دولة الإمارات العربية المتحدة

جامعة أبو ظبي – كلية القانون

برنامج الماجستير في القانون

جامعة أبوظبي
ABU DHABI UNIVERSITY

رسالة ماجستير بعنوان:

الابتزاز الإلكتروني

(دراسة مقارنة)

Electronic blackmail

(A comparative study)

بحث مقدم لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام

إعداد الباحث: سيف عبدالله الشحي.

الرقم الجامعي: 1077589

إشراف الدكتور: حسين المحمد

لجنة الحكم والمناقشة

الدكتور/ حسين عيسى المحمد .....(مشرفًا).

الدكتورة/ سناء عبدالله رواقة .....(عضوًا).

العام الجامعي

2021/2020

إقرار الباحث

أقر أنا الموقع أدناه الطالب/ **سـيف عبدالله الشـحي** المقيد ببرنامج الدراسـات العليا أن هذا البحث المقدم مني للحصول على درجة الماجستير في القانون العام، هو نتاج عملي وجهدي العلمي الخالص، ولم يســـبق لي التقدم به لأي جهة علمية أو إدارية أو غيرها داخل الدولة أو خارجها للحصول على أي درجة علمية أخرى أو لأي سبب من الأسباب، وأن مضمون هذه الرسالة يعكس آراء الباحث الخاصة وهي ليست بالضرورة الأراء التي تتبناها الجهة المانحة للدرجة العلمية، كما أقر بقبول قيام الجامعة في حالة إجازة الرسـالة من قبل لجنة المناقشـة والحكم بطباعة الرسـالة ونشـرها بالكيفية التي تراها محققة لأغراضـــها وأهدافها، دون أن يكون لي حق العدول عن هذا الإقرار بعد إجازة الرسالة.

اسم الباحث: سيف عبدالله الشحي

الرقم الجامعي: 1077589

توقيع الباحث:

إجازة أطروحة الماجستير

عنوان الرسالة: (الابتزاز الإلكتروني- دراسة مقارنة).

نوقشت هذه الرسالة وتم إجازتها من قبل أعضاء لجنة المناقشة المشار إليهم أدناه بتاريخ:

المشرف على الرسالة: **الدكتور/ حسين عيسى المحمد** أستاذ القانون الجنائي المساعد.

كلية- قسم القانون العام - جامعة أبوظبي.

التاريخ 2020/12/7 التوقيع

عضو لجنة المناقشة: **الدكتورة/ سناء عبدالله رواقة** أستاذ القانون الدولي المساعد.

كلية القانون- قسم القانون العام- جامعة أبوظبي.

التاريخ 07/12/2020 التوقيع

RAWAQA Sana

بسم الله الرحمن الرحيم

(يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ).

صدق الله العظيم

الحجرات : الآية (12)

الإهــداء

إلى من غرسا في نفسي حب العلم والفضيلة وحب الأوطان ((والدي ووالدتي))

أقول لهم: أنتم وهبتموني الحياة والأمل والنشأة على شغف الاطلاع والمعرفة

وإلى إخوتي وأسرتي جميعاً

و إلى كل من علمني حرفاً أصبح سنا برقه يضيء الطريق أمامي

الشـكر والتقدير

أتقدم بخالص الشكر والتقدير لكل من ساهم في إنجاز هذا العمل المتواضع وأخص بالشكر والتقدير الدكتور/ حسين عيسى المحمد أستاذ القانون الجنائي بجامعة أبو ظبي على تفضله بقبول الإشراف على هذه الرسالة، وإحاطتي بتوجيهه ونصحه وإرشاده رغم مسؤولياته وأعبائه المتعددة، فجزاه الله عني خير الجزاء.

كما أتوجه بالشكر الجزيل للسادة أعضاء لجنة الحكم والمناقشة، ولكل من وقف وأعانني في كتابته وطبعه وإخراجه لكم مني الشكر و العرفان ومن الله جزيل الجزاء ووافر الإحسان.

الباحث

الملخص

إن إنتشـــــار ظـاهرة الابتزاز الإلكتروني واســـتغلال الجنـاة للثورة التكنولوجيـة في مجـال الاتصـالات الإلكترونية في ارتكاب هذه الجريمة، خاصة أن معظم مستخدمي الاتصالات الإلكترونية يجهلون التعامل السـليم مع هذه التقنية، فيقعون فريسـة للمبتزين الذين يقومون بإغراء المجني عليهم ونصـب شـراكهم الالكترونية للايقاع بهم، ومن ثم يتم اسـتغلالهم، فضـلًا عن سـهولة ارتكاب هذه الجريمة لأنها ترتكب عن بعد، ويمكن أن تُرتكب في أي مكان في العالم.

لقد تناول الباحث البنيان القانوني لجريمة الابتزاز الإلكتروني من حيث التعريف والأركان وأنواع وأســـاليـب الابتزاز الإلكتروني وآثـاره، وإجراءات التحقيق وجمع الأدلـة في جرائم الابتزاز الإلكتروني وما يواجهه المحقق من صـــعوبات أثناء التحقيق. وأخيرا تطرق الباحث إلى العقوبات المقررة لجريمة الابتزاز الإلكتروني بصورتها البسيطة والمشددة في التشريعين الإماراتي والمصري.

وتكمن مشـكلة البحث في بيان عدم كفاية النصـوص القانونية في قانون الجرائم الالكترونية لمواجهة ومكافحة الابتزاز الالكتروني، وغياب تعريف لهذه الجريمة في (المرسوم بقانون اتحادي رقم (5) لســـنة 2012 المعدل بالقانون الاتحادي رقم (2) لســـنة 2018 بشـــأن مكافحة جرائم تقنية المعلومات). حيث لم يعرف جريمة الابتزاز الالكتروني ولم يُقرر لها العقوبة المناسبة.

وتوصـل الباحث لبعض النتائج من أهمها غياب النص الصـريح على هذا النوع من الجرائم إذا ما اقترفت بوسـائل إلكترونية والاعتماد على النصـوص العامة في قانون العقوبات الاتحادي. كما توصل الباحث لبعض التوصيات تتعلق بضرورة تعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لســـنة 2018 بشـــأن مكافحة جرائم تقنية المعلومات، والتوعية

بكافة الطرق بأخطار هذه الجريمة، خاصة أن ضحاياها عادة من صغار السن أو النساء، ورغم الجهود المبذولة لمكافحة هذا النوع من الإجرام إلا أنها لا زالت في تفاقم وازدياد لعدم مواكبة الآليات التشريعية والتنفيذية لوسائل وأساليب ارتكاب هذه الجرائم وصعوبة تتبعها والكشف عنها.

ABSTRACT

The spread of the phenomenon of electronic blackmail and the perpetrators' exploitation of the technological revolution in the field of electronic communication in committing this crime, especially since most users of electronic communication are ignorant of the proper handling of this technology, so they fall prey to blackmailers who lure the victims and set up their electronic traps to trap them, and then they are exploited, In addition to the ease of committing this crime because it is committed from a distance, and it can be committed anywhere in the world.

The researcher dealt with the legal structure of the crime of electronic extortion in terms of definition, elements, types and methods of electronic extortion and its effects, investigation procedures and evidence gathering in crimes of electronic extortion and the difficulties the investigator faces during the investigation. Finally, the researcher touched on the penalties prescribed for the simple and severe crime of electronic extortion in the UAE and Egyptian legislation.

The research problem lies in showing the insufficient legal texts in the Cyber Crime Law to confront and combat electronic extortion, and the absence of a definition of this crime in (Federal Decree Law No. (5) of 2012 amended by Federal Law No. (2) of 2018 regarding combating information technology crimes) As he did not know the crime of electronic blackmail and did not decide on the appropriate punishment.

The researcher reached some results, the most important of which is the absence of an explicit provision on this type of crime if it is committed by electronic means and reliance on general texts in the Federal Penal Code.

The researcher also reached some recommendations related to the need to amend Federal Decree Law No. (5) of 2012 amended by Federal Law No. (2) of 2018 regarding combating information technology crimes, and awareness in all ways of the dangers of this crime, especially since its victims are usually young or women, despite The efforts exerted to combat this type of crime are still exacerbating and increasing because the legislative and executive mechanisms do not keep pace with the means and methods of committing these crimes and the difficulty of tracking and detecting them.

قائمة المحتويات

المقدمة:

يعتبر الأمن والطمأنينة من أعظم النعم، والخوف والاضـــطراب من أســـوء النقم، لذا كان الابتزاز من أبشع الجرائم؛ لأنه يؤثر في شعور الإنسان بالأمن، فيثير الرعب والفزع لديه، ويترك أثرًا في نفسه أشد من إصابة جسده، فيدفعه لإتيان فعل أو الامتناع عنه، سواء أكان مشروعا أم غير مشروع دون إرادته، مما يشكل عدوانا على حقه في الرفاه الاجتماعي والنفسي كأحد حقوق الإنسان، فالتشريعات لا تقيم وزنا للتصرفات التي ترتكب دون إرادة حرة مستنيرة.

ونتيجة للثورة المعلوماتية الضـخمة التي أثرت بشـكل كبير في حياة أفراد المجتمع من حيث الشكل والمضمون، وأدت إلى خلق بيئة اجتماعية لم تكن مألوفة من قبل، يطلق عليها البيئة الرقمية أو الإلكترونية، التي كان من نتائجها المباشـرة أنها أصـبحت أداة للكثير من العلاقات، ولممارسـة العديد من الأنشطة، ورافق هذا النشـاط العديد من الأفعال التي شـكلت أفعالا مجرمة بحكم القانون، وأبرزت شـكلا من الجريمة أطلق عليها الجريمة الإلكترونية أو الجريمة (السـيبرانية)، وشـكل هذا النشـاط المسـتحدث تحديا واضـحا للتشـريعات التي عانت لفترة طويلة من النقص التشـريعي وغياب الأحكام الخاصـة بهذا النوع من الجرائم، التي تعتمد في وجودها على هذا الفضـاء الخاص، والذي سـاعد في انتشـارها بسـرعة مذهلة، وجود ما يعرف بالشـبكة العنكبوتية (الإنترنت) باسـتخداماتها المتعددة، حيث إنها توسعت وانتشرت انتشارا سريعا، وأصبح مستخدموها من جميع الفئات العمرية، باختلاف مسـتوياتهم العلمية، فبقيت كثير من الأفعال عبر هذه الشـبكة، بدون قيود قانونية ويغيب عنها التنظيم التشـريعي، خاصـة في مجال الجريمة المقترفة بواسـطتها، وغياب هذا الجانب صـعّب مهمة القضـاء في تطبيق قانون العقوبات على هذه الأشـكال المسـتحدثة من الأفعال، التي شـكلت

ضررا اجتماعيا ونفسيا وماليا على المجتمع، مما استوجب إصدار تشريعات خاصة تتضمن تجريما واضحا لهذه الأفعال وتحديد عقوبات خاصة لها، كمحاولة من المشرعين في التصدي لهذه الجرائم والحد من آثارها.

ويزداد الأمر خطورة عندما يتم الابتزاز من خلال وسيلة إلكترونية، حيث يصعب محو آثاره منها، أو تحديد الأشخاص الذين تمكنوا من الاطلاع على ما يتم ابتزاز الشخص به، أو أن يكون بشيء تم الاطلاع عليه من خلال وسيلة إلكترونية وتم خرقها، فالابتزاز هو داء العصر، لكونه قد يصل بالإنسان إلى درجة الرق والعبودية، فهو تهديد الآخرين بوسائل شتى لإشعارهم بالخطر، مما يجعلهم ينزفون دائما، ويكونون تحت إمرة الجاني، لاسيما أن نطاق الضرر الناتج عن النشر الإلكتروني يفوق أضعاف الضرر الناشئ عن النشر الورقي.

وضحايا الابتزاز كثيرون جدا؛ منهم: الحكومات والشركات والأفراد العاديون سواء أكانوا رجالا أم نساء، أحداثا أم بالغين، وأيا كان مركزهم السياسي أو الاجتماعي، ويقوم به الجاني من خلال أشياء توصل إليها بنفسه، أو أشياء أطلعه عليها المجني عليه فاستغلها الجاني.

أهمية البحث:

أعادت أنظمة المعلومات وشبكاتها، تشكيل ثقافة الأفراد وسلوكياتهم في شتى المجالات، وخاصة في ميدان أنشطة الحصول على المعلومات والتواصل فيما بينهم، وتهدد هذه التقنيات سلوكيات استهداف الخصوصية وكشف الأسرار والتعرض لمصالح الأفراد المختلفة. ولأن جريمة الابتزاز الإلكتروني تنطوي على السلوك الإجرامي الأخطر الذي يؤثر على مدى ثقة الأفراد بتقنية المعلومات وتطبيقاتها المختلفة، فإن البحث يتخذ أهمية بالغة لجهة بيان عناصر وأركان هذه الجريمة

وأوجه اختلافها عن عناصـــر وأركان الابتزاز التقليدي، لما له من أثر فعال في إدراك حجم مخاطرها والتوعية بذلك، ولغايات نجاعة التصـــدي لها ومكافحتها والتخفيف من آثارها المدمرة على النســـيج الاجتماعي.

مشكلة البحث:

تتمثل مشكلة البحث في بيان مدى كفاية النصوص الالتشريعية لمواجهة الابتزاز الإلكتروني، حيث يكشف التنظيم التشريعي عن عدم وجود نص قانوني صريح يجرم الابتزاز الإلكتروني، ويحمي ضـــحاياه، خصـــوصـــا النســـاء والأطفال، ومن ثم فرار الجاني من العقاب رغم خطورة جريمته التي تشكل عدوانا على حريات الأشخاص، وشرفهم وسمعتهم، وأموالهم. فالنصوص الحالية في **(المرسوم بقانون اتحادي رقم (5) لســـنة 2012 المعدل بالقانون الاتحادي رقم (2) لســـنة 2018 بشـــأن مكافحة جرائم تقنية المعلومات)**. ليست كافية للعقاب على الابتزاز الإلكتروني وصوره المختلفة.

تساؤلات البحث:

يثير البحث جملة من التساؤلات يمكن إيجازها في الآتي:

- ما المقصود بجرائم الابتزاز الإلكتروني وما صورها؟
- ما أنواع وأساليب الابتزاز الإلكتروني؟
- ما مدى جسامه جريمة الابتزاز الإلكتروني وآثارها على كلا من الفرد والمجتمع؟
- ما هي أركان جريمة الابتزاز الإلكتروني؟
- ما هي طرق التحقيق وجمع الأدلة بصدد جريمة الابتزاز الإلكتروني؟

- ما صعوبات الإثبات في جرائم الابتزاز الإلكتروني؟
- ما العقوبات الأصلية والتكميلية لجرائم الابتزاز الإلكتروني؟
- ما العقوبة المقررة للشروع والمساهمة التبعية لجريمة الابتزاز الإلكتروني؟

أهداف البحث:

يسعى البحث إلى تحقيق الأهداف التالية:

- بيان مفهوم الابتزاز الإلكتروني.
- بيان أنواع وأساليب وآثار الابتزاز الإلكتروني.
- كيفيه إثبات جريمة الابتزاز الإلكتروني من حيث إجراءات التحقيق وجمع الأدلة.
- بيان الصعوبات التي تواجه التحقيق في جرائم الابتزاز الإلكتروني.
- بيان العقوبات المقررة لجرائم الابتزاز الإلكتروني.

حدود البحث:

-**الحدود الموضوعية:** جريمة الابتزاز الإلكتروني من حيث العناصر والأركان ومسؤولية الجاني.

الحدود المكانية: دولة الإمارات العربية المتحدة.

الحدود الزمانية: العام الأكاديمي 2020- 2021م.

منهج البحث:

اعتمد الباحث المنهج الوصـــفي التحليلي المقارن، للوقوف على إشـــكالية جرائم الابتزاز الإلكتروني ووضع حلول لها، من خلال الرجوع إلى الأراء الفقهية، والأحكام القضائية وتحليلها، وربط ذلك بالأفكار الأصـــولية، وبيان مدى ملاءمتها معها، أو خروجها عنها، وفي الســـياق ذاته يســـير البحث معتمدا على المنهج المقارن في جزيئات عديدة من البحث كلما كان ذلك متاحا للمقارنة بين التشـــريع الإماراتي والتشـــريع المصـــري للمقارنة بين الابتزاز التقليدي والابتزاز الإلكتروني من حيث أوجه الشبه والاختلاف بخصوص الأركان الأحكام الخاصة بجرائم الابتزاز الإلكتروني.

الدراسات السابقة:

الدراسة الأولى– وائل سليم عبد الله شاطر، (الإطار القانوني لجريمة الابتزاز الإلكتروني في الألعاب الإلكترونية)، دراســـة مقارنة وفق النظام الســـعودي والقانون الكويتي، المجلة العربية للنشـــر العلمي، 2020م[1].

تناول الباحث خطة النظام الســـعودي والنظام الكويتي في تجريم الابتزاز الإلكتروني، حيث ناقش الباحث المصـــلحة القانونية في دراســـة جريمة الابتزاز الإلكتروني والتعرض لأركانها والكشـــف عن أجهزة الضـــبط القضـــائي الخاصـــة بها والمعوقات التي تحول دون الإثبات في مثل هذا النوع من الجرائم.

(1) – وائل سليم عبد الله شاطر، (الإطار القانوني لجريمة الابتزاز الإلكتروني في الألعاب الإلكترونية)، دراسة مقارنة وفق النظام السعودي والقانون الكويتي، المجلة العربية للنشر العلمي، 2020م.

الدراســة الثانية– أمينة بنت حجاب، بعنوان (تصــور مقترح لتنمية الوعي الوقائي لدى الفتيات للوقاية من جرائم الابتزاز)، رسالة دكتوراة في العلوم الأمنية، تخصص علم اجتماع الجريمة، الرياض، جامعة نايف للعلوم الأمنية، 2016م[2].

هدفت الدراسـة إلى الخروج بتصـور مقترح لتنمية الوعي الوقائي لدى الفتيات لوقايتهن من جرائم الابتزاز، وقد توصلت الدراسة إلى وجود ضعف في بعض جوانب الوعي بجرائم الابتزاز وأشكاله، كما كشفت النتائج عن وجود حاجة لتنمية الوعي القائم بجرائم ابتزاز الفتيات.

ركزت الدراسـة في الجانب التوعوي والاجتماعي لجريمة الابتزاز؛ **في حين سـتقوم هذه الدراسـة بالوصول إلى الجانب التشريعي والحماية التشريعية لضحايا جريمة الابتزاز الإلكتروني.**

الدراسة الثالثة– طارق بن عبد الرازق المطيري، (الأحكام الخاصة بحريمة الابتزاز المقررة في نظام مكافحة الجرائم المعلوماتية السـعودي، دراسـة مقارنة، المعهد العالي للقضـاء، الرياض، السـعودية، 2010م[3].

تناولت الدراسة أحكام جريمة الابتزاز التي نظمها (نظام مكافحة الجرائم المعلوماتية السعودي)، من حيث عناصرها وأركانها وما امتاز به النظام السعودي عن غيره من التشريعات العربية المماثلة في هذا الخصوص في ضوء اتساع انتشار هذه الجريمة وتأثيرها السلبي على المجتمع السعودي،

---

(2)– أمينة بنت حجاب، بعنوان (تصور مقترح لتنمية الوعي الوقائي لدى الفتيات للوقاية من جرائم الابتزاز)، رسالة دكتوراة في العلوم الأمنية، تخصص علم اجتماع الجريمة، الرياض، جامعة نايف للعلوم الأمنية، 2016م.

(3) – طارق بن عبد الرازق المطيري، (الأحكام الخاصة بحريمة الابتزاز المقررة في نظام مكافحة الجرائم المعلوماتية السعودي، دراسة مقارنة، المعهد العالي للقضاء، الرياض، السعودية، 2010م.

إلا أن هذه الدراســـة لم تقف على أوجه الاختلاف بين الابتزاز الإلكتروني والابتزاز التقليدي ولم تتناول أحكام الابتزاز المقررة في تشريعات الجزاء التقليدية.

خطة البحث:

الفصل الأول- البنيان القانوني لجريمة الابتزاز الإلكتروني.

المبحث الأول: مفهوم جريمة الابتزاز الإلكتروني.

المطلب الأول- تعريف الابتزاز الإلكتروني.

المطلب الثاني- أنواع وأساليب الابتزاز الإلكتروني.

المطلب الثالث- آثار الابتزاز الإلكتروني.

المبحث الثاني: أركان جريمة الابتزاز الإلكتروني.

المطلب الأول- الركن الشرعي لجريمة الابتزاز الإلكتروني.

المطلب الثاني- الركن المادي لجريمة الابتزاز الإلكتروني.

المطلب الثالث- الركن المعنوي الابتزاز الإلكتروني.

الفصل الثاني- إثبات جريمة الابتزاز الإلكتروني والعقوبات المقررة لها.

المبحث الأول- التحقيق في جرائم الابتزاز الإلكتروني.

المطلب الأول- إجراءات التحقيق وجمع الأدلة في جرائم الابتزاز الإلكتروني.

المطلب الثاني- الصعوبات التي تواجه التحقيق في جرائم الابتزاز الإلكتروني.

المبحث الثاني- الجزاءات المقررة لجرائم الابتزاز الإلكتروني.

المطلب الأول- **الجزاءات المقررة لجريمة الابتزاز الإلكتروني بصورتها البسيطة.**

المطلب الثاني- **الجزاءات المقررة لجريمة الابتزاز الإلكتروني بصورتها المشدّدة.**

الخاتمة

النتائج والتوصيات.

الفصل الأول- البنيان القانوني لجريمة الابتزاز الإلكتروني:

يقتضـي مبدأ الشـرعية لاعتبار الفعل جريمة وجود نص يجرم الفعل ويعاقب على إتيانه، وهذا هو الركن الشـرعي للجريمة، كما يوجب إتيان سـلوك الجريمة سـواء كان فعلاً أو امتناعاً، وهذا ما يسـمى بالركن المادي للجريمة، وأن يكون الجاني مكلفاً أي مسـؤولاً عن الجريمة، وهذا ما يسـمى بالركن المعنوي[4]. وهذه الأركان هي الأركان العامة في الجريمة، التي يتوجب وجودها في كل جريمة، وتوافر هذه الأركان لا يغني عن توافر الأركان الخاصـة لكل جريمة على حده، ولمعرفة هذه الأركان لابد من معرفة موضـوع الجريمة المراد بحثه، ويتمثل هنا بالابتزاز الإلكتروني، وهو التهديد الذي يقع على المجني عليه أو ماله أو أي شخص يهمه أمره[5].

وتجدر الإشارة إلى أن الأصل في كل الأفعال الإباحة سواء في الشريعة أو القانون، حتى يأتي نص من الشـريعة، أو القانون بتجريم الفعل، فالأمر الذي لا تعده الشـريعة أو القانون جريمة، هو مباح بصفة أصلية من الناحية الجنائية بصرف النظر عن الظروف التي وقع فيها، بحيث لا يكون على القاضي لكي يحكم بالبراءة إلا أن يتحقق من عدم وجود نص يجرم الفعل المسند للمتهم.

فجريمة الابتزاز الإلكتروني تؤرق الآمنين والمسالمين، وتحول حياتهم من حياه مستقرة هادئة إلى حياه يعتريها الخوف والاضطراب من الذي يهددهم، وينتظرون وقوعه، فالابتزاز الإلكتروني جريمة تضج منها شتى المجتمعات[6]، ومختلف الشخصيات، خصوصا مع التطور التكنولوجي المذهل، الذى

---

(4)- عبد القادر عودة، التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي، مؤسسة الرسالة ناشرون، لبنان، بيروت، ط1، 2008م، ص 69/1.

(5)- عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، دار الكتب القانونية، القاهرة، مصر، 2010م، ص 349.

(6)- عبد العظيم مرسي، جرائم الاعتداء على الأموال، دار النهضة العربية، القاهرة، مصر، 1993م، ص126.

أثر على طبيعة الجريمة والوسائل المستخدمة فيها، وعلى الرغم من ذلك قد يبدو أحيانا أن تجريم الابتزاز الإلكتروني يتعارض مع حريه التعبير، أو يشكل إحدى المعاملات الاقتصادية المشروعة، الأمر الذى يتطلب بيان ملاءمة تجريمها. وبناء على ما سبق سيتناول الباحث هذا الفصل في المبحثين التاليين:

المبحث الأول– مفهوم جريمة الابتزاز الإلكتروني.

المبحث الثاني– أركان جريمة الابتزاز الإلكتروني.

المبحث الأول- مفهوم جريمة الابتزاز الإلكتروني:

تمهيد وتقسيم:

أصبحت جريمة الابتزاز الإلكتروني ظاهرة تخترق المجتمع وتهدد دعائمه، وتضرب في مقتل أهم أهداف أي مجتمع متحضر في تحقيق الأمن لأفراده، وشعورهم بالأمان في حياتهم، ولعل جوهر وسبب تجريم جريمة الابتزاز الإلكتروني هو التهديد والابتزاز، فجريمة الابتزاز الإلكتروني يمكن تعريفها على إنها تهديد شخص بهدف ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً بواسطة شبكة معلوماتية أو وسيلة تقنية معلومات.

وبناء على ما سبق سيتم تقسيم هذا المبحث إلى ثلاثة مطالب وفق الآتي:

المطلب الأول- تعريف الابتزاز الإلكتروني.

المطلب الثاني- أنواع وأساليب الابتزاز الإلكتروني.

المطلب الثالث- آثار الابتزاز الإلكتروني.

المطلب الأول- تعريف الابتزاز الإلكتروني:

يقتضي الوقوف على مفهوم الابتزاز الالكتروني؛ بيان تعريفه، والخصائص التي يتميز بها من غيره. فالابتزاز في اللغة هو الحصول على المال أو المنافع من شخص تحت التهديد بفضح بعض أسراره، أو غير ذلك، وابتز المال من الناس: سلبهم إياه، نزعه منهم بجفاء وقهر، وابتز قرينه: سلبه، تكسب منه بطرق غير مشروعه، والبز السلب ومنه قولهم في المثل: من عز بز معناه من غلب سلب، وابتززت الشيء استلبته، وبزه يبزه بزا غلبه وغصبه، وبز الشيء بزاً انتزعه، وبزه ثيابه بزا وبزه حبسه، مني أي قسرا، وابتزه ثيابه سلبه إياها[7]. وفيما يأتي بيان تعريف الابتزاز الإلكتروني:

الفرع الأول- التعريف الضيق للابتزاز الإلكتروني:

الابتزاز يعني الحصول على الأموال بالتهديد، أو هو: الإكراه من خلال التهديد الذي لا مبرر له للكشف لشخص آخر أو للجمهور عن معلومات حقيقية محرجة أو ضارة، أو غير حقيقية، وعلى الرغم من أن الكشف عن هذه المعلومات ليس في حد ذاته جريمة ، فإن الابتزاز الذي يأتي في شكل مطالبة بالمال مقابل حجب المعلومات يعد سلوكا إجراميا[8].

ويعرف البعض بأنه[9]: "الحصول على معلومات سرية أو صور شخصية أو مواد فيلمية تخص الضحية، واستغلالها لأغراض مالية أو القيام بأعمال غير مشروعة"، ويرى آخرون أنه[10]: "نوع من السلب يقضي بالحصول على تسليم أموال، أو قيم، أو سندات، أو تواقيع تحت تهديد إفشاء مشين

(7) – ابن منضور، لسان العرب، مادة بز، ج1، دار المعارف، ص 275.

(8)– تامر محمد صالح، الإبتزاز الإلكتروني" دراسة تحليلية مقارنة"، جامعة المنصورة، الطبعة الأولى، 2018، ص 16.

(9) – عبد العظيم مرسي، جرائم الاعتداء على الأموال، مرجع سابق، ص 129.

(10)– جيرار كورنو، ترجمة منصور القاضي، معجم المصطلحات القانونية، المؤسسة الجامعية للدراسات والنشر والتوزيع، 1998، ص22.

صحيح، أو كاذب ".

ويلاحظ على هذه التعريفات أن الابتزاز الإلكتروني يتخذ مضـــمون التهديد فيه شـــكلا مختلفا وأغراض شتى، ذلك المضمون وهذه الغاية قد تكون محددة، فنكون أمام تعريف ضيق له.

الفرع الثاني– التعريف الواسع للابتزاز الإلكتروني:

يرى جانب من الفقه أن الابتزاز الإلكتروني هو[11]: "محاولة الحصـــول على مكاســـب مادية أو معنوية من خلال التهديد بإيقاع أذى سواء بكشف أسرار، أو معلومات خاصـه، أو إلحاق أذى بنفس الضـحية أو ماله، أو شـخص عزيز لديه، معتمدا في ذلك على قوته ونفوذه لاسـتخراج ما يرغب من ضحيته.

ويرى جانب آخر أن الابتزاز الإلكتروني هو[12]: "محاوله الحصـول على شـيء من شـخص ما عن طريق التهديد– بالكلمات أو الإيماءات، أو الاتهام بشيء ما، أو عن طريق العنف أو التخويف، مثل: طرد الشـخص، والصـراخ عليه، ورمي أو كسر الأشياء... للحصـول على أي شـيء ذي قيمه، ومفهوم "شـــيء ذي قيمه". كما يرى البعض أن الابتزاز الإلكتروني لا يشـمل المال والممتلكات فقط، بل يشمل أيضا الأمور المعنوية[13].

وذهب المشـــرع الإماراتي الى الاتجاه ذاته في المادة 16 من القانون رقم 2 لســـنه 2018 م المتعلق بمكـافحـة جرائم تقنيـة المعلومـات، حيث تنص على أن: "يعـاقب بـالحبس مـدة لا تزيـد عن سـنتين والغرامة التي لا تقل عن مئتين وخمسـين ألف درهم ولا تجاوز خمسـمائة ألف درهم أو بأحدى

(11)– رمسيس بهنام، قانون العقوبات جرائم القسم الخاص، الطبعة الأولى، منشأة المعارف، 1999، ص 1204.

(12)– تامر محمد صالح، الابتزاز الإلكتروني – دراسة تحليلية مقارنة، جامعة المنصورة، 2018، ص27.

(13) – المرجع السابق، ص 28.

هاتين العقوبتين كل من ابتز أو هدد شـــخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار". وعرفت المادة الأولى من القانون الإماراتي رقم 2 لسـنة 2018 م بشـأن مكافحة جرائم تقنية المعلومات الشـبكة المعلوماتية بأنها: "ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسـائل تقنية المعلومات التي تتيح للمسـتخدمين الدخول وتبادل المعلومات، كما يقصـد بوسـيلة تقنية المعلومات: أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين.

وقد يبدو للبعض أن ذلك التعريف يتعارض مع مبدأ شـــرعية الجرائم والعقوبات الذي يفرض على السلطة التشريعية أن تصدر تشريعاتها بصورة واضحة ومحددة بعيدة عن الغموض والإبهام بقصد تحقيق الجودة التشريعية [14].

وقد أكدت المحكمة الدستورية العليا المصرية ذلك المبدأ بقولها أن: "الأصل في النصوص العقابية أن تصاغ في حدود ضيقة تعريفاً بالأفعال التي جرمها المشرع، وتحديدا لمضمونها، فلا يكون التجهيل بها من خلال انفلات عباراتها، وإرهاقها بتعدد تأويلاتها موطنًا للإخلال بحقوق كفلها الدستور للمواطنين، كما يجب ألا تكون النصوص العقابية شباكاً أو شركاً يلقيها المشرع متصيداً

(14)- محمد محمد عبد اللطيف، مبدأ الأمن القانوني، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد السادس والثلاثون، أكتوبر 2004م، ص 104م.

باتساعها أو بخفائها من يقعون تحتها أو يخطؤون مواقعها"[15].

بناء عليه قد يبدو للبعض أن التعريف الواسع للابتزاز يصطدم بمبدأ الشرعية الجنائية؛ لأنه غير محدد من حيث مضمون الوعيد الذي يؤثر على إرادة الشخص، كما أنه لم يحدد أيضًا الغرض من الفعل سواء أكان أداء عمل أم الامتناع عنه. بينما لا يصطدم التعريف الواسع للابتزاز مع مبدأ شرعية الجرائم والعقوبات، لأن المشرع حدد السلوك والنتيجة في جريمة الابتزاز الإلكتروني، لكنه لم يبين الوسيلة أو مضمون الفعل الذي تقع به الجريمة؛ حيث لا عبرة بالوسيلة، وأكدت ذلك محكمه النقض المصرية بقولها "يجب لكي يحقق النص التشريعي العله من وضعه أن يكون كاملا مبينا الفعل الإجرامي والعقوبة واجبة التطبيق، غير أنه لا حرج أن ينص القانون على الفعل بصوره مجمله، ثم يحدد العقوبة"، والاتجاه الموسع هو الأولى بالاعتبار؛ حيث يبدو متفقا مع العله من تجريمه[16].

بناء على ذلك فالابتزاز الإلكتروني هو: كل تهديد يقوم به الجاني، أو وسيط عنه يتم عبر وسيلة إلكترونية، ويؤثر في نفسية المجني عليه، أو شخص عزيز لديه، ويدفعه إلى القيام بما طلبه منه الجاني أو كلفه به، سواء أكان مشروعا أم غير مشروع. وتحديد من هو الشخص العزيز لديه قد يكون مصدره القانون أو الواقع، فمجرد إحساس الشخص بالمسؤولية ناحية الغيركاف لتوافر الابتزاز[17]، فالولد عزيز على والده، وكذلك الخادم عزيز على سيده من الناحية الواقعية وليس

(15)- دستورية عليا، قضية رقم 28 لسنه 17 قضائية دستورية، جلسة 2 ديسمبر 1995م، الجريدة الرسمية، العدد 51 الصادر ي 21 ديسمبر 1995م، ص 2914.- مشار إليه في تامر محمد صالح، الابتزاز الإلكتروني، ص30.

(16)- تامر محمد صالح، الابتزاز الإلكتروني، ص32.

(17)- أشرف توفيق شمس الدين، الجنائية للحرية الشخصية من الوجهة الموضوعية، دراسة مقارنة، دار النهضة العربية، 2007م، ص 263.

القانونية كما في الابن.

المطلب الثاني– أنواع وأساليب الابتزاز الإلكتروني:

تختلف عادة صور أي جريمة تبعا لتقرير النص القانوني السلوكيات التي تقوم بها الجريمة، أو ما يمكن اعتباره ركنها المادي، وتتعدد صور الجريمة أيضا تبعا لنتائجها، وأحيانا تبعا للأغراض التي يستهدف الجاني تحقيقها، وهو ما سيتناوله الباحث في الفرع الأول. فيما سيتناول في الفرع الثاني الأساليب الأكثر شيوعا في ارتكاب جريمة الابتزاز الإلكتروني مع الإشارة إلى أن هذه الأساليب تتعدد أيضا تبعا للصور، وترتكب الصورة الواحدة بها جميعا أو ببعضها. أما الفرع الثالث فسوف يتناول فيه أطراف جريمة الابتزاز الإلكتروني وفقا للآتي:

الفرع الأول– صور الابتزاز الإلكتروني:

إن تقرير الصور التي تنطوي عليها جريمة الابتزاز الإلكتروني، يشوبه قدر من الصعوبة، مرجعه وجود نصوص حديثه عددت الصور التي تقع من خلالها جريمة الابتزاز الإلكتروني، فضلا عن النص التقليدي الذي يحدد بشكل عام مفهوم وصور الابتزاز الإلكتروني. أما السبب الثاني لهذه الصعوبة فيتمثل في قلة الدراسات الفقهية التي تناولت صور هذه الجريمة وقواعدها الموضوعية والإجرائية نظرا لحداثتها نسبيا. والابتزاز بالمعني التقليدي، له صورتان[18]:

الصورة الأولى– تهديد الشخص بفضح أمر أو إفشاءه أو الإخبار عنه بقصد النيل من شرفه أو اعتباره أو شرف أو اعتبار أحد أقاربه: تمثل هذه الصورة المعني الاصطلاحي للابتزاز، فهو كما تقدم تهديد بفضح أمر ينال من شرف أو اعتبار الشخص، هذا (الأمر) أشارت اليه مختلف

(18)– مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 9.

التشـريعات بأنه الشـيء الذي يحرص الشـخص على إخفائه، فإذا ما فضـح يؤدي إلى عدم قبول المجني عليه في الوسـط الاجتماعي، أو أنه أمر غير أخلاقي لا تتقبله الفطرة أو ترتضـيه العادات الشائعة[19].

الصورة الثانية– ابتزاز الشخص (من خلال تهديده) لحمله على جلب منفعة غير مشروعة لمرتكب الابتزاز أو لغيره: تثير هذه الصورة التساؤل عن وجه الاختلاف بينها وبين الصورة الأولى، خاصة أن النص الأصلي قبل التعديل كان في الصورة الأولى يضيف عبارة **(لكي يحمله على جلب منفعة غير مشروعة له أو لغيره)**، ومن ثمّ فإن تهديد الشخص في الصورة الأولى بفضح أمر يراد منه دفع من يجري تهديده لجلب منفعة لمرتكب فعل التهديد[20].

فالفارق بين الصورتين، أن الصورة الأولى تتضمن مجرد إفشاء لأمر غير مشروع، كالقول مثلا أن فلان يمارس أفعال الجنس مع فلانه، ونشـر حوارات بينهما مثلا أو صـورة لهما، فهذا فعل إفشاء وإخبار وفضح ينال من اعتبار وشرف المعنيين فيه. لكن في الصورة الثانية إذا قام الشخص بالتهديد بنشـر هذه المواد فهو لا يمتنع عن نشـرها إلا بحصـوله على مال أو مقابل من المعنيين بالواقعة، فهذه جلب منفعة، وقد تكون المنفعة طلبه من السيدة مثلا أن يمارس هو معها الأفعال الجنسية مقابل أن يمتنع عن نشر صورها. أي أن الفيصل في التمييز بين الصورتين هو السعي إلى جلب المنفعة[21].

إن ما أتاحه قانون الجرائم الإلكترونية بتطبيق النص التقليدي حين يرتكب الفعل بوسيلة

---

(19)– المرجع السابق، ص 10.

(20)– خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، 2020، ص 220.

(21)– مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 11.

الكترونية يجعلنا أمام الصور المقررة في النص التقليدي فقط ، سندا لقاعدة **(لا جريمة ولا عقوبة الا بنص)**. وإذا كان ما تقدم هو صور الابتزاز.

كما يجد الباحث أن المشرع الاتحادي في القانون الاتحادي رقم 2 لسنة 2018م في شأن مكافحة جرائم تقنية المعلومات نص في المادة 16 منه على أن: (يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شـــخص أخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار.

ويثار التســاؤل وفقا للنص المتقدم، فيما إذا كانت الغاية من الابتزاز الإلكتروني هي تحقيق منفعة مشروعة، هل تقع الجريمة بموجب القانون الاتحادي أم لا؟

قد يقول قائل إن القياس متاح في مثل هذه الحالة لنجيبه بأن القياس محظور في النصوص الجزائية الموضوعية (نصوص العقوبات)، إذ لا وجه للقياس مطلقا لغايات التجريم.[22]

الفرع الثاني– أساليب الابتزاز الإلكتروني:

يساعد بيان أساليب ارتكاب جريمة الابتزاز الإلكتروني على معرفة وتحديد عدة أمور؛ منها على سبيل المثال:

1. المعرفة أو الإحاطة بالأساليب التي قد يكون ضحيتها مستخدم التكنولوجيا.

(22)– مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، مرجع سابق، ص 12، وأيضا: أحمد فؤاد عبد المجيد، الحجية القانونية لوسائل التقدم العلمي، الدار العلمية الدولية للنشر والتوزيع، عمان، الطبعة الثانية، 2012، ص45.

2. الوقاية أو الحماية اللازمة التي يجب على مستخدم التكنولوجيا اتباعها لتجنب الوقوع فيها.

3. مساعدة مستخدم التكنولوجيا تحديد فيما إذا كان المرسل:

أ. صاحب صفحة وهمية. أو

ب. مخترق حسابات الكترونية. أو

ت. إذا كان من يتم التعامل معه لغرض ما هو محل ثقة لتسليمة أشياء مادية معينة أم لا؟

(كالصور أو المستندات أو المعلومات ...الخ)

وتتنوع أساليب ارتكاب جريمة الابتزاز الإلكتروني تبعا لتنوع التقنيات والتطبيقات التي تكون محلا أو وسيلة ليرتكب فيها أو بواسطتها الشخص فعل الابتزاز، على أن يكون مدركا أن تنوع الأساليب لا يخرجنا من دائرة السلوك والغرض اللذان سيمثلان الركنين المادي والمعنوي للجريمة بغض النظر عن اختلاف الأسلوب، وفي سياق ما عرضته مرجعيات الدراسة، تتمثل أبرز أساليب ارتكاب هذه الجريمة بما يلي:

أولا- الدخول غير المصرح به إلى النظام للاستيلاء على المادة محل الابتزاز:

الدخول غير المصرح به إلى نظام المعلومات هو الأسلوب الأساسي والأول لارتكاب جميع صور الجرائم الإلكترونية دون استثناء، إذ بدونه لا يوجد السلوك الجرمي لأية جريمة. ويتم ذلك عن طريق تجاوز كلمات السر أو وسائل حماية الدخول المختلفة بحيث يصبح مرتكب الفعل داخل النظام المستهدف، ويتاح له كل أمر يرغب القيام به، كأنه مستخدم مشروع للنظام. وقد حرص المشرع الإماراتي كما في نص الفقرة الأولى من نص المادة (2) من قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة " المرسوم بالقانون الاتحادي رقم 5 لسنه 2012، على تجريم الدخول

غير المصـــرح به إلى الشـــبكة المعلوماتية أو نظام المعلومات، وظهر ذلك من خلال اعتبار مجرد الدخول إلى النظام دون إذن أو تصـــريح جريمة بذاته، ومن خلال تجريم كل فعل متوقع كأثر لهذا الدخول[23].

ويقصد مرتكب الفعل عبر أسلوب الدخول غير المصرح به في جريمة الابتزاز الإلكتروني، الاطلاع على مادة محفوظة في النظام يحرص صاحبها على عدم إفشائها، وقد يتجاوز مرتكب الفعل غرض الاطلاع إلى الحصول على المادة تمهيداً لإفشائها أو فضح مشتملاتها.

ثانياً- التقاط المواد المرســـلة عبر البريد الإلكتروني أو التطبيقات الإلكترونية الأخرى المتضـــمنة مادة الابتزاز.

تضـــمنت المادة 21 من القانون اتحادي رقم 2 لسـنة 2018 في شـأن مكافحة جرائم تقنية المعلومات عقوبة الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا باستخدامه شبكة معلوماتية أو نظام معلومات الكتروني أو احدى وسائل تقنية المعلومات؛ حيث جاء نصها كما يلي: (يعاقب بالحبس مدة لا تقل عن ستة أشـهر والغرامة التي لا تقل عن مائة وخمسـين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا بإحدى الطرق التالية:

---

(23)- نص الفقرة الأولى من المادة(2) من قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة " المرســـوم بالقانون الاتحادي رقم 5 لسنه 2012، بأنه" يعاقب بالحبس والغرامة التي لا تقل عن مائه ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونيا أو شـــبكة معلومات، أو وســـيلة تقنية معلومات، بدون تصـــريح....."، عبد الرازق الموافي عبد اللطيف، شـــرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة " المرسـوم بالقانون الاتحادي رقم 5 لسـنه 2012، الكتاب الأول، إصـدار معهد دبي القضـائي، 20114، ص 42.

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

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

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

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

يستفاد من النص اعلاه أن هناك صورتين للالتقاط هما:

أ. الالتقاط المرئي أو السمعي للمادة محل جريمة الابتزاز الإلكتروني.

ب. الالتقاط الإلكتروني للمادة محل جريمة الابتزاز الإلكتروني.

استنادا إلى ذلك قد يكون الحصول على مادة الابتزاز بإحدى هاتين الصورتين، ففي الصورة الأولى يأخذ الالتقاط أحد شكلين الأول مرئي والثاني سمعي، الالتقاط المرئي كأن يشاهد رب عمل إحدى الموظفات وهي تستخدم هاتفها الشخصي ويلاحظ أنها تنظر إلى ملفات تنطوي على صور إباحية محفوظة في هاتفها، فهو بذلك التقط ذهنيا مادة تنطوي على أمر تحرص صاحبة الهاتف على إخفائه، فيستغل ذلك بتهديدها بفضح أمرها بين زميلاتها بقصد جلب منفعة غير مشروعة لنفسه جنسية أو غير ذلك[24].

(24)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 15.

فالالتقاط السمعي هو ما يصل للأذن من أصوات صادرة عن أحد الأجهزة لشخص ما، ثم يقوم هذا الملتقط بابتزاز الضحية، كأن يسمع شخص أخته تتحدث عبر الهاتف مع أخرى يعرفها من أحد الجيران المجاورين تقول لها أنا حامل من فلان، ثم يقوم بالتواصل مع هذه الفتاة عبر أحد مواقع التواصل الاجتماعي ويطلب منها المال مقابل سكوته عما سمعه[25].

أما الالتقاط الإلكتروني للمادة محل جريمة الابتزاز، فيتم بكافة الوسائل الإلكترونية التي تتيح اعتراض البيانات خلال إرسالها والاستيلاء عليها أو إعادة توجيهها أو مجرد الاطلاع عليها، ويتم ذلك بالوسائل اللاسلكية كالتقاط البث والترددات المرسلة من أحد الأنظمة إلى نظام آخر عبر الشبكة، كما قد تتم سلكيا بإجراء اتصال سلكي بالجهاز والتقاط ما يرسل إليه ونسخه وإتلافه بعد الاطلاع عليه، أو إعادة توجيهه ثم تهديد الضحية بما تم التقاطه، من أجل جلب منفعة مشروعة أو غير مشروعة للجاني[26]. والجاني فى جريمة الابتزاز الإلكتروني قد يحصل عبر التقاط الحصول على مادة تمثل أمر يحرص صاحب المادة على إخفائه، كأن يلتقط صور لعلاقة جنسية بين فتاة وعشيقها، فيهدد هذه الفتاه بإفشاء هذه المادة مقابل تحقيق منفعة – مادية أو غير مادية– له أو لغيره، ويكون الالتقاط هنا وسيلة الجاني لارتكاب الفعل وتحقيق غرضه[27].

ثالثا– تخفية وانتحال الشخصية أو التغرير لدفع الضحية إلى فعل أو تصريح يمثل مادة الابتزاز:

يتواصل الجاني في هذا الأسلوب، مع شخص عبر أحد التطبيقات الإلكترونية كالواتس أب أو تيليجرام أو فيسبوك أو غيره ويظهر له عبر الكاميرات بغير الحقيقة؛ كأن يكون ذكر ويظهر

---

(25)– المرجع السابق، ص 15.

(26)– عمر سالم، المراقبة الإلكترونية، دار النهضة العربية، القاهرة، 2000، ص43 وما بعدها، وكذلك، محمد تيمور عبد الحسيب، ط2، الحاسبات الإلكترونية وتكنولوجيا الاتصال، دار الشروق، القاهرة، 2014، ص79 وما بعدها.

(27)– مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 15.

للمتواصـــل معه على أنه فتاه تدعوه لفعل غير أخلاقي، ثم يقوم بتصـــويره وهو مثلا يمارس العادة السرية أو يقوم بسلوك أو يطلق عبارات غير أخلاقية، ويخزن لديه هذه المادة ويبدأ بتهديد صاحبها بإفشائها. ومن الأمثلة الواقعية لهذا الأسلوب قيام شاب بالتواصل عبر كاميرة السكاي بي مع شاب آخر، ووضع صورة فتاه على أنها هي التي تتواصل مع هذا الشاب، هذه الفتاة تبدأ بالتعري وتطلب من المجني عليه المستهدف أن يمارس العادة السرية وفعلا يقوم بتصويره ويتصل به بعد ثلاثة أيام ليبلغه أن لديه فيديو يتضمن ما قام به المجني عليه، ويطلب منه تحويل مبلغ خمسة آلاف دولار إلى حسابه وإلا سيقوم بنشر الفيديو.

قام المجني عليه بإبلاغ وحدة الجرائم الإلكترونية عبر شـــكوى تقدم بها للمدعي العام بما حصـل معه، وقد تمكنت الوحدة المذكورة من معرفة الجاني ومنعه من اسـتغلال المجني عليه وإنفاذ غرضه من فعل الابتزاز[28].

وهذا الأسلوب هو الأسهل والمفضّل لدى مرتكبي جرائم الابتزاز الإلكتروني لأنه لا يحتاج إلى جهد أو خبرة تكنولوجية عالية للقيام بجريمة الكترونية معينة أو على مســـتوى معين، فوفق إحصائية أعدها أحد المراكز المتخصصة بالدراسات القانونية؛ يعد الأردن في المرتبة الثانية من بين الدول العربية كأكثر تواجدا لمرتكبي جريمة الابتزاز الإلكتروني تحت هذا الأسلوب بعد المغرب"[29].

ومواجهة هذا الأسـلوب يحتاج إلى أنشـطة توعية واسـعة لمسـتخدمي التكنولوجيا – مواقع التواصـل الاجتماعي– خاصـة الشـباب كونهم الفئة الأكثر وقوعا تحت هذا الأسـلوب الجرمي، لذلك

(28)– مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 16.

(29)– تقرير صادر عن مركز الشرق الأوسط للدراسات، الحملة الوطنية لمكافحة الابتزاز الإلكتروني (2017 /2/21)، سلطنة عمان.

يتطلب الأمر التنبيه والتوعية من قبل أرباب الأســر والجهات المختصـــة كوحدة الجرائم الإلكترونية حول تجنب الدخول بعلاقات كهذه، أو التعامل مع أسـماء غير معروفة أو مشـكوك بها على مواقع التواصل الاجتماعي[30].

رابعا- استغلال المواد المستلمة أو المرسلة طوعا كمادة للابتزاز:

تتمثل هذه الصـورة بأن يقوم أحد ما باسـتغلال بيانات أو معلومات سـلمت له أو أرسـلت له طوعا بحكم علاقته بالضـحية أو لأي سبب آخر، دفع الضـحية طوعا إلى تسليم الجاني المادة التي سـتصـبح محل للابتزاز فيما بعد. ومن الأمثلة على قيام المجني علية بتسـليم مادة طوعية يسـتغلها الفاعل لابتزازه، قيام فتاة بإرسال صـورها إلى خطيبها الذي يهددها بنشر هذه الصـور جراء ما حدث بينهما من خلاف لقاء تنازلها عن حقوق عقد الزواج[31].

وغالبا ما يرتبط هذا الأسلوب بوجود علاقات اجتماعية أو عاطفية بين الجاني والمجني عليه، لكن قد تكون العلاقة بين الجاني والمجني عليه عابرة أو ناتجة عن تعامل لحظي، كما يحدث في التعارف بين الشـباب والفتيات على صـفحات ووسـائل وتطبيقات التواصـل الاجتماعي. وأهم ما يتصـل بهذا الأسـلوب وجوب الوعي لعدم إرسـال أية مواد قد تسـتغل لاحقا كمادة للابتزاز، مالم يكن ثمة ثقة عالية بين طرفي التعامل أو معرفة مسبقة وطويلة[32].

خامسا- استغلال المواد التي يحصل عليها الشخص بحكم مهنته أو وظيفته المحاطة أساسًا بالسرية:

---

(30)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 16وأيضا: محمد تيمور عبد الحسيب، ط2، الحاسبات الإلكترونية وتكنولوجيا الاتصال، مرجع سابق، ص 91.

(31)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 17.

(32)- تامر محمد صالح، الابتزاز الإلكتروني، مرجع سابق، ص 33.

يتلخص هذا الأسلوب بحصول أشخاص بحكم مهنتهم أو وظيفتهم على أسرار أو معلومات أو بيانات أو غيرها تتعلق بالآخرين، ومن شأن الإفشاء بأي من هذه الأسرار أو المعلومات الخاصة بصاحبها الإضرار به بشكل ما، ومثال ذلك الصور أو الفيديوهات التي يقدمها موكل لمحاميه من أجل الاستناد إليها في إثبات واقعة ما، ثم يقوم المحامي بتهديد هذا الموكل أو حتى الطرف الآخر بنشر هذه الصور أو الفيديوهات إذا لم يقدم له مبلغ مالي معين(33).

أو قيام موظف حصل على معلومات عن طريق وظيفته بتهديد الضحية بأنه إذا لم يقم بعمل ما أو بدفع مبلغ معين فإنه سيقوم بالإفصاح عن هذه المعلومات، ومثال ذلك: تهديد الكاتب لدى المدعي العام لفتاة بأنه سيخبر أهلها بأنها حضرت لديهم في واقعة فعل فاضح في الطريق العام مع شخص ما، إذا لم تقم بالخروج معه من أجل القيام بعلاقة(34).

يرى **الباحث** أن هذا الأسلوب يعد أخطر الأساليب وأشدها تأثيرا على نفس المجني عليه، لأن فيه استغلال الجاني لصفته بحكم مهنته أو وظيفته، ولأن ضحايا هذا الأسلوب يهتمون جدا في مادة الابتزاز نظرا لخصوصيتها أو خطورتها في بعض الأحيان.

سادسا- الحصول على مادة الابتزاز الإلكتروني عبر الجريمة التقليدية:

كأن يرتكب الجاني سلوكا ماديا مجرما للوصول إلى المادة التي يستخدمها للابتزاز، فقد يكسر أحدهم باب غرفة مقفلة ليصل إلى الصور الموجودة داخل الغرفة التي تخص شخصا آخر يحرص على إخفائها وعدم فضح أمره بشأنها، فيرتكب الجاني بهذا جرما تقليديا منصوصا عليه

(33)- محمد تيمور عبد الحسيب، ط2، الحاسبات الإلكترونية وتكنولوجيا الاتصال، مرجع سابق، ص 82.

(34)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 17.

ليحصل على مادة قد تتخذ شكلا ملموسا أو إلكترونيا، ثم يستخدمها لابتزاز الضحية أو المجني عليه مستخدما الطرق أوالوسائل الإلكترونية لتنفيذ هذا الابتزاز. ففي هذا الأسلوب نواجه ابتداء جريمة عادية كالسرقة أو انتهاك حرمة المنازل أو غير ذلك، وبنفس الوقت مادة الابتزاز تستخدم لتهديد شخص بفضح أمره أو إفشائه مقابل منفعة، فنكون بصدد أمام عدة جرائم وليس جريمة واحدة، لأن الجاني سيسأل عن السرقة والابتزاز، فيدان الجاني عندها بالجريمتين وتطبق عليه العقوبة الأشد وفقا للقواعد العامة[35].

الفرع الثالث- أطراف جريمة الابتزاز الإلكتروني:

يتضح من التعريف السابق أن للابتزاز طرفان هما الجاني، والمجني عليه، وهذا الأخير قد يكون الضحية أو لا، كما أنه قد يكون من الحكومات والشركات، أو الأفراد العاديين رجالاً ونساءً، أحداثا وبالغين، فالأشخاص المعنوية عرضة للابتزاز الإلكتروني مثل الأفراد، ويتم العدوان عليها وتهديدها[36].

ويرى البعض أن الابتزاز لا يقع على الشخص المعنوي؛ لأن هذه الجريمة عدوان على الحرية الشخصية، وهي من الحريات الفردية التي لا تثبت إلا للأفراد، وإذا وجه التهديد الى ممثل الشخص المعنوي فإن المجني عليه في هذه الحالة ليس الشخص المعنوي، وإنما من وجه إليه التهديد[37].

وقد يتعدد المجني عليهم في جريمة الابتزاز الإلكتروني كما في حصول الجاني على مقطع فيديو لشاب، فيقوم بتهديده، وتهديد والده بأنه سينشره إن لم يدفعا له مبلغاً من المال، وضحايا

---

(35)- أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، ص 33

(36)- المجني عليه في جريمة التهديد قد يكون شخصاً معنوياً أو طبيعياً؛ تامر محمد صالح، الابتزاز الإلكتروني ، ص 34.

(37)- أشرف توفيق شمس الدين، الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية، دراسة مقارنة، مرجع سابق، ص 292.

الابتزاز بصفة عامة لا يشترط أن يكونوا مشهورين، بل يكفى فقط أن يكون لديهم شيء يريده شخص آخر، فيمارس الضغوط عليهم للحصول عليه[38].

وتتعدد صور الابتزاز الإلكتروني حسب المحل الذي يرد عليه؛ فقد يكون جنسيًا عندما يتعلق بعرض المجني عليه، وقد يكون اجتماعياً عندما يتعلق بالكيان الأدبي للفرد في المجتمع الذي ينتمى إليه، وقد يكون مهنياً عندما يتصل بحياة الإنسان المهنية، وقد يكون سياسيًا عندما يتعلق بالوضع السياسي للفرد. وبناء عليه يتضح أن الابتزاز الإلكتروني يتسم بعدد من الخصائص؛ أهمها:

1. تعدد المصلحة محل الحماية الجنائية؛ فالابتزاز الإلكتروني عدوان على الحرية الشخصية على أساس أن الحق في الأمن هو أحد عناصر الحرية الشخصية، فالتهديد في ذاته مجرم سواء اقترن بطلب أو تكليف بأمر أو لا؛ لأنه إكراه لإرادة المجني عليه لتنفيذ ما طُلب منه، مما يدفع الفرد إلى العزلة وعدم الاختلاط بالغير، والخوف من إقامه روابط اجتماعية ربما تعود عليهم بالضرر، مما يترتب على ذلك من انهيار الصلات الاجتماعية وتفككها بين الأفراد، كما أنه اعتداء على الملكية، والشرف والسمعة، والكرامة، والسلامة الشخصية[39].
2. الابتزاز الإلكتروني جريمة قد يكون السلوك الإجرامي فيها وقتيًا، مثل من يهدد إمرأة شفاهة بفضح سر لزوجها ما لم تسلم له مبلغاً مالياً، فتقوم بتسليمه في الحال، كما أنه قد يتخذ صورة الجريمة المتتابعة مثل من يقوم بتهديد فتاة كل يوم بإفشاء أسرارها ما لم تسلم له مبلغًا من المال، أو يتخذ صورة الجريمة المستمرة[40]. حيث جاء في قضاء المحكمة الإتحادية العليا " ... وحيث

---

(38)- تامر محمد صالح، الابتزاز الإلكتروني، ص35.

(39)- تامر محمد صالح، الابتزاز الإلكتروني، مرجع سابق، ص35.

(40)- عبد العظيم مرسي، جرائم الاعتداء على الأموال، مرجع سابق، ص 32.

إن وسائل التقنية الحديثة والمواقع الإلكترونية يستطيع الولوج إليها الملايين من الناس على الكرة الأرضـــية والاطلاع على محتوياتها من قراءة ونظر وســماع وبالتالي فإن ما ينشـــر على هذه الوســائل والمكون لجريمة تعتبر الجريمة فيه مســتمرة، ويعتبر مكاناً للجريمة كل محل يقوم فيه الاستمرار عملاً بنص المادة (143) سالفة البيان"[41].

3. جريمة الابتزاز الإلكتروني من جرائم الضـرر أي ذات النتيجة، وليسـت من جرائم الخطر؛ حيث أنها لا تقع كاملة وتامة إلا بقيام المجني عليه بتنفيذ المطلوب منه أو الامتناع عنه.
4. الجناة في جريمة الابتزاز الإلكتروني غالباً من الأصدقاء والأقارب لعلمهم بمواطن الضعف، كما أن الضـحية قد يكون سببا فيها، فالمرأة التي تمارس الرذيلة مع شـخص لا شك في أنها شـريكة معه، ومع ذلك تهدده بنشر مقاطع فيديو لهما إن لم يقم بتنفيذ المطلوب منه، وقد تقع في صورة أخرى تتمثل في قيام شخصين بالسرقة، فيهدد أحدهما الأخر بالذهاب والاعتراف بالجريمة ما لم يحقق له ما يريد؛ لأنه موظف عام ويخشى على مركزه الوظيفي.
5. قد يكون المقابل المطلوب القيام به من قبل المجني عليه مشـــروعًا أو غير مشـــروع، وقد يكون عملاً أو امتناعًا عن عمل.
6. الابتزاز الإلكتروني جريمة تعبيرية، أي تتم من خلال التعبير بأي وسيلة من وسائل التعبير عن أمور معينة.
7. تعدد مراحل الابتزاز الإلكتروني؛ حيث يمر غالبا أياً كانت وسيلته بست مراحل هي: الطلب،

(41)– المحكمة الاتحادية العليا، الطعن رقم 263لسنه 2013 جزائي– تقنية معلومات، جلسة الاثنين الموافق 22 سبتمبر سنه 2014م.

والمقاومة، والضغط، والتهديد، والإذعان، والتكرار[42].

المطلب الثالث– آثار الابتزاز الإلكتروني:

رغم الإيجابيات الجمة التي يوفرها استخدام تكنولوجيا المعلومات والاتصالات، إلا أن لها محاذير عديدة إذا ما استخدمت بصورة سلبية للإضرار بالآخرين، كما هو الحال في الجريمة محل الدراسة (الابتزاز الإلكتروني). ولم يعد غريبا سماع أو رؤية أن (س) من الناس قد أجبر على الخضوع إلى مطلب شخص أخر، والسر في ذلك أن الأخير تحصل على معلومات حساسة بوسيلة ما مشروعة أو غير مشروعة، قام بواسطتها بتهديد أو ابتزاز ذلك الشخص مقابل الحصول على منفعة. ولا يوجد أدنى ريب بأن هذا الفعل الجرمي له دوافع في نفس الجاني يريد تحقيقها من خلال ارتكابه، مما يترتب عليه آثار سلبية عديدة تؤدي إلى الإضرار في نفس المجني عليه أو في ماله أو إلى إحداث الإرباك بينه وبين أفراد عائلته وغيرها من الآثار التي قد تترتب على ارتكاب هذا الفعل الإجرامي[43].

وبناء على ما سبق سيتناول الباحث في هذا المطلب؛ دوافع ارتكاب جريمة الابتزاز الإلكتروني، وآثار الابتزاز الإلكتروني في الفرعيين التاليين:

الفرع الأول– دوافع ارتكاب جريمة الابتزاز الإلكتروني:

غالبا ما يكون مرتكب جريمة الابتزاز الإلكتروني شخصا يتمتع باحترافية لكونه يحتاج إلى المعرفة في التعامل مع تكنولوجيا المعلومات والاتصالات لتنفيذ الجريمة، وما من شك في أن مرتكب الجريمة لديه أهداف ودوافع شخصية يريد تحقيقها من خلال هذه الجريمة، فغايته ليست فقط

(42)– تامر محمد صالح، الابتزاز الإلكتروني، مرجع سابق، ص 37.

(43)– مصطفي خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 18.

الدخول للنظام وســـرقة معلوماته كهكر عابر على أي نظام، وإنما هدفه تحقيق الغاية التي أراد الوصـول إليها من خلال استخدامه لأحد أساليب ارتكاب جريمة الابتزاز الإلكتروني. ورغمًا عن أن هذه الدوافع تتأثر تبعا للتغيرات التي تشـــهدها التكنولوجيا يوما بعد يوم؛ إلا أنه يمكن حصـــر هذه الدوافع فيما يلي:

1- دوافع مادية (مالية):

ورد النص على جريمة الابتزاز في المادة (398) من قانون العقوبات الاتحادي في الباب الثامن المتعلق بالجرائم الواقعة على المال في الفصـــل الأول الخاص بجرائم الســـرقة، واعتبار الابتزاز من جرائم الأموال إنما اســـتند إلى أن الدافع الرئيســـي لدى الجناة على ارتكاب مثل هذه الجرائم هو الحصـــول على منافع مادية قد تكون أموالا وقد تكون غير ذلك. مع مراعاة أن جريمة الابتزاز الإلكتروني قد تستهدف النفس فتكون مصنفة عندها من الجرائم الواقعة على الأشخاص[44].

والشـائع في جرائم الابتزاز الإلكتروني، التي ترتكب بواسـطة الشـبكات والتطبيقات الإلكترونية، ســـعي الجاني إلى الحصـــول على منفعة مالية، لأنه في الغالب لا يعرف المجني عليه ولا تهمه أحواله، حيث توصـل عبر التطبيقات الإلكترونية إلى الحصـول على مادة يخشـى المجني عليه من فضح أمره بشأنها، فيقبل طلبات الجاني بدفع أموال أو تنفيذ ما يطلبه من منافع مادية، كالإبراء من دين مثلا ... مقابل عدم فضح أمره[45].

والدافع المادي المنسجم مع تصنيف الابتزاز ضمن جرائم الأموال يتسع ليشمل ارتكاب جريمة

(44)- عمر سالم، المراقبة الإلكترونية، مرجع سابق، ص52.

(45) - محمد تيمور عبد الحسيب، الحاسبات الإلكترونية وتكنولوجيا الاتصال، ص92.

الابتزاز من شـــخص طبيعي على شـــخص معنوي، أو ارتكابها من شـــخص معنوي عبر ممثليه لمصـلحة هذا الشـخص ضـد شـخص طبيعي أو معنوي أخر. وأوضـح الأمثلة على التهديد بفضـح أمرها من قبل أحد العاملين فيها مثلا، والمتعلق بتهربها من دفع الضرائب في مقابل سعي الفاعل إلى ترقية أو زيادة راتب أو الحصول على أموال[46].

وترتبط جرائم الابتزاز ضد الأشخاص المعنوية أو المرتكبة من قبلها بأنشطة التجسس الصناعي، وهي الأنشطة المتعلقة بأسرار الإنتاج والعمل والمعلومات التي قد تحرص الشركة على عدم إفشائها، ســـواء أكانت معلومات مشـــروعة متعلقة بالإنتاج أو معلومات تنطوي على أمور غير مشـــروعة، كالمعلومات الخاصـة بطرق تسريب المخلفات الضـارة بالبيئة[47]. والدوافع المادية تتعدد لكنها تشـمل بشـكل عام: الحصـول على مبالغ مالية، الإبراء من مبالغ مالية، الترقيات الوظيفية، الحصـول على زيادات أومكافآت أوعلاوات، التعيين في مناصب معينة وغيرها.

2- دوافع سياسية:

يعدُّ هذا الدافع الأكثر خطورة من بين دوافع الابتزاز الإلكتروني، لكونه يرتبط بالصـراع السـياسـي والأحداث الواقعة في الدولة، ومن أوضـــح الأمثله على الدوافع الســـياســـية اســـتغلال الأجهزة الأمنية لمعلومات عن الحياة الخاصة للوزراء والنواب بقصد دفعهم الى تنفيذ طلبات معينة أو الموافقة على مسائل تتعارض مع قناعاتهم ومواقفهم المعتادة[48].

(46)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 19.

(47)- أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2009، ص22.

(48)- ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، الجريمة عبر النت، مكتبة دار الحقوق، الشارقة، 2010، ص125.

وأطراف جريمة الابتزاز الإلكتروني ذات الدوافع السياسية، غالبا من أصحاب النفوذ السياسي بحكم ما تستلزمه الصراعات السياسية من منافسة وتحديات، لكن هذا لا يمنع من استغلال الدوافع السياسية ضد أشخاص عاديين، كما في استغلال الأجهزة الأمنية الأحوال الشخصية لممثلي العمال إبان الإضرابات العمالية في الدولة.

يرى **الباحث** أن العقوبة المقررة لجريمة الابتزاز في القانون الإماراتي لا تتناسب مع جسامة الجريمة في حالة ارتكابها لدوافع سياسية، لأن آثار ابتزاز السياسيين قد تنعكس على المجتمع أو على قطاعات واسعة منه، وهو ما يستلزم عقوبات رادعة لتضييق فرص الابتزاز السياسي.

3- دوافع جنسية:

إن تهديد المجني عليه بفضح أمره، كنشر أو إفشاء محادثة أو صورة أو تسجيل صوتي أو مرئي، لدفعه إلى ارتكاب فعل جنسي يمثل جريمة واقعة على الأشخاص، لأنها تستهدف جسد وشرف وإرادة المجني عليه. وتمثل الدوافع الجنسية لجريمة الابتزاز، الصورة الأكثر انتشارا مع تنامي وتزايد استخدام التكنولوجيا وتطور التطبيقات الإلكترونية، خاصة ظهور تطبيقات تتيح البث الإلكتروني المباشر وتشكيل المجموعات وخضوعها إلى وسائل تقنية يعتقد البعض أنها غير مخترقة في حين هي وسائل كبقية وسائل التكنولوجيا يمكن اختراقها واستغلال ما فيها من محتويات[49].

ومادة الابتزاز بقصد تحقيق منفعة جنسية قد يتوصل إليها الجاني بواحد من الأساليب السابق بيانها، بمعني أن المادة قد تكون سلمت إلى الجاني طوعا أو توصل إليها بحكم العلاقة أو الوظيفة أو المهنة، أو يكون قد توصل إليها بأساليب جرمية غير مشروعة لتحقيق ملذات جنسية تنطوي

(49)- محمد تيمور عبد الحسيب، الحاسبات الإلكترونية وتكنولوجيا الاتصال، ص95.

بذاتها على جرائم مقررة في التشريع، حيث يعد المساس بالجسد حيلة أو تهديدا إحدى الوسائل التي تقرر المسؤولية الجنائية عن جرائم هتك العرض والاغتصاب وغيرها[50].

أما بخصوص الابتزاز الإلكتروني لدوافع جنسية، فإن المادة محل الابتزاز غالبا ما تتخذ شكلا إلكترونيا أو يتم الحصول عليها بوسيلة إلكترونية، ويتخذ شكل الإفشاء شكلا إلكترونيا أو باستعمال تطبيق إلكتروني، ولا يوجد ما يمنع حصول الإفشاء بصورة غير الكترونية، كما يتخذ التهديد بفضح الأمر عادة استغلال كافة الوسائل الإلكترونية[51].

4- دوافع انتقامية:

قد يسعى البعض بحكم العلاقة الاجتماعية السابقة، أو بحكم المنافسة في مكان العمل أو الدراسة أو في أي قطاع أخر، إلى الاعتداء على شخص آخر للحط من مكانته واعتباره تنفيذا لرغبة انتقامية.

مثل تهديد موظف لزميله بفضح ملفه الوظيفي المتضمن ارتكاب هذا الشخص أفعال جرمية تمس شرفه كالسرقة مثلا، ويكون الدافع من وراء هذا التهديد؛ الانتقام من المجني عليه بقصد المساس بمكانته الوظيفية[52].

والابتزاز الذي قد يكون لغرض انتقامي غالبا ما يشكل جريمة اكتملت كل عناصرها، ونفذها الجاني دون إخبار أو حتى إعلام المجني عليه، حيث يقوم الجاني بإفشاء أو فضح الأمر دون تهديد

(50)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 21.

(51)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 17.

(52)- أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآليمرجع سابق، ص 25، وأيضا- مصطفي خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 17.

المجني عليه بذلك، وغالبا لا ينتظر مصلحة مالية أو منفعة أخرى وإنما يريد التشفي بالمجني عليه، وفي هذه الحالة لا نكون أمام جرم ابتزاز، بل قد نكون أمام إفشاء معلومات أو ذم أو قدح أو تحقير أو غيرها حسب العناصر التي يتكون منها الفعل، لأن جريمة الابتزاز تستلزم التهديد بفضح الأمر، أما فضحه فيخرجنا من الابتزاز إلى جرم آخر مكتمل الأركان[53].

الفرع الثاني – آثار الابتزاز الإلكتروني:

أصبحت المعلومات والبيانات الشخصية أو الخاصة التي تم التوصل إليها بطريق غير مشروع أو حتى مشروع، محل تأثير سلبي على أصحابها نتيجة الجرائم الإلكترونية، كما أصبحت هذه البيانات والمعلومات مصدر رزق أو فائدة غير مشروعة لمرتكبي هذه الجرائم. وبهذا تبدو صائبة مقولة الأديب آرثر ميلر:

"ان الحاسب بشراهته التي لا تشبع للمعلومات، والسمعة التي ذاعت حول عدم وقوعه في الخطأ وذاكرته التي لا يمكن لما يختزن فيها أن ينسي أو ينمحي، قد تصبح المركز العصبي لنظام رقابي يحول المجتمع إلى عالم شفاف ترقد فيه عارية بيوتنا ومعاملاتنا المالية واجتماعاتنا وحالتنا العقلية والجسمانية لأي مشاهد عابرة"[54].

فقد لحقت كثير من الأشخاص أضرار مادية ومعنوية نتيجة التعدي على خصوصياتهم ومحاولة استعمال ما تم الحصول عليه كمادة للابتزاز الإلكتروني، وكذلك الكثير من المؤسسات الكبرى والشركات الخاصة التي واجهت خسارات مادية كبيرة بسبب محاولات الابتزاز الإلكتروني من قبل المنافسين أو الطامعين أو حتى الموظفين الذي تحت يديهم بيانات أو معلومات هامة، قد يكون

(53)– عمر سالم، المراقبة الإلكترونية، مرجع سابق، ص55.

(54)– ميللر آثر، الحماية القانونية لبرامج الكمبيوتر والبيانات، منشورات سويت ماكسويل، لندن، ترجمة الدار العربية للعلوم، نقوسيا، 1985، ص112.

الإفشاء عنها من شأنه أن يلحق الضرر بهذه الشركة. ويمكن إجمال أبرز آثار الابتزاز الإلكتروني بما يلي[55]:

1- انتشار الجريمة في المجتمع:

الابتزاز بكافة أشكاله هو عبارة عن حبس الضحية، بحيث يصبح الضحية كعبد أسير خاضع لمطالب سيده، مما يؤدي إلى قيام حالة نفسية لدى الضحية بسبب الضغوطات تجعله يفكر بالتخلص من ظلم الجاني بأي طريقة كانت، خاصة إذا تمادى الجاني في إيقاع ظلمه على الضحية، فذلك قد يؤدي الى أن يفكر الضحية بإيذاء نفسه كالانتحار مثلا، أو أن يفكر بقتل الجاني أو قتل أحد أفراد عائلته انتقاما أو خطفه للتخلص من شعوره بأنه سجين الجاني. وقد يؤدي في المجتمعات المحافظة إذا كانت الضحية فتاة إلى سعي عائلتها أو زوجها إلى الانتقام لها من الجاني الذي حاول ابتزازها، أو إلى قتل الضحية نفسها إذا علموا بأن مادة الابتزاز التي تخص ابنتهم جنسية فاضحة أو غير مشروعة، كصور لها أو فيديوهات تمس سمعتها وعرضها، فجريمة الابتزاز الإلكتروني لها تأثير أكبر في انتشار أثر الجريمة في المجتمع مقارنة مع غيرها من الجرائم الإلكترونية كالسرقة والاحتيال الإلكتروني[56].

2- اضطراب الجانب الاجتماعي للمجتمع[57]:

أثرت مواقع التواصل الاجتماعي بشكل واضح على الأسرة والمجتمع، حيث فتحت بشكل واسع

---

(55)- نوال عبد العزيز العيد، آثار جريمة الابتزاز الإلكتروني الابتزاز المفهوم، والأسباب، والعلاج، بحث منشور على الشبكة العنكبوتية في موقع: نوال عبد العزيز العيد، تحت العنوان: http://nawalaleid.com/cnt/lib/768

(56)- نوال عبد العزيز العيد، آثار جريمة الابتزاز الإلكتروني الابتزاز المفهوم، والأسباب، والعلاج، مرجع سابق، ص4.

(57)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 22، وأيضا، أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 29.

أبواب التعارف والتواصل بكافة أشكاله صوتًا وصورة، مما أدى إلى سهولة تحقق جريمة الابتزاز الإلكتروني، ما يؤدي بالنتيجة إلى خلخلة الجانب الاجتماعي للأسرة والمجتمع[58]. وهذا النوع من الجرائم له تأثير أشد على الجانب الاجتماعي وخلخلته من بقية الجرائم الإلكترونية، خاصة لدى الفتيات كونهن الحلقة الأضعف والأكثر تأثراً وخوفاً على سمعتهن، التي قد تكون على المحك بسبب ما تعرضوا له، وكذلك بالنسبة للصغار بسبب خوفهم من إبلاغ أرباب أسرهم أو القائمين على أمرهم عما حصل معهم من تعدي أو استغلال جنسي، الأمر الذي يؤدي إلى هدم مستقبلهم.

3- إفساد حياة الأشخاص (الضحايا):

تؤثر جريمة الابتزاز الإلكتروني على المستوى الفردي للضحايا بشكل كبير مما يجعل الضحية تشعر بأنها ضعيفة مهزولة لا حول لها ولا قوة، فيولد لديها اضطرابات نفسية وعصبية كالاكتئاب والتوتر، أو قد تعاني الضحية من اضطرابات في التكيف الاجتماعي، تدفعها إلى العزلة عن المجتمع والناس خوفًا من مواجهتهم، لشعورها بأنها قد تصبح محل حديث يشمت بها ممن هم حولها، وقد تؤدي إلى إحداث اضطرابات (شخصية) بحيث تصبح الضحية عدوانية مضادة للمجتمع غير قادرة على تقبل من حولها أوالتجانس معهم[59]. حيث تصبح الضحية كعبد راضخ لمطالب سيده غير قادر على ممارسة حياته الطبيعية، بسبب الخوف والضغط والتوتر الذي تعيشه كل ليلة خشية إقدام الجاني على نشر أو الإبلاغ أو الإفصاح عن المادة التي تحت يده بقصد ابتزازها، مما يؤثر سلبًا على الجانب الاجتماعي بالنسبة لأشخاص الضحايا[60].

(58)- نوال عبد العزيز العيد، آثار جريمة الابتزاز الإلكتروني الابتزاز المفهوم، والأسباب، والعلاج، مرجع سابق، ص4.

(59)- المرجع السابق، ص5.

(60)- محمد تيمور عبد الحسيب، الحاسبات الإلكترونية وتكنولوجيا الاتصال، ص102.

4- شيوع الفحش والحض عليه[61].

إن من شـأن جرائم الابتزاز الإلكتروني، إشـاعة الفحش في المجتمع والحض عليه، لأن الجناة في هذه الحالة يسـعون إلى علاقات جنسـية غير مشـروعة عبر التهديد بفضـح الأمر أو ابتزاز الشـخص بما تحت أيديهم من مواد يحرص المجني عليه على عدم افتضـاحها. وإشـاعة الفحش أمر يتحقق في غالبية جرائم الابتزاز الإلكتروني، بل لعله الأثر الأكثر وضوحا في هذه الجريمة، نظرا لما يدور في عقل الجاني من ثقة بأن مطلبه غير المشـروع قد يتحقق أو سـيناله لحرص المجني عليه على سـمعته ومكانته، ومن شـأن الابتزاز الإلكتروني توفير سـبب إضـافي للحض على الفجور في المجتمع والعلاقات الجنسية غير المشروعة، بما يضعف خطط وسياسات مواجهة انتشار هذا الأمر أو منعه.

5- انتشار الفوضى وعدم الطمأنينة.

إن التمادي في الظلم والطغيان، يؤدي على عدم الاسـتقرار المجتمعي وعدم شـعور الأشـخاص بالأمان على بيوتهم وأعراضـهم وخصـوصـيتهم، مما يترتب على ذلك ضـعف الكفاءات الشـخصـية وكذلك الاقتصـادية والسياسية، وحتى الشركات يمكن أن تستبعد فكرة الاستثمار لهذه الأسباب التي تشعرها بأن بنيانها المادي أو المعلوماتي عرضة للابتزاز الإلكتروني بأساليبه المختلفة[62].

إن جانب الخطورة الذي ينطوي عليه الابتزاز الإلكتروني يظهر من الآثار العديدة التي تشيع عدم الطمأنينة في التعامل مع أنظمة المعلومات والأشخاص، مما يترتب عليه ضعف الشعور بالأمان

(61)- مصطفى خالد الرواشدة، جريمة الابتزاز الالكتروني في القانون الاردني، مرجع سابق، ص 24.

(62)- نوال عبد العزيز العيد، آثار جريمة الابتزاز الإلكتروني الابتزاز المفهوم، والأسباب، والعلاج، مرجع سابق، ص5.

وانتشـار الفوضـى وكذلك الجريمة. ويبرز هنا الدور الفعال للجهات المختصـة كوحدة مكافحة الجرائم الإلكترونية بضـــرورة الســـعي بجهد أكبر عبر أنشـــطة التوعية المجتمعية للحد من هذه الجريمة ومكافحتها، بغية المحافظة على الاستقرار المجتمعي والشعور بالطمأنينة لدى الأفراد.

فالابتزاز الإلكتروني عمومًا ذو أثر على الاعتبار الشـخصـي للإنسـان، يسـتهدف قهر إرادته وإرهاب المجني عليه، ووضـــعه تحت تأثير الخوف والفزع، ودفعه إلى أفعال لا يمكنه أن يقبلها في الأحوال الاعتيادية، كما أنه يهدد أمن المجتمع وسـلامة علاقات الأفراد في نطاقه، ناهيك عن الآثار الاقتصادية والمالية الناجمة عن هذه الجريمة(63).

(63)- محمد تيمور عبد الحسيب، الحاسبات الإلكترونية وتكنولوجيا الاتصال، ص109.

المبحث الثاني- أركان جريمة الابتزاز الإلكتروني:

تمهيد وتقسيم:

ســـــاهم التقدم الهائل في مجال التقنيات الحديثة وثورة التكنولوجيا، والزيادة الكبيرة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة من أشخاص طبيعية أو هيئات أو أشخاص معنوية، فضلا عن الاســتخدام المتزايد لوســائل التواصــل الاجتماعي؛ في ظهور طائفة جديدة من الإجرام مرتبطة بالتكنولوجيا منها جريمة الابتزاز الإلكتروني.

ونظرًا لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة، سيما وأن لهذه الجريمة خصوصية تختلف عن بقية الجرائم التقليدية، الأمر الذي أدى إلى انعكاس هذه الخصــوصــية على مضــمون القوانين حتى تتماشــى مع طبيعة الجريمة ومعطياتها وآثارها، فجريمة الابتزاز الإلكتروني هي إحدى صــور الجرائم الإلكترونية. ويســتخدم مصــطلح الإلكترونية لوصــف فكرة أن الجريمة تتم من خلال استعمال التقنيات الحديثة، وهي الجرائم التي ترتكب ضد الأفراد أو المجموعات بقصد إيذاء المجنى عليه ماديًا أو معنويًا باســتخدام شــبكات الاتصــال مثل البريد الإلكتروني، الهاتف النقال، الحاســب الآلي... وتعدّ جريمة الابتزاز الإلكتروني ثمرة للاستخدام السلبي لثورة التكنولوجيا التي لحقت بالعالم وأثرًا من الآثار غير المرغوب بها للتقدم العلمي، وتتم عن طريق قيام الجاني بالضــغط على المجنى عليه تارة وبالوعيد تارة أخرى من خلال التهديد بنشــر معلومات أو صــور أو تســجيلات لا يرغب المجنى عليه في إظهارها على الناس.

فالابتزاز الإلكتروني هو تهديد شخص بهدف ابتزازه لحمله على القيام بفعل أو الامتناع عنه و لو كان القيام بهذا الفعل أو الامتناع عنه مشروعا، وتأخذ جريمة الابتزاز الإلكتروني صورًا مختلفة

بالنسبة للمجنى عليه والهدف والدافع من الجريمة[64]؛ فقد تستهدف الأشخاص المعنوية كالشركات أو المؤسسات وقد تستهدف الأحداث من الأطفال عن طريق استغلالهم وتهديدهم بنشر صور أو تسجيل مرئي أو محادثات على مواقع الدردشة أو أي مادة أخرى، حيث يستغل الجاني صغر سن الأحداث وقلة خبرتهم، وقد يكون المستهدف من النساء، فأكثر أنواع الابتزاز الإلكتروني شهرة وانتشارا عن طريق الابتزاز بنشر صور فاضحة أو محادثات خادشه للحياء، كما قد يكون المستهدف من الرجال عن طريق استغلال وسائل الاتصال للحصول على صور أو مقاطع فيديو ومن ثم التهديد بنشرها مما يؤدي إلى تشويه سمعتهم أو المساس بشرفهم، حيث تكون دوافع الابتزاز إما ماديه أو أخلاقية أو عاطفية، وتعتبر جريمة الابتزاز الإلكتروني من الجرائم الخطيرة حيث تهدد أمن المجتمع إضافة إلى تأثيرها على الجوانب الاجتماعية كالتفكك الأسري والطلاق وفقدان الثقة، ناهيك عن الآثار النفسية (القلق، الخوف، الاكتئاب...)[65]، كما تتميز هذه الجريمة بصعوبة إثباتها لأنها من الجرائم الحديثة التي يستعين الجاني بالتكنولوجيا الحديثة في ارتكابها.

وبناء على ما سبق ستتم دراسة هذا المبحث من خلال ثلاثة مطالب وفق الآتي:

المطلب الأول– الركن الشرعي لجريمة الابتزاز الإلكتروني.

المطلب الثاني– الركن المادي لجريمة الابتزاز الإلكتروني.

المطلب الثالث– الركن المعنوي الابتزاز الإلكتروني.

---

(64)– محمد تيمور عبد الحسيب، الحاسبات الإلكترونية وتكنولوجيا الاتصال، ص10

()65– عمر سالم، المراقبة الإلكترونية، مرجع سابق، ص55.

المطلب الأول- الركن الشرعي لجريمة الابتزاز الإلكتروني:

تناول المشـــرع الاتحادي جريمة الابتزاز الإلكتروني في القانون الاتحادي رقم 2 لســـنة 2012 بشأن مكافحة جرائم تقنية المعلومات حيث نصت المادة (16) منه على أن:" يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار".

كما حدّد المشرع المصري مضمون التهديد في الابتزاز والغرض منه في المادة 325 من قانون العقوبات التي تنص على أن: "كل من اغتصـــب بالقوة أو التهديد ســـندا مثبتا أو موجدا لدين أو تصرف أو براءة أو سندا ذا قيمة أدبية أو اعتبارية أو أوراقا تثبت وجود حالة قانونية أو اجتماعية أو أكره أحدا بالقوة أو التهديد على إمضاء ورقة مما تقدم أو ختمها يعاقب بالسجن المشدد".

وتنص المادة 326 من القانون ذاته على أن: "كل من حصـــل بالتهديد على إعطائه مبلغا من النقود أو أي شيء أخر يعاقب بالحبس، ويعاقب الشروع في ذلك بالحبس مده لا تتجاوز سنتين".

وذهب المشرع المصري في بعض النصوص الأخرى الى العقاب على الابتزاز محددًا مضمون التهديد في الابتزاز دون تحديد الغرض من التهديد، ومن ثم يقع الابتزاز طالما تم التهديد بالإفشـــاء مثلا للقيام بعمل أو الإمتاع عن عمل، حيث تنص المادة 309 مكررا (أ) على أن: "يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في علانيه تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن[66].

(66)- تنص الماده309 مكررا عن قانون العقوبات علي أنه": يعاقب بالحبس مده لا تزيد علي سنه كل من اعتدى علي حرمه الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الأتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجنه عليه:

ويعاقب بالسجن مده لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار اليها لحمل شخص على القيام بعمل أو الامتناع عنه.

ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته".

وتنص المادة 327 من القانون السابق على أن: "كل من هدّد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو بالسجن المؤبد أو المؤقت أو بإفشاء أمور أو نسبة أمور مخدشه بالشرف وكان التهديد مصحوبا بطلب أو بتكليف بأمر يعاقب بالسجن. ويعاقب بالسجن إذا لم يكن التهديد مصحوبا بطلب أو بتكليف بأمر.

وكل من هدد غيره شفهياً بواسطة شخص آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوباً بتكليف بأمر أم لا.

وكل تهديد سواء أكان بالكتابة أم شفهياً بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة، يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنية".

ورغمًا عن عدم استخدام المشرع المصري للفظ الابتزاز، فإن القضاء لم يجد غضاضة من

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محدثات جرت في مكان خاص أو عن طريق التليفون.

ب- التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صوره شخص في مكان خاص.

فاذا صدرت الأفعال المشار اليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فان رضاء هؤلاء يكون مفترضا ويعاقب بالحبس الموظف العام الذي يرتكب احد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته.

ويحكم في الجميع الأحوال بمصادره الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما يحكم بمحو التسجيلات المتحصلة عنها أو أعدمها".

استعماله في بعض الحالات. كما استخدم الفقه المصري مصطلح الابتزاز للتعبير عن الجريمة المنصوص عليها في الماده 326 من قانون العقوبات[67]، والمتعلقة بالحصول على مال بطريق التهديد.

يتضح من ذلك أن هذا الاتجاه يرى أن فعل الابتزاز لا يقع إلا بشرط أن يأخذ التهديد مضمونا معينا كالعنف، أو إفشاء أمور مخله بالشرف أو الاعتبار، وأن يستهدف ذلك الفعل غرضا محددا هو الحصول على مال أو سندات، أو توقيع، أو القيام بفعل، أو امتناع عنه، ومن ثم فالابتزاز يقع بتحديد المحل والغرض، أو تحديد أيهما فقط.

المطلب الثاني- الركن المادي لجريمة الابتزاز الإلكتروني:

يقوم الركن المادي على عناصره، التي هي السلوك الإجرامي، والنتيجة الإجرامية، وعلاقة السببية، فالسلوك الإجرامي هو التهديد؛ ويتمثل في كل قول أو فعل من شأنه أن يبث الخوف في نفس من يتوقع الإضرار به، أو بأي شخص آخر يهمه أمره، فيحمله هذا الخوف إلى أن ينفذ ما يريده الجاني[68].

وهذا التهديد قد يكون بارتكاب جريمة اعتداء على العرض، أو المال، أو بتشويه سمعه المجني عليه بنشر معلومات يخشى المجني عليه منها، إذ إنها تسبب له الاحتقار عند أهله ووطنه، فمتى ما حصل الابتزاز ووقع الخوف في نفس المجني عليه، وقعت الجريمة، بغض النظر عن الأسلوب في تنفيذ الجريمة، والطريقة المتبعة في أدائها[69].

---

(67)- رمسيس بهنام، قانون العقوبات جرائم القسم الخاص، الطبعة الأولى، منشأة المعارف، 1999م، ص 1204.

(68)- عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، مرجع سابق، ص 351.

(69)- محمود نجيب حسنى، شرح قانون العقوبات القسم الخاص، ط8، منشورات دار العربية، مصر،1984، ص982.

أولا- السلوك الإجرامي:

يتمثل السلوك الإجرامي في جريمة الابتزاز بالتهديد، وهو كل فعل أو سلوك من شأنه أن يبعث الخوف في النفس للمجني عليه بهدف الإضرار به، أو بأي شخص آخر يهمه أمره، مما يحمل المجني عليه على تنفيذ ما يريده الجاني[70]، ويشترط لوقوع الجريمة أن يكون الابتزاز أو التهديد جديًا بدرجة تكفي لجعل الشخص المقصود به يعتقد تحقيقه، بحيث يكون الابتزاز قد أثر في نفس المجني عليه[71]، فإذا كان الابتزاز ظاهره الهزل ، فلا تقوم الجريمة، أو إذا لم يكن ظاهره الهزل، لكن المتهم بادر على الفور أو بعد برهة يسيرة من الزمن فأفصح للمجني عليه عن نيته فلا ابتزاز هنا[72]. ولا يشترط في الابتزاز أن يكون لدى الجاني نية تحقيق الفعل المهدد بارتكابه، لأنه متى ما وقع التأثير في نفس المجني عليه تمت الجريمة[73].

ويجب أن يكون الابتزاز بأمر غير مشروع كأن يبتز الجاني للحصول على متعة جنسية، أو الحصول على أمر غير مستحق له، أما إذا كان موضوع الابتزاز على أمر لا يعده النظام جريمة في ذاته كأن يهدد شخص أحد التجار بمقاطعة تجارته إن لم يستجب لمطالبه، فلا جريمة هنا[74].

ولا فرق في موضوع الابتزاز أن يكون صحيحا، أو غير صحيح، بل إن التهديد بأمر غير صحيح قد يكون أبلغ تأثراً على المجني عليه، وإذا كان الموضوع صحيحاً فلا يجوز للمتهم إثباته[75].

وقد يكون الابتزاز صريحاً كما قد يكون غامضاً ملتوياً، كما لو رسم الجاني على منزل

---

(70)- عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، مرجع سابق، ص 351.

(71)- محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص 980.

(72)- جندي عبد الملك، موسوعة الأحكام الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2011، ص 982.

(73)- محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص985.

(74)- رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، 1985م، 423.

(75)- المرجع نفسه، ص 984.

المجني عليه علامات تدل على التهديد، لكن لابد أن يكون معنى التهديد بارزاً بما فيه الكفاية بما يؤثر جدياً في نفسية شخص عاقل[76].

وقد يساعد القاضي على تحديد نية الجاني، الظروف التي صدرت فيها العبارة، وعلاقته بالمجني عليه والأسلوب الذي صدرت به ونفسيه الجاني، ويتوافر التهديد ولو لم تصدر من الجاني عبارات على الإطلاق، بل لو اقتصر الأمر على إبداء إشارات رمزية مفهومة الدلالة كالتلويح بخطابات، أو أشرطة فإن الجريمة تقع[77]، وهذا ما قضت به محكمة النقض المصرية حيث جرى قضاؤها على: "إن القانون لم يبين ما هو التهديد، ولم يشترط لذلك عبارات خاصة بل ترك الأمر في ذلك لتقدير المحكمة، فكل عبارة من شأنها إزعاج المجنى عليه، وإلقاء الرعب في نفسه، أو إحداث الخوف عنده من خطر يراد إيقاعه بشخصه، أو ماله يعتبر تهديداً معاقباً عليه"[78].

والأصل أن يكون المجني عليه هو المهدد بالابتزاز، بأن يناله الأذى في حق من حقوقه، ومع ذلك يجوز أن يكون الابتزاز ضد شخص آخر له علاقه بالمجني عليه[79]. كما تتوفر الجريمة إذا وصل التهديد بالفعل إلى المجني عليه أو إذا كان احتمال علم المجني عليه بالابتزاز أمرا محتملاً[80].

وأما عن محل جريمة الابتزاز الإلكتروني فهو أمر أو واقعة يكون من شأن إسنادها الى

(76) – عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، مرجع سابق، ص 351.

(77) – محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص 982.

(78)– المرجع نفسه، ص 983، عبد العظيم مرسي، جرائم الاعتداء على الأموال، ص 424.

(79)– المرجعان السابقان 970 و343.

(80)– عبد العظيم مرسي، جرائم الاعتداء على الأموال، مرجع سابق، ص 434.

المجني عليه الحط من قدره أو قدر غيره أو المساس بشرفه أو شرف غيره[81].

ولا يهم القانون أن تكون الواقعة التي يهدد الجاني بإسـنادها إلى المجني عليه صـحيحة أو غير صحيحة، ولا يهمه أيضا أن يكون من ستناله الواقعة هو المجني عليه بالذات، فقد يكون شخصا أخر يهم المجني عليه كزوجته أو ابنته أو أحد أقاربه، والعبرة فيما يهتم له القانون من حيث المحل المادي لجريمة الابتزاز الإلكتروني أن يكون من شان الواقعة المساس بشرف المجني عليه أو الحط من مكانته أو المساس بشرف أو مكانة أحد أقربائه[82].

أما من حيث السلوك الجرمي (الفعل) لجريمة الابتزاز الإلكتروني، فإن الفعل الرئيس لجرمية الابتزاز هو التهديد بفضـح أمر، وهو في جوهره وعيد بإيقاع شـر بهدف الضـغط على إرادة المجني عليه، ليحقق من خلاله الجاني الهدف من هذا التهديد[83]. " وأهم ضـابط لهذا السـلوك المادي هو درجة المساس بالمكانة الاجتماعية للمجني علية أو المساس بالشرف، أو المساس بالذمة المالية"[84].

ويجدر بالذكر أن التهديد كسلوك في هذه الجريمة لا يأخذ صورة الإكراه المادي فحسب؛ بل يكفي فيه الإكراه المعنوي للتأثير في حرية اختيار المجني عليه بحيث يحمله على تنفيذ مطلب الجاني[85]. فالتهديد من شـأنه الترويع والحد من الحرية وفعاليته في خوف المجني عليه من فضـح

---

(81) – كامل حامد السعيد، شرح قانون العقوبات– الجرائم الواقعة على الأموال، ط3، منشورات دار الثقافة للنشر والتوزيع، 2014، ص169. محمد صبحي نجم، قانون العقوبات القسم الخاص – الجرائم المخلة بالمصلحة العامة والثقة العامة والواقعة على الأموال وملحقاتها، منشورات دار الثقافة للنشر والتوزيع، 2014، ص209.

(82) – محمود نجيب حسنى، شرح قانون العقوبات القسم الخاص، ص197.

(83)– حسن صادق المرصفاوي، قانون العقوبات الخاص– منشاة المعارف– الإسكندرية مصر،1991، ص940 وما بعدها– مصطفى مجدي هرجة، التعليق على قانون العقوبات في ضوء الفقه والقضاء، ط2، منشورات روز اليوسف، القاهرة، 1992، ص1245 وما بعدها.

(84)– كامل حامد السعيد، شرح قانون العقوبات– الجرائم الواقعة على الأموال، المرجع السابق، ص191.

(85)– فخري عبد الرزاق الحديثي، شرح قانون العقوبات القيم الخاص، الجرائم الواقعة على الأموال، الطبعة الثانية، منشورات دار الثقافة، عمان، 2011، ص89.

أمر يحرص على إخفائه، بحيث يطال قدرة أو شرفه أو يجلب الاحتقار له ... ولا تقع جريمة الابتزاز دون التهديد، وبالتالي ليس ثمة جرم ابتزاز في أي طلب يطلبه شخص ويستجيب إليه المجني عليه بإرادة حرة واختيار صحيح، لأن العبرة في فعل التهديد، أثر هذا الفعل في نفس المجني علية[86] .

وإذا كان التهديد هو السلوك المادي لجرم الابتزاز أو التهويل التقليدي، وإذا كان المشرع لم يحدد وسيلة معينة لمباشرة الجاني هذا السلوك، بحيث يقع شفاهية أو كتابة، فإنها في النطاق الإلكتروني تقع باستخدام تطبيقات الملفات الصوتية والمرئية المختلفة.

أما من حيث اكتمال الركن المادي لجريمة الابتزاز الإلكتروني مباشرة من الجاني ضد المجنى عليه، فإنه قد يقع بواسطة طرف ثالث وبصورة غير مباشرة، كأن يبلغ الجاني ضد المجنى عليه بواسطة شخص قريب من الأخير أو على علاقة بالطرفين، لأن العبرة ليست بتأثير الشخص على الآخر، وإنما بمادة التهديد التي تصل إلى المجنى عليه.

ثانيا- النتيجة الإجرامية:

موضوع جريمة الابتزاز هو التهديد بإفشاء معلومات عن المجني عليه تجعله في موطن الذم والتحقير عند أهله ووطنه، فمتى صدر من الجاني هذا الفعل، وكان التهديد لأمر غير مشروع، ووقع تأثيره في نفس المجني عليه، بحيث ينشأ لديه الخوف مما هدده الجاني به، فهذه هي النتيجة للابتزاز، سواء أوقع الجاني ما هدد به أم لم يوقعه، لأن الضرر الذي هو الخوف قد وقع في نفس المجني عليه[87].

فإذا سعى الجاني بالتهديد إلى مجرد الإرهاب، أو طلب منفعة، أو أراد أن يحمل المجني عليه على

---

(86)- المرجع السابق، ص90. والسعيد، المرجع السابق، ص182. ومحمد صبحي نجم، قانون العقوبات القسم الخاص – الجرائم المخلة بالمصلحة العامة والثقة العامة والواقعة على الأموال وملحقاتها، المرجع السابق، ص209.

(87)- محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص 977.

أداء عمل أو الامتناع عن عمل، فهنا تقع الجريمة سواء فعل المجني ما طلب منه، أم لم يفعل[88].

ثالثًا- علاقة السببية بين السلوك والنتيجة:

تتمثل عموماً في أن يكون الإسناد سبباً في امتهان كرامة المعتدي عليه، واحتقاره، وتعريضه لبغض الناس[89]. كما توجد علاقة السببية بين الابتزاز والتسليم في حال كان الباعث للجاني الحصول على المال، إذ يلزم أن يكون تسليم المال نتيجة ما أحدثه ذلك في نفس المجني عليه من خوف، وإرهاب، فإذا لم يحدث التهديد هذا الأثر، وجرى تسليم المال لاعتبارات أخرى انقطعت علاقة السببية، ووقف نشاط الجاني عند حد الشروع في ابتزاز المال بالتهديد[90]. ولا يشترط لقيام علاقة السببية هنا أن يكون الابتزاز سابقاً على إعطاء المال مباشرة، بل يصح أن يكون سابقاً عليه بزمن متى كان له أثره في ذلك[91].

أما إذا كان الابتزاز للقيام بعمل أو الامتناع عن أداء عمل، فإن النتيجة هنا وقوع الضرر وهو الخوف في نفس المجني عليه، وتكون السببية بينه وبين الابتزاز في أن يكون الإسناد سبباً في امتهان كرامة المعتدى عليه واحتقاره وتعريضه لبغض أهله وأبناء موطنه.

ومما لا يدخل في علاقة السببية، امتناع من وقع عليه الابتزاز عن أداء العمل؛ لأن القانون يحظر عليه أداء هذا العمل، وكان الجاني قد طلب منه الامتناع عن أداء هذا العمل، وكان امتناعه ليس بسبب الخوف، إنما لرغبة المجني عليه الالتزام بالقانون، فهنا لا تقع جريمة الابتزاز؛ لعدم

---

(88)- عبد العظيم مرسي، جرائم الاعتداء على الأموال، مرجع سابق، ص 344.

(89)- محمد صبحي نجم، قانون العقوبات القسم الخاص – الجرائم المخلة بالمصلحة العامة والثقة العامة والواقعة على الأموال وملحقاتها، مرجع سابق، ص 211.

(90) – عادل عزام، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، مرجع سابق، ص103.

(91)- عبد العظيم مرسي، جرائم الاعتداء على الأموال، مرجع سابق، ص 344.

وجود علاقة السببية في الجريمة[92].

المطلب الثالث– الركن المعنوي الابتزاز الإلكتروني:

جريمة الابتزاز الإلكتروني جريمة عمدية، إذ لا يتصور حصولها أبدا بغير قصد جرمي، كحصولها بالخطأ أو بأي صورة من صوره. والمراد بالقصد الجنائي هو تعمد إتيان الفعل المجرم، أو تركه مع العلم بأن المشرع يجرم الفعل أو يوجبه[93].

والسؤال الذي قد يثار في هذا المقام هو هل تستلزم هذه الجريمة قصد خاص أم يكفي لقيامها توافر القصد العام بعنصرية (العلم والإرادة)؟

هذه الجريمة لا يكفي لقيامها توافر القصد العام، بل تحتاج إلى توافر قصد خاص معاصر لفعل التهديد، إذا انتفى تنتفي معه الجريمة، ويتمثل القصد الخاص لجريمة الابتزاز وفق الغالب من الفقه[94]، بجلب المنفعة غير المشروعة للجاني أو لغيره، بحيث لا يقوم القصد ولا يتكون الركن المعنوي للجريمة إذا انتفى غرض الجاني من الحصول على المنفعة غير المشروعة، ووفق هذا الرأي لا تقع جريمة الابتزاز حين تكون المنفعة التي يقصدها الجاني مشروعة، كأن يهدف مثلا إلى مجرد الإزعاج، أو يهدده ليدفعه إلى فعل يخدم المجنى عليه نفسه، كتهديده بفضح أمر إذا لم يتوقف عن تعاطى المخدرات، وفى هذه الحالات فإن القصد الذى يستهدف منفعة مشروعة لا تقوم به الجريمة[95].

---

(92)– محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص 977.

(93)– عبد القادر عودة، التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي، مرجع سابق ص 241.

(94)– محمد صبحي نجم، قانون العقوبات القسم الخاص – الجرائم المخلة بالمصلحة العامة والثقة العامة والواقعة على الأموال وملحقاتها، المرجع السابق، ص210.

(95)– كامل حامد السعيد، شرح قانون العقوبات– الجرائم الواقعة على الأموال، المرجع السابق، ص183. وحسنى، المرجع السابق، ص206.

بينما يرى جانب آخر أنه يكفي لارتكاب جريمة الابتزاز أن يقوم الجاني بارتكاب الفعل بعلمه وإرادته، وبنيه إحداث النتيجة المعاقب عليها، أي يثبت لديه القصـد الإجرامي في إحداث الخوف في نفس الشـخص الذي وجه إليه فعل الابتزاز، وهو قصـد جنائي عام، ولا يلزم لقيام جريمة الابتزاز قصداً خاصاً من أي نوع كان لدى الجاني[96].

ولا يشترط أن يكون لدى مرتكب جريمة الابتزاز نية تحقيق الفعل المهدد بارتكابه؛ لأن جريمة الابتزاز معاقب عليها بذاتها، إذ أنه يعاقب عليها بسـبب ما تحدثه من رعب في نفس الشـخص المهدد، وإكراهه تحت وطأة الابتزاز على القيام بعمل، أو الامتناع عن القيام به، متى كان من شـأن الابتزاز التأثير في نفس المجني عليه، وأن يكون الجاني عالماً بما يمكن أن يحدثه ذلك التهديد. وفي هذا المقام قضـت محكمة النقض المصـرية بأنه :"يتوافر القصـد الجنائي في جريمة التهديد متى ثبت أن الجـاني ارتكـب التهديـد وهو يـدرك أثره من حيـث إيقـاع الرعـب في نفس المجني عليـه، وأنـه يريـد تحقيق ذلك الأثر، بغض النظر عما إذا كان الجاني قد قصـد إلى تنفيذ التهديد فعلاً، من غير حاجة إلى تعرف الأثر الفعلي الذي أحدثه التهديد في نفس المجني عليه"[97].

كما أنـه لا أثر للباعث في توافر القصـد الجنائي طبقاً للقاعدة العامة من أن الباعث ليس عنصـرا في القصـد الجنائي، فيسـتوي في الابتزاز أن يكون الباعث شـريفاً أو وضـعياً، كانتقامه من المجني عليه، وذلك لاعتدائه على عرضـه، أم لتحقيق مصـلحة معينة إذا كان مصـحوباً بطلب، أو بتكليف أمر، أم حتى لمجرد حب اسـتطلاع ورغبة امتحان شـجاعة المجني عليه[98]. وفي حال كان

(96)- عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، مرجع سابق، ص355.

(97)- رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، مرجع سابق، 428.

(98)- المرجع السابق، 429.

الباعث على الابتزاز هو المزاح والدعابة، فإنه وفقا للقاعدة العامة من أنه لا عبرة بالباعث في الجريمة، فإن العمل هنا يعد جريمة ابتزاز، إلا أنه يلاحظ أن الجريمة تفترض وقوع ضرر مباشر، وهو الذي يحظره القانون ويعاقب عليه، شأنها في ذلك شأن كل جريمة أخرى، والضرر هنا هو بث الذعر والقلق في نفس المجني عليه، وهو ضرر لا يتصور وقوعه عندما يكون التهديد ببث الدعابة أو المزاح فحسب، وذلك إذا كشف المجني عليه حقيقة الدعابة فور وصول التهديد، أو إذا كشفها له الجاني، أو غيره قبل حدوث أي قلق، أو خوف لديه فهنا يمكن القول بعدم وقوع الجريمة[99]. أما إذا انتزع الجاني المال من المجني عليه انتزاعاً، فإن الجريمة تنتقل من جريمة ابتزاز إلى جريمة سرقة بالإكراه[100].

وإذا كان القصد الجنائي العام ركناً في جريمة الابتزاز، فإنه يترتب على ذلك أنه إن لم يوجد القصد الجنائي، فلا جريمة ابتزاز، إذ أن من عناصر الابتزاز وجود إرادة محققة بإيقاع الأذى وإثارة الخوف في نفس المجني عليه، ومن ثم يختلف الابتزاز عن تمني الشر، فلا جريمة هنا[101].

كما يفترض في الابتزاز، أن نزول الضرر بالمجني عليه مُرتهن بإرادة المتهم نفسه، سواء مباشرة، أو عن طريق شخص آخر يعمل لحسابه، وبناء عليه يخرج من نطاق الابتزاز إنذار المجني عليه بشر تنزله قوة طبيعية لا سيطرة للمتهم عليها، أو بواقعة خرافية لا وجود لها[102]، ولكن لا يتنافى مع وجود الإرادة المحققة أن يكون نزول الأذى المهدد به معلقاً على شرط، وهو ما يتحقق

(99)– رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، مرجع سابق، 429 – عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، مرجع سابق، ص 355.

(100)–عبد العظيم مرسي، جرائم الاعتداء على الأموال، مرجع سابق، ص 344.

(101)– محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص981.

(102)– عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، مرجع سابق، ص 355.

حين يصطحب التهديد بطلب أو تكليف بأمر[103].

وتجدر الإشـــارة هنا إلى أن بعض الفقه[104] لا يعتبر جلب المنفعة غير المشـــروعة من قبيل القصد الخاص لأنه يراها الدافع إلى ارتكاب الجريمة، فالدافع هو العلة التي تحمل الفاعل على الفعل أو الغاية القصـوى التي يتوخاها، لأن جريمة الابتزاز الإلكتروني تسـتلزم القصـد الخاص، وهو جلب المنفعة غير المشـروعة للجاني أو لغيره، فجريمة الابتزاز لا تقوم إذا كان غرض الجاني جلب منفعة مشروعة. حيث "... لا يتوافر القصد الجنائي إذا أراد الفاعل مجرد الإزعاج، أو أن تهديده استهدف الحصول على منفعة مشروعة له أو لغيره، فمن يهدد شخصا بالإبلاغ عن جريمة ارتكبها ضده فعلا ما لم يعوضه عن الضرر الذي أصابه منها ينتفي لديه قصد الابتزاز، لأنه يبغي الحصول على حقه أو يعتقد أنه حقه، وكذلك الحكم فيما لو كان غرض التهديد حمله على وفاء دينه تجاهه. ومن باب أولى ينتفي القصد إذا حصل التهديد دون غاية الحصول على المال وإنما المشاحنة لدفع المال ... ولا مجال لقيام هذه الجريمة بحق الزوج الذي يكتشف أن زوجته تخونه فيطالبها بالتعويض عن ذلك مقابل سكوته، ولكن الحكم يختلف فيما لو أن هذا الزوج كان مفتريا أو كاذبا[105]".

ويبدو القصد الخاص في جريمة الابتزاز الإلكتروني أكثر وضوحا ويتميز عن الباعث غير المجرم، ففي جريمة الابتزاز الإلكتروني بالصور المتقدمة يظهر القصد الخاص جليا وتتوافر بشأنه الأدلة وبالحد الأدنى القرائن، حين يوجه الفاعل علمه العميق بشؤون التكنولوجيا إلى استغلال تطبيق وجد في الأساس للمنفعة العامة ولدعم توظيف التكنولوجيا في المجتمع، فنجده بدلا من ذلك يوجه

(103)– محمد نجيب حسني، شرح قانون العقوبات القسم الخاص، مرجع سابق، ص981.

(104)– المرجع نفسه، ص91.

(105)– كامل حامد السعيد، شرح قانون العقوبات– الجرائم الواقعة على الأموال، مرجع سابق، ص183.

جهده ليطال شرف ومكانة واعتبار الشخص المستهدف بفعل الابتزاز، مع إدراكه بأنه إن فعل ذلك سيكون الشخص المستهدف عرضه للمساس بمكانته واعتباره وسط أكبر قطاع من البشر، ونظرًا لما تتميز به تكنولوجيا المعلومات وتطبيقاتها من انتشـــار واســـع، وتتيح أوســـع الاطلاع على الأخبار والمواد المنشورة على تطبيقاتها المختلفة، في هذه البيئة وعبر هذا السلوك يكون قصد الجاني الخاص بتحقيق المنفعة متاحاً أكثر، لما يحدثه تهديده من أثر عميق وهلع شديد في نفس المجنى عليه.

ومن زاوية أخرى، فإن اســـتمرار الجاني في ابتزاز المجني عليه متيســـر أكثر في الوســـائل الإلكترونية، لقدرته على الاحتفاظ بنسـخ متعددة وبأشـكال مختلفة من المادة موضـوع الابتزاز، وهذا سيتيح له مزيدا من الكسب من خلال التهديد، أي أن القصد بتحقيق المنفعة غير المشروعة يتنامى ويتعزز مع توافر فرص تكرار فعل الابتزاز المرة تلو الأخرى.

الفصل الثاني – إثبات جريمة الابتزاز الإلكتروني والعقوبات المقررة لها :

ظهرت في الأونة الأخيرة –مع تنامي ظاهرة الجريمة المعلوماتية– العديد من المشكلات في نطاق قانون الإجراءات الجزائية، حيث وضعت نصوصه لتحكم الإجراءات المتعلقة بالجرائم التقليدية التي لا تثير مشاكل في إثباتها أو التحقيق وجمع الأدلة بصددها، مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع وصولاً إلى الحقيقة الموضوعية بشأن الجريمة المرتكبة والمجرم. وحيث إن البحث يتناول أحد الجرائم المعلوماتية؛ فإنه يثير مجموعة من المشكلات تتمثل في كيفية التعامل مع بيانات معالجة آلياً، وكيانات افتراضية غير محسوسة، مما يترتب عليه:

- صعوبة اكتشافها من ناحية.
- صعوبة البحث عن الأدلة بصددها من ناحية أخرى.

إضافة إلى سهولة وسرعة ودقة الجرائم المعلوماتية، مع إمكانية محو آثارها، وإتلاف الأدلة التي تخلفها عقب التنفيذ مباشرة، وإمكانية لجوء مرتكبي هذه الجرائم إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة إلكترونية محمية بشفرات أو رموز سرية بغية إخفائها عن أعين سلطات التحقيق والعدالة.

لكل ما سبق فإن عملية التحقيق في الجريمة المعلوماتية تواجه العديد من العقبات التي تحول دون الوصول إلى الحقيقة والكشف عن الجريمة وإثباتها، ومن ثم إيقاع الجزاء العادل بالجناة.

بناء على ما سبق سوف يتطرق الباحث إلى كيفية **إثبات جريمة الابتزاز الإلكتروني والعقوبات المقررة لها** وذلك في المبحثين التاليين:

المبحث الأول– التحقيق في جرائم الابتزاز الإلكتروني.

المبحث الثاني– العقوبات المقررة لجرائم الابتزاز الإلكتروني.

المبحث الأول- التحقيق في جرائم الابتزاز الإلكتروني:

تمهيد وتقسيم:

يتضح للباحث من دراسة الطبيعة الخاصة للجريمة المعلوماتية أنها تختلف اختلافاً جذرياً عن الجريمة التقليدية، وذلك من حيث:

1. الجريمة المعلوماتية عابرة للحدود:

تتميز الجرائم المعلوماتية بطابع عالمي، لأن جميع الدول مرتبطة ببعضها البعض وفي حالة اتصال دائم، فالجريمة المعلوماتية لا تعرف حدود وبذلك أصبح مسرح الجريمة المعلوماتية عالمياً[106].

الأمر الذي يطرح العديد من الإشكاليات القانونية، خاصةً أثناء عدم تواجد الجاني في مسرح الجريمة، وكذلك التباعد الزماني والمكاني، بين السلوك الإجرامي والمتمثل في جهاز الكمبيوتر والنتيجة الإجرامية التي تمثل قاعدة البيانات والمعطيات محل الاعتداء، مما يثير إشكالية التعارض مع السيادة الوطنية فيزيد الأمر تعقيدًا، من خلال صعوبة اللجوء إلى عمل دولي مشترك للحد من هذه الجرائم، مما يستوجب الاعتماد على التشريعات الوطنية لكل دولة[107].

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

---

(106)- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الإسكندرية، 2002، ص 351.

(107) - خالد حسن لطفي، التقاضي الإلكتروني كنظام قضائي معلوماتي، دار الفكر الجامعي، 2020، ص 125.

2. صعوبة إثبات الجريمة المعلوماتية:

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

- أنها جريمة لا تترك آثاراً مادية بعد ارتكابها، وغالباً ما يتم اكتشافها بالمصادفة وبعد وقت طويل من حدوثها.
- صعوبة الاحتفاظ بالدليل الفني على ارتكاب الجريمة، لأن الجاني يستطيع في ظرف وجيز جداً أن يمحو أو يُحرف 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، من خلال معرفة تقنيات الكمبيوتر ونظم المعلومات ســواء في مجال الأدلة والتحقيق أو المتابعة القضـــائية، لذلك فإن رجال الضـــبطية القضـــائية غير قادرين على التعامل مع هذه الفئة من الجرائم بالطرق التقليدية، ناهيك عن صعوبة تتبع مسار العمليات إلكترونياً خصوصاً إذا كانت عابرة للقارات.
- إن هذه الجرائم تعتمد في ارتكابها على الخداع والتضـــليل؛ مما يســـاعد على عدم التعرف على الفاعل الحقيقي، والشيء الملاحظ هو أن المؤسسات والبنوك خصوصاً تحجم عن الإبلاغ تجنباً للإساءة إلى سمعة العملاء والخوف من هز ثقتهم بها، إضافة إلى إخفاء أسلوب ارتكاب الجريمة خوفا من تكرارها مما يزيد في فرص إفلات الجاني من العقاب[108].

(108)– خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، لإسكندرية، 2008، ص 47.

- تعتمد كل الجرائم المعلوماتية على الذكاء ولهذا تسمى جرائم الذكاء، وهي ليست جريمة منظمة فغالباً ما ترتكب بصفة فردية، وأهم دوافعها الطمع والجشع والانتقام وأحيانا بدافع إثبات الذات. فالإجرام المعلوماتي هو إجرام الأذكياء الذي يعتمد على مهارات فنية وتقنية وإلمام بنظم المعلومات مقارنة مع الإجرام التقليدي الذي يعتمد على العنف.

3. عدم وجود مفهوم محدد ومشترك للجريمة المعلوماتية:

يرجع هذا الأمر إلى اختلاف النظم القانونية في دول العالم، ويظهر هذا جلياً 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[109]. استنادًا لما سبق سوف يقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول– إجراءات التحقيق وجمع الأدلة في جرائم الابتزاز الإلكتروني.

المطلب الثاني– الصعوبات التي تواجه التحقيق في جرائم الابتزاز الإلكتروني.

(109)– المرجع السابق، ص 48.

المطلب الأول- إجراءات التحقيق وجمع الأدلة في جرائم الابتزاز الإلكتروني:

عدّل نص المادة (75) من قانون الإجراءات الجزائية الاتحادي رقم 35 لسنة 1992 الخاصة بمدى صلاحية النيابة العامة في التفتيش، بموجب المادة الأولى من القانون الاتحادي رقم 2005/29 تاريخ 2005/11/30م. وأصبح على الوجه التالي:" لعضو النيابة العامة أن يفتش المتهم ولا يجوز له تفتيش غير المتهم أو منزل غير منزله إلا اذا اتضح من أمارات قوية أنه حائز لأشياء تتعلق بالجريمة. ويجوز له بموافقة النائب العام أن يضبط لدى مكاتب البريد جميع المكاتبات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات، وأن يراقب ويسجل المحادثات بما في ذلك السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك".

وتبعا لنص المادة (75) سالفة الذكر فإن من يتولى التحقيق هو النيابة العامة كجهة ادعاء، وهي التي تحيل الشكوى المقدمة من المجني عليه أو الشخص المعني إلى وحدة الجرائم الإلكترونية لإجراء التحقيق [110].

الفرع الأول- التحقيق التمهيدي (الاستدلال):

يتمثل في الجرائم الإلكترونية بضباط فنين ومختصين في هذا المجال وهو لا يعد تحقيقًا بالمعنى القانوني البحت، إنما إعداد تقارير فنيه وأخذ الإفادات الأولية من أصحاب العلاقة بناء على شكوى محالة من قبل النيابة، ويباشر التحقيق الفني التمهيدي بعد توجيه كتاب من قبل النيابة العامة لوحدة الجرائم الإلكترونية، لأن التحقيق في هذه الجرائم بحاجة إلى إمكانيات فنية معينة مخصصة،

(110)- محمد صبحي نجم، قانون أصول المحاكمات الجزائية الأردني، منشورات الجامعة الأردنية، عمان، الأردن، الطبعة الأولى، ص 233 وما بعدها.

حيث يقوم الضـابط المعني من وقت وصـول كتاب النيابة بسـماع إفادة الشـاكي، وهي هنا ليسـت اسـتجواباً وإنما إفادة بالواقعة التي حصـلت مع الشـاكي وخاصـة الوسـائط الإلكترونية ذات الصـلة بالجريمة محل التحقيق، فإن كان الهاتف مثلاً يقوم الشاكي بتسليمه أو الدخول إليه أمام المحقق[111].

وفي ضوء أقوال صاحب الشكوى وما يسلمه لوحدة الجرائم الإلكترونية من أوراق أو تطبيقات أو أجهزة، يشرع الضابط المسؤول بجمع الأدلة ، وفي مقدمتها ما يتلقاه من شركات الاتصالات المختلفة وهيئة تنظيم الاتصـالات أو أي جهة أخرى بشـأن أرقام الهواتف والمواقع الإلكترونية وعناوين البريد الإلكتروني التي تكون على صلة بالواقعة مدار التحقيق، وفي جزء من عمله هذا لابد أن يتخلله البعد الفني، بحيث يقوم المحقق أو أي من زملائه المختصـين في الوحدة باسـتخدام الوسـائل الفنية للتتبع وتحليل المعطيات ومحتويات الصـفحات والمواقع الإلكترونية وبيانات الاتصـالات وغيرها[112]، وهذا كله يقع في نطاق إجراءات جمع الأدلة في مرحلة التحقيق الاستدلالي الفني.

وقد تشمل إجراءات التحقيق الانتقال والمعاينة وإن كنا أمام انتقال محصور للكشف على الأجهزة والتطبيقات ذات الصـــلة بالجرائم، إذ لا يعد التتبع الإلكتروني داخل الشـــبكات من قبيل المعاينة المعروفة في القانون، وإنما ينتسب إلى دائرة التحقيق الفني الرقمي المتعلق بالجرائم الإلكترونية، حيث يسـتخدم فيه إلى جانب خبرة المحقق تقنيات وبرامج خاصـة بتتبع آثار ونشـاطات الشـخص المعني داخل الشبكة الإلكترونية وأنظمة المعلومات، وتنظيم التقارير والضبوط بشأنها[113].

---

(111)- خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، 2020م، ص 320.

(112)- عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت، المرشـد الفيدرالي للتفتيش وضـبط الحواسـيب، بدون جهة نشر، وبدون مكان نشر، ص 281 وما بعدها.

(113)- أحمد أبو الروس بسيوني، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، مرجع سابق، ص 32 وما بعدها.

وقد ظهر في واقعة عملية تتعلق بإجراءات تحقيق استدلالي، ادعاء أحدهم بوصول رسالة أو مادة مشينة إلى هاتفه، قام بنقلها أو تخزينها على واسطة أخرى، ولم يعد الهاتف الأصلي معه. في هذه الحالة مثلاً قد يوثق المحقق الفني الواسطة التي تحمل المادة ويتأكد من وقت نقلها وسلامة المحتوى دون تعديل، وهو ما يسمى تفريغ الدليل، ولكنه في الغالب يحتاج إلى ضبط مشاهدة ليس له أدنى علاقة بالصفة الإلكترونية للدليل[114].

ينتقل المحقق بعد جمع الأدلة وربما خلالها إلى استدعاء الشخص المشتبه به أو المشتكى عليه وفق الأوراق، أو الذي أظهرت التحقيقات الأولية صلته بالسلوك الجرمي المذكور في الشكوى، ويستدعيه لأغراض سماع إفادته تمهيداً لإحالته مع الأوراق إلى عضو النيابة المختص باستجوابه، وصلاحية مأمور الاستدلال محصورة بسماع إفادة، أي لا يملك حق الاستجواب بالمطلق، لأن ذلك محصور بالنيابة العامة وفقًا لنص المادة (75) من قانون الإجراءات الجزائية الاتحادي، مع الإشارة إلى أن الواقع العملي أظهر في حالات كثيرة حصول الاستجواب من قبل رجل الضبط القضائي على النحو الذي ترتب عليه بطلان التحقيق[115].

ولا يملك مأمور الاستدلال أمراً تجاه إفادة المشتبه به أو المشتكى عليه، وإنما يلتزم بإحالته إلى النيابة مع الأوراق.

وتجدر الإشارة في هذا المقام إلى وجود فترة زمنية فاصلة بين سماع وحدة الجرائم الإلكترونية للمشتبه به أو المشتكى عليه وبين إحالة الأوراق إلى النيابة، وإيداع الأطراف أمامه، سبب ذلك حاجة

(114)- أميرة محمود الفقي، الإثبات الجنائي للجرائم المرتكبة عبر الإنترنت، رسالة دكتوراة، جامعة عين شمس، ص591.

(115)- سعد عاطف عبد المطلب، الحماية الجنائية للمصنفات الرقمية" دراسة مقارنة"، دار الفكر الجامعي، 2019م، ص 258.

الوقائع عادة إلى مزيد من جمع الأدلة التقنية وتتبع ما أشـــارت إليه أقوال الأطراف المعنيين في الشكوى الواقعة، ولا يعتبر ذلك مما يقع في نطاق ما قررته المادة (76) من قانون الإجراءات الجزائية الاتحادي رقم 35 لسنة 1992 الخاصة بالاطلاع على الرسائل والأوراق المضبوطة: "يطلع عضو النيابة العامة وحده على المكاتبات والرسائل والأوراق الأخرى المضبوطة وله حسب ما يظهر من الفحص أن يأمر بضـــم تلك الأوراق الى ملف الدعوى أو بردها الى من كان حائزا لها أو من كانت مرســـلة إليه"، لأن الأمر هنا ليس إلقاء قبض وإنما ســـماع إفادات تمهيداً لتوديع الأطراف ونتائج التحقيق الأولي.

وتجدر الإشارة أيضا أن مراكز الأمن ووحدات البحث الجنائي المختصة، عادة ما تنظم تعهداً من قبل أقارب أو أصدقاء المشتبه به يتضمن التزاماً بإحضاره عند الطلب، لتغطية الفترة بين سماع إفادته وتركه وبين إعادة استدعائه وحضوره أمام النيابة العامة[116].

الفرع الثاني- تحقيق النيابة العامة:

فور وصول الأوراق إلى مقر النيابة العامة، والمرسلة مع الأطراف من وحدة الجرائم الإلكترونية أو المركز الأمني المختص، (أو حتى عن طريق النائب العام مباشرة في أحوال التحقيق بنشر مواد تستوجب حماية المجتمع منها)، فإن النيابة تقوم بقيد الأوراق كدعوى تحقيقية تتخذ رقما في سجلات النيابة العامة، يحدد فيها المشتكي، والمشتكى عليه، وموضوع الشكوى، والنيابة التي تتولاها[117].

ويشير الباحث هنا إلى أن الشكوى التي تقدم في بداية الأمر للنيابة العامة في جريمة الابتزاز

(116)- سعيدي سليمة، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، 2017م، ص 336.

(117)- محمد علي ســـويلم، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية" دراســـة مقارنة"، دار المطبوعات الجامعية، 2018م، ص 147.

الإلكتروني لا تقيد تحت رقم في سجلات الادعاء العام، بل تحال مباشرة من النيابة العامة إلى مأمور الضبط القضائي، ولا تأخذ رقم القيد إلا بعد إعادتها إليها من مأمور الضبط القضائي المختص.

ووفق القواعد المقررة في قانون الإجراءات الجزائية تشرع النيابة العامة بالتحقيق، فيستمع للمشتكي في جرم الابتزاز الإلكتروني، ويستمع لشهوده إن كان ثمة شهود، ويبرز المستندات والكتب والتقارير الواردة من وحدة الجرائم الإلكترونية المتضمنة أدلة التحقيق الابتدائي، التي ستكون محل بحث وتمحيص، ويستمع للمشتكى عليه إن كان قد تم توديعه من قبل وحدة الجرائم الإلكترونية، أو يصدر التبليغات والمذكرات اللازمة حسب قواعد التبليغ والإحضار المقررة في قانون الإجراءات الجزائية، كما له اعتبار المشتكى عليه غير مقبوض عليه ليتمكن من استكمال التحقيق وفق الأصول[118].

وأهم إجراءات التحقيق في جرائم الابتزاز الإلكتروني، إجراء الخبرة الفنية على مشتملات وبيانات الأدلة الرقمية للتأكد من سلامة محتواها وللتأكد من ارتباطها بأطراف دعوى التحقيق، ويشمل ذلك تفريغ الملفات الصوتية وضبوط مشاهدة الصور والأفلام والمواد المرئية، إضافة إلى التثبيت من سلامة بيانات الاتصالات، وسلامة الأجهزة والتقنيات المرتبطة بالواقعة، وتجري النيابة عمليات الإفراز والتحريز والحفظ للأدلة الإلكترونية التي وصلت إليها أو قدمت لها من قبل الجهة المشتكية خلال تحقيق النيابة بالصورة التي تتوافق مع حفظ خصائصها وسلامتها.

لدى استجواب النيابة العامة للمشتكى عليه أو المشتبه به، سواء حضر عن طريق الدعوة أو

(118)- خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، دار الفكر الجامعي، 2020م، ص98.

التبليغ بمحض إرادته، أو جرى اســـتدعاءه مع الأوراق من قبل وحدة الجرائم الإلكترونية، أو تم إلقاء القبض عليه وعرضـــــه على النيابة، فإن النيابة ملزمة وفق قانون الإجراءات الجزائية، بمواجهة المشــتكى عليه بالتهمة المســند إليه، وهو الإجراء الذي لا يملكه غيرها، وللمشــتكى عليه الرد على الاتهام بنفسه أو طلب الاستعانة بمحام يمثله في إجراءات التحقيق أمام النيابة العامة.

ويجوز للنيابة العامة حبس المشـــتكى عليه احتياطيا اســـتنادًا لنص المادة (106) من قانون الإجراءات الجزائية حيث نصت على أنه:" مع مراعاة الأحكام المنصوص عليها في قانون الأحداث الجانحين والمشردين يجوز لعضو النيابة العامة بعد استجواب المتهم أن يصدر أمرا بحبسه احتياطيا اذا كانت الدلائل كافية وكانت الواقعة جناية أو جنحة معاقبا عليها بغير الغرامة"، وهنا يخضـــع الحبس الاحتياطي للشـــروط المقررة في قانون الإجراءات الجزائية، تبعا لنص المادة (110) التي تنص على أن: "الأمر بالحبس الصادر من النيابة العامة يكون بعد استجواب المتهم ولمدة سبعة أيام يجوز تجديدها لمدة أخرى لا تزيد على أربعة عشر يوما"، ومن حيث إخلاء السبيل وإجراءات الطعن في قرارات النيابة العامة برفض إخلاء الســـبيل تبعاً لما هو مقرر في نص المادة (110/ 2) من قانون الإجراءات الجزائية التي جاء نصها وفق الآتي:" فإذا استلزمت مصلحة التحقيق استمرار حبس المتهم احتياطيا بعد انقضاء المدد المشار اليها في الفقرة السابقة، وجب على النيابة العامة أن تعرض الأوراق على أحد قضـاة المحكمة الجزائية المختصـة ليصـدر أمره بعد الاطلاع على الأوراق وسماع أقوال المتهم بعد الحبس لمدة لا تجاوز ثلاثين يوما قابلة للتجديد أو الإفراج عنه بضـــمان أو بغير ضمان[119].

(119) – خالد حسن لطفي، التقاضي الإلكتروني كنظام قضائي معلوماتي، مرجع سابق، ص 129.

وللمتهم أن يتظلم الى رئيس المحكمة من الأمر الصادر في غيبته بمد الحبس وذلك خلال ثلاثة أيام من تاريخ إبلاغه الأمر أو علمه به[120].

ويجوز للنيابة العامة ووفق نص المادة (111) من قانون الإجراءات الجزائية الخاصـــة بالإفراج المؤقت عن المحبوس احتياطيا؛ الأمر بالإفراج المؤقت عن المتهم المحبوس احتياطيا في جناية أو في جنحة في كل وقت سـواء من تلقاء نفسـها أو بناء على طلب المتهم، ما لم يكن المتهم قد أحيل إلى المحكمة المختصة لمحاكمته فيكون الإفراج عنه من اختصاص هذه المحكمة[121].

كما يحق للنيابة العامة الأمر بالإفراج المشـــروط تبعا لنص المادة (112) من قانون الإجراءات الجزائية حيث نصـــت بأنه:" في غير الحالات التي يكون فيها الإفراج المؤقت وجوبيا، يجوز تعليق الإفراج على تقديم ضمان شخصـي أو مالي ويقدر عضـو النيابة العامة أو القاضـي حسب الأحوال مبلغ الضـمان المالي ويخصـص هذا المبلغ ليكون جزءا كافيا لتخلف المتهم عن الحضـور في أي إجراء من إجراءات التحقيق والدعوى وعدم التهرب من تنفيذ الحكم والقيام بكل الواجبات الأخرى التي تفرض عليه[122].

وفي جريمة الابتزاز الإلكتروني فإن للنيابة العامة أن تحيل الأوراق إلى المحكمة المختصة التي تدخل الجريمة في اختصـــاصـــها بوصـــفها جنحة، وبإحالة الدعوى إلى المحكمة المختصـــة تنتهي إجراءات التحقيق وترفع يد النيابة العامة عن الجريمة مدار البحث.

---

(120) – خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، مرجع سابق، ص 324.

(121) – خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، مرجع سابق، ص 100.

(122) – المرجع السابق، ص 101.

المطلب الثاني – الصعوبات التي تواجه التحقيق في جرائم الابتزاز الإلكتروني:

اســـتنادا لما تقدم كان إلزاماً على المشـــرع الجنائي التدخل بقواعد إجرائية جديدة أكثر فاعلية، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الاعتماد عليها في الكشـــف عن المجرم المعلوماتي والوصول إلى الدليل بسرعة وسهولة، علماً بأن هناك العديد من الصعوبات التي تواجه جهات التحقيق في استخلاص الدليل الرقمي نظراً لطبيعته الخاصة. لذلك سوف يتناول الباحث المعوقات التي تواجه جهات التحقيق في استخلاص الدليل الرقمي، حيث يصطدم التحقيق في الجرائم المعلوماتية بالعديد من المعوقات، فنظراً لوقوع الجريمة المعلوماتية ضمن بيئة رقمية كامنة في أجهزة الحاســب الآلي والخوادم والمضــيفات والشــبكات بمختلف أنواعها، أدت إلى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري في تطبيق القواعد الإجرائية التي نظمت مسألة استخلاص الدليل الرقمي، وتضـــعف قيمتها في مكافحة هذا النوع من الجرائم، وتؤثر على عملية التحقيق وتؤدي إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة بأجهزة التحقيق، وتنعكس على المجرم نفسه حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على مكافحة الجريمة والتحقيق فيها لا تجاري خبرته، الأمر الذي يعطيه ثقة أكـــــبر في ارتكاب المزيد من هذه الجرائم[123]. تباينت هذه الصـــعوبات أو المعوقات ما بين معوقات تتعلق بطبيعة الدليل الرقمي، وأخرى متعلقة بجهات التحقيق، وأخرى متعلقة بالجهات المتضررة من الجريمة المعلوماتية بالإضافة إلى صعوبة تحديد الجاني.

(123) – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، 2011 ص 220.

الفرع الأول – المعوقات التي تتعلق بطبيعة الدليل الرقمي:

أولا: الدليل الرقمي دليل غير مرئي:

يتميز الدليل الرقمي أنه دليل غير مرئي، فهو عبارة عن نبضات مغناطيسية إلكترونية تتكون من سلسلة طويلة من الأرقام، أي أنه ذو طبيعة ثنائية لا تفصح عن الشخصية المعنوية. فدائماً ما يكون الدليل في الجريمة التقليدية ذو طبيعة مادية مرئية بحيث يمكن للمختصين في عملية التحقيق بمعاينة مسرح الجريمة، وضبط أي دليل يفيد الكشف عن الجريمة، لكن الجريمة الإلكترونية تقع في بيئة تختلف عن البيئة التقليدية، لأن الأدلة فيها عبارة عن نبضات مغناطيسية تشكل بيانات رقمية في العالم الافتراضي، فعدم رؤية الدليل الرقمي يشكل العديد من المعوقات خلال جمعه وتحليله مما يستوجب توفر لدى المحققين الفنيين دراية كافية في التعامل مع هذا النوع من الأدلة[124].

ثانياً – سهولة إخفاء الدليل:

يتميز الجناة الذين يستخدمون الوسائل الإلكترونية في ارتكاب جرائمهم بالذكاء والإتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية، لذلك فإنهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها أثناء تشغليهم لهذه الوسائل الإلكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها[125]. وهناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الإلكترونية ويكون أمرها حكراً عليهم؛ كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار، كما أنهم قد ينسخون هذه

(124)–عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006، ص 79.

(125) – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994، ص16.

الملفات ويحصلون على نسخ منها بقصد استعمالها تحقيقاً لمصالحهم الخاصة، كذلك فإنهم قد يقومون باختراق قواعد البيانات والتغيير في محتوياتها تحقيقاً لمآرب خاصة، وقد يخربون الأنظمة تخريباً فنيًا بحيث يمكن تمويهه، كما لو كان مصدره خطأ في البرنامج أو في الأجهزة أو في أنظمة التشغيل أو التصميم الكلي للنظام المعالج آلياً للمعلومات، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون أن يترك وراءه ما يشير إلى حدوث هذا الإدخال أو التعديل[126].

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جداً، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي حال علمت بها فليس في استطاعتها إقامة الدليل ضده[127].

ثالثاً – صعوبة الحصول على الدليل الرقمي:

غالبًا ما يلجأ مرتكبو الجريمة المعلوماتية إلى الوسائل التي تعرقل جمع أدلة الإدانة، ومن أهم هذه الوسائل استخدام تقنية التشفير[128]، أو استخدام التدابير الأمنية لمنع التفتيش والاطلاع على الأدلة أو ضبطها، باستخدام كلمة سر، أو لجوئهم إلى إخفاء هويتهم، خاصة عند استخدامهم شبكة الإنترنت وذلك باستعمالهم للعديد من البرامج والتطبيقات التي تعمل على طمس هويتهم في شبكة

(126) – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994، ص 17، ص 20.

(127) – جميل الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، 198، ص 4.

(128) – عبد الفتاح بيومي حجازي، المرجع السابق، ص 89.

الإنترنت[129]. انطلاقا من أنّ الدليل الرقمي هو دليل فني مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، بعكس الدليل التقليدي 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 إلكترونية 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، مثال ذلك أن إثبات التدليس الذي 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 الأمر يتطلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا التدليس[130]، وقد يستعصي فهم هذا الأمر على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة التي يتولد من خلالها الدليل المتحصل من الوسائل الإلكترونية. فضلًا عن أن الكثير من العمليات الآلية للبيانات قد يقوم بها الحاسب بطريقة آلية دونما حاجة إلى عمليات إدخال، كما هو الحال في احتساب الفائدة على الإيداعات البنكية والتي تقيد آلياً بأرصدة حسابات العملاء على ضوء الشروط المتفق عليها مسبقاً والمخزنة في برنامج الحاسب، فقد يكون من السهل اختراقها وارتكاب جرائم تزوير واستيلاء تقع عليها عن طريق إدخال بيانات غير معتمدة في نظام الحاسب أو

(129) – ممدوح عبد المطلب، المرجع السابق، ص 121.

(130) – جميل الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2001، ص 113.

إجراء تعديلات في برامجه أو القيام بالتلاعب في البيانات المخزنة[131]. ونظرًا لطبيعة هذه العمليات يصعب أن تخلف وراءها آثار مادية ملموسة تكشف عنها، مما يزيد من صعوبة عمل المحققين الذين يعملون في حقل الجرائم التي تتمخض عن هذه العمليات الإلكترونية، فقد يستعصي عليهم فهم الأدلة المتحصلة عن هذه الوسائل بسبب تعقيدها وصعوبة الوصول إلى مرتكبي الجرائم الواقعة في سياق هذه العمليات[132].

ويزداد الأمر صعوبة في فهم الدليل الموصل إلى إثبات الجرائم التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية، ففي تلك الحالات التي يتصل فيها الحاسب الآلي بشبكة الاتصالات العالمية، يتطلب الأمر خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار أفضل السبل لضبطه[133]. مما يتطلب تدريب جهات الضبط القضائي والتحقيق والقضاء على فهم طبيعة المعطيات التي تقع عليها الجرائم الإلكترونية، والعمل على إلمامهم بمكونات الحواسب الآلية وكيفية عملها ومعرفة اللغة التي تتعامل بها.

وقد أصدر المجلس الأوربي في عام 1999 إحدى توصياته في هذا الصدد بضرورة تكوين وتدريب الشرطة وأجهزة العدالة، بما يواكب التطور المتلاحق لتقنية المعلومات، واستخدامها لتحقيق التوازن بين أجهزة ارتكاب الجريمة وطرق مكافحتها.

وقد عقدت المنظمة الدولية للشرطة (الإنتربول) العديد من الدورات التدريبية لمحققي الجرائم المعلوماتية. وفي نفس الإطار بادرت مختلف الدول إلى إنشاء وحدات متخصصة للضبطية القضائية

(131) – محمد الألفي، بحث في الدليل الرقمي وحجيته في الإثبات، بحث منشور على الإنترنت، ص 205.

(132) – هشام محمد رستم، مرجع سابق، ص 20.

(133) – محمد الألفي، مرجع سابق، ص 210.

في مجال البحث والتحري عن الجريمة المعلوماتية داخل الأجهزة الحكومية [134].

الفرع الثاني – المعوقات التي تواجهه جهات التحقيق:

تتعلق هذه المعوقات بالعامل البشـــري القائم بالتحقيق في الجريمة المعلوماتية، فإذا كانت السلطات القائمة بالتحقيق من رجال الضبطية القضائية وأعضاء النيابة، بما لهم من خلفية قانونية، تلعب دوراً كبيراً في التحري عن الجرائم والبحث عن مرتكبيها في إطار الجريمة التقليدية، فإن وظيفتها في مكافحة الجرائم المعلوماتية لا ترقى إلى نفس الدرجة، حيث إن دور هذه الجهات سيكونمحدوداً يرجع للأسباب التالية:

- أحيانا يهاب المحقق من استخدام وسائل تكنولوجيا المعلومات والاتصال الحديثة والإنترنت.
- عدم اهتمام هذه الجهات بمتابعة المستجدات الحاصلة في مجال الإجرام الإلكتروني.
- قلة خبرة هذه الجهات بتقنيات البحث والتحقيق بخصوص الجرائم المتصلة بهذه الوسائل الناتج عن عدم إلمامهم بأساليب ارتكاب الجرائم الإلكترونية، وعدم معرفتهم باللغة العلمية الرقمية.

لذا فإن نقص المهارة الفنية في استخدام الحاسب الآلي والإنترنت وعدم توفر معرفة أساليب ارتكاب الجريمة المعلوماتية وقلة الخبرة في مجال التحري والتحقيق في هذه الجرائم، من أهم العوامل التي تضعف دور الأجهزة المختصة بالتحقيق في الجرائم وكشف النقاب عنها، كما أنها قد تؤدي إلى تدمير الدليل وإتلافه، على اعتبار أن جهلهم بأساليب ارتكاب الجرائم المعلوماتية يجعلهم في كثير من الأحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها[135]، وأحيانا ترتكب الجرائم

(134) – عبد الفتاح بيومي حجازي، مرجع سابق، ص 90.

(135) – جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2002، ص 115.

المعلوماتية على مرأى ومسمع من سلطات الضبط بل قد يقدمون على تقديم يد العون لمرتكبي هذه الجرائم عن جهالة دون أن يشعروا بذلك.

ويرى المتخصصون في مجال مكافحة هذه الجرائم أن الأنظمة المعلوماتية وما يقع عليها من جرائم، تعد تحدياً حقيقياً لأجهزة العدالة الجنائية، لأن رجل الأمن غير المتخصص الذي تنحصر معلوماته في الجرائم التقليدية، لن يكون قادراً على التعامل مع الجريمة الإلكترونية الحديثة التي ترتكب بواسطة تقنيات عالية[136]. الأمر دفع بعض الدول إلى استقطاب المتخصصين وذوي الكفاءات العالية في مجال التكنولوجيا ضمن أجهزتها الأمنية والقضائية وتنظيم دورات تدريبية متخصصة وندوات تبادل المعارف والخبرات، بقصد رفع خبرات العاملين في مكافحة الإجرام الإلكتروني[137]. ورغم ذلك فإن أجهزة القضاء والشرطة غير قادرة على مواكبة التطور السريع في مجال تكنولوجيا المعلومات[138]. حيث ذهب البعض إلى أنه من الأفضل توكيل مهمة التحقيق في هذه الجرائم إلى شركات عالمية متخصصة في التحقيق في هذا النوع من الجرائم[139].

إلا أن هذا الرأي لم يلقَ قبولا لدى الأنظمة القانونية المختلفة، تأسيساً على أن متطلبات العدالة الجنائية تقتضي تحمل الأجهزة الأمنية الحكومية كامل المسؤولية في اكتشاف كافة الجرائم، ومن بينها الجرائم المعلوماتية، ومن هنا ألزمت اتفاقية بودابست 2001 الدول الأعضاء بضرورة تبني الإجراءات

---

(136) – حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراة، كلية القانون، جامعة عين شمس، 2005، ص 410.

(137)– محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الألي والأنترنت، بحث مقدم في الحلقة العلمية بعنوان " الإنترنت والإرهاب" المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، دبي، 2008، ص 32.

(138) – محمد الأمين البشري، التحقيق في جرائم الأنترنت، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، 2000، 107.

(139)– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 81.

التشريعية وأية إجراءات أخرى ترى أنها ضرورية وفقاً لقانونها الداخلي من أجل إنشاء وتأسيس سلطات متخصصة في مجال التقنيات والإجراءات الجنائية النوعية في مجال الجريمة المعلوماتية. وانطلاقا من ذلك بادرت مختلف الدول إلى إنشاء وحدات متخصصة في مجال البحث والتحري عن الجريمة المعلوماتية داخل الأجهزة الحكومية. فعلى سبيل المثال أنشأت مصر على مستوى وزارة الداخلية إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، وبالمثل في دولة الإمارات العربية المتحدة تم إنشاء الخط الساخن والإبلاغ عنها في دولة الإمارات عبر منصة

. (eCrime) (www.ecrime.ae)

الفرع الثالث – المعوقات التي تكون بسبب الجهات المتضررة وصعوبة تحديد هوية الجاني:

أولاً – المعوقات التي تكون بسبب الجهات المتضررة:

قد تكون الجهات المتضررة من الجريمة المعلوماتية سبباً في عدم الوصول إلى الدليل لإثبات الجريمة، وذلك للأسباب الآتية:

1- تتعمد أغلب الشركات والأشخاص إلى الصمت والتستر على الجريمة المعلوماتية وعدم إبلاغ الجهات المختصة، وهو ما يكون غالباً في جرائم الابتزاز الإلكتروني، وهذا يؤدي إلى عدم التعاون مع السلطات المختصة لمكافحة هذا النوع من الجرائم[140].

2- يؤدي الاستثمار في نظم المعلومات إلى التسابق بين الشركات، مما يدفعها في مقابل تحقيق الربح إلى تبسيط الإجراءات وتسهيل استخدام البرامج وملحقاتها وزيادة المنتجات، واقتصار تركيزها على تقديم الخدمة في مقابل إهمال الجانب الأمني، فبعض الشركات لا تطلب من المشتركين هويتهم عند الاشتراك في خدمة الإنترنت مما يحول دون معرفة هوية المستخدم في

(140) – خالد حسن أحمد، جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دار الفكر الجامعي، 2019.

حالة البحث والتحري[141].

ثانياً- صعوبة تحديد هوية الجاني:

أغلب المعوقات التي تواجه الوصـــول إلى الدليل الرقمي تتمثل في أن المجرم المعلوماتي يعمل على إخفاء هويته للحيلولة دون تعقبه وكشـــف أمره، حتى تظل أعماله الإجرامية بعيدة عن علم السلطات المعنية بمكافحة الجريمة.

وتعد مسـألة صـعوبة تحديد هوية مرتكب الجريمة المعلوماتية إحدى المشـاكل التي تطرح عند الحديث عن مكافحة الجريمة المعلوماتية. حيث يتميز المجرم المعلوماتي بالقدرات الفنية والتقنية العالية التي تسمح له بفرض سياج أمني على أفعاله غير المشروعة قبل ارتكابه لها، مما يزيد من صـــعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه. ويتم ذلك من خلال ترميز أو تشـفير المعلومات المخزنة إلكترونياً والمنقولة عبر شـبكات الاتصـال، بحيث يستحيل على غيره الاطلاع عليها، وهذا يشكل عائقا أمام سلطات البحث والتحقيق[142].

وقد أثير هذا الموضوع في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو عام 2000 حيث تناول موضوع عدم إمكانية البنية التحتية للإنترنت من التوصل إلى تحديد شخصية مرتكب الجريمة أو المصدر لها، وإن كانت توفر إمكانية التعرف فقط على عنوان ورقم الحاسوب المرتبط بالإنترنت والمستعمل كوسيلة لارتكاب الجريمة عن طريق عنوان (IP) الذي يشير إلى رقم يعين الحاسوب الموصل على الإنترنت، لكن في المقابل فإن هذا الرقم ليس موحداً على المستوي العالمي.

---

(141) – سعيدي سليمة جرائم المعلومات والشبكات في العصر الرقمي، مرجع سابق، ص 341.

(142) – خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الإسكندرية، 2018، ص 119.

ويزداد الأمر صـــعوبة حينما تكون المعلومات المحملة في عناوين (IP) غير حقيقية، وهذا ممكن في حال اسـتخدام الحزم المعلوماتية عنوان (IP) زائف بحيث يظهر أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاء من جهاز كمبيوتر أخر[143].

وقد ذهب جانب من الفقه الجنائي إلى أن مسألة عدم معرفة شخصية وهوية الفاعل الذي يقوم بالعمل الإجرامي، هي مسـألة نسـبية حيث أنه لا يوجد تجهيل بالمعني الصـحيح بالنسـبة لشـبكة المعلومات، لأن الفاعل أثناء تنقله في طرقات الإنترنت يترك آثار، ومن خلالها يمكن للمحققين الوصـول إليه، فالأمر كله متروك لفطنة جهاز التحقيق من خلال الاسـتناد إلى فكرة الدلائل الكافية وما ينبثق عنها من شـبهات[144]. إضـافة إلى أنه لو كان الحاسـوب الذي تم من خلاله ارتكاب الجريمة المعلوماتية هو حاسوب شخصي، فإن الأمر في هذه الحالة يستوجب ضبط الجهاز وسؤال صاحبه إذا كان قد استخدم أحد أخر الحاسب المذكور أو كان الجهاز موجود في شركة أو مكتب.

ويلاحظ أن هذا الإجراء من شـأنه توفير الشـفافية بالنسـبة للخدمات الموضـوعة تحت تصـرف الجمهور، ويسـاعد على سـهولة تحديد هوية الجاني، إضـافة إلى تحديد هوية المشـتركين بشـبكات المعلومات لتسـهيل عملية الضـبطية في حال وقوع أي مخالفة، بحيث يجب على مؤدي الخدمة، أن يكون قادراً على تقديم بيانات شخصية عن زبائنه في إطار التحقيقات عندما يطلب منه ذلك[145].

(143) – محمد علي سويلم، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية، مرجع سابق، ص151.

(144) – المرجع السابق، ص 154.

(145) – صالح أحمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في إطار اتفاقية بودابست، 2017.

ثالثًا- قيام المجرم المعلوماتي باتخاذ أساليب أمنية وتدابير الحماية الفنية التي تحول دون كشف أمره:

يمثل المجرم المعلوماتي بالنسبة للإجرام الطبيعي شخصية مستقلة قائمة بذاتها، فهو من جهة مجرم ذكي، ومن جهة أخرى إنسان اجتماعي بطبعة[146]، ناهيك عن معرفته التقنية الواسعة التي تمكنه من إحاطة جريمته بأساليب أمنية، وتدابير الحماية الفنية، التي تحول دون كشف أمره، وتمنع جهات الاستدلال والتحقيق من الوصول إلى الدليل. فالمجرم المعلوماتي غالباً ما يضرب سياجاً أمنياً على أفعاله غير المشروعة قبل ارتكابها وذلك باستخدام كلمات المرور السرية، وترميز البيانات المخزنة إلكترونياً والمنقولة عبر شبكات الاتصال، وتشفيرها بشكل يجعل من المستحيل على سلطات البحث والتحري تعقب آثار الجريمة واستخلاص الدليل دون الحصول على هذه الرموز والشيفرات[147].

رابعاً- عدم قيام المجني عليه بالإبلاغ عن الجريمة المعلوماتية:

عدم قيام المجني عليهم بالإبلاغ عن الجاني أو الجريمة من أهم الأسباب التي تحول دون اكتشاف الجريمة المعلوماتية، فإذا كان غالبًا ما يكون مرتكب الجريمة المعلوماتية شخصاً طبيعياً، فإن المجني غالبًا ما يكون شخص معنوي كالبنوك والشركات الكبرى والمؤسسات الحكومية والوزارات والمنظمات والهيئات المالية وغيرها من الأشخاص الاعتبارية، التي تعتمد في إنجاز أعمالها على الحاسب الآلي[148]. وأكثر الفئات تضرراً من الجريمة المعلوماتية:

---

(146) – محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1998، ص 24.

(147)- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2002، ص 115 .

(148)- قاسم محمد عبد الله، الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، 2010، ص 148.

1. المؤسسات المالية والجهات الحكومية

حيث تعتبر هذه القطاعات من أكثر الأماكن اســـتهدافا نظراً لملاءتها المالية، ومن أهم هذه المؤســـســـات المالية البورصـــة، ذلك أن أي تعطيل لحركة البورصـــة يؤثر بدرجة كبيرة على حجم التعاملات المالية ليس فقط بالأشـــخاص العاديين بل يصـــل الأمر إلى التعاملات المالية بين الدول[149].

وقد تعدت حدود الجرائم المعلوماتية القطاعات المدنية إلى القطاعات الخاصة بالقوات المسلحة نظراً لطبيعة وأهمية المعلومات التي تحتويها تلك القطاعات، مما اســتتبع ظهور حرب من نوع جديد وهي الحرب المعلوماتية فتعاظم دور النظم المعلوماتية في هذا المجال[150].

2. الأشخاص الطبيعيون:

يتعرض كثير من الأشـخاص الطبيعيين لأشـكال من الجريمة المعلوماتية؛ خاصـة الأشـخاص الذين يحفظون أسرارهم التجارية وأعمالهم وشؤونهم داخل الحاسب الخاص بهم. وينبغي لقيام الجريمة المعلوماتية هنا أن يكون الشـــخص العادي –المجني عليه– من بين الأشـــخاص الذين قد ينجذب إليهم الجناة، كأن يكون ذا منصب سياسي رفيع أو رجل أعمال مرموق أو صاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أو الاجتماعية أو العسكرية[151].

ويلاحظ أن تحديد نطاق خاص يضم فئات المجني عليهم في الجرائم المعلوماتية يعد أمراً صعباً لأن المجني عليهم في هذه الجرائم غالباً ما يكتشـفون الجرائم بعد حصـولها، الأمر الذي يدفعهم في

(149)– محمد علي سويلم، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية، مرجع سابق، ص155.

()– 150خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 150.

(151) – محمد الدسوقي، الحماية الدولية لسرية المعلومات، دار الفكر العربي، 2003، ص 56.

غالب الأحيان إلى السكوت أو الإذعان لها، وتفضيل الموقف السلبي عن القيام بالتصريح عن تعرض أجهزتهم ومعلوماتهم التي يفترض فيها الأمان والسرية إلى الدخول غير المشروع والانتهاك[152]،الأمر الذي يشكل بحد ذاته سبباً في ازدياد معدل الجرائم المعلوماتية وصعوبة اكتشافها أو الحد منها، ومن ثم كثرة مشكلاتها على الصعيدين القانوني والعملي.

وسعياً نحو تقليل هذه الظاهرة، فرضت بعض الدول التزاماً على عاتق المجني عليهم بالإبلاغ عن هذه الجرائم بمجرد علمهم بوقعوها، وجعلت أي تقصير أو إخلال بهذا الالتزام يعرض صاحبه إلى عقوبات جنائية. إلا أن هذا الحل تعرض لانتقادات عديدة من الفقه والقضاء الدوليين، استنادا إلى أنه ليس من المقبول أبداً تحول المجني عليه إلى مجرم يتم معاقبته بمجرد عدم تبليغه عن الجريمة التي وقع ضحية لها، في حين يبقي المجرم الحقيقي دون عقاب[153]. انطلاقا من ذلك سعت بعض الدول إلى وضع سياسات تشجع وتحفز الأشخاص على التبليغ عن وقوع الجرائم المعلوماتية بعد اكتشافها، من خلال تنظيم حملات توعية لبث روح المسؤولية في المجني عليهم، وقد تتخذ هذه الإجراءات شكل تدابير إدارية تشترط من خلالها على الجهات المجني عليها التبليغ عن الجريمة لكي تستفيد من بعض الحقوق والامتيازات.

بناء على ما سبق يمكن إجمال أبرز الصعوبات التي تعترض الإثبات والتحقيق في جرائم الابتزاز الإلكتروني في الآتي:

1. **البعد الدولي:** يجري النفاذ إلى أنظمة الحاسوب في أحد البلدان ويتم التلاعب بالبيانات في بلد

(152) – سامي الشوا، الغش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، 2003، ص 158.

(153)–هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، 1994، ص438.

آخر، وتســـجل النتائج في بلد ثالث، غير أنه يمكن تخزين أدلة الجريمة الإلكترونية في جهاز حاســوب موجود في بلد غير الذي ارتكب فيه المجرم فعله، بالتالي يســتطيع المجرم الإلكتروني إخفاء هويتـه، ونقل المواد من خلال قنوات موجودة في بلدان مختلفة، وفي قارات مختلفة قبل الوصـول إلى المرسل إليهم، نتيجة القدرة على التنقل إلكترونياً من شبكة إلى شبكة أخرى والنفاذ إلى قواعد البيانـات في قارات مختلفة، بحيث تقع الجريمـة في عدة دول وتحكمها عدة قوانين وقواعد معنية بذلك، مما يشكل تحدياً أمام الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها[154].

2. مهارة التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مدركة بالعين المجردة.
3. تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال.
4. سهولة محو الأدلة في وقت قصير.

انطلاقا من ذلك فإن إعداد رجال الضـــبط الجنائي وقضـــاة الحكم، للبحث عن أدلة الإثبات في ميدان الجرائم الإلكترونية، يكتسـب أهمية بالغة في عالم "المعلومات وشـبكات الكمبيوتر" القائم على تقنية الاتصـــالات والتوصـــيلات والوســائط الإلكترونية، حيث لا تســتطيع ســلطات البحث والتحري والتحقيق تطبيق الإجراءات التقليدية على غالبية جرائم تقنية المعلومات. لذلك لابد من تدريب وتكوين رجال الضـبط الجنائي والتحقيق والقضـاة المختصـين بجرائم تقنية المعلومات فيما يتعلق بالأسـاليب الفنية المستخدمة في ارتكاب الجريمة وفيما يتعلق بالكشف عنها، والقرائن والدلائل والأدلة المستحدثة

(154)- بندر عقاب الدرويش، الإثبات في رائم الإرهاب الإلكتروني" دراســـة مقارنة"، عمان، الأردن، 2017، ص 122، نقلا من الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية، ضـــمن أعمال الندوة الإقليمية حول الجرائم المتصـــلة بالكمبيوتر، 19-20 يونيو 2007، المملكة المغربية، ص 119.

في مجال إثباتها، وكيفية معاينتها والتحفظ عليها وفحصـــها فنيا، مع ضـــرورة تدريب القضـــاة على معالجة هذا النوع من القضايا لتمكينهم من الفصل فيها.

وتكمن الصعوبة الأساسية التي تعترض سلطات البحث والتحري في ميدان الجرائم المعلوماتية، في أن مرتكبي هذه الجرائم لا يتركون في غالب الأحيان آثاراً تدل على ارتكابهم لهذه الجرائم؛ إذ تكون المعلومات محفوظة تحت رقم ورمز ســري ومشــفرة كلياً؛ إذ يصــعب الولوج إليها أو معرفتها، وإقامة الدليل ضد هؤلاء الجناة، لذا لابد من خلق وحدات خاصة تكون مهمتها الأساسية مراقبة وتتبع الشبكة عن طريق الإبحار فيها، فالمراقبة القبلية قد تعطي نتائج هامة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها[155].

(155)- عبد الرزاق ســندالي، التشــريع المغربي في مجال الجرائم المعلوماتية، ضــمن أعمال الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر، 19-20 يونيو، المملكة المغربية، ص 71-72.

المبحث الثاني – الجزاءات المقررة لجرائم الابتزاز الإلكتروني:

تنص المادة (16) من (المرســـوم بقانون اتحادي رقم (5) لســـنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات). على أن: "يعاقب بالحبس مدة لا تزيد على ســنتين والغرامة التي لا تقل عن مائتين وخمســين ألف درهم ولا تجاوز خمســمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شـــخص آخر لحمله على القيام بفعل، أو الامتناع عنه، وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون العقوبة السجن مدة لا تزيد على عشـــر ســـنوات إذا كان التهديد بارتكاب جناية أو بإســـناد أمور خادشـــه للشـــرف أو الاعتبار"[(156)].

يستفاد من النص أعلاه أن المشرع جرم التهديد أو الابتزاز الذي يحدث باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات؛ حيث يستغل بعض الأشخاص قدرتهم على استخدام تقنية المعلومات في ارتكاب أعمال غير مشروعة، كتهديد وابتزاز الأشخاص، وقد يكون ذلك من خلال الإنترنت أو البريد الإلكتروني أو الهواتف النقالة. ويقع التهديد أو الابتزاز بقصـــد حمل المجني عليه على القيام بفعل معين أو الامتناع عنه، وقد يكون التهديد أو الابتزاز جسيما بارتكاب جناية أو بإسناد أمور خادشه

(156)– نص المشرع على جريمة التهديد أيضا في قانون العقوبات الاتحادي على النحو التالي:
المادة (351) يعاقب بالسجن مدة لا تزيد على سبع سنوات من هدد آخر كتابة أو شفاهه بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره أو بإسناد أمور خادشه بالشرف أو إفشائها، وكان ذلك مصحوبا بطلب أو بتكليف بأمر أو الامتناع عن فعل أو مقصودا به ذلك.
المادة (352) يعاقب بالحبس من هدد آخر بارتكاب جناية ضد نفسه أو ماله أو ضد نفس أو مال غيره أو بإسناد أمور خادشه للشرف أو الاعتبار أو إفشائها في غير الحالات المبينة في المادة السابقة.
المادة (353) كل من هدد آخر بالقول أو بالفعل أو بالإشارة كتابة أو شفاهه أو بوساطة شخص آخر في غير الحالات المبينة في المادتين السابقتين يعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على عشرة آلاف درهم.

للشرف أو الاعتبار. هذا وقد تضمنت المادة أعلاه صورتين من التجريم:

- صورة الجريمة غير المشددة، وتتعلق بتهديد أو بابتزاز شخص آخر لحمله على القيام بالفعل أو الامتناع عنه باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.
- صورة الجريمة المشددة، وتتعلق بالتهديد بارتكاب جناية أو بإسناد أمور خادشه بالشرف أو الاعتبار.

وبناء على ما سبق سيجري تقسيم هذا المبحث إلى مطلبين، يتناول المطلب الأول العقوبات المقررة لجريمة الابتزاز الإلكتروني بصورتها البسيطة، بينما يتناول الثاني العقوبات المقررة لجريمة الابتزاز الإلكتروني بصورتها المشدّدة. استنادًا لما سبق سوف يقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول– الجزاءات المقررة لجريمة الابتزاز الالكتروني بصورتها البسيطة.

المطلب الثاني – الجزاءات المقررة لجريمة الابتزاز الإلكتروني في صورتها المشدّدة.

المطلب الأول- العقوبات المقررة لجريمة الابتزاز بصورتها البسيطة:

تقع جريمة الابتزاز الإلكتروني تامة، عندما يؤدي المجني عليه المقابل المطلوب منه، ويستحق الجاني العقوبة المقررة للفعل، وقد تتوافر ظروف يترتب عليها تشديد العقوبة المقررة للإبتزاز الإلكتروني.

أولا- العقوبات في التشريع الاتحادي:

تنص المادة (16/ 1) من **(المرســـوم بقانون اتحادي رقم (5) لســـنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات)**. على أن: "يعاقب بالحبس مدة لا تزيد على ســـنتين والغرامة التي لا تقل عن مائتين وخمســـين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات. وتكون العقوبة...".

يتضح من النص أعلاه أن المشرع فرض على جريمة تهديد أو ابتزاز الأشخاص باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات للقيام بفعل أو الامتناع عنه في صورتها البسيطة عقوبة الحبس مدة لا تزيد على ســـنتين والغرامة التي لا تقل عن مائتين وخمســـين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين. ويلاحظ أن المشرع وضع حدا أقصى لعقوبة الحبس، وترك الحد الأدنى للقواعد العامة المنصـــوص عليها في المادة (69) من قانون العقوبات؛ أي لا يقل عن شـــهر، بيد أن المشـــرع خرج في مقدار الغرامة على القاعدة المقررة في المادة (71) من قانون العقوبات التي حددت عقوبة الغرابة في الجنح بين ألف وثلاثمئة ألف درهم[157]. حيث قرر الحد

(157)- نص المادة 71 – عقوبة الغرامة: هي إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، ولا يجوز أن تقل الغرامة عن ألف درهم ولا أن يزيد حدها الأقصى على مليون درهم في الجنايات وثلاثمائة ألف درهم في الجنح، وذلك كله ما لم ينص القانون على خلافه.

الأدنى لعقوبة الغرامة لجريمة الابتزاز الإلكتروني بصورتها البسيطة بمبلغ مئتين وخمسين ألف درهم، فيما رفع حدها الأقصى إلى خمسمئة ألف درهم. وللقاضي سلطة تقديرية في الجمع بين عقوبتي الحبس والغرامة أو الحكم بإحداهما فقط.

وأضاف المشرع إلى العقوبة الأصلية عقوبات فرعية؛ حيث نصت المادة (41) **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات)** على عقوبة المصادرة، ومحو أو إعدام المعلومات أو البيانات وإغلاق المحل أو الموقع الذي ترتكب فيه الجريمة. ونصت المادة (42) **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات)**. على جواز إبعاد الأجنبي الذي يحكم عليه بالإدانة في جريمة الابتزاز الإلكتروني في صورتها البسيطة باعتبارها جنحية الوصف، حيث جاء نص المادة (42) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات)** وفق الآتي: (مع مراعاة حكم الفقرة الثانية من المادة (121) من قانون العقوبات تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجناية في أي من الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها)، حيث يستفاد من هذا النص وبمفهوم المخالفة أن تدبير الإبعاد جوازي في جرائم الابتزاز الإلكتروني إذا لم تكن بوصف الجناية أو من الجنح الواقعة على العرض. يضاف إلى ذلك أنه لا يجوز الحكم بتدبير الإبعاد على الأجنبي الذي يرتكب جريمة الابتزاز الإلكتروني إذا كان زوجا أو قريبا من الدرجة الأولى لمواطن ما لم تكن الجريمة من الجرائم الماسة بأمن الدولة، استنادًا إلى الفقرة الثالثة من المادة (121) من قانون العقوبات التي تنص على أن: (استثناء من نص

الفقرتين الســـابقتين ومن أي نص ورد في أي قانون آخر، لا يجوز الحكم على الأجنبي بالإبعاد إذا كان زوجًا أو قريبا بالنسـب من الدرجة الأولى لمواطن، وذلك مالم يكن الحكم صـادرا في جريمة من الجرائم الماسة بأمن الدولة).

كما نصت المادة (43) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات)**. على مجموعة من التدابير الأخرى التي يجوز للمحكمة الحكم بها، كتدبير وضـــع المحكوم عليه تحت الإشـــراف أو المراقبة، وتدبير حرمانه من اسـتخدام أي شـبكة معلوماتية، أو نظام معلومات إلكتروني، أو أي وسـيلة تقنية معلومات أخرى، وتدبير وضـعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسـبة، ونصت المادة (48) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسـنة 2018 بشـأن مكافحة جرائم تقنية المعلومات)**. على تطبيق أي عقوبة أشـد ينص عليها قانون العقوبات أو أي قانون آخر [158].

ثانيًا– العقوبات في التشريع المصري:

أصـدر المشرع المصـري قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م، غير أنه لم ينص على تجريم الابتزاز الإلكتروني بصـورة مباشـرة وشـاملة؛ حيث تطرق لبعض صـوره في المادة 25 من القانون المذكور بنصها على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسـين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادىء أو القيم الأسـرية في المجتمع المصـري أو انتهك حرمة الحياة الخاصـة، أو

(158) – عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة" المرسوم بالقانون الاتحادي رقم 5 لسنه 2012"، الكتاب الأول، 2014، ص 179.

أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارا أو صورا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة"[159].

ورغمًا عن أن المشرع المصري لم يذكر لفظ الابتزاز في قانون العقوبات، فإنه عاقب على أفعال تعد ابتزازا منها المادة 327 منه، التي تنص على أن: "كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو بالسجن المؤبد أو المؤقت أو بإفشاء أمور أو نسبة أمور مخدشة 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 آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوبا بتكليف بأمر أم لا.

وكل تهديد، سواء أكان بالكتابة أم شفهيا بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه".

وتنص الفقرات الثانية، والثالثة، والرابعة من المادة 309 مكررا (أ) من قانون العقوبات المصري على أن: "يعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه.

()- 159تامر محمد صالح، الابتزاز الالكتروني، مرجع سابق، ص 186.

ويعاقب بالســـجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته".

ويلاحظ الباحث هنا أن المشــرع المصــري فرق بين الابتزاز بالوســائل المكتوبة، والابتزاز بالوسـائل الشـفهية، ولم يعاقب على التهديد الشـفهي إلا إذا تم من خلال وسـيط، كما أنه سـاوى في العقوبة بين التهديد المقترن بطلب أو تكليف بأمر، وبين التهديد المجرد؛ حيث من الملائم التفرقة في العقاب بينهما، وهذا أمر محل نظر بالنسـبة لجميع التشـريعات المذكورة؛ حيث سـاوت بين التهديد المجرد، والابتزاز، وإن كانت فرقت في العقاب حسب مضمون الابتزاز[160].

ويلاحظ الباحث أيضًـا أن التشريعين الاتحادي والمصري بصدد الابتزاز الإلكتروني قد جمعا بين العقوبات المالية والســالبة للحرية، أو حق القاضـــي في الاختيار من بينهما، مما يكشــف عن إدراكهما لخطورة هذه الأفعال، كما عاقبا على الابتزاز أيا كانت صورته تقليديا أم الكترونيا.

كما نص المشــرع المصــري على المصــادرة، والرد كإحدى العقوبات التبعية المقررة لجريمة الابتزاز الالكتروني؛ وفيما يلي بيان ذلك[161]:

1- المصادرة:

تنص الفقرات الثانية، والثالثة، والرابعة من المادة 309 مكررا (أ) من قانون العقوبات المصري على أن: "ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصــل عليها بإحدى الطرق المشــار إليها لحمل شــخص على القيام بعمل أو الامتناع عنه. ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة

(160)- المرجع السابق، ص 188

()161- المرجع نفسه، ص 189

وظيفته.

ويحكم في جميع الأحوال بمصـــادرة الأجهزة وغيرها مما يكون قد اســـتخدم في الجريمة، أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها".

وقد قرر ذلك الفصل الثامن من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018م في المادة (1/38) المصـادرة بقوله: "مع عدم الإخلال بحقوق الغير حسـن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد اسـتخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها".

ويقصد بالشخص حسن النية كل شخص أجنبي عن الجريمة، أي لم يسهم فيها بأي صورة من الصـور سواء أكان فاعلا أصـليا أم شـريكا، فحسـن النية يتوافر لدى الشـخص إذا لم يكن عالما بأن الشيء الذي تعلق به حقه قد تحصل أو استخدم أو أعد للاستعمال في ارتكاب جريمة.

والعلة من مصـادرة جميع الأموال المتحصـلة من مثل هذه الجريمة تتناسـب جزئيا مع الباعث من الجريمة الذي يكون مالياً غالبا[162].

2- الرد:

تنص المادة (3/41) من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018 م على: "... وجوب القضاء برد المال المتحصل من الجرائم المنصوص عليها في هذا القانون".

---

(162)- رامى متولى القاضـي، الحماية الجنائية للمرأة من الاتجار بها في ضـوء أحكام القانون رقم 14 لسنة 2010م، المؤتمر الدولي السـنوي الثامن عشـر لكلية الحقوق، جامعة المنصـورة، تحت عنوان " المرأة والقانون"، في الفترة من 15-16 إبريل 2018م، ص 44.

المطلب الثاني – الجزاءات المقررة لجريمة الابتزاز الإلكتروني في صورتها المشدّدة:

تتمثل أغلب الظروف المشددة لعقوبة الابتزاز الالكتروني في ظرفين ينحصر أولهما في مضمون التهديد بوصفه وسيلة للابتزاز الإلكتروني؛ وهما: التهديد بالعنف، والتهديد بالإفشاء والتشهير، ويتمثل ثانيهما في أطراف التهديد؛ وبناء على ما سبق يتناول الباحث المطلب كالأتي:

– موقف المشرع الاتحادي:

تناولت المادة (16/ 2) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لســـنة 2018 بشـــأن مكافحة جرائم تقنية المعلومات)** عقوبة جريمة الابتزاز الإلكتروني في صورتها المشدّدة حيث نصت على أن: (وتكون العقوبة السجن مدّة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار).

استنادا إلى النص أعلاه اعتبر المشرع التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار ظرفا مشــددا للعقوبة يدخل هذه الجريمة في زمرة الجنايات؛ حيث حدد العقوبة بالســجن مدة لا تزيد على عشر سنوات.

ويمكن أن يوجه الجاني تهديده بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار إلى المجني عليه أو إلى شـــخص آخر ممن تربطه بهم علاقة وثيقة، ومن أمثلة ذلك، تهديده بإيذاء أحد أبنائه، لأن علة التجريم متحققة في هذه الحالة. ويلزم لقيام الجريمة في صـــورتها المشـــددة توافر عنصرين:

العنصـر الأول: ارتكاب الجاني جريمة التهديد أو الابتزاز التي نصـت عليها الفقرة الأولى من المادة (16) **من (المرســـوم بقانون اتحادي رقم (5) لســـنة 2012 المعدل بالقانون الاتحادي رقم (2)**

لسـنة 2018 بشـأن مكافحة جرائم تقنية المعلومات). أي التهديد باسـتخدام شـبكة معلوماتية أو بإحدى وسائل تقنية المعلومات[163].

العنصـر الثاني: التهديد بارتكاب جناية أو إسـناد أمور خادشـه للشـرف أو الاعتبار؛ وهذا العنصـر يتجسد في حالتين، الأولى هي التهديد بارتكاب جناية، والحالة الثانية هي إسناد أمور خادشه للشرف أو الاعتبار.

الحالـة الأولى- التهديـد بـارتكـاب جنـايـة: يجب أن يكون التهديد بارتكاب جناية أي التهديد بارتكاب جريمة نص قانون العقوبات على أنها جناية، وقد عرف قانون العقوبات الجنايات في المادة (18) الجناية هي الجريمة المعاقب عليها بإحدى العقوبات الآتية:

1. أية عقوبة من عقوبات الحدود أو القصاص فيما عدا حدي الشرب والقذف.
2. الإعدام.
3. السجن المؤبد.
4. السجن المؤقت.

اسـتنادا إلى ما سـبق، يتوافر التشـديد عندما يكون التهديد بارتكاب جناية، ومثال ذلك تهديد الشـــخص المجني عليه من خلال البريد الإلكتروني، أو من خلال الهاتف المحمول، بالقتل العمد المنصـــوص عليه في المادة (332) من قانون العقوبات الاