في ذلك: ياسر محمد الجبور، تسليم المجرمين او تقديمهم في الاتفاقيات الدولية والنظام الاساسي للمحكمة الجنائية الدولية، رسالة ماجستير، جامعة الشرق الاوسط، سنة 2011، ص9.

158) راجع في ذلك: د. عبد العظيم مرسى وزير، المبادئ العامة لتسليم المجرمين في ضوء المجهودات الفقهية والمعاهدات الدولية، المؤتمر العلمى السنوى الثالث، كلية الحقوق ، جامعة المنصورة، تحت عنوان المواجهة التشريعية لظاهرة الارهاب على الصعيدين الوطنى والدولي ، القاهرة ، بتاريخ 21 – 22 ابريل 1998 ، ص 127 وما بعدها، وايضا عبدالفتاح محمد سراح، النظرية العامة لتسليم المجرمين، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، مصر، سنة 1999، ص 57.

1- مبدأ الاختصاص الإقليمي:

تأخذ أغلب التشريعات الوضعية بهذا المبدأ من تطبيق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الاقليم.

كما أخذ بهذا المبدأ المشرع الفرنسي في المادة 113 ف 02 من قانون العقوبات الجديد التي تنص على ان "يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية، وتعتبر قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم.[159]

ويعني هذا المبدأ أن قانون العقوبات يطبق على أي جريمة تقع داخل القطر الوطني، بغض النظر عن جنسية مرتكبيها أو المجني عليه، وينعقد الاختصاص وفقا لهذا المبدأ بتحقق أحد العناصر المكونة للجريمة سلوكا أو نتيجة .

كما أن هذا المبدأ يسمح بمتابعة كل من ارتكب أحد العناصر المكونة للجريمة ولو كان الفعل غير معاقب عليه في بلد المنشأ الأصلي أي بداية السلوك الإجرامي، ومن ثم تنقل البيانات والمعلومات بين العديد من الدول وبمجرد اقتراف أحدى سلوكيات الجريمة في القطر الوطني ينعقد الاختصاص للقاضي الوطني، ومن ثم يجب تطبيق قانون العقوبات الوطني كما يمكن بناء على هذا المبدأ متابعة الجاني خارج القطر متى كان مساهما أو شريكا في الجريمة التي وقعت داخل القطر لأن العبرة بمكان وقوع الجريمة .

غير إن هذا المبدأ يجد صعوبة كبيرة في تطبيقه بالنسبة لجرائم الابتزاز الالكتروني، وهذا بالنظر لطبيعتها والخصائص التي تميزها عن جريمة الابتزاز التقليدية، وخصوصا صعوبة تحديد مكان وقوعها وارتكابها بدقة وكذا زمان حدوثها .

كما أن هذا المبدأ يجد صعوبة في تطبيقه في قانون العقوبات الفرنسي حيث تنص المادة 113 فقرة 5 علي ان "يطبق القانون الفرنسي على كل من ارتكب فعلا في إقليم الجمهورية يجعله شريكا في جناية أو جنحة وقعت بالخارج إذا كانت الجناية أو الجنحة معاقبا عليها في القانون الفرنسي والقانون الأجنبي وكانت ثابتة بمقتضى حكم نهائي من القضاء الأجنبي".

وعليه، وبناء على نص المادة أعلاه، فإنه لكي يسئل الشريك يجب توافر ما يلي:

1-) أن يكون الفعل مجرما في البلد المنشأ – الفعلي الأصلي.

2-) أن يصدر حكم الإدانة عن الفاعل الأصلي في البلد المنشأ.

(159) VIDAL (G) , Cours de droit criminal et de science penitenterntniaire 8eme ed,mis a jour par Magnol , libraie Arthur Rousseau, paris,1935,N 0 1,p1071

وعليه، فإن تطبيق هذا النص يصطدم بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي، لأنه شرط أولي لعقد الاختصاص للقاضي الوطني، لأن ذلك يترتب عليه معرفة ما إذا كان الفعل مباحا أو مجرما في ذلك البلد.

وأخيرا، جدير بالذكر أن مبدأ الإقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية وهذا المبدأ غير ملائما لجرائم الابتزاز الالكتروني، وهذا بالنظر لطبيعتها غير المادية من جهة ومن جهة أخرى لصعوبة اكتشافها وتحديد مكان وزمان وقوعها بدقة.

2- مبدأ الاختصاص الشخصي:

يأخذ هذا المبدأ وجهان وجه إيجابي ووجه سلبي وسنحاول توضيح ذلك كما يلي:

- **الوجه الإيجابي:** ويعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها.
- **الوجه السلبي:** ويعني تطبيق القانون الجنائي على كل جريمة يكون فيها المجني عليه ينتمي إلى جنسية الدولة، ولو كان الجاني أجنبيا وارتكب الفعل خارج إقليم الدولة.[160]

ولا شك ان المشرع المصرى، على غرار باقي التشريعات لا يعترف بمبدأ الشخصية في وجهه السلبي، لأن جنسية المجني عليه ليست محل اعتبار في تطبيق القانون الجنائي من حيث المكان، وعلى العكس من ذلك يأخذ المشرع المصرى بمبدأ الشخصية في شقه الإيجابي.

غير أن هذا المبدأ وردت عليه قيود بصفة عامة، وبالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج بل يجب علم النيابة العامة بها، كما أنه لا يجوز محاكمة الشخص على نفس الفعل الواحد مرتين وهذه الإجراءات طويلة ومكلفة وتقيد تطبيق مبدأ الاختصاص الشخصي.

والملاحظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته، ومن ثم التعرف عن جنسيته، وهذه المعلومات تعد صعبة وعسيرة في جرائم الابتزاز الالكتروني، ومنها أين يستعمل التشفير، والأسماء المستعارة، بالإضافة إلى اللغة الصعبة والمعقدة في كشفها والتعامل معها.

كما أن محاكمة المجرم الذي يقيم في دولة أجنبية تحتاج إلى إجراءات طويلة وشاقة ومعقدة ومكلفة، وهذا ما يصدق كذلك بالنسبة لتنفيذ الأحكام الصادرة في الخارج.

---

160) راجع في ذلك: جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالانترانت، دار النهضة العربية، الإسكندرية، سنة 2002، ص55.

كذلك من مخاطر تطبيق القانون الوطني على الجرائم التي تقع في الخارج، والتي يختص بها القانون الأجنبي في ذات الوقت أنه قد يؤدي إلى المساس بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة وهو إحدى المبادئ الأساسية للقانون الجنائي.

وعلى العكس من ذلك، إذا لم يكن القانون الوطني مختص بنظر الواقعة فتثار الإشكالية بالنسبة للمضرور من الجريمة الذي يجب عليه التنقل إلى الدولة حيث ارتكب الفعل لرفع دعواه المدنية.[161]

والأخطر من ذلك، أن يكون الفعل غير معاقب عليه في هذه الدولة، ولذلك نري بأنه يجب أن يكون هناك اتفاقية دولية تتبنى معيار جنائي دولي على غرار القانون الدولي الخاص ليطبق على جرائم الابتزاز الالكتروني.

3 – مبدأ الاختصاص العيني:

طبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بصرف النظر عن جنسية مرتكبها، ويرجع هذا المبدأ إلى المساس بسيادة الدولة [162] وحقها في الدفاع عن جميع صور الاعتداء على مصالحها الحيوية والأساسية ولو وقعت تلك الجرائم خارج إقليمها.

وعلى هذا الأساس يمكن أن يطبق هذا المبدأ على جرائم الابتزاز الالكتروني، إذا كانت تمس بالسيادة الوطنية ووحدة الدولة أو تعمل على المساس بالمصالح الحيوية ولو ارتكبت من قبل أجانب وخارج إقليم الدولة.

غير أن هذا المبدأ في الواقع يصادف العديد من الصعوبات، ترجع بالأساس إلى طبيعة وخصائص جرائم الابتزاز الالكتروني، حيث لا تظهر مادياتها بوضوح، كما أن الفاعل يبقى مجهولا بالإضافة إلى تعدد وتنوع الأنظمة القانونية في العالم واختلافها مما يترتب عليه البطء والتعقيد وطول مدة الإجراءات.

4– مبدأ الاختصاص العالمي:

يطبق وفقا لهذا المبدأ القانون الجنائي على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان مكان ارتكابها وجنسية الفاعل أو الجاني.[163]

---

161) راجع في ذلك: جمال محمود الكردي: المحكمة المختصة والقانون الواجب التطبيق بشان دعاوى المسؤولية والتعويض عن مضار التلوث البيئة العابرة للحدود، الطبعة الاولى، دار النهضة العربية، الإسكندرية، سنة 2003، ص132.

162) راجع في ذلك: د. مأمون محمد سلامة شرح قانون العقوبات القسم العام – ط 3 – دار النهضة العربية، الإسكندرية، سنة 2002 ، ص75.

وهذا المبدأ يعطي لقانون العقوبات مجال متسعا يشمل العالم كله، فلا يتقيد بمكان ارتكاب الجريمة، أو احد سلوكياتها، ولا بجنسية مرتكبها، ولا بطبيعة الجريمة ومساسها بالسيادة والمصالح الوطنية.

وإنما يتطلب فقط القبض على الجاني في إقليم الدولة ليعطى للقانون الجنائي الوطني الاختصاص، وهذا المبدأ يتلائم كثيرا وطبيعة جرائم الابتزاز الالكتروني رغم ما يطرحه من تنازع حاد بين التشريعات الجنائية في الدول.

وعليه فانه يمكننا القول بأن أهمية هذا المبدأ ومدى ملائمته لجرائم الابتزاز الالكتروني، مستمدة من خطورتها من جهة، ومن طبيعتها من جهة أخرى، لكونها سهلة الوقوع من أشخاص يحملون جنسيات مختلفة وتمتد عناصرها المادية وسلوكياتها الإجرامية بين أكثر من دولة، وفي فترات زمنية قصيرة جدا، ومبدأ العالمية يبقى عاجزا عن معالجة جميع القضايا في هذا الشأن ما لم يكن هناك تعاون دولي جاد وسريع، وكذا وجوب إعداد تشريعات وطنية لتجريم الظاهرة، ومنها إمكانية معاقبة كل من يتم القبض عليه على إقليم الدولة دون مراعاة لجنسيته أو مكان وقوع الفعل الإجرامي.

والملاحظ أن اغلب التشريعات الوضعية ومنها التشريع المصرى، لم ينص على هذا المبدأ بالرغم من أهميته الجلية خصوصا في مجال جرائم الابتزاز الالكتروني، ونرى وجوب النص عليه عند إعداد قانون خاص بمعالجة جرائم الابتزاز الالكتروني، وهذا بالرغم من أن الاتفاقيات الدولية تركز بل وتعول عليه كثيرا في هذا المجال، خاصة اتفاقية بودابست 2001 لمكافحة الجرائم المعلوماتية وكذا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية 2003 في المادة 26 منه، كما أن الفقه يرى وجوب الأخذ به على غرار جريمة القرصنة في القانون الدولي الجنائي.[164]

ونحن نعتقد أن من اهم واخطر جرائم الابتزاز الالكتروني، جريمة القرصنة، لكونها تهدد امن وسلامة المجتمع الدولي من خلال اهتزاز الثقة في التعامل بالبيانات والمعطيات على الشبكة العنكبوتية، مما يهدد الاقتصاد العالمي الذي يشهد وتيرة متصاعدة في المجال المالي والمصرفي، وعليه أصبح من الضروري الاخذا بهذا المبدأ ومعاقبة الجاني في أي إقليم يتم فيه القبض عليه دون مراعاة لجنسيته أو مكان ارتكاب جريمته لارتكابه جريمة عالمية

) راجع في ذلك: د. محمود نجيب حسني، مرجع سابق، ص163140(

) راجع في ذلك: د. محمود نجيب حسني، مرجع سابق، ص141. 164(

المطلب الرابع

التحديات التي تواجه الجوانب الإجرائية في جريمة الابتزاز الالكتروني

بالنظر لطبيعة جرائم الابتزاز الالكتروني، فإنها لا تترك اثرا ماديا في مسرح الجريمة، بالإضافة إلى قدرة الجاني على إتلاف وتشويه الدليل في وقت قصير وتظهر جملة من التحديات تتعلق أساسا بما يلي:

أولا : بالنسبة لإجراءات التفتيش:

ذلك إن جرائم الابتزاز الالكتروني تعتمد على نظم المعلومات، وقد تتجاوزه إلى أنظمة أخرى غير نظام المشتبه به، وهذا الإجراء يعتمد على مد نطاق التفتيش الى نظام غير نظام محل المشتبه به، وهذا من شانه أن يطرح جملة من الإشكاليات القانونية من خلال مدى احترام وعدم المساس بالحريات الشخصية ومبدأ سرية الاتصالات للأشخاص التي يمتد إليهم التفتيش.[165]

ثانيا : بالنسبة لإجراءات الضبط:

حيث لا تتوقف إجراءات الضبط على جهاز الحاسب، بل تمتد من ضبط المكونات المادية إلى مختلف أجزاء النظام، وعليه فتمتد إلى المعلومات والمعطيات والبيانات والبرامج المخزنة في النظام أو إلى النظم المرتبطة بالنظام محل الاشتباه وكل الأشياء ذات الطبيعة المعنوية لأنها معرضة بسهولة للتلف والضياع، وهذا ما يثير إشكالية من الجهة القانونية خصوصا ما تعلق بالحقوق المحمية قانونا، وكذا الحق في سرية البيانات واحترام سرية الاتصالات. [166]

ثالثا: بالنسبة لأدلة الإثبات والإدانة:

وهي كلها بيانات معنوية كسجلات الحاسب ومعلومات الدخول والاشتراك والنفاذ، وهي تثير جملة من الإشكاليات أمام القضاء من حيث مدى قبولها وحجيتها مع وسائل الإثبات التقليدية.

---

165) راجع في ذلك: د. عبد الفتاح حجازي: مكافحة جرائم المعلوماتية والانترنت، دراسة معمقة في القانون المعلوماتي، ط 1، دار الفكر الجامعي، الإسكندرية، سنة 2006،ص14

166) راجع في ذلك: عبد الله عبد الكريم عبد الله: جرائم المعلوماتية والانترنت دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، ط 1، منشورات الحلبي الحقوقية، لبنان، سنة 2007، ص 47.

وخلاصة القول أن أهم التحديات التي تواجه جرائم الابتزاز الالكتروني تتمثل في: [167]

- الحاجة إلى سرعة الكشف عن الجريمة وتعقبها وخشية ضياع الدليل بالإضافة إلى خصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم.
- مدى قانونية وحجة الأدلة في جرائم الابتزاز الالكتروني التي تقع عن الانترنت.
- الحاجة إلى المزيد من التعاون الدولي في مجال التحقيق وتسليم المجرمين[168][169] وتنفيذ الأحكام القضائية[170].

الفصل الرابع

الادلة المعلوماتية في جرائم الابتزاز الالكتروني

تمهيد وتقسيم:

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

) انظر في ذلك: محمد الشكوابة، جرائم المعلوماتية والانترنت، دار الثقافة للنشر، الأردن، سنة 2004، ص16713(

) انظر في ذلك: توصيات مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين لسنة 1995م منشورات168(الأمم المتحدة، ص 120، وايضا راجع في ذلك: د. عبدالعظيم مرسى وزير، المبادئ العامة لتسليم المجرمين في ضوء المجهودات الفقهية والمعاهدات الدولية، المؤتمر العلمى السنوى الثالث، كلية الحقوق، جامعة المنصورة، تحت عنوان المواجهة التشريعية لظاهرة الارهاب على الصعيدين الوطنى والدولي، القاهرة ، بتاريخ 21 – 22 ابريل 1998، ص 127 وما بعدها، وايضا: عبدالفتاح محمد سراج، النظرية العامة لتسليم المجرمين، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، مصر ، سنة 1999، ص 57.

) انظر في ذلك: ياسر محمد الجبور، تسليم المجرمين او تقديمهم في الاتفاقيات الدولية والنظام الاساسي 169(للمحكمة الجنائية الدولية، رسالة ماجستير، جامعة الشرق الاوسط، سنة 2011، ص9.

) انظر في ذلك: حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء 170(الجنائى الوطنى، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، سنة 2000 ، ص 25 ، 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 20 – 21 مايو 2003 ، ص 10.

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[171] 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[172] .

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

---

(171) 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

) راجع في ذلك: د. محمد مدحت عزمى، المعاملات التجارية الالكترونية، الاسس القانونية والتطبيقات، الطبعة 172(الاولى، مركز الاسكندرية للكتاب، مصر، سنة 2009، ص 354، وايضا : د. احمد سفر، العمل المصرفي الالكترونى في البلدان العربية، الطبعة الاولى، المؤسسة الحديثة للكتاب، لبنان، سنة 2006، ص 219

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.

غير ان جرائم الابتزاز الالكتروني قد اتسمت بطبيعة خاصة، وهذه الطبيعة الخاصة تثير بعض المشكلات عند ضبط وتحقيق وإثبات تلك الجرائم، والتى تتمثل في كون الحاسب الآلي أداة الجريمة وأن الجريمة غالباً ما تتم على بيانات ومعلومات متخزينة داخل الحاسب وأن هذه النوعية من الجرائم لا تقع إلا من أشخاص لهم خبرة فنية كبيرة في مجال الحاسب الآلي ويتسمون بالذكاء الشديد، وكذلك تثير العديد من الصعوبات في مجال إثبات هذه الجرائم.

وترتيبا على ذلك، يتعين علينا التعرض لمعوقات الاثبات الجنائي في اطار جرائم الابتزاز الالكتروني من خلال المبحث الاول، على ان نخصص المبحث الثاني لتناول طرق اثبات جرائم الابتزاز الالكتروني ، على السياق التالي:

- **المبحث الاول:** معوقات الاثبات الجنائي في جرائم الابتزاز الالكتروني.
- **المبحث الثاني:** طرق اثبات جرائم الابتزاز الالكتروني.

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[173].

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.
- **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** : الضخامة البالغة لكم البيانات المتعين فحصها.

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

---

173) انظر في ذلك: حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء الجنائى الوطنى، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، سنة 2000 ، ص 25 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 20 – 21 مايو 2003 ، ص 10.

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 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.

ولعل هذا الامر يكشف عن اهمية التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للقارات والتي منها تلك الجرائم التي تقع بسبب ثورة الإتصالات عن بعد[174].

المطلب الثاني

سهولة إخفاء الدليل او محوه في جرائم الابتزاز الالكتروني

---

174) انظر في ذلك: حمد عبدالحليم شاكر على، الاحكام الاجرائية والموضوعية للمعاهدات الدولية امام القضاء الجنائى الوطنى، مرجع سابق ، ص 55 وايضا : عبدالرؤوف مهدى، التعاون القضائى كاحد موجبات الاختصاص الوطنى، مرجع سابق ، ص 10.

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.

ويلاحظ أن المجني عليهم قد يساهمون بدورهم في عدم كشف هذه الجرائم، فقد يحجمون عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم، وقد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم، أو رغبتهم في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليدها من الآخرين.

وهذا الأمر قد تلجأ إليه عادة المؤسسات المالية كالبنوك والمؤسسات الإدخارية وشركات الإقراض والسمسرة، حيث يخشى القائمون على إدارتها من شيوع أمر الجرائم التي تقع داخلها على زعزعة الثقة فيها.

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[175].

المطلب الرابع

صعوبة فهم الدليل المتحصل من الوسائل

) انظر في ذلك: د. ابراهيم بن عوض العتيبى، استخدام التقنية في التحقيقات الامنية، مقال منشور بمجلة 175(التقنية والامن، مجلة كلية الملك خالد العسكرية، العدد 80 ، سنة 2005 ، ص 7.

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 1985 و 1995 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[176].

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.

المبحث الثاني

طرق اثبات جرائم الابتزاز الالكتروني

176) انظر في ذلك: د. ابراهيم بن عوض العتيبى، استخدام التقنية في التحقيقات الامنية، مقال منشور بمجلة التقنية والامن، مجلة كلية الملك خالد العسكرية، العدد 80 ، سنة 2005 ، ص 7.

مـع تزايـد اسـتخدام الحاسـب والشـبكة العالميـة للمعلومـات (الإنترنـت) والشـبكات الداخليـة والخارجية تزايدت نسبة الجريمة المرتكبة باستخدام هذه التقنيات الجديدة، ويعمد مرتكبو الجرائم سواء أكانت جريمة تمت عبر الحاسب أم جريمة تمت على الحاسب بمشتملاته المادية والمعنوية وقواعد البيانات المستخدمة به، إلى استخدام الحاسب وشبكة الإنترنت ما داموا يشعرون أن أجهزة إنفاذ القانون ورجال القضاء والنيابة والمحامين ورجال البحث الجنائي عاجزون عن ضبطهم واستخلاص دليل إدانتهم سواء أكان دليلاً حسياً أم رقمياً.

وعلى الرغم من أن التعامل في مسرح الجريمة، سواء أكان مسرحاً مادياً أم مسرحاً إلكترونياً، يتطلب إجراءات روتينية معينة متفق عليها لحماية الدليل وإبراز قيمته الاستدلالية، إلا أن طرق حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة المادي إلى مسرح الجريمة الإلكتروني أو الرقمي، ذلك أن التطبيقات أو البرامج والبيانات المرقمة عنصران أساسيان يتحتم على أجهزة إنفاذ القانون وخبراء الأدلة الجنائية، جمعهما واستخلاصهما.

ويتطلب تشغيل نظم الاتصالات الحاسبية، أن تكون هناك آلية لعَنْوَنة الأجهزة، سواء المرسلة أو المستقبلة، كما تتطلب أيضاً أن تكون هناك آلية لضمان وصول أو التحقق من وصول الاتصال أو الرسالة للجهة المقصودة فعلاً وأن يكون هناك ضمان أو تحقق من جهة الإرسال.

وتستخدم برتوكولات الاتصالات والتطبيقات المعلوماتية، لتحقيق هذه الغاية، حيث إن الأنشطة التي يجريها مستخدمو شبكة الإنترنت تشكل جانباً بالغ الأهمية في تحقيق جرائم الابتزاز الالكتروني، نظراً لاحتواء هذه البروتوكولات والتطبيقات على كافة المعلومات والبيانات المتعلقة بنشاط مستخدم الشبكة إذا كان نشاطه إجرامياً، سواء من حيث التحدي الزمني للاستخدام غير المشروع أم من حيث تحديد مكان صدور أو نشأة الفعل الإجرامي ومدى اتساع هذا النشاط وتحديد المجني عليه أو عليهم، من حيث المكان أو الزمان أو تحديد من أصابهم الضرر الجرمي من النشاط الإجرامي.

ويعتبر نظام TCP/IP من أكثر البروتوكولات المستخدمة في شبكات الإنترنت فهي جزء أساسي منه، لذلك نبرز أهمية الاستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها هذا البروتوكول في تحقيق جرائم الابتزاز الالكتروني، حيث أنها تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة التي أصابها الضرر من الفعل الإجرامي وتحديد نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة، أو إحداث الضرر المدني .

ومع التطور التقني لأساليب ارتكاب جرائم الابتزاز الالكتروني، أصبح واجبا على سلطات إنفاذ القانون أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي.

وتتحدد أهداف هذا البحث في إلقاء الضوء على العلاقة بين الجرائم على الحاسب والدليل الرقمي المستخرج من أجهزة الحاسب ما يُمكّن كلاً من:

أ- تدريب أجهزة إنفاذ القانون ونعنى بها الشرطة، النيابة، القضاء، من التعامل مع الدليل الرقمي، لبناء دليل جنائي أو مدني مقبول أمام العدالة، يُمكّن القاضي من إصدار حكم بالإدانة أو البراءة أو الحكم بتعويض في القضايا المدنية، وتمكن هذه الأجهزة أيضاً من معرفة متى وأين يمكن استدعاء خبراء الحاسب وكيفية المحافظة على مسرح الجريمة المعلوماتي وكيفية استخلاص الدليل الرقمي.

ب- تدريب مسؤول أمن الحاسب سواء في القطاع الخاص أو الأجهزة الحكومية من التعامل مع الدليل الرقمي وكيفية استكشافهم بأن النظام المعلوماتي المسؤولين عن حمايته قد تعرض لإحدى صور الجريمة عبر الحاسب وكيفية محافظتهم على الدليل الرقمي لحين استدعاء أجهزة إنفاذ القانون.

ج- المحامون، ليتعرفوا عن قرب على إمكانية الإدانة أو البراءة باستخدام الدليل الرقمي مما يمكنهم من إعداد دفاعهم بالشكل المتفق مع الدليل المستخرج.

د- خبراء الأدلة المعاونين لأجهزة إنفاذ القانون، لبيان كيفية مقارنتهم للدليل الرقمي وإعطاء الخبرة القائمة على يقين علمي بشأن الدليل المقدم في الحالة المعروضة عليهم.

ويُعرّف الدليل الرقمي بأنه هو المأخوذ من أجهزة الحاسب، وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.

ويمتاز الدليل الرقمي عن الدليل المادي المأخوذ من مسرح الجريمة المعتاد، بما يلي:

1. طريقة نسخ الدليل الرقمي من أجهزة الحاسب تقلل أو تعدم تقريباً مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء.
2. باستخدام التطبيقات والبرامج الصحيحة، يكون من السهولة تحديد ما إذا كان الدليل الرقمي، قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل.

3. الصعوبة النسبية لتحطيم أو محو الدليل، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الحاسب، فيمكن للدليل الرقمي أن يعاد تظهيره من خلال الحاسب دسك.
4. نشاط الجاني لمحو الدليل، يسجل كدليل أيضاً، حيث أن نسخة من فعل الجاني لمحو الدليل، يتم تسجيلها في الحاسب ويمكن استخلاصها لاحقاً لاستخدامها كدليل إدانة ضده.
5. الاتساع العالمي لمسرح الدليل الرقمي، حيث يُمَكّن مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية، وبمناطق مختلفة من العالم، مما يساهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبياً.
6. امتيازه بالسعة التخزينية العالمية، فآلة الفيديو الرقمية، يُمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين مكتبة صغيرة وهكذا.
7. يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت فالدليل الرقمي يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

وترتيبا على ذلك، نعرض لوسائل إثبات جرائم الابتزاز الالكتروني، من خلال المطلب الاول على ان يختتم هذا المطلب بالأدلة المعلوماتية في الدعوى الجنائية في مطلب ثان، على السياق التالي:

- **المطلب الاول:** وسائل إثبات جرائم الابتزاز الالكتروني.
- **المطلب الثاني:** الأدلة المعلوماتية في الدعوى الجنائية .

المطلب الاول

وسائل إثبات جرائم الابتزاز الالكتروني

من المقرر ان وسائل الاثبات الالكترونية المعروفة حتى الان، هى البريد الالكترونى، والتوقيع الالكتروني، والعقد الالكتروني، نعرض لكل منهم في فرع مستقل.

الفرع الاول : البريد الالكتروني.

الفرع الثاني : التوقيع الالكترونى.

الفرع الثالث : العقد الالكترونى.

الفرع الاول

البريد الالكتروني

يمكن تعريف البريد الالكترونى على انه تلك الرسالة التي تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل، كليا أو جزئيا بوسيلة الكترونية أو رقمية.

وعرفه القانون العربي النموذجي الموحد: بانه نظام للتراسل باستخدام الحاسب وهذا البريد يستخدم لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم لا يمكن الدخول إليه إلا عن طريق كلمة مرور، وتكمن الخطورة في أن الولوج اليه من شخص غير صاحبه بعد حصوله على كلمة المرور بأي طريقة سواء كانت عن إهمال صاحبه بتسريب كلمة المرور منه دون قصد متعمد أو إهماله فنيا ومن ثم يصيبه ضرر.

وفي البداية كان التراسل بالبريد يوجب دخول كلا من الراسل والمرسل إليه إلى الشبكة في الوقت ذاته لتنتقل الرسالة بينهما آنيا، كما هو الحال في محادثات التراسل اللحظي المعروفة اليوم، إلا أن البريد الإلكتروني لاحقا أصبح مبنيا على مبدأ التخزين والتمرير، حيث تُحفظ الرسائل الواردة في صناديق بريد المستخدمين ليطلعوا عليها في الوقت الذي يشاؤون.

وقد ظهرت بدايات ما أصبح لاحقا البريد الإلكتروني على شبكة أربانت، سلف الإنترنت التي تعرفها اليوم، وتطوّر في مراحل عديدة كان من بينها أن أرسل راي توملينسون سنة 1971 أوّل رسالة تستخدم الرمز "@" للفصل بين اسم المستخدم وعنوان الحاسب كما استقر عليه الوضع اليوم، ومع هذا لا يوجد مخترع فرد للبريد الإلكتروني إذ أنه تطوّر في عدة خطوات أسلمت كل منها إلى التالية.

ومن اهم مميزات البريد الإلكتروني، إمكانية إرسال رسالة إلى عدة متلقين، وإرسال رسالة تتضمن نصا صوتيا أو فيديو والصور والخرائط، والسرعة في إرسال الرسائل حيث لا تستغرق إرسال الرسالة بضع ثوانٍ فقط لكي تصل إلى المرسل إليه وفي حال عدم وصول الرسالة فإن البرنامج يحيط المرسل علما بذلك.

ويمكن للمستخدم أن يستخرج الرسائل من صندوق البريد عن طريق برنامج البريد الذي يمكن المستخدم من مشاهدة الرسائل وبناء على رغبته إذا شاء أن يرسل جوابا لأي منها وعندما يبدأ طلب بريد الإلكتروني يتم إخبار المستعمل بوجود رسائل بالانتظار في صندوق البريد عن طريق عرض سطر واحد لكل رسالة بالبريد الإلكتروني قد وصلت السطر يعطي اسم المرسل ووقت وصول الرسالة وطول الرسالة في القائمة.

ويمكن للمستخدم أن يختار رسالة من الموجز ونظام البريد الإلكتروني يعرض محتوياتها وبعد مشاهدة الرسالة على المستخدم أن يختار العملية التي يرغب فيها فإما أن يرد على المرسل أو يترك الرسالة في صندوق البريد لمشاهدتها ثانية عند الحاجة أو يحتفظ بنسخة عن الرسالة في ملف أو التخلص من الرسالة بإلغائها.

ومن الأمثلة لخدمات البريد الإلكتروني على الويب

- زمبرا.
- بريد جوجل (جيميل).
- بريد ياهو!
- ويندوز لايف هوتميل.
- بريد ياندكس.

وغالباً ما يكون التعامل معه من خلال صفحة البريد الإلكتروني للجهة التي تقدم خدمة البريد الإلكتروني على الشبكة العنكبوتية لإرسال واستقبال الرسائل، ويمكن استخدام برامج خاصة لإرسال واستقبال الرسائل مثل :

- برنامج أوت لوك (OutLook).
- برنامج أوت لوك إكسبريس (OutLook Express).
- برنامج إيودورا (Eudora).
- برنامج ميل (Mail) بالنسبة لأجهزة الماك.
- برنامج ثندربرد.

ويلاحظ ان أمن البريد الإلكتروني هو الوسيلة الأساسية لقطاع الأعمال والاتصالات، يزداد استخدامه يوما بعد يوم، ويستخدم لنقل الرسائل النصية ونقل المستندات وقواعد البيانات، وبما أن عملية نقل البيانات عملية حساسة جدا فسلامة هذه البيانات هي موضع تساؤل، وهذا ما يمثل المشكلة، فالباب مفتوح على تفاصيل العقود بين الشركات المتنافسة، والأسوء من ذلك أن هناك قدرات لتزوير البريد الإلكتروني، وهناك عدد من الاعتداءات مبلغ عنها من هذا القبيل.

الفرع الثاني

التوقيع الالكتروني كوسيلة إثبات حديثة في القانون

من المقرر ان التوقيع الالكترونى هو عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز الإلكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا

ودوليا ويطلق عليها الشهادة الرقمية Digital Certificate ويتم تخزين فيها جميع معلومات الشخص وتاريخ ورقم الشهادة ومصدرها، وعادة يسلم مع هذه الشهادة مفتاحان أحدهما عام والآخر خاص.

- أما المفتاح العام فهو الذي ينشر في الدليل لكل الناس.
- والمفتاح الخاص هو توقيعك الإلكتروني.

ويمكن أن نعرف التوقيع الإلكتروني على أنه طريقة اتصال مشفرة رقميا تعمل على توثيق المعاملات بشتى أنواعها والتي تتم عبر صفحات الإنترنت.

وتكمن وظيفة التوقيع الإلكتروني في وظيفتين أساسيتين:

1- أن التوقيع الرقمي يثبت ان الشخص الذي وقع الوثيقة انصرفت إرادته إلى الالتزام بما وقع عليه، ذلك أن التوقيع الرقمي يحدد الشيء أو الوثيقة التي تم توقيعها بشكل لا يحتمل التغيير.

2- **التوقيع الرقمي:** يقوم على وسائل التشفير الرقمي الذي يعتمد على خوارزمات او معادلات حسابية لضمان سرية المعلومات.

حيث يتم التوقيع باستعمال مفتاحين عام وخاص يكونان مصادقا عليهما من طرف ثالث هي سلطة مختصة تصدر شهادة مصادقة للتوقيعات الرقمية، حيث ان المفتاح الأول يستعمل لتشفير الرسالة الالكترونية، والثاني يعتمد عليه مستقبل الرسالة بفتح ذلك التشفير، وبذلك يتم توقيع المرسل.

أما التوقيع الالكتروني: ولما يتطلبه من تدخل شخص ثالث هي هيئة التصديق الالكتروني تمنع التلاعب به وبمضمون الرسالة الالكترونية، وبذلك يتم توفير التعرف على المستخدم ويتوفر عدم القدرة على الانكار، فالتوقيع يستخدم على كافة الرسائل الالكترونية، والعقود الالكترونية فهي بيانات مشفرة تضاف الى البريد الالكتروني او العقد الالكتروني.

الفرع الثالث

العقد الالكتروني كوسيلة اثبات حديثة

(le contract électronique)

ظلت العقود وطرقها ووسائلها تتطور بسرعة وبصفة مستمرة مما أدي إلى ظهور عقود جديدة، وفي خضم الثورة الرقمية والطفرة المعلوماتية التي عرفها العالم اليوم، حيث ان تكنولوجيا المعلومات أصبحت تشكل الجهاز العصبي للمجتمعات الحديثة، عرفت العمليات التعاقدية مجموعة

من التغيرات مست نظامها وبنيتها القانونية، فأصبح إبرام العقود يتم عن طريق وسائل الاتصال الحديثة، فنشأ ما يعرف بالعقد الالكتروني.

ولقد أورد الفقه عدة تعريفات للعقد الإلكتروني، فمنهم من عرفه بالاعتماد على إحدى وسائل إبرامه معتبرا أن: " العقد الإلكتروني هو العقد الذي يتم إبرامه عبر الأنترنت."

وعلى صعيد التشريعات العربية نجد المادة 14من قانون إمارة دبي في شأن المعاملات والتجارة الالكترونية رقم 2 لسنة 2002م قد اجازت التعاقد بوسائط الكترونية حيث نصت فقرتها الأولى على أنه : "يجوز أن يتم التعاقد بين وسائط الكترونية مؤتمنة، متضمنة نظامي معلومات الكترونية أو أكثر تكون معدة ومبرمجة مسبقا للقيام بمثل هذه المهمات ويتم التعاقد صحيحا ونافذا ومنتجا آثاره القانونية على الرغم من عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الأنظمة".

كما أجاز المشرع الأردني إبرام العقود إلكترونيا بواسطة الرسائل الالكترونية بتقريره في المادة 13 من قانون المعاملات الالكترونية رقم 85 لسنة 2001م : حيث اعتبر الرسالة الالكترونية وسيلة من وسائل التعاقد فنص علي الاتي:

"تعتبر الرسالة الالكترونية وسيلة من وسائل التعبير عن الإرادة المقبولة قانونا لإبداء الإيجاب والقبول بقصد إنشاء التزام تعاقدي".

ايضا نص قانون المعاملات الالكترونية السوداني في المادة الثانية منه والخاصة بالتعريفات علي ان العقد الالكتروني : هو الاتفاق الذي يتم انعقاده بوسائل الكترونية، كليا او جزئيا، وهو ايضا يعترف بالعقد الالكتروني ايا كانت وسيلته .

وإذا انتهينا إلى اعتبار رسائل البريد الإلكتروني بهذا المعنى أدلة إثبات، إلا أن حجية هذا الدليل الاتفاقي أي العقد الالكتروني بهذه الوسيلة, تبقي خاضعة للسلطة التقديرية للقاضي، من حيث كونها دليلاً كاملاً أو ناقصاً، فقواعد حجية الأدلة الكتابية تتعلق بالنظام العام باعتبار أن هذه القواعد ترتبط بأداء القضاء لوظيفته، فهذا الاتفاق لا يجب أن يقف حائلاً أمام ممارسة القاضي لسلطته التقديرية لتقدير حجية الدليل المقدم في الإثبات، وهو ما يعني أن رسالة البريد الإلكتروني لا تعتبر بحال دليل إثبات قاطع في النزاع، بل تخضع حجيتها في الإثبات لتقدير القاضي، فهي حجية نسبية، بحيث يستطيع قاضي الموضوع دائما التحقق من عدم وقوع أي تلاعب أو تحريف في الرسالة الإلكترونية، وفي حالة عدم اقتناعه يمكنه عدم الأخذ بهذه الرسالة ونخلص إلي نتيجة مؤداها أن الرسالة الإلكترونية لا تتمتع بالثقة فيما يتعلق بهوية مرسلها ومدي إمكانية نسبة الرسالة إليه وسلامة

محتواها، وبالتالي فإن قوتها في الإثبات ستخضع لسلطة القاضي التقديرية، ومدي إلمامه وتفهمه بالنواحي التقنية الخاصة بتكنولوجيا المعلومات والحاسب والأدوات المعلوماتية.

وغالبا ما تشترط التشريعات المتعلقة بقواعد الإثبات وجود سند محرر كتابي أصلي، لإثبات اي تصرفات قانونية معينة، ونظراً لكون المعاملات الالكترونية قائمة على التعاقد دون مستندات ورقية، فإن مسألة الإثبات قد تشكل عائقاً أمام تطورها، إذ أن اشتراط وجود مستندات ورقية هو أمر لا يتفق وطبيعة التجارة الالكترونية التي تهدف إلى التخلص من أكوام المستندات الورقية والاستعاضة عنها بوثائق الكترونية محفوظة على أجهزة الحاسب أو على أقراص تخزين، إذ أن مثل هذه المتطلبات تلزم المتعاملين بالاحتفاظ بمحررات ومستندات لجميع التصرفات التي يجرونها، بما فيها التصرفات اليومية الأمر الذي يصعب مهمة ممارسة التجارة ويزيد تكاليفها.

وفي قانون التجارة الالكترونية الاماراتي جاء تعريف السجل او المستند الكتروني في المادة الثانية منه تعريفا له علي انه "كل سجل او مستند يتم انشاؤه او تخزينه او استخراجه او نسخه او ارسالة او ابلاغه او استلامه بوسيلة الكترونية، على وسيط ملموس او على اي وسيط الكتروني اخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه."

اما في قانون المعاملات الالكترونية السوداني فقد جاء تعريف المستند الالكتروني تحت مفهوم التوقيع الرقمي, في المادة 3 منه بانه "يقصد به التوقيع الذي يتم انشاؤه وارساله واستقباله وتخزينه بوسيلة الكترونية ويتخذ شكل حروف او ارقام او رموز او اشارات يكون لها طابع متفرد ويسمح بتحديد هوية وتمييز شخصية الموقع عن غيره."

وقد تطرّق البند 3 –3 من القواعد النموذجية والارشادات حول التجارة الدولية (URGETS) الصادر عن غرفة التجارة الدولية اللبنانية, الى تعريف المستند الإلكتروني بأنه محتوى أي اتصال يفترض عملية نقل الكترونية لمعلومات رقمية عبر شبكات الإتصال المفتوحة للعموم أو المغلقة, أو عبر أية وسيلة اتصال الكترونية ممكن الوصول اليها, أي قابلة للاستعمال في مراجعات لاحقة.

وفي القانون المصري ورد تعريف المستند الالكتروني في المادة الاولى من قانون التوقيع الالكترونى, ووصفه بانه رسالة بيانات الكترونية او رقمية او ضوئية تخزن او ترسل او تستقبل كليا او جزئيا بوسيلة الكترونية او رقمية او ضوئية او باي وسيلة اخرى مشابهة .

ويبدو ان المشرع المصري قد تبنى التعريف الوارد في قانون الاونسترال النموذجي للتجارة الالكترونية.

من كل ذلك يتضح لنا، ان هنالك نقاط للاتفاق والاختلاف, بين المستند الالكتروني والمستند التقليدي, وان الاختلاف الاساسي والجوهري بينهما هو الدعامة التي يكون عليها كل منهما, فالمستند التقليدي دعامته ورق ملموس, بعكس المستند الالكتروني, فان دعامته برامج الحاسب, او اي وسائط تقنية حديثة.

واعتمادا علي هذا الفارق في التكوين، والوجود، يري البعض ان المستند الالكتروني، لا يكتسب صفة الدوام والاستقرار والثبات، اذ انه قابل للمحو والتعديل، كما انه غير قابل للقراءة خاصة عندما تتغيير التقنيات، او البرمجيات، وعلي وجه التحديد التقنيات البرمجية النصية (OFFECE) والبرامج التشغيلية المتجددة، في اطار المنافسة والاحتكار لسوق البرمجيات من بعض الشركات الكبرى مثل شركة مايكورسوفت.

الا ان كانت هذه الاشكالية في سبيلها للحل النهائي بادخال بعض برامج المعالجة التوافقية النصية والبرمجية، لدى شركات البرمجيات، وذلك وفقا لخصائص كل برنامج علي حده، بحيث يكون هناك نموذج برمجي عالمي يقلل من حدة الاحتكار لهذه الخدمة والاختلاف البرمجي، ويساعد علي عرض النصوص الالكترونية بواسطة اي برنامج مستخدم ايا كان نوعه.

كما انه ومن الجانب الاخر، فان البعض يرى ان المستند التقليدي, يتفوق علي المستند الالكتروني, في ان الاخير تسهل قراءته، بينما يحتاج المستند الالكتروني الي وسائط الكترونية لقراءته من خلال حاسب وخلافه من الوسائط الالكترونية, بينما يمكن قراءة المستند التقليدي بسهولة ومباشرة من دعامته الورقية.

ايضا يري البعض، ان المستند الورقي قابل للنقل الي اي مكان وبسهولة, بينما المستند الالكتروني يتوجب توافر وسائل تقنية لقراءته ونقله وهي الدعامة الالكترونية نفسها.

اما انصار المستند الالكتروني فيرون ان المستند الالكتروني ووفقا لدعامته الالكترونية، او ركيزته الالكترونية، والتي تستوعب معلومات كبيرة تبعا لحجم الوسيط ومقدار المعلومة، فان ذلك يتيح الفرصة لعرض عدد غير محدود من المستندات، في مساحة صغيرة من الوسيط الالكتروني، كما ان المستند الالكتروني يسهل البحث عنه وادارته، والتعديل فيه، وتخزينه واسترجاعه، وتبويبه، باستعمال بعض خصائص البرمجة الالكترونية، بعكس المستند التقليدي الذي يثبت علي حالة التي اعد بها.

فيما يري البعض ان المستند الالكتروني معرض للخلل تبعا لتعرض الوسائط الالكترونية للخلل التقني في اطار التعدي علي البرامج او الاجهزة بواسطة البرمجيات الضارة كالفيروسات.

المطلب الثاني

الأدلة المعلوماتية في الدعوى الجنائية

مع ازدياد الاتجاه الى الاعتماد على نظم الحاسب والشبكات في الاعمال، أثيرت ولا تزال تثار مشكلة امن المعلومات، أي حماية محتواها من أنشطة الاعتداء عليها، سواء من داخل المنشاة او من خارجها، وانماط الاعتداء عديدة تبدأ من الدخول غير المصرح به لملفات البيانات الى احداث تغيير فيها وتحوير بمحتواها او اصناع بيانات وملفات وهمية، او اعتراضها اثناء نقلها، او تعطيل عمل النظام، او الاستيلاء على البيانات لاغراض مختلفة او احداث تدمير او احتيال للحصول على منافع ومكاسب مادية او لمجرد الاضرار بالاخرين، وحتى لاثبات القدرة واحيانا مجرد أنشطة تستهدف المزاح الذي سرعان ما يكون عملا مؤذيا يتجاوز المزاح.

ولا شك ان الحماية من هذه الاعتداءات واثبات قدرة النظام على التعامل الآمن مع البيانات يثير مشكلات اجرائية عديدة في معرض تفتيش نظم الحاسب او تقديم الدليل في الدعوى الجنائية، وفي النظم القانونية التي تنص على تجريم افعال الاعتداء على المعلومات.

والقاعدة العامة في الدعاوى الجنائية جواز الإثبات بكافة طرق الاثبات القانونية، والقيد على هذه القاعدة ان الدليل يتعين ان يكون من الادلة التي يقبلها القانون، وبالتالي تظهر اهمية اعتراف القانون بالادلة ذات الطبيعة الالكترونية، خاصة مع احتمال ظهور أنشطة إجرامية عديدة في بيئة الاعمال والتجارة والبنوك الالكترونية.

والمعلومات، وان كانت قيمتها تزيد شيئا فشيئا عن الماديات والطاقة، إذ أنها ليست ماديات لتقبل كبينة في الإثبات، ووسائط تخزينها غير الورق كمخرجات لا تحظى من حيث محتواها بقبولها دليلا ماديا، علي اقل تقدير فيما صدر من أحكام حتى الآن.

ومن هنا كان البحث القانوني في العديد من الدول ومن بينها مصر، يتجه وبجدية إلى الاعتراف بالحجية القانونية لملفات الحاسب ومستخرجاته, والرسائل الالكترونية ذات المحتوى المعلوماتي, ليس بصورتها الموضوعة ضمن وعاء مادي ولكن بطبيعتها الالكترونية المحضة.

ونخلص إلي أن المشكلة تكمن في القواعد المخزنة، في صفحات الفضاء الالكتروني، وفي الوثيقة الالكترونية, إذ أن ما تحتويه من بيانات قد يكون الدليل بناءا علي الفعل المرتكب إن كان تحريفا أو دخولا غير مصرحا به, أو تلاعبا، فكيف يقبلها القضاء وهي ليست دليلا ماديا يضاف إلى محضر كالمستند الخطي، أو أقوال الشاهد أو تقرير الخبرة.

ولتجاوز هذه المشكلة يلجا القضاء الى انتداب الخبراء لاجراء عمليات الكشف والتثبت من محتوى الوثائق الالكترونية، ومن ثم تقديم التقرير الذي يعد هو البينة والدليل وليس الوثائق الالكترونية، لكنه مسلك تأباه بعض النظم القانونية عوضا عن مخالفته لأسس واغراض اجراء الخبرة وطبيعتها كبينة تخضع للمناقشة والاعتراض والرفض والقبول والرد والطعن فيها.

ولقد اتجه الاتحاد الاوروبي منذ منتصف الثمانينات الى توجيه مشرعي دول اوروبا لاقرار حجية الوثائق الالكترونية ومساواتها بالوثائق الكتابية من حيث الحجية، والاهم من ذلك التوجيه بعدم اشتراط ان تبرز من قبل منظميها، والاستعاضة عن ذلك بشهادات خطية صادرة عن الجهات مالكة النظم او جهات وسيطة, لما ظهر عمليا من مشكلات أبرزها ان جانبا من المعلومات لا يدخلها او ينظمها الأشخاص وانما يخلقها الجهاز نفسه ضمن عمليات المعالجة وفي اطار تقنيات البرمجيات القائمة على الذكاء الصناعي.

ذلك ان تفتيش مسرح الجريمة وما يتصل به من اماكن وضبط الاحراز ذات العلاقة بالجريمة امور نظمتها قوانين الاجراءات الجنائية، ويثور التساؤل حول مدى انطباق القواعد الاجرائية القائمة على حالة تفتيش نظم الحاسب وقواعد البيانات.

ليس ذلك فحسب، بل تثير اهمية الخبرة في هذا الحقل اذ كما يرى احد اشهر محققي التحقيقات الفيدرالية الامريكية ان الخطا في تفتيش وضبط الدليل قد يؤدي الى فوات فرصة كشف الجريمة او فوات فرصة الادانة حتى مع معرفة الجاني.

ذلك ان تفتيش نظم الحواسب هو تفتيش للفضاء الافتراضي ولحاويات التخزين، وتفتيش للإجراءات التي يحفظها الجهاز ان كان مزودا بحافظات الكترونية للعمليات المنفذة عبره، وهو امر يتعلق بالقدرة على تحديد المطلوب مسبقا وليس مجرد سبر غور نظام الكتروني، لان التعامل وفق المسلك الاخير قد يكون له عواقب قانونية، اهمها بطلان الاجراءات لانها خارج نطاق امر التفتيش والضبط او قد تنطوي الاجراءات على كشف خصوصية البيانات المخزنة في النظام.

كما إن البيانات المخزنة داخل النظم ليس جميعا تتصل بجريمة الاعتداء على النظام، فمنها بيانات خاصة واخرى ذات قيمة استراتيجية، لهذا اهتم الخبراء القانونيين بمخاطر الاعتداء على الخصوصية او الحياة الخاصة في معرض الكشف عن الدليل, أو في معرض الاقرار باستخدام دليل ذي طبيعة الكترونية.

سيما مع انعدام التنظيم لقواعد حماية الخصوصية, سواء من حيث تنظيم اعمال جمع وتخزين ومعالجة ونقل البيانات، او من حيث حقوق الدخول اليها وحق اصحابها بسلامتها وصحتها

وتعديلها، او من حيث اقرار الحمايات الادارية التنظيمية والمدنية والجزائية لهذه البيانات، يكون ثمة صعوبة في حماية الخصوصية ويكون ثمة احتمالات اكبر لاهدار الادلة غير القانونية ونشوء نزاعات في هذا الحقل .

ذلك إن النظم القانونية المقارنة وفي الوقت الذي تحركت فيه نحو حماية المعلومات واقرار حجية الادلة ذات الطبيعة التقنية، اتجهت ايضا من زاوية اخرى لاقرار ضمانات دستورية للمتهم المعلوماتي وضمانات اجرائية لكفالة سلامة اجراءت الملاحقة الجنائية في الدعاوى المتصلة بالمعلومات ونظم الحاسب، أبرزها الحق بالخبرة المقابلة للخبرة التي تجريها النيابة، والحق بعدم اجراء اية عمليات ضبط وتفتيش على نظم الحاسب دون حضور المعني او من يمثله قانونا.

واذا كانت الخصوصية وسرية البيانات امر ذو اهمية بالغة في شتى المواقع والقطاعات، فانها تكتسي اهمية أوسع في القطاع المصرفي، مرد ذلك التزام البنك القانوني بالحفاظ على السرية واحترام الخصوصية وتحمله مسؤوليات الإفشاء بالسر المصرفي .

كما ان من أكثر المسائل اهمية في حقل الاجراءات لدعاوى المعلوماتية في نطاقيها الحقوقي والجنائي، هي مسالة نطاق الافشاء بالمعلومات المطلوب او المتاحة للشاهد المعلوماتي، ان جاز التعبير، فالشاهد يشهد فيما شهد بذاته او قال او علم، لكن الامر في دعاوى المعلوماتية مختلف، اذ ثمة نظام معين للمنشأة وثمة اعمال لا تتصل بالشاهد بذاته بل ربما لا تتصل بشخص طبيعي وقد تكون متصلة بنظام الكتروني او نحوه، كما ان الشاهد يعلم الكثير وجزء مما يعلم واقع ضمن اطار الخصوصية والسرية.

فضلا عن ان التنظيم القانوني للقواعد الاجرائية والثبوتية المعتمدة في ادلة المعلوماتية او المتصلة بعوالم التقنية والالكترونية يجب اعادة توصيفها قانونا, بل وتنظيمها بشكل لا يضع الشاهد موضع المساءلة, ولا يحرم القضاء فرصة الافادة من شهادة الشاهد في سبر غور الحقيقة التي تتوقف في احيان كثيرة على ما يعلمه الشاهد بالخبرة النظرية, لا بما يعلمه بالواقع من حقائق رآها, او سمعها او نقلت له.

ولذلك يجب ان يكون التشريع موسعا من حيث الاجراءات وقواعد الاثبات ليواكب التطور التقني المتسارع في شأن اثبات جرائم الابتزاز الالكتروني.

الفصل الخامس

تطبيقات عملية لجرائم الابتزاز الالكتروني

تمهيد وتقسيم:

مـع المقرر ان استخدام الحاسب الآلـي فـي أواخـر سـبعينات القرن الماضـي، ترتـب عليـه انتشار ظـاهرة 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 555 مليون مستخدم سنويا، وأكثر من 1.5 مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات، وأكثر أنواع الجرائم سرقة هويات وابتزاز اصحابها، وعددها 224 مليون سرقة.

ويلاحظ أن مواقع التواصل الاجتماعي هي الأكثر اختراقا، إذ أن أكثر من 600 ألف حساب فيسبوك يتم اختراقها بغرض الابتزاز يوميا، وأن التكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ 100 مليار دولار، بعدما كانت في حدود 63,1 مليار دولار سنة 2011، وانها تجاوزت 120 مليار دولار بحلول سنة 2017.

وحسب تقرير نشرته شركة مشروعات الأمن المعلوماتي (CYBERSECURITY VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته 1 تريليون دولار خلال الفترة التي تمتد من 2017 الى غاية 2021 على منتجات وخدمات الأمن المعلوماتي لمكافحة تلك الجرائم.

وفي هذا الإطار فقد سجل هذا التقرير فتح حوالي مليون وظيفة خاصة بالأمن المعلوماتي خلال سنة 2016، ومن المتوقع أن يكون هناك عجز بحوالي 1.5 مليون وظيفة خلال عام 2019.

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 6 تريليون دولار بحلول سنة 2021 وهي ضعف الخسائر المسجلة سنة 2015 والمقدرة بحوالي 3 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، على ان يعرض المبحث الثاني لحالات عملية لجرائم الابتزاز الالكتروني على الصعيد العربي، واخيرا نتناول نماذج خاصة لبعض القضايا المتعلقة بجرائم الابتزاز الالكتروني في مصر من خلال المبحث الثالث والاخير، على الترتيب التالي:

- **المبحث الاول:** حالات عملية لجرائم الابتزاز الالكتروني على المستوى على الدولى.
- **المبحث الثاني:** حالات عملية لجرائم الابتزاز الالكتروني على الصعيد العربي.
- **المبحث الثالث:** نماذج لبعض القضايا المتعلقة بجرائم الابتزاز الالكتروني في مصر.

المبحث الاول

حالات عملية لجرائم الابتزاز الالكتروني

على المستوى على الدولى

هناك العديد من جرائم الابتزاز الالكتروني على الصعيد الدولى، منها حوادث الاختراق والقرصنة، والنصب الالكترونى بغية الابتزاز، والتجسس الالكترونى والمعلوماتي، وغيرها من مختلف جرائم الابتزاز الالكتروني الدولية، ومن أهمها التالي:

أولا: ظاهرة النصب الإلكتروني:

ظاهرة النصب الالكترونى هي ظاهرة منتشرة لدى الكثير من مستخدمي الإنترنت، حيث يحاول بعض الأشخاص الحصول على المعلومات الخاصة بمستخدمي الإنترنت، سواء كانت معلومات شخصية أو مالية، عن طريق الرسائل الإلكترونية أو مواقع الإنترنت التي تبدو وكأنها مرسلة من شركات أو مؤسسات موثوقة، سواء أكانت مالية أو حكومية، وصولا الي التهديد بمضمون الاحتيال، بغية الابتزاز.

وفي الفترة الأخيرة، ظهرت نماذج عديدة للنصب الإلكتروني، حيث أنتحل أحد الأشخاص صفة مدرس، وتحدث مع طالبات حول الدروس الخصوصية، واستدراجهم في حوار جنسي، وبعد ذلك أبتز أولياء الأمور لدفع أموال باهظة خوفًا من الفضيحة، وهناك حالات نصب واختراق شهيرة، جذبت اهتمام وسائل الإعلام العالمية.

ثانيا: اختراق العسكرية الأمريكية:

حيث جندت هيئة الاستخبارات السوفييتية (كي جي بي) المواطن الألماني ماركوس هيس، في ثمانينات القرن الماضي، للتجسس على أجهزة الحاسب العسكرية التابعة للجيش الأمريكي، وبالفعل تمكن من الحصول على المعلومات السرية المطلوبة، ومن جامعة بريمن الألمانية، استخدم «هيس» شبكة P-Datex للاتصال عبر الأقمار الاصطناعية، وشبكة Tymnet لمهاجمة 400 جهاز حاسب تابع للقوات الأمريكية بما فيها المنشآت العسكرية في ألمانيا واليابان، كما استطاع أيضًا اختراق بيانات معهد ماساتشوستس للتكنولوجيا، وقاعدة بيانات وزارة الدفاع الأمريكية، وهى البنتاجون، إلى أن تم كشف أمره بفضل كليفورد ستول، الذي ساعد السلطات الأمريكية في تعقب عمليات هيس واختراقاته، وحكم عليه بالسجن لمدة ثلاث سنوات بتهمة التجسس.

ثالثا: اختراق وكالة ناسا:

حيث تمكن عمر جوناثان جيمس، المعروف باسم comerade، وهو في السادسة عشرة من عمره، من الدخول على منظومة بيانات مركز مارشال لرحلات الفضاء، في هانتسفيل بولاية ألاباما الأمريكية، وبدأ تحميل الوثائق والبرمجيات الخاصة بمحطة الفضاء الدولية وهى ناسا عام 1999.

وقدر المسئولون في ناسا قيمة الوثائق التي سرقها جيمس بنحو 7.1 ملايين دولار، وأُجبرت هذه الحادثة الوكالة على إغلاق شبكاتها لمدة 3 أسابيع لإصلاح الأضرار الجسيمة بتكلفة 41 ألف دولار.

رابعا: اختراق سوني:

حيث اخترقت مجموعة من القراصنة في يونيو 2011، يطلقون على أنفسهم اسم «لولزيك» شركة «سوني بيكتشرز»، وسرقوا بيانات تضمنت أسماء وكلمات سرية وعناوين الآلاف من عملاء الشركة، وقالت المجموعة إن هذا الهجوم كان انتقامًا من «سوني» لأنها اتخذت إجراء قانونيا ضد جورج هوتز، الذي اخترق نظام تشغيل منصة الألعاب «بلاي ستيشن 3» في وقت سابق، للتوصل الي فرض مطالبه.

خامسا: روبرت موريس يخترق الانترنت:

بعد تخرجه في جامعة كورنيل في العام 1988 صمم روبرت موريس أول دودة تجسس WORM، وكان دافعه الفضول في معرفة عدد الحواسب المتصلة في الشبكة العنكبوتية، لكن حدث ما لم يكن في الحسبان، حيث فقد موريس السيطرة على الدودة التي بدأت تنسخ نفسها وتتكاثر على الشبكة ما أدى إلى حدوث أضرار جسيمة لعدد هائل من أجهزة الحاسب حول العالم، وقد تم إلقاء القبض عليه ليصبح موريس بذلك أول شخص يدان بموجب قانون الاحتيال الالكتروني وسوء استخدام الحاسب، وحكم عليه بالسجن مدة ثلاث سنوات ودفع غرامة قيمتها 10 آلاف و50 دولاراً.

سادسا: فلاديمير ليفين يسطو على مصرف سيتي بنك:

ففي عام 1995 تمكن الروسي فلاديمير ليفين من الوصول إلى حسابات العملاء في مصرف سيتي بنك الموجودة على الشبكة وابتزاز ملايين الدولارات، وكان ليفين يعمل ضمن مجموعة إجرامية، ويستخدم جهاز حاسب في لندن لسرقة الكلمات السرية لحسابات العملاء في البنك وابتزاز الأموال إلى حسابات المجموعة، حيث تمكن من تحويل ما لا يقل عن 7 .3 مليون دولار بشكل غير قانوني إلى أن تمكن مكتب التحقيقات الفيدرالية إف بي آي من القبض عليه في مطار لندن، ومن ثم تم نقله إلى الولايات المتحدة ليحكم عليه بالسجن ثلاث سنوات في عام 1998 وأمرته المحكمة أيضاً بدفع تعويضات بقيمة 240 ألف دولار لمصرف سيتي بنك.

سابعا: أدريان لامو يخترق نيويورك تايمز:

في عام 2002 اخترق أدريان لامو البالغ من العمر 19 عاماً الشبكة الداخلية لصحيفة نيويورك تايمز ووصل إلى سجلات حساسة بما فيها قاعدة بيانات واسعة لبعض المقالات الافتتاحية

والأوراق الأرشيفية التي كانت تحتوي على أرقام هواتف وعناوين الأشخاص الذين كانوا يساهمون في الكتابة في الصحيفة، ومنهم على سبيل المثال السياسي الديمقراطي جيمس كارفيل، وجيمس بيكر وزير الخارجية الأمريكي السابق، والممثل روبرت ريدفورد.

ثامنا: غاري ماكينون يخترق بيانات الجيش الأمريكي:

ما بين عامي 2001 و 2002 اتُهم الاسكتلندي غاري ماكينون باختراق أجهزة حاسب خاصة بالجيش الأمريكي، وكان دافع ماكينون وراء ذلك هو جمع المعلومات التي بحوزة أمريكا عن الأجسام الغريبة الطائرة UFO.

وذكر المسؤولون العسكريون أن من ضمن الأضرار الناجمة عن الاختراق حذف ملفات مهمة من أنظمة التشغيل، مما أدى إلى إغلاق شبكة المنطقة العسكرية التابعة للجيش في واشنطن والمكونة من ألفي جهاز حاسب لمدة 24 ساعة.

وقام ماكينون أيضاً بحذف سجلات خاصة بالأسلحة في محطة إيرل، وقد واجهً حكماً بالسجن لمدة 60 عاماً إذا تمت إدانته بالتهم الموجهة إليه.

تاسعا : ألبرت غونزاليس يخترق شركة ظتش:

حيث أدين ألبرت غونزاليس وهو رئيس عصابة مكونة من هاكرز بسرقة أكثر من 90 مليون بطاقة ائتمان وأرقام بطاقات السحب الآلي من TJX وغيرها من شركات تجارة التجزئة، بما فيها DSW وOfficeMax وسلسلة محال ديف وبسترز، وفي عام 2009 أدين غونزاليس بتهمة الاحتيال والسرقة بغية الابتزاز، وحكم عليه بالسجن لمدة 20 عاماً.

عاشرا: أنونيموس تخترق بيانات شركة أتش بي غاري للتكنولوجيا:

ففي أوائل عام 2011 اخترقت مجموعة أنونيموس حسابات شركة أتش بي غاري وقامت بنسخ ونشر الآلاف من الوثائق ورسائل البريد الالكتروني الخاصة بالشركة بغرض ابتزازها.

حادى عشر: لولزيك تخترق سوني:

في يونيو من عام 2011 اخترقت مجموعة من القراصنة يطلقون على أنفسهم اسم لولزيك شركة سوني بيكتشرز وسرقوا بيانات تضمنت أسماء وكلمات سرية وعناوين الآلاف من عملاء الشركة، وقالت المجموعة إن هذا الهجوم كان بغرض الابتزاز من سوني لأنها اتخذت إجراءً قانونياً ضد جورج هوتز الذي اخترق نظام تشغيل منصة الألعاب بلاي ستيشين 3 في وقت سابق.

ثانى عشر: فضيحة صحيفة نيوز أوف ذا وورلد:

حيث كان العاملون في صحيفة نيوز أوف ذا وورلد البريطانية يتجسسون على المكالمات الهاتفية للسياسيين والمشاهير للسعي في تحقيق مكاسب صحفية ومالية.

وفي تحقيق يعود تاريخه إلى عام 2002 قامت الصحيفة بالاستعانة بمحققين مأجورين للتنصت والدخول على حسابات البريد الصوتي الخاصة بمشاهير من ضمنهم عارضة الأزياء ايل ماكفرسون والممثلة سيينا ميلر، فضلاً عن شخصيات من العائلة الملكية البريطانية، وقد أغلقت الصحيفة في أعقاب هذه الفضيحة.

ثالث عشر: شادو بروكرز يستولى على مبلغ580 مليون دولار:

حيث ان أحدث عمليات الاختراق وقعت في 17 أغسطس 2015، بعد إعلان هاكرز يطلقون على أنفسهم اسم "شادو بروكرز" Shadow Borkers وهى اختراق وكالة الأمن القومي الأميركية NSA والحصول على أنظمة اختراق وقرصنة إلكترونية أنشأتها الوكالة وحليفاتها الأربع، بريطانيا وكندا وأستراليا ونيوزيلندا.

وادعى الهاكرز حصولهم على ما أسموه "أسلحة سايبرية" تتضمّن برامج تشغيل استخدمتها الولايات المتحدة في تخريب البرنامج النووي الإيراني، وعرضوا ما بحوزتهم للبيع مقابل مبلغ 580 مليون دولار.

رابع عشر: اختراق الكونجرس بتاريخ أغسطس 2016:

حيث نشر أحد القراصنة الأمريكيين أرقام هواتف وعناوين البريد الإلكتروني لـ200 عضو ديمقراطي سابقين وحاليين في الكونغرس، في شهر أغسطس من عام 2016، ومن ضمن الأرقام المنشورة رقم هاتف زعيمة الأقلية الديمقراطية نانسي بيلوسي.

خامس عشر : واقعة أشلي ماديسون في أغسطس 2015:

كانت بيانات أكثر من 30 مليون شخص حول العالم، بينهم مشاهير، على موعد مع الإشهار، بعد قيام هاكرز "امباكت تيم" The Impact Team بتسريب بيانات الملايين من زبائن موقع "أشلي ماديسون" Ashley Madison المعروف بوساطته لتقديم خدمات علاقات جنسية خارج إطار الزواج.

وأسفرت عملية الاختراق عن نشر بيانات مسؤولين وشخصيات عامة، وأعلن القراصنة أنهم حصلوا على البيانات الشخصية وأرقام بطاقات الائتمان وحتى التخيلات الجنسية للزبائن وصورهم، وبالفعل نشروا حوالي 10 جيجا من البيانات التي تم الحصول عليها كدفعة أولى، ثم أتبعوها بدفعة ثانية من 20 جيجا في أغسطس 2015.

وتسببت عمليات التسريب في انتحار عدة أشخاص، منهم كنديان، بحسب صحيفة "الجارديان"، كما انتحر القسيس وأستاذ اللاهوت الأميركي جون جيبسون، بعد ستة أيام من عملية التسريب خوفاً من العار.

سادس عشر: كشف 4 ملايين موظف فدرالي أميركي – يونيو 2015:

في يونيو 2015، أفاد مكتب الإدارة الشخصية التابع للحكومة الأمريكية أن قراصنة تمكّنوا من سرقة بيانات قرابة أربعة ملايين موظف فيدرالي.

واتهم مسؤولون أميركيون حكومة الصين بالوقوف خلف هذه العملية التي تُعدّ الفاجعة الأكبر في تاريخ البلاد، واعتبر الخبراء أن الهدف من هذه العملية هو تحسين الصين لقدراتها على تجنيد جواسيس، نظراً لأن المعلومات المسروقة تكشف هويات مَن يمكنهم الوصول إلى أسرار الدولة، كما تكشف المعلومات المسرّبة هويات بعض عملاء أجهزة الاستخبارات الأمريكية.

سابع عشر: أكبر عملية سرقة بيانات في أغسطس 2014:

تمكّن قراصنة روس يعرفون باسم سايبر فور من قرصنة أكثر من 500 مليون حساب بريد إلكتروني، وكشفوا أسماء مستخدميها وكلمات سر الحسابات.

وقد سرقت البيانات من 420 ألف موقع إلكتروني، تشمل مواقع شركات كبرى، وبيانات يمكن استخدامها للتواصل مع أصحابها ولإرسال فيروسات يمكن عبرها اختراق حواسبهم.

ثامن عشر: هجمات أنونيموس في أبريل من كل عام:

مع بداية كل أبريل، منذ عام 2012، تستعد إسرائيل لمواجهة هجمات مجموعة أنونيموس Anonymous التي تخترق سنوياً مواقع إسرائيلية حكومية وغير حكومية، رداً على سياسة الاستيطان والاحتلال.

وقد شهد أبريل سنة 2016 رسالة بثها الهاكرز للإسرائيليين توعّدوا فيها بأن هجماتهم ستكون حرباً إلكترونية ضد إسرائيل، وقال احد تابعى تلك المجموعة في فيديو معلن عنهم " لن نقف مكتوفي الأيدي، سندافع عن البشرية ضد الجرائم الصهيونية ".

وقرر جهاز الأمن العام الإسرائيلي إنشاء غرفة إلكترونية خاصة لمواجهة عدوان تلك المجموعة، وفي آخر عمليات الاختراق لإسرائيل من قبل أنونيموس، نجح الهاكرز في اختراق موقع التربية والتعليم، وعطلوا خدمات البريد في إسرائيل، واخترقوا موقع مكتب رئيس الوزراء.

تاسع عشر : اختراق تي موبيل الأميركية – أكتوبر 2015:

بتاريخ شهر اكتوبر عام 2015، تعرّضت بيانات عملاء شركة الاتصالات الأميركية T-Mobile للاختراق، بعد هجوم إلكتروني استهدف أحد الأقسام التابعة لوكالة " إكسبريان " الائتمانية التي تستعين بها الشركة لمعالجة بيانات المشتركين.

وجرى تسريب أسماء وتواريخ ميلاد نحو 15 مليون عميل لشركة الاتصالات الأمريكي، وأصدر المدير التنفيذي للشركة بياناً تحدث فيه عن الاختراق وعن حرص الشركة على الحفاظ على سرية بيانات العملاء.

ولم تنشر بيانات مالية للعملاء، وأكدت وكالة "إكسبريان" حرصها على اتخاذ خطوات جديدة لتحسين حماية بيانات العملاء التابعين للشركة.

عشرون : Carbanak cybergang . فبراير 2015:

هي عملية استغرقت نحو عامين وكانت محصلتها الاستيلاء على قرابة المليار دولار، فقد أقدم قراصنة على اختراق الأنظمة المالية لعدة بنوك حول العالم، معظمها في روسيا، واليابان، وسويسرا والولايات المتحدة، وبحسب شركة "كاسبرسكاي" المتخصصة في مكافحة الفيروسات وأمن الحاسبات، تعرّضت 30 دولة ونحو مئة مصرف عالمي للهجمة التي أطلق عليها اسم Carbanak cybergang، وهو اسم البرنامج الذي استخدمته المجموعة في فبراير 2015.

وقد استخدم القراصنة ملفات وورد خبيثة لزرعها للدخول إلى البيانات ومن ثم الحصول عليها، واستمرت العملية عامين حتى نجح القراصنة في الوصول إلى مبتغاهم، من خلال رسائل الاحتيال عبر البريد الإلكتروني للبنوك.

وأشار أحد خبراء الأمن المعلوماتي إلى أن القراصنة اخترقوا الحواسب، واحداً تلو الآخر، وكانوا يرسلون الأموال إلى أجهزة الصراف الآلي في وقت معين فتخرج منها بشكل أوتوماتيكي في الوقت نفسه الذي ينتظر شركاء القراصنة لدى الأجهزة للحصول على الأموال.

الحادى والعشرين: اختراق سوني بيكتشرز – عام 2014:

كانت مجموعة "حراس السلام" المتعاطفة مع كوريا الشمالية على موعد في ديسمبر 2014 مع حادث هز العالم، باختراقها موقع شركة Sony Pictures Entertainment، بسبب الفيلم الذي انتجته الشركة باسم The Interview والذي يحكي قصة صحفيين أمريكيين أرادا اجراء مقابلة زعيم كوريا الشمالية، وأثناء اللقاء يقتلانه بعد تجنيدهما من المخابرات الأميركية.

ونجح الهاكرز في نشر بيانات سرية عن مخططات الشركة حول الأفلام المقرر إنتاجها، وتم تسريب 4 أفلام، مما كبّد الشركة خسائر بالمليارات، كما سرّبوا بيانات وعناوين بريد كبار الموظفين في الشركة.

الثاني والعشرين: اختراق الكنائس – عام 2008:

لم تسلم دور العبادة من هجمات الهاكرز، ففي عام 2008 اخترقت مجموعة مجهولة أجهزة كنيسة Scientology ونشرت فيديوهات سرية تشير إلى تورطها في تدبير عمليات وهجمات إرهابية، وكذلك نشروا فيديوهات تتعلق بالتوظيف والتجنيد.

والأمر نفسه تكرر مع كنيسة Westboro Baptist من خلال قرصنة موقعها الرسمي على تويتر، وبعض حساباتها على مواقع التواصل الاجتماعي بدعوى كشف الحقائق.

الثالث والعشرين : اختراقات yahoo في سبتمبر عام 2016:

كشفت شركة ياهوو(yahoo) عن أكبر عمليات قرصنة وابتزاز لقاعدة بيانات مستخدميها، هذه العملية تُعتبر من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل القراصنة على بيانات أكثر 500 مليون مستخدم، وفي ديسمبر من نفس السنة تعرضت الشركة نفسها، لصدمة أخرى حيث أعلنت أن بيانات أكثر من مليار مستخدم قد تم الاستيلاء عليها وأصبحت معروضة للبيع، منها كلمات السر وأسئلة الأمان وأرقام هواتف وتواريخ ميلاد، وهذه الحوادث خفضت من أسهم الشركة الأمريكية اقتصاديا وإعلامياً بشكل ملحوظ.

الرابع والعشرين: هجمات DNS :

لقد واجه مستخدمو الإنترنت حول العالم يوم 2016/10/21، 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 ترجمة عنوان الموقع إلى عنوان IP، وأبرز المواقع الرئيسية التي تعرضت للسقوط هي Twitter، Amazon، Spotify ,Etsy Github 43.

الخامس والعشرين: الاستيلاء على مليار دولار.

وتعد من أكبر جريمة ابتزاز الكترونية في التاريخ، تلك التى تحصل خلالها قراصنة روس من العديد من بنوك دول العالم، شملت مصارف في اليابان والصين والولايات المتحدة، مروراً

بمصارف في الدول الأوروبية، ما يصل إلى مليار دولار، وهي العملية التي وصفت بأنها "ثورة في عالم الجريمة الإلكترونية" ، وهذه السرقة تشكل علامة فارقة على بداية مرحلة جديدة في ثورة النشاط الإجرامي الإلكتروني، حيث استولي المستخدمون الأموال بطريق الابتزاز المباشر من البنوك.

السادس والعشرين: قضية الجحيم العالمي.

فقد تمكنت مجموعة من اختراق مواقع البيت الأبيض، والجيش، ووزارة الداخلية الأمريكية، وقد أدين اثنين من هذه المجموعة، وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق اكثر من التدمير او التقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة.

السابع والعشرين : قضية التجسس الاسرائيلية.

في مطلع عام 1998 تمكن أحد الهاكرز الإسرائيليين من اختراق عشرات النظم لمؤسسات عسكرية ومدنية وتجارية في الولايات المتحدة وإسرائيل، وتم متابعة نشاطه من المحققين الأمريكيين، وتبين أن مصدر هذه الاختراقات هو حاسب في الكيان الصهيوني، وتم التوصل للفاعل، وبالرغم من أن المحققين أكدوا عدم توصله لمعلومات حساسة، إلا ان وسائل الإعلام الأمريكية ذكرت أن هذا الشخص كان يقوم بهذه الأنشطة بوصفه عميلا لإسرائيل ضد الولايات المتحدة الأمريكية.

الثامن والعشرين: قضية القنبلة الالكترونية.

بعد 20 يوما من فصل مصمم ومبرمج حاسب ورئيس سابق لشركة أوميجا، ويدعى "تيموثي ألين لويد" يبلغ من العمر 35 عاما، تم اعتقاله في 1998/2/17م، بسبب إطلاقه قنبلة إلكترونية في عام 1996م، استطاعت ان تلغي كافة التصاميم وبرامج الإنتاج في أكبر مصانع التقنية العالية في نيوجرسي، والمرتبطة والمؤثرة على نظم تحكم مستخدمة في وكالة الفضاء الأمريكية (ناسا)، والبحرية الأمريكية، ملحقا خسائر بلغت 10 مليون دولار، وتعتبر هذه الحادثة اكثر جرائم تخريب الحاسب خطورة.

التاسع والعشرين: قضية فيروس ميلسا MELISSA.

حيث انخرطت العديد من الدول في تحقيق واسع حول إطلاق فيروس عبر الإنترنت، حيث تم اعتقال مبرمج كمبيوتر من ولاية نيوجرسي في سنة 1999م، واتهم باختراق اتصالات عامة والتآمر لابتزاز خدمات الحاسب، ووصلت عقوبة الاتهامات في هذه القضية إلى السجن لمدة 40 عام، وغرامة 500 ألف دولار، وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة.

الثلاثون: قضية اختراق ZYKLON .

في سنة 1999م تم إدانة "إيرك بيرنز" من قبل محكمة فيرجينيا الغربية بالحبس لمدة 15 شهرا والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد اقراره بذنبه، وقيامه متعمداً باختراق حواسب محمية، وإلحاق الضرر البالغ بها في فيرجينيا وواشنطن ولندن، وقد تضمن هجومه الاعتداء على مواقع لحلف الأطلسي، وموقع نائب رئيس الولايات المتحدة، كما اعترف بأنه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق حواسب البيت الأبيض، كما قام بتصميم برنامج أطلق عليه web bandit ليقوم بعملية تحديد الحواسب المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها، فقام في الفترة ما بين 1998 وحتى 1999 باختراق هذه النظم 4 مرات، مما اثر على العديد من المواقع الحكومية التي تعتمد على نظام وموقع USIA للمعلومات، وفي إحدى المرات جعل آلاف الصفحات من المعلومات غير المتوفرة، مما أدى إلى إغلاق هذا الموقع لثمانية أيام، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال، ومواقع حكومية وتعليمية يستضيفها خادم شبكة LASER.NET ، وكان يستبدل صفحات المواقع بصفحات خاصة به تحت اسم ZYKLON أو باسم فتاته "كريستال".

الحادى والثلاثين: قضية اختراق بنك لويدز.

وهناك العديد من الأمثلة لجرائم ارتكبت بالفعل من خلال الانترنت ففي بنك لويدز في أمستردام قام شاب عمره 26 عاماً بابتزاز مبلغ 8.4 مليون دولار عبر نظام الحوالات العالمية من مطلب هذا البنك في نيويورك إلى حساب في بنك آخر في سويسرا.

المبحث الثاني

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 2015

إلى 160 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 2016، في الوقت الذي أكدت هيئة تنظيم الاتصالات على فعالية منظومة الحماية الإلكترونية في الدولة[177].

وفي لبنان، ارتفعت معدلات جرائم الابتزاز الالكتروني منذ عام 2014، 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 المصارف اللبنانية حصراً منذ عام 2011 حتى الفصل الثالث من سنة 2016، وفق أرقام هيئة التحقيق الخاصة لدى مصرف لبنان، الى نحو 233 عملية، وصلت فيها قيمة الأموال التي تعرضت للقرصنة إلى نحو 26 مليوناً ونصف مليون دولار، من ضمنها 15 مليون دولار بين عامي 2015 و2016 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 500 جريمة إلكترونية في الجزائر خلال سنة 2016، 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

---

177) راجع في ذلك: د. علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، ايتراك للطباعة والنشر والتوزيع، الطبعة الاولى، مصر، سنة 2000، ص 197.

يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة 385 جريمة معلوماتية من قبل الفرق المتخصصة في مكافحة الجريمة المعلوماتية التابعة للأمن الداخلي، إلى جانب تسجيل 57 قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية.

وفي سنة 2014، أجرى أحد المصارف في لبنان تحويلاً بقيمة 48 ألف يورو بناء لطلب من شركة موجودة في لبنان (عميل) ورد الى المصرف عبر البريد الإلكتروني، طلبت فيه الشركة إجراء التحويل من حسابها إلى حساب مصرف موجود في دولة أوروبية، تمت حينها العملية بنجاح، وبعد فترة وجيزة عاد وتلقى المصرف طلباً آخراً من الشركة نفسها يحمل توقيع ممثلها القانوني، يطلب فيه تحويل المبلغ المذكور ولكن إلى حساب لدى مصرف آخر في أوروبا، غير الذي تم الإرسال إليه في المرة الأولى، فأجرى المصرف التحويل المطلوب من الشركة بحسب المعلومات الواردة في الطلب، إلا أن الشركة المورّدة الموجودة في الخارج لم تتلقَ الأموال في حسابها، فأبلغت الشركة الموجودة في لبنان بذلك، عندها تبين أنه تمت قرصنة الأموال التي أرسلت في الطلب الثاني من قبل شخص مجهول الهوية إستخدم ذات البريد الإلكتروني العائد للشركة المورّدة في الخارج وانتحل صفة مديرها، ما أدى إلى وقوع الشركة العاملة في لبنان في خسائر مادية.

وطلبت هيئة التحقيق الخاصة من وحدة الإستخبار المالي النظيرة في البلد التي توجد فيه الشركة الموردة، تزويدها بالمعلومات المتوفرة عن أصحاب الحسابات في الخارج، وما إذا كان لهم أسبقية اجرامية لشركاء في لبنان، والسماح لهيئة التحقيق بتزويد هذه المعلومات الى النيابة العامة التمييزية ومكتب مكافحة جرائم المعلوماتية في المديرية العامة للأمن الداخلي.

وفي سنة 2015، أجرى مصرف آخر في لبنان، عملية تحويل بقيمة 220 ألف دولار، بطلب من عميل لديها، تبين لاحقاً من خلال التحقيق الذي أجرته هيئة التحقيق الخاصة في مصرف لبنان، أنه تمت قرصنة تلك الأموال بطريق الابتزاز وتم تحويلها خارج لبنان أيضاً.

وهذه الحالات جاءت ضمن سلسلة حالات تم عرضها دون ذكر البيانات، حرصاً على السرية المصرفية[178] [179] في ملتقى "مكافحة الإحتيال والقرصنة الإلكترونية في القطاعين

) راجع في ذلك: د. سميحة القليوبي، الأسس القانونية لعمليات البنوك، مكتبة عين شمس، القاهرة، سنة 1992 178(
، ص 224.

(179) Pino ARLACCHI: under secretary general, executive dirctor, united nations office for Drug control and crime prevention, introduction to the penal discussion "Attacking the profits of crime: Drugs, Money and Laundering" (New York – 10 June 1998.

المصرفي والتجاري في لبنان"[180] وتشير إحصاءات الهيئة الخاصة في مصرف لبنان، أن عدد البلاغات المقدمة إليها بلغت 35 بلاغاً و80 طلب مساعدة في العام 2015، تم تصنيفها ضمن عمليات قرصنة جرت عبر شبكة الإنترنت لسحب أموال من حسابات لدى مصارف ومؤسسات مالية عاملة في لبنان، وهو ما يطرح التساؤلات حول من يتحمل مسؤولية وقوع خطأ في المعاملات المصرفية الالكترونية، المصرف أم العميل.

فعلى الرغم من النتائج الايجابية التي تحققها لبنان في مجال الاقتصاد الرقمي، فإنها ما تزال تعاني قصوراً في إصدار البنى التشريعية مع غياب القوانين الخاصة في مجال التجارة الالكترونية وحماية المعلومات والبيانات، ومكافحة جرائم الانترنت وجرائم سوء استخدام أنظمة الحاسب.

ذلك إن "القانون الرقيم 133 الصادر في عام 1999 قد وسع من مهام المصرف المركزي في مجال الصيرفة الالكترونية، بما أتاح له إصدار تعميم تنظيمي لتطوير وسائل وأنظمة الدفع وبصورة خاصة العمليات المجراه عن طريق الصرف الآلي وبطاقات الإيفاء أو الدفع أو الائتمان، وعمليات التحويلات النقدية بما فيها التحويلات الالكترونية، وعمليات المقاصة والتسوية العائدة لمختلف وسائل الدفع والأدوات المالية".

ومن أهم التعاميم التي أصدرها مصرف لبنان في هذا المجال التعميم الأساسي الرقم 69 تاريخ 2000/3/30 المتعلق بالعمليات المالية والمصرفية بالوسائل الالكترونية وتعديلاته، وقد إستطاع من خلاله التوسع في تعريف العمليات المالية والمصرفية بالوسائل الالكترونية، وحصر ممارسة "العمليات المالية والمصرفية بالوسائل الالكترونية" بالمصارف وسائر المؤسسات المسجلة لدى مصرف لبنان، وحظر منذ سنة 2013 إصدار النقود الالكترونية من أي مكان والتعامل بها بأي شكل من الأشكال، كما نظم في ذات السنة عمليات التحويلات النقدية بالوسائل الالكترونية الداخلية والخارجية، التي تقوم بها المؤسسات غير المصرفية[181]، وحظر في سنة 2014 قبول التوقيع

---

180) راجع في ذلك: د. محمد على القرى، السرية في العمليات المصرفية – مفهومها وضوابطها ، بحث منشور على الموقع الالكترونى

http//:www.elgari article67.htm-68k.com

181) وهى شركات ومؤسسات casas de cambio) ومن امثلة هذه المؤسسات المالية غير المصرفية ما يعرف بـ نشات بغرض استبدال العملة المكسيكية "البيزو" بالدولار الامريكى ويقدر عددها حاليا باكثر من الف شركة ومؤسسة، ويتراوح حجم الاموال التى يتم غسلها شهريا عن طريقها بحوالى خمسة ملايين دولار، ووصل اكبر معدل لغسل الاموال في احدى التقديرات الى اكثر من مائتى مليون دولار في غضون ستة اشهر، ويقرر البعض ان مؤسسات

الالكتروني إلا عند توافر بعض الشروط كوجود اتفاق صريح بين المؤسسة المعنية والعميل يبين المخاطر المحتملة عند اللجوء إلى التوقيع الالكتروني[182].

ومن وجهة نظر أخرى، فإن الحديث عن الحماية التقنية التي تعتمدها المصارف في لبنان، في ظل غياب التشريعات اللبنانية، تتحمل مسؤوليتها المصارف وليس العميل، نظراً لأن العميل قد منح ثقته للمصارف حين أودع أمواله لديها، ما يتطلب من العملاء الحذر الشديد في كيفية إجراء عملياتهم المصرفية الإلكترونية، ولكن في ظل التطور التكنولوجي الذي نعيشه كيف يمكن للعملاء حماية أموالهم من القرصنة في ظل وجود قراصنة محترفين، يعملون بحرفية تامة.

وبصفة عامة، فإن وجود شبكات إجرامية تعمل على سرقة الأموال والإحتيال على الشركات وتزوير ملفات، ليس بجديد، لكن ارتكابها عبر شبكات الإنترنت زاد من انتشارها وصعوبة مواجهتها، وعلى الرغم من أن حالات القرصنة الإلكترونية التي حصلت في لبنان ما زالت قليلة نسبياً، إلا أن هذه الحالات معرضة للإرتفاع في ظل قصور التشريعات التي لا تنهي وجود عمليات القرصنة الإلكترونية فعلياً، ولكنها تقلل من نسبة التعرض لها.

وجدير بالذكر، وفي مصر، تزعم عصابة من "الهاكرز" بمدينة الإسكندرية، تضم خمسة أشخاص للاستيلاء بطريق الابتزاز على حسابات بطاقات "في" الخاصة بعملاء البنوك.

تتقاضى نسبة تتراوح بين 3% الى 5% للقيام بمثل هذه العمليات، ومن ابرز المؤسسات casas de cambio وهى لا تقوم باى نشاط اجرامى، كما American expressالمالية غير المصرفية ايضا شركة امريكان اكسبرس تلتزم بجميع الاجراءات والقواعد المنصوص عليها في القانون، ولها اكثر من 37000 وكيل ومطلب في انحاء العالم، ومع ذلك فان الشيكات التى تصدرها مثل الشيكات السياحية وغيرها تعتبر وسائل لغسل الاموال المشبوهة يستغلها غاسلوها، كما تورطت بعض كبرى شركات الشحن والتعامل في الاوراق المالية في (وول ستريت) في نيويورك في عمليات غسل الاموال، ومثال ذلك انه تم تغريم شركة بمقدار مليون دولار لدورها في احدى تلك العمليات لقبولها كمية ضخمة من الاموال السائلة وعدم كتابة التقرير اللازم عنها الى الجهات المختصة وفقا للقانون، راجع في ذلك :

Scott seltzer, mony laundering : the scope of the problem and attempts to combat It…

مشار اليه كذلك في: د. جلال وفاء محمدين – دور البنوك في مكافحة غسل الاموال – مجلة الحقوق بالاسكندرية – العدد الاول – سنة 2000 – ص 610 وما بعدها.

) أنظر للتفصيل: محمد إبراهيم محمود الشافعي، النقود الإلكترونية (ماهيتها، مخاطرها وتنظيمها القانوني)، مجلة 182(الأمن والقانون، أكاديمية شرطة دبي، السنة الثانية عشر، العدد الأول، يناير 2004، ص 146.

وفي عام 2011 ألقت السلطات الإسرائيلية القبض على شابين شقيقين من الفلسطينيين ووجهت إليهما تهمة اختراق مواقع وزارة الدفاع الإسرائيلية، بغرض ابتزاز اسرارا عسكرية.

المبحث الثالث

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.
- **المطلب الثاني:** قضية تهديد وابتزاز وتشهير الكتروني.

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 12 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 19 سنة – طالب – مقيم .....

لانه في يوم 2019/6/24 بدائرة مركز شرطة ثاني – محافظة 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 .

- **ثالثـا** : 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.
- **خامسـا** : أنشا حسابات الكترونية علي الشبكة المعلوماتية لمواقع التواصل الاجتماعي (الفيس بوك – انستجرام) باسم (.... – .... – ....) بهدف ارتكاب جريمة معاقب عليها قانونا .
- **سادسـا** : 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.
- **ثامنـا** : 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 268 ، 309 مكرر ا بند (أ ، ب) ، 4 ، 309 مكرر (1) / 1 – 2 – 4 ، 326 من قانون العقوبات والمادتين 25 ، 27 من القانون رقم 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات، والمادة 2/76 من القانون رقم 10 لسنة 2003 ، والمادتين 1/2 ، 116 مكرر / 1 من القانون رقم 12 لسنة 1996 بشأن قانون الطفل المعدل بالقانون رقم 126 لسنة 2008 .

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 6854 سنة 2003 الحوامدية (رقم 3261 سنة 2003 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 2003/10/19م إلى 2003/10/22م بدائرة قسم الحوامدية محافظة الجيزة .

1- 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.

2- 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 .

3- 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 2003/10/19م وحتى 2003/10/22م 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.

فقد شهدت المجني عليها xxxxxx أنها في الفترة من اليوم التاسع عشر إلى اليوم الثاني والعشرين من شهر أكتوبر 2003م تلقت رسائل مكتوبة على تليفونها المحمول من مجهول رقمه xxxxxx كانت تحمل سبا وقذفا موجها إليها، ورغبة مرسلها في إقامة علاقة غير شريفة معها، وتهديد لها بالقتل، وبإقامة موقع على شبكة الانترنت إن لم تتجاوب مع مرسل تلك الرسائل، كما تلقت مكالمات على تليفونها المحمول يطلب فيها المتحدثون معها أمورا غير طيبة، ولما سألتهم عن مصدر علمهم برقم هاتفها المحمول فأخبروها أن لها موقعا على شبكة الانترنت يتضمن كل بياناتها ورقم هاتفها المحمول، ويتضمن دعوتها لهم وطلبها تلك الأمور غير الطيبة.

واثر ذلك أبلغت الشرطة وطلبوا منها رقم البريد الالكتروني ورقم موقعها على شبكة الانترنت وطلبوا إليها التحدث إلى صاحب الرقم المجهول xxxxxx والذى وردت إليها المكالمات من خلاله، وقامت الشرطة بتتبع المحادثة المكتوبة بينهما على شبكة الانترنت وفي تلك المحادثة طلب منها أن تدفع له مبلغ خمسة آلاف دولار والموافقة على إقامة علاقة غير مشروعة معه واخذ يسمعها ألفاظا بذيئة وعبارات جنسية، ومن خلال تلك المحادثة الأخيرة تمكنت الشرطة من التوصل إلى مصدر تلك المحادثات والرسائل جميعها، وهو المتهم xxxxxx الذي كانت قد تعرفت عليه خلال دورة لدراسة اللغة الإنجليزية والذى كان يحاول التقرب إليها ولكنها صدته.

وشهد المقدم xxxxxx انه بتاريخ 2003/10/12م أبلغته الشاهدة الأولى بتضررها من قيام مجهول بإنشاء موقع لها على شبكة الانترنت يتضمن بياناتها الشخصية، ودعوى كاذبة منها بإقامة علاقة جنسية مع من يطلب، وأنها تلقت رسائل على هاتفها المحمول يطلب فيها مرسلوها إقامة علاقة معها، وتلقت أيضا رسائل يهددها فيها مرسلها بأنه سيقيم لها موقعا على شبكة الانترنت إن لم تستجب لرغبته إقامة علاقة معها وان لم تدفع له مبلغ خمسة آلاف دولار أو خمسة آلاف جنيه، فقام بعرض الأمر على العقيد xxxxxx رئيس قسم المساعدات الفنية للتوصل إلى مرتكب الواقعة، وشهد العقيد xxxxxx رئيس قسم المساعدات الفنية بإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ان هناك ما يسمى بـ " آى سى كيو " وهو برنامج للمحادثة على شبكة الانترنت، ويقوم بإنشاء رقم عضوية واسم مستعار، ويضع عليه كافة البيانات التى يريدها، ويقوم من خلال هذا الرقم والاسم المستعار بمحادثة الآخرين من كافة أنحاء العالم وتكون المحادثة بالكتابة أو بالصوت ويمكن من خلال هذا الموقع برقم عضويته أن يرسل رسائل قصيرة على التليفونات المحمولة الخاصة بأصدقائه أو معارفه وانه يمكن للشخص إنشاء أكثر من موقع مادامت أرقامها مختلفة.

وأضاف الشاهد انه أمكنه التوصل إلى رقم تليفون المتهم وتحديد شخصيته بعد أن طلب إليها مجاراة المرسل إليها، وتلقت منه رسالتين تتضمنان عبارات وصور جنسية، ودعوة منها للغير بإقامة علاقة معها، وبفحص الموقع الذي أرسل منه المتهم رسائله تبين انه نفس الموقع الذي أرسل منه الرسائل القصيرة على تليفون المجني عليها المحمول الخاص بالمجني عليها والمتضمن تهديدات لها، وتمكن بعد التوصل إلى الموقع الذي يرسل منه المتهم هذه الرسائل إلى رقم التليفون الخاص بالمتهم وهو رقم xxxxxx وبذلك امكن التوصل إلى المتهم وعنوانه، وأضاف انه قدم تقريره الفني بذلك.

وثبت من التقرير الفني الذي قدمه الشاهد الثالث انه قد تم فحص الرسائل الواردة على تليفون المجني عليها المحمول، وتبين أنها مرسلة من البرنامج الذي يحمل رقم xxxxxx، وتم تفريغ محتويات الرسائل وترجمتها إلى العربية، وتبين أنها تحمل عبارات جنسية فاضحة، وعنوان بريد الكتروني انشأه الراسل للشاكية، وتهديد في حالة عدم الرد عليه أنها ستفقد حياتها وانه سيرسل إلى أكثر من أربعين ألف شخص بياناتها ونشر صورتها الشخصية على الموقع المنشأ لها، إضافة إلى رغبته في إقامة علاقة جنسية معها، وان منشأ هذا الموقع الذي يحمل رقم العضوية xxxxx والذى ينتحل فيه مؤسسه صفة المجني عليها والإعلان عن رغبتها في إقامة علاقات جنسية هو نفس الشخص الذي تم رصده تحت نفس الرقم وهو ذاته الذي استبان من تتبعه على الشبكة الدولية للمعلومات (الانترنت) انه استخدم التليفون المنزلي رقم xxxxxx كما ثبت من التقرير أيضا انه بفحص محتويات جهاز الحاسب الشخصي (الحاسب) الخاص بالمتهم والمضبوط بمسكنه تبين وجود دلائل للرقم التسجيلي لبرنامج (آى سى كيو) تم حذفها بمعرفة مستخدم الجهاز إلا انه أمكن التوصل إلى الرقم المذكور وهو xxxxxx كما تبين بفحص الجهاز وجود الصورة الخاصة بالمجني عليها والمدونة على الجهاز باسم xxxxx كما تبين من فحص الجهاز وجود آثار ودلائل للرسائل التى أرسلت من جهاز الحاسب الآلي الخاص بالمتهم ومن الرقم التسجيلي لبرنامج (آى سى كيى) xxxxxx على هاتف المجني عليها المحمول.

وثبت من الإطلاع على تفريغ الرسائل الالكترونية المرسلة من المتهم إلى المجني عليها على بريدها الالكتروني (جهاز الحاسب الآلي الخاص بها) أن مرسلها يراود المجني عليها عن نفسها، وان يطلب منها دفع مبلغ خمسة آلاف دولار، ولما استكثرت مثل هذا المبلغ اخبرها إنها تتخيل والدتها عنما ترى صورها وكذلك زملاءها في العمل كما تضمن التقرير ألفاظا موجهة إلى المجني عليها مثل " Fucken " و " Bitch " و " Fuckers " وثبت من إطلاع وكيل النيابة المحقق على هاتف المجني عليها المحمول وجود تسعة عشر رسالة مرسلة من الرقم xxxxxx تتضمن مراودة المرسل للمجني عليها عن نفسها وتهديدها بأنه سيرسل صورتها الحقيقية مركبة في وضع جنسي لجميع معارفها والتهديد لها بالقتل.

وبما أن المتهم اعتصم بتحقيق النيابة بالإنكار وجرى دفاعه على انه تعرف على المجني عليها أثناء دراستهما لدورة للغة الإنجليزية بالمركز الثقافي البريطاني وأنها اقترضت منها شريطا مسجلا لتعليم اللغة ولكنها لم ترده وانهما كانا يتبادلان الرسائل الالكترونية حتى فوجىء بالقبض عليه.

وبجلسة المحاكمة ثبت المتهم على إنكاره، وترافع ممثل النيابة العامة ودلل على ثبوت الاتهام قبل المتهم وأركان الجرائم المسندة إليه، والدفاع الحاضر مع المتهم شرح ظروف الدعوى وقال أن الأوراق خلت من دليل ضد المتهم، وان الإجراءات قد شابها البطلان لعدم استئذان القاضي الجزئي لتسجيل المحادثات، وقال الدفاع دون ذلك ما يراه ينال من أدلة الثبوت في الدعوى وقدم المتهم مذكرة بدفاعه كما قدم الدفاع تقريرا فنيا استشاريا.

وبما أن المحكمة وقد اطمأنت إلى أدلة الثبوت سالفة البيان فإنها تلتفت عن إنكار المتهم، وترى فيه محاولة للتنصل من الاتهام الثابت قبله بيقين، كما أنها ليست بحاجه إلى رد مستقل على كل ما آثاره الدفاع من جدل موضوعي.

أما عن الدفع ببطلان الإجراءات لعدم استئذان القاضي الجزئي فهو مردود بأن مأمور الضبط لم يراقب تليفون المتهم وإنما خاطبه على رقم البريد الالكتروني الخاص به وهو رقم xxxxxx وهو أمر متاح لمأمور الضبط وللكافة، وكان هدف مأمور الضبط من الاتصال بالمتهم هو الوصول إلى رقم الهاتف الارضى المرتبط بالحاسب الآلي الخاص بالمتهم توصلا لمعرفة شخصية هذا الأخير وعنوانه، وللتوصل إلى ما هو مسجل عليه من مكالمات، وهو إجراء تفتيش للبحث عن أدلة جريمة وقعت فعلا وليس تصنتا على هاتف، ذلك ان هناك فرق فنى كبير بين مراقبة الاتصالات الصوتية الهاتفية والتنصت عليها وبين البحث عن أدلة الجريمة في مكمن السر وهذا لا يستلزم سوى استئذان النيابة العامة، كما أن التنصت يستلزم فرض رقابة ايجابية على الهاتف المراد مراقبته وحماية لحريات الأفراد استلزم المشرع أن يكون ذلك بإذن من القاضي المختص، أما ما لا يستلزم رقابة ايجابية على هاتف الشخص فهو لا يستلزم استئذان القاضي وغنى عن البيان أن من وسائل المراقبة السلبية وسيلة إظهار رقم الطالب على الهواتف المحمولة وكثير من الهواتف الأرضية، ولم يقل احد بأن إظهار رقم الطالب يستلزم إذنا من جهة ما.

وخلاصة القول أن مراقبة هاتف المتهم لم تتم عبر هذا الهاتف، ولكن ما حدث أن مأمور الضبط استخدم الحاسب الآلي للمجني عليها كوسيلة لمعرفة الرقم الالكتروني لمرسل الرسائل، وكان ذلك عن طريق حاسبها الآلي وهاتفها المحمول، دون تدخل على هاتف المتهم الذي لم يكن الضابط يعرفه أصلا، فلما توصل اليه فانه استأذن النيابة العامة لتفتيش مسكن المتهم للبحث عن أدلة الجريمة، ومنها جهاز الحاسب الآلي الخاص بالمتهم وهو ما يكفي لصحة وسلامة الإجراءات.

وبما أن الثابت أن المتهم هدد المجني عليها كتابة بنسبة أمور مخدشة بالشرف إليها، وذلك بأن هددها بنشر صور لها عارية، وإقامة موقع لها على شبكة الانترنت ودعوة أربعين ألف شخص

إليها حسبما ورد بالرسائل، فكان في تهديده هذا يعلم تمام العلم مدى ما يحدثه هذا التهديد من تأثير بالخوف في نفس المجني عليها كما كان تهديده مصحوبا بطلب وهو أن يضاجعها وان تدفع له مبلغ خمسة آلاف دولار، ولا مراء في أن ما صدر من المتهم هو تهديد كتابي بالمفهوم المقصود بنص المادة 327 من قانون العقوبات في فقرتها الأولى، ذلك أن الثابت أن وسيلة المتهم في تهديده للمجني عليها كان إرسال الرسائل المكتوبة عبر الانترنت والتي لا يمكن للمجني عليها إدراك مضمونها إلا بقراءتها، ويكفي أن المتهم وجه التهديد إلى المجني عليها وهو يدرك أثره من حيث إيقاع الرعب في نفسها وانه جاد في تهديده بما قد يترتب عليه أن تذعن المجني عليها بطلبه بدليل انه يفترض رؤية والدتها لصورها، وزملائها في العمل مما يؤكد أن قصد تخويف المجني عليها وبث الرعب في نفسها حتى تستجيب إلى طلبه ومن ثم تكاملت أركان الجريمة المؤثمة بنص المادة 1/327ع في حق المتهم.

وبما أن الثابت بالأوراق أن المتهم هدد المجني عليها بإنشاء موقع لها على شبكة الانترنت على النحو سالف البيان أن لم تدفع له مبلغ خمسة آلاف دولار، ولكن المجني عليها سارعت بالإبلاغ وذلك حسبما وردت في إحدى المحادثات عندما سألته عما يضمن لها عدم تكرار تهديده فأجابها بأنه ليس هناك ضمان، فما كان منها إلا أن أبلغت الشرطة ولم يحصل على المبلغ النقدي الذي طلبه، فان أركان الجريمة المؤثمة بنص المادة 326 من قانون العقوبات تكون قد توافرت.

وبما أن الثابت بالأوراق أن المتهم أقام للمجني عليها موقعا على شبكة الانترنت ينسب إليها كذبا أنها تبيع جسدها وتعرضه على راغبيه، وكان ذلك بطريق العلنية، إذ اثر هذا النشر أن تحدث بعض الأشخاص إلى المجني عليها دون أن تعرفهم أو يعرفونها طالبين منها اللقاء غير المشروع بناء على ما اطلعوا عليه منسوبا إليها كذبا من الموقع الذي أقامه المتهم لها وبذلك تحقق ركن العلانية في جريمة القذف المؤثمة بنص المادة 302 من قانون العقوبات.

وبما انه اذا كان ما تقدم، فانه يكون قد وقر في وجدان المحكمة بيقين لا يخالطه شك ان المتهم xxxxxx في الفترة من التاسع عشر إلى الثاني والعشرين من شهر أكتوبر سنة 2003م بدائرة قسم الحوامدية محافظة الجيزة.

- **أولا:** هدد المجني عليها/ xxxxxx بنسبة أمور مخدشة للشرف إليها، وكان ذلك مصحوبا بطلب بأن بعث إليها برسائل عبر شبكة المعلومات العالمية (الانترنت) مهددا إياها بوضع صورتها الحقيقية على صور مخلة ونشرها عبر تلك الشبكة

وبإنشاء موقع لها على شبكة الانترنت يتضمن ما يسيء إليها، طالبا منها أن تدفع له مبلغ (خمسة آلاف دولار امريكى)، وأن يمارس معها الرذيلة.

- **ثانيا** : شرع في الحصول على مبلغ (خمسة آلاف دولار امريكى) من المجني عليها سالفة البيان بأن هددها بنسبة أمور مخدشة للشرف إليها وخاب اثر جريمته لا دخل لإرادته فيه وهو القبض عليه.
- **ثالثا** : قذف في حق المجني عليها سالفة البيان بان اسند إليها بواسطة الكتابة الالكترونية أمرا لو كان صادقا لاستوجب احتقارها عند لدى عشيرتها وأهلها وعقابها قانونا، وهو أنها تمارس الرذيلة مع الغير بدون تمييز لقاء مقابل مادي.

مما يتعين معه عملا بالمادة 2/304 من قانون الإجراءات الجنائية عقابه بالمواد 1/45، 47 ، 1/171 ، 5 ، 1/302 ، 1/303 ، 308 ، 2/326 ، 1/327 من قانون العقوبات.

وبما أن الجرائم الثابتة في حق المتهم قد انتظمها نشاط اجرامى واحد مما يتعين معه إعمال حكم المادة 1/32 من قانون العقوبات، وبما أن المحكمة تأتى رخصتها المقررة بنص المادة 17عقوبات.

- وبما انه يتعين إلزام المحكوم عليه بالمصروفات الجنائية عملا بالمادة 313أ.ج.
- فلهذه الأسباب
- 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 2004/1/18م.

التوصيـــات

أولاً : التوصيات المتعلقة بآليات التدخل التشريعى والسياسى:

- الإسراع في إصدار القوانين المنظمة بجرائم الابتزاز الالكتروني، الموضوعية والاجرائية، من خلال وضع قواعد السلوك في مجال المعلوماتية، تتناسب والتطورات التي يعرفها الإجرام المعلوماتي.
- اعتبار الوقاية عاملاً أساسياً في مواجهة جرائم الابتزاز الالكتروني، وهي تتحقّق من خلال اعتماد تدابير إحترازية مناسبة والإستمرار في مراجعتها وتطويرها.
- أهمية التأكد من مراعاة السرية وحماية الخصوصية ومراعاة النوع الإجتماعي في النصوص التشريعية وفي التطبيقات والإجراءات والممارسات ذات الصلة.
- 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.
- ضرورة استحداث قواعد مناسبة في مجال الإجراءات الجنائية لعدم ملائمة الإجراءات الجنائية الحالية في مجال تحقيق جرائم الابتزاز الالكتروني.
- ضرورة إصدار تشريعات جديدة لمواجهة هذه الظاهرة المستحدثة من الجرائم لوجود الفراغ التشريعي في مجال مكافحة الجرائم الرقمية، وأن مواجهة هذا النوع من الجرائم يقتضي ضرورة إعداد أطر أمنية وقضائية للبحث والتحقيق والمحاكمة مع تطوير التشريعات الجنائية بإدخال نصوص التجريم والعقاب.
- ضرورة الالتزام بأحكام الدستور بشأن حماية سرية المراسلات والخصوصية والحرية الشخصية ونشر المعرفة بها.
- ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني – بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات؛ طالما أن ضبط هذه الأدلة جاء وليد إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير، وبما يحقق مبدأ المواجهة بين الخصوم.

- ضرورة ان تكون العقوبات رادعة ومؤثرة في مواجهة جرائم الابتزاز الالكتروني من خلال إساءة استخدام وسائل التواصل الاجتماعي وتكنولوجيا المعلومات كجرائم التنصت وسرقة البيانات والابتزاز والتحرش والإيذاء والملاحقة وغيرها من الجرائم، وخاصة جرائم الابتزاز ضد النساء والأطفال.
- ضرورة تعديل بعض التشريعات المصرية الحالية، وخاصة في مجال الملكية الفكرية والتوقيع الالكترونى، بما يتلائم مع طبيعة جرائم الابتزاز الالكتروني، والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات وشرحها لهم بشكل واضح.
- ضرورة متابعة التطورات والإرشادات الدولية لمواجهة المخاطر المرتبطة بجرائم الابتزاز الالكتروني .
- النص على إلزام شركات الإتصالات بإلغاء المحتوى الإلكتروني المنطوي على ضرر وإساءة بأمر مستعجل من الجهة القضائية المختصة بناء على طلب المتضرر/ة.
- النص على عدم جواز إفشاء أو تقديم بيانات تتجاوز حدود البيانات اللازمة في قضية ما والنص على وجوب تحديد طلبات الجهات الرسمية الإدارية والقضائية بصورة شديدة التحديد والوضوح وخاصة لجهة تحديد أطراف القضية لمنع سوء الاستخدام واقتصار الطلب على هذه البيانات دون تعميم.
- يلزم تعديل قانون ونظم الإجراءات الجنائية، بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته.
- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل، والكشف عن الحقيقة.

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.

- 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.
- التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الابتزاز الالكتروني، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم.
- حث جامعة الدول العربية لإصدار قانون نموذجي موحد لمكافحة جرائم الابتزاز الالكتروني.
- الدعوة إلى إنشاء قسم خاص داخل إدارات مكافحة الجريمة بوزارات الداخلية العربية يكون متخصصاً في مكافحة جرائم الابتزاز الالكتروني مع تدريب العاملين به على أساليب التحري والضبط في هذا النوع من الجرائم.
- ضرورة إبرام اتفاقات عربية ودولية في مجال مكافحة جرائم الابتزاز الالكتروني، وذلك لتحديد إطار الاختصاص القضائي الدولي والتعاون في الكشف وإثبات جرائم الابتزاز الالكتروني.
- ضرورة التعاون الدولى لمواجهة مشكلات صور السلوك المنحرف في البيئة المعلوماتية . الاهتمام بالطرق الفنية لتحقيق جرائم الابتزاز الالكتروني، وذلك بعمل دورات تدريبية للقائمين على ذلك وتوعيتهم بالأساليب المتطورة والمستحدثة في هذا المجال.
- ضرورة التعاون الدولي بتبادل المعلومات والخبرات، والتعاون في المجال الأمني والقضائي بصوره المختلفة، فضلا عن التعاون بينها وبين الدول الأخرى في هذا المجال لتوقيع اتفاقيات مع دول أخرى لتسليم مقترفي هذا النوع من الجرائم، وهو الأمر الذي انتبهت إليه السلطات وتحاول جاهدة تجاوزه، لاسيما مع حداثة جرائم الابتزاز الالكتروني، والمتسمة بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها.

- ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة جرائم الابتزاز الالكتروني، من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم، كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والحاسب وشبكة الانترنت ككل.

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.
- تأهيل القائمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال جرائم الابتزاز الالكتروني، وذلك من خلال تدريب وتأهيل القائمين بالضبط والخبراء وسلطات التحقيق والقضاة، وخاصة تدريب القضاة على التعامل وتفهم هذا النوع من القضايا التي تحتاج إلى خبرات فنية عالية لملائمة قبول هذا النوع من الأدلة في الإثبات وتقديرها، حتى يتمكن قاضي الموضوع من الفصل في القضايا المتعلقة بهذا النوع من جرائم الابتزاز الالكتروني.
- توظيف محققين ذات معرفة تقنية عالية ومواكبة أحدث التقنيات في هذا المجال، وينبغي إنشاء مختبرات الطب الشرعي على الحاسب لجمع الأدلة الرقمية من أجهزة الحاسب وتوفير التدريب للمحققين.
- ضرورة إعداد الكوادر الأمنية، وسلطات التحقيق من الناحية الفنية للبحث والتحقيق وجمع الأدلة في مجال جرائم الابتزاز الالكتروني، مما يستلزم إنشاء مراكز متخصصة في المعهد القضائي وكلية الشرطة تحقيقا لهذا الغرض.

- اعتماد السياسات والإجراءات والنظم المناسبة للتصدّي لجرائم الابتزاز الالكتروني، ورصد الميزانيات والبرامج الواجّبة لذلك وتدريب الموظفين على تطبيقها.
- عقد دورات مكثفة للكوادر البشرية من العاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسب، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الابتزاز الالكتروني.
- يتعين تدريب وتحديث اعضاء النيابة العامة والقضاء بشأن التعامل مع أجهزة الحاسب والإنترنت.

رابعـــا: آليـــات التـــدخل علـــى مســـتوى رفـــع الـــوعي وبنـــاء المهـــارات والقـــدرات- االبـــرامج والخدمات والتوعية:

- تفعيل دور المجتمع المدني، ولاسيما الجمعيات الأهلية للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيا عبر شبكة الانترنت.
- التقيّد بإرشادات الدليل الإرشادي للوقاية من الأفعال الاجرامية بالوسائل الالكترونية والمُمارسات السلوكية المثلى Best Practices التقنية والقانونية.
- ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم الابتزاز الالكتروني مع تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية وحثهم على الاستخدام الأمثل لهذه التقنيات.
- ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.
- ضرورة نشر الوعي بين صفوف المواطنين- ولا سيما الشباب – بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت، مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للانترنت وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة، وذلك بأسلوب غير مباشر من خلال المواد الدرامية.
- ضرورة مشاركة المجتمع المدني في مناقشة مشروعات القوانين المتعلقة بجرائم الابتزاز الالكتروني وأمن المعلومات الشخصية وضمانات الحق في الخصوصية دون مساس بحرية الرأي والتعبير ودون تضييق على المساحة التي يتيحها الإنترنت للحصول على المعرفة والمعلومات ولتسهيل التواصل الإجتماعي.
- إعداد ونشر مواد توعية وتثقيف وتوزيعها على نطاق واسع وإتاحتها إلكترونياً لنشر الوعي بالاستخدام الآمن لتكنولوجيا المعلومات والإتصال ومسألة الخصوصية ووسائل الوقاية من جرائم الابتزاز الالكتروني، وإنشاء وإتاحة برامج وخدمات متخصصة موجهة للفئات الأكثر عرضة لمثل هذه الجرائم.

- أهمية نشر الوعي لتعزيز الثقة بسرية وسرعة الإجراءات المتاحة قانونياً لملاحقة جرائم الابتزاز الالكتروني والتحقيق فيها ومحاكمة مرتكبيها.
- تعزيز منهج الحذر والتعامل الواعي مع البرامج والخدمات الإلكترونية وتحفيز الإستعانة بالمختصين لضمان الحماية والأمان.
- تكثيف برامج بناء القدرات والتدريب الموجهة للوالدين والمرشدات والمرشدين التربويين والقائمين على إنفاذ القانون بشأن جرائم الابتزاز الالكتروني وسبل الوقاية منها والتعامل معها وحماية الأطفال بشكل خاص منها.
- زيادة استخدام الفنون والإبداع والإبتكار لنشر الوعي بأسلوب محبب وسهل الفهم كإنتاج أعمال مسرحية وأفلام ورسوم كاريكاترية وألعاب إلكترونية وإعتماد مبدأ الترغيب لا الترهيب من التكنولوجيا وكسر حواجز الخوف وتذليل المعيقات المعرفية لدى الناشئين.
- ضرورة تكثيف الجهود الوطنية لنشر المعرفة وزيادة الوعي بجرائم الابتزاز الالكتروني ومدى خطورتها ووسائل الوقاية منها وسبل مواجهتها.
- ضرورة نشر المعرفة والمعلومات حول جهات الإرشاد والمساعدة القانونية والفنية للمتضررات والمتضررين والجهات الرسمية التي تستقبل الشكاوى المتعلقة بجرائم الابتزاز الالكتروني.
- نشر الإحصائيات والأرقام المتعلقة بجرائم الابتزاز الالكتروني والأحكام القضائية الصادرة بها لتحقيق المزيد من الردع وللتوعية وتحفيز المزيد من الحذر من الاستخدام الخاطئ لوسائل التواصل الإجتماعي والإنترنت.
- إتخاذ التدابير اللازمة لحماية الأجهزة الالكترونية والبريد االالكتروني من الفيروسات ومن أية عمليات قرصنة بغرض الابتزاز .

خامسا: آليات تدخل مؤسسية وتنظيمية:

- تشكيل تحالف واسع من منظمات المجتمع المدني المعنية لمتابعة موضوع جرائم الابتزاز الالكتروني والاستخدام الآمن لتكنولوجيا المعلومات والاتصال الحديثة والمحوسبة.
- العمل علي تنمية الكوادر البشرية العاملة في مجالات مكافحة جرائم الابتزاز الالكتروني.
- مساعدة شركات التقنية والإنترنت في اتخاذ إجراءات أمنية مناسبة، سواءً من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة، والبرامج.
- يتعين اتاحة الفرصة للمواطنين في المشاركة في مكافحة جرائم الابتزاز الالكتروني، وذلك من خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم، ولاسيما الجرائم الأخلاقية كحالات الإعلان عن البغاء وممارسة الفجور أو الاستغلال الجنسي للأطفال عبر الانترنت .

- توفير خدمات الإرشاد والمساعدة الفنية والقانونية لدى منظمات المجتمع المدني المتخصصة والقادرة على التعامل واستقبال طلبات ضحايا جرائم الابتزاز الالكتروني والمساهمة في حل المنازعات ومتابعة وحل المشكلات بأقل الأضرار.
- العمل على عقد مؤتمر وطني سنوي لبحث قضايا جرائم الابتزاز الالكتروني بمشاركة جميع الأطراف وعقده بالتناوب في مختلف محافظات الجمهورية.
- توعية الموظفين والعُملاء على كيفية تطبيق إجراءات العناية الواجبة للوقاية من الأفعال الاجرامية والتعامل بحذر مع رسائل البريد الإلكتروني والأطراف التي يجري تبادل الرسائل معها.
- رفع التوصيات اللازمة بشأن مكافحة جرائم الابتزاز الالكتروني إلى كافة الجهات المعنية، ونشرها على نطاق واسع من خلال الصحافة والإعلام، ومختلف مواقع التواصل الاجتماعي.
- توظيف الخبراء وتدريبهم لمواكبة أحدث التطورات التكنولوجية وفهمها وتطوير القوانين الوطنية وفق ذلك.
- معالجة ومتابعة إشكاليات توقيع المشتركات والمشتركين على عقود وشروط إذعان عند طلب الحصول على الخدمات والتأكد من عدم مخالفة شروط الشركات والجهات مقدمة الخدمة للقانون بما فيه إنتزاع الموافقة على انتهاك الخصوصية أو على الاحتكار، واعتبار مثل هذه الشروط باطلة لا أثر لها.

ثامنا : فيما يتعلق بدور الجامعات والمؤسسات التربوية المتنوعة:

- تشجيع الباحثين بالدعم المعنوي، والمادي، لإجراء المزيد من البحوث والدراسات حول جرائم الابتزاز الالكتروني المستحدثة.
- حث الجامعات والمراكز البحثية العربية للبحث والدراسة في جرائم الابتزاز الالكتروني، ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة جرائم الابتزاز الالكتروني.
- يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم الاساسي وما قبل التعليم الجامعي .
- ضرورة تضمين المناهج الدراسية كافة المعارف والمعلومات والقيم السلوكية المتعلقة بإستخدام تكنولوجيا المعلومات والاتصال الحديثة ومتطلبات صيانة الخصوصية والأمن الشخصي وسبل مواجهة مخاطرها.
- توثيق وإنتاج مواد مستوحاة من قصص نساء وأطفال تعرضوا لجرائم الابتزاز الالكتروني، وبيان طرق الوقاية وسبل الملاحقة ووقف الإعتداءات ونشرها عبر مختلف الوسائل بما فيه استخدامها كأداة لتوعية الطلاب في المدارس.

- التوعيـة بأسـاليب التحايـل والابتـزاز الالكترونـي والجوانـب السـلبية لعـدم الاسـتخدام الآمـن لوسـائل التواصل الاجتماعي والإنترنت بشكل عام.

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.

المراجع والمصادر

أولاً: المراجع العربية:

- القرآن الكريم.
- الحديث الشريف.

أ) المراجع والمؤلفات العامة:

- حسنى الجندى: شرح قانون العقوبات، هدى حامد قشقوش دن، سنة 1999.
- رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، الطبعة الثانية، سنة 1985.
- السعيد مصطفي السعيد، الاحكام العامة في قانون العقوبات، دار المعارف، الطبعة الرابعة، سنة 1962.
- طارق سرور، الجماعة الاجرامية المنظمة (دراسة مقارنة)، دار النهضة العربية، سنة2000.
- عبد الأحد جمال الدين، النظرية العامة للجريمة، دار الثقافة الجامعية، طبعة 1995– 1996.
- عبد الرؤوف مهدي: شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، الإسكندرية، سنة 1996.
- عبد العظيم مرسي وزير: شرح قانون العقوبات، دار النهضة العربية، دت، سنة 1999
- عبد الواحد العلمي، المبادئ العامة للقانون الجنائي المغربي، الجزء الأول "الجريمة"، مطبعة النجاح الجديدة، سنة 1990.
- عبد الواحد العلمي، شرح القانون الجنائي المغربي، القسم العام، مطبعة النجاح الجديدة– المغرب، طبعة 2007.

- مأمون محمد سلامة ، قانون العقوبات (القسم العام)، الطبعة الثالثة، دار الفكر العربي، القاهرة، سنة 1983.
- مأمون محمد سلامة، شرح قانون العقوبات القسم العام – ط 3 – دار النهضة العربية، الإسكندرية، سنة 2002
- محمد أبو الفتوح، الشائعات في قانون العقوبات المصري والقوانين الأخرى تأصيلا وتحليلا، دار النهضة العربية، سنة 1995.
- محمد عبد المحسن المقاطع، حماية الحياة الخاصة للافراد وضماناتها في مواجهة الحاسوب الآلي، مطبوعات جامعة الكويت، سنة 1992.

ب) المراجع والمؤلفات المتخصصة:

- أيمن عبد الحفيظ: الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، بدون دار نشر، سنة 2005.
- جعفر حسن جاسم الطائي: جرائم تكنولوجيا المعلومات، دار البداية، ليبيا، 2007.
- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، سنة 1998م.
- حسين بن سعيد الغافري: السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، دار النهضة العربية، سنة 2009.
- خالد المختار واسماعيل ببكر محمد، التحقيق الجنائئ في جرائم الحاسوب – دراسة سيكولوجية – اساليبه القانونية– ادواته العلمية – دار عزة للنشر والتوزيع، السودان، سنة 2010م.
- خالد محمد كدفور المهيري: جرائم الكمبيوتر والانترنت والتجارة الالكترونية، دار العزيز للطباعة والنشر، دبي ، سنة 2005.
- خالد ممدوح ابراهيم : امن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، سنة 2008.
- خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، سنة 2009.
- رامى متولي القاضي: مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، ط1، سنة 2011.
- سامى على حامد عياد، الجريمة المعلوماتية واجرام الانترنت – دار الفكر الجامعى، سنة 2007م.
- شمسان ناجى صالح ألخيلي: الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت – دراسة مقارنة، دار النهضة العربية، سنة 2009.
- عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت – دار الكتب القانونية، مصر، سنة 2002 .

- عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية–القاهرة، طبعة سنة 2007 .
- عبد الله عبد الكريم عبد الله: جرائم المعلوماتية والانترنت دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، طبعة اولى، منشورات الحلبي الحقوقية، لبنان، سنة 2007.
- علاء الدين شحاتة : التعاون الدولي في مجال مكافحة الجريمة– رؤية لاستراتيجة وطنية للتعاون الدولي في مكافحة المخدرات، بدون دار نشر، سنة2000..
- علي عبد القادر القهوجي : الحماية الجنائية لبرامج الحاسوب الالي . الدار الجامعية للطباعة والنشر، بيروت، سنة 1999 .
- عمر فاروق الحسيني : المشكلات الهامة في الجرائم المتصلة بالحاسب الالي وابعادها الدولية . الطبعة الثانية، دار النهضة العربية، سنة 1995.
- فريد منعم جبور ، حماية المستهلك عبر الانترنت ومكافحة الجرائم الالكترونية – دراسة مقارنة، منشورات الحلبي، بيروت – لبنان، الطبعة الأولى، سنة2010 .
- محمد أمين الرومي – جرائم الكمبيوتر والانترنت – دار المطبوعات الجامعية، سنة 2003 .
- محمد امين الشوابكة – "جرائم الحاسوب والانترنت الجريمة المعلوماتية" دار الثقافة للنشر والتوزيع الطبعة الاولى – الاصدار الثاني، سنة 2007 .
- محمد حسام، محمود لطفي، "الحماية القانونية لبرامج الحاسب الالكتروني" دار الثقافة للطباعة والنشر القاهرة، الطبعة الأولى، سنة 1978.
- محمد عبد الله ابوبكر سلامة، جرائم الكمبيوتر والانترنت، منشاة المعارف بالاسكندرية، سنة 2006م.
- محمد محمد شتات: فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، سنة 2001.
- محمود شريف بسيوني "المحكمة الجنائية الدولية مدخل لدراسة احكام وأليات الانفاد الوطني للنظام الاساسي" دار الشروق الطبعة الاولى، سنة 2004.
- مصطفي محمد مرسي، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة– القاهرة، الطبعة الأولى، سنة 2008.
- نبيلة هروال : الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي ، الإسكندرية، سنة 2006.
- هشام محمد رستم . الجرائم المعلوماتية . كلية الشريعة والقانون بجامعة الامارات العربية المتحدة – المجلد الثاني – الطبعة الثانية.

- هشام محمد رستم: الجوانب الاجرائية للجرائم المعلوماتية . مكتبة الالات الحديثة . اسيوط، سنة 1994.
- هلال عبد الله أحمد: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية علي ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية، سنة 2002.
- هلالي عبد الاله أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – طبعة اولى، دار النهضة العربية، القاهرة، سنة 1997 .
- يونس عرب: جرائم الكمبيوتر والانترنت، طبعة اولى، منشورات اتحاد المصارف العربية، بيروت، سنة 2002.
- أحمد عوض بلال، الجرائم المادية والمسؤولية الجنائية دون خطأ، دراسة مقارنة، دار النهضة العربية، سنة 1993.

ج – رسائل الدكتوراه المتخصصة:

- سالم محمد سليمان الاوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، سنة 1997.
- أحمد العجلونى، قواعد تفسير النصوص وتطبيقاتها في الاجتهاد القضائي الأردنى دراسة أصولية مقارنة، رسالة دكتوراه، كلية الدراسات العليا، الجامعة الأردنية، سنة 2005.
- أحمد محمد خليفة، النظرية العامة للتجريم، دراسة في فلسفة القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 1959م.
- سيد حسن عبد الخالق، النطرية العامة لجريمة إفشاء الأسرار في التشريع الجنائي المقارن، رسالة دكتوراه كلية الحقوق، جامعة عين شمس، سنة 1987.
- عبد الرحمن محمد إبراهيم خلف، الحماية الجنائية للحق في الشرف والإعتبار، دراسة تحليلية تأصيلية، رسالة دكتوراه كلية الحقوق، جامعة القاهرة، سنة 1992م.
- عبد المنعم محمد إبراهيم رضوان، موضع الضرر في البنيان القانوني للجريمة، دراسة تحليلية تأصيلية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 1994م.
- عبد الحميد حسب النبى الشورى، اثر الارهاب على الاقتصاد القومى في مصر، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، سنة 2000.
- عبد المولى على متولى، النظام القانونى لحسابات السرية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 2002.

د – رسائل الماجستير المتخصصة:

- سليمان بن مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2003م

- عبد الرحمن البحر، معوقات التحقيق في جرائم الأنترنت."رسالة ماجستير غير منشورة" الرياض، أكاديمية نايف العربية للعلوم الأمنية، سنة 1999.
- محمد بن نصير محمد السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت "دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2004،
- يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري– تيزي وزو– الجزائر، سنة 2013، ص 114
- عاطف وليم اندروس، الاقتصاد الظلى وأثره على الموازنة العامة في مصر من1980 – 1990، رسالة ماجستير غير منشورة، كلية التجارة، جامعة الاسكندرية.
- مشعل بن عبد الله بن عويض العتيبي، إجراءات التحقيق في جريمة غسل الأموال في المملكة العربية السعودية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، سنة 2008.
- المهدي ناصر، ظاهرة غسل الأموال، (مذكرة ماجستير)، جامعة سعد دحلب، كلية العلوم الاقتصادية وعلوم التسيير، قسم العلوم الاقتصادية، البليدة، الجزائر، 2005، (غير منشورة).

و– احكام المحاكم:

- حكم المحكمة الدستورية العليا المصرية في القضية رقم 114 لسنة 21 قضاء دستوري، جلسة 2001/6/2.
- حكم المحكمة الدستورية العليا المصرية في القضية رقم 48 لسنة 17 قضاء دستوري، جلسة 1997/2/22.
- حكم المحكمة الدستورية العليا المصرية في القضية رقم 49 لسنة 17 قضاء دستوري، جلسة 1996/6/15.
- المحكمة الدستورية العليا – الطعن رقم 24 – لسنة 18 قضائية – تاريخ الجلسة 5–7–1997 – مكتب فني 8 – رقم الجزء 1 – رقم الصفحة 709
- المحكمة الدستورية العليا – الطعن رقم 3 – لسنة 10 قضائية – تاريخ الجلسة 2–1–1993 – مكتب فني 5 – رقم الجزء 2 – رقم الصفحة 103

– ثالثا: أبحاث ودراسات واوراق عمل ودورات تدريبية:

- إبراهيم بن عوض العتيبى، استخدام التقنية في التحقيقات الامنية، مقال منشور بمجلة التقنية والامن، مجلة كلية الملك خالد العسكرية، العدد 80، سنة 2005
- إبراهيم بن محمد الزبن وغادة بنت عبد الرحمن الطريف، الخوف من جرائم الجوال، ندوة المجتمع والأمن، الرياض، كلية الملك فهد الأمنية، 5 أبريل، سنة 2007.

- أحمد الطالب، تقنيات البحث وإجراءات المسطرة المتبعة في جرائم الانترنت والمعلوميات، مجلة الملف، العدد الصادر بتاريخ 9 نوفمبر من سنة 2006.
- إدريس النوازلي، قراءة في الجريمة السيبيرية على ضوء الاتفاقية الأوروبية، مجلة المحاكم المغربية، العدد 104 ، سبتمبر – أكتوبر من سنة 2006 .
- إيهاب ماهر السنباطي، الجرائم الإلكترونية "قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد"، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 20– 19 يونيو من سنة 2007، المملكة المغربية.
- البروتوكول الإضافي لاتفاقية الجريمة المعلوماتية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهة الأجانب التي ترتكب عبر أنظمة الكمبيوتر، عرض للتوقيع بستراسبورغ بتاريخ 28 يناير 2003 ، بمناسبة الدورة الأولى للجمعية البرلمانية لسنة 2003.
- صباح محمد عبد الكريم، أخلاقيات مجتمع المعلومات في عصر الإنترنت، بحث منشور، الرياض، مجلة الملك فهد الوطنية، المجلد الثالث عشر، العدد الأول، يناير 2007.
- عبد الحكيم الحكماوي، الإثبات في الجريمة الالكترونية، سلسلة ندوات محكمة الاستئناف بالرباط ، العدد السابع ، سنة 2014 .
- عبد الرحمان اللمتوني، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط ، العدد السابع ، سنة 2014.
- عبد الله حسين على محمود:إجراءات جمع الأدلة في مجال سرقة المعلومات، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، إمارة دبي بدولة الإمارات العربية المتحدة – 26–2003/4/28م، المجلد الأول.
- فتيحة محمد قوارري" المواجهة الجنائية لقرصنة المصنفات الإلكترونية Peer to peer " مجلة الحقوق الكويت العدد الأول، السنة الرابعة والثلاثة مارس من سنة 2010.
- كريستينا سكولمان، المعايير الدولية المتعلقة بجرائم الانترنت (مجلس أوروبا)، أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 20– 19 يونيو من سنة 2007، المملكة المغربية.
- كمال احمد الكركي، النواحي الفنية لاساءة استخدام الكمبيوتر ورشة عمل في دورة جرائم التطور التقني المنعقدة بعمان . سنة 1998.
- محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية.
- محمد الجندي، الجريمة الالكترونية في الشرق الأوسط، مجلة أمن المعلومات، القاهرة، يونيو، 2008 ، برنامج الأمم المتحدة الإنمائي، سنة 2003.

- محمد أمين البشري: التحقيق في جرائم الحاسب الآلي والإنترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض 1421هـ
- محمد جوهر، خصوصية زجر الإجرام المعلوماتي، مجلة الملف، العدد 9 نوفمبر، سنة 2006.
- محمد حجازي، جرائم الحاسبات والمعلوماتية، بحث منشور، المركز المصري للملكية الفكرية، القاهرة، سنة 2006.
- محمود كبيش، الحماية الجنائية لسرية الحسابات البنكية في القانون المصري، مجلة القانون والإقتصاد، العدد التاسع والستون 1999م.
- المرشد الامريكي الصادر عام 1994م، المعد من قبل قسم جرائم الحاسب الآلي والملكية الفكرية بإشراف الأستاذ Orin Kerr، والمعدل سنة 2002 الذي تضمن تطبيقا للقانون الوطني الأمريكي الصادر في 2001/10/26.
- مصطفي سمارة، الجريمة الالكترونية، مجلة المعلوماتية، العدد 29– سنة 2008.
- مقتضيات تعامل أجهزة النيابة العامة مع الجريمة السيبرانيَة (الحاسوبية)، ورقة عمل قدمت إلى مؤتمر القمة العالمي لأعضاء ورؤساء النيابة العامة، المنعقد بالعاصمة القطرية الدوحة في الفترة من 14– 16 /2005/11.
- نجوى عبد السلام، أنماط و دوافع استخدام الشباب المصري لشبكة الإنترنت دراسة استطلاعية، المؤتمر العلمي الرابع لكلية الإعلام وقضايا الشباب، كلية الإعلام، جامعة القاهرة، 25 – 27 مايو، سنة 1998.
- نور الدين الواهلي، الإختصاص في الجريمة الإلكترونية، سلسلة ندوات محكمة الاستئناف بالرباط ، العدد السابع ، سنة 2014.
- هاني محي الدين عطية، تجربة في أخلاقيات مجتمع المعلومات: دراسة استطلاعية لرؤية طلاب علم المعلومات، مجلة المكتبات والمعلومات العربية، الدوحة، السنة السابعة و العشرون، العدد الثالث، يوليو من سنة 2007.
- هدى قشقوش: جرائم الكمبيوتروالجرائم الاخرى في مجال تكنولوجيا المعلومات . بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان: الجرائم الواقعة في مجال تكنولوجيا المعلومات . القاهرة اكتوبر من سنة – 1983 دار النهضة العربية.
- هشام ملاطي، خصوصية القواعد الإجرائية للجرائم المعلوماتية– محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية، سلسلة ندوات محكمة الاستئناف بالرباط، العدد السابع، سنة 2014.
- هند علوي، حماية الملكية الفكرية في البيئة الرقمية من خلال منظور الأساتذة الجامعيين: أساتذة جامعة منتوري نموذجا، بحث منشور، الجزائر، المركز الجامعي العربي، سنة 2006.

- وليد عالكوم: مفهوم وظاهرة الاجرام المعلوماتي . بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت . جامعة الامارات – مايو سنة 2000 .

رابعا : المراجع الأجنبية:

- BECCARIA:"Traité des délits et des peines".Nouvelle Traduction jrançaise,Introduction de ANCEL et STEFANI,Paris,Cujas 1966.
- BERNA RDINI(R.),Droit Pénal general,Paris,2003,No193.
- Cohen Frederick: Protection and security on the information super high way,Wiley&sons,Inc,1995.
- D.B Parker,combattre la crimipin alite informatique,1985.
- DRADEL(J.),Droit penal général ,CuJus,2002-2003,No181.
- J.P.Delms saint hilair: un probleme qui évolue, le principe de la léqali –té en matiére d'attante á la liberté de l'ass.inter.de droit penal-bordeaux 1984.
- D.B Parker,combattre la crimipin alite informatique,1985,p18.
- Cohen Frederick: Protection and security on the information super high way,Wiley&sons,Inc,1995,p66.ets.
- BECCARIA:"Traité des délits et des peines".Nouvelle Traduction jrançaise,Introduction de ANCEL et STEFANI,Paris,Cujas 1966,p.67.
- J.P.Delms saint hilair: un probleme qui évolue, le principe de la léqali –té en matiére d'attante á la liberté de l'ass.inter.de droit penal-bordeaux 1984.p12.etss.
- Malcom Anderson : " Policing the world : Interpol the Politics of International Police Co- Operation'', Clarendon press.Oxford,1989,p 168-185
- VIDAL (G), Cours de droit criminal et de science penitenterntniaire 8eme ed,mis a jour par Magnol, libraie Arthur Rousseau, paris,1935,N 0 1,p1071.
- John Eaton & jermy smithers, A managers Guide to information Technology, London, Philip Allan,1982,p263
- BERNA RDINI(R.),Droit Pénal general,Paris,2003,No193,p171.
- Yann padova, Un aperçu de la lutte contre la cybercriminalité en France , revue de science criminelle et de droit pénal comparé , N°4 octobre-décembre 2002, p .767
- Myriam Quéméner & Yves charpenel , cybercriminalité – droit pénal appliqué- Economica paris France,2010, p .161 et s
- GIMENO(BJ),peoiection de lenvironnement par le droit penal, pour une approche communautaire, R,E 2 er anee N 05 Mai 2002,p8.

- Myriam Quéméner & Yves charpenel , op .cit , p .161
- OMPI / UNESCO, Rapport de groupe de travail chargés des questions technqiues relatives à la protection juridique du logicial.
- DRADEL (J.), Droit penal général, CuJus, 2002-2003,No181,p.175.

خامسا : المراجع من الانترنت:

- Arthur, C. (2011). Guardian.co.uk. available at: http://www.guardian.co.uk
- Posetti, J. (2011). Twitter. Available at: http://twitter.com
- Tinker, T., Mc Laughlin, G., & Dumlao, M. (2009-2010), «Crisis Communication and Response», Retrieved April 4, 2011, from Disaster Resource Guide:, available at: http://www.disaster-resource.com
- Council of Europe Organized Crime Report 2004 available at: http://www.coe.int
- ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int
- ITU, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February2009. available at: http://www.itu.int
- United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org
- O'Connell, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: http://www.ibls.com
- Schjolberg and Hubbard, «Harmonizing National Legal Approaches on Cybercrime», 2005, page 5. available at: http://www.itu.int
- Simon and Slay, «Voice over IP: Forensic Computing Implications», 2006, available at: http://scissec.scis.ecu.edu.au
- Sofaer and Goodman, «The Transnational Dimension of Cyber Crime and Terrorism», 2001, page 14, available at: http://media.hoover.org
- The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. available at: http://www.oecd.org
- WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/
- WSIS Tunis Agenda for the Information Society, 2005, available at: http://www.itu.int
- ITU Global Cybersecurity Agenda, High-Level Experts Group, Global Strategic Report, 2008..
- UN report on the Internet, available at: http://documents.latimes.com//
- Protocol Address Space

- Assigned Names and Numbers
- The Internet Corporation for Assigned Names
- The European Cybercrime Council Convention
- ITU: Understanding Cyber Crime : A guide for developing countries, draft, April 2009,cybmai@itu.int
- G8 recommandations on transnational crimes, 2011¡

" تمت بحمد الله تعالي"

الفهرس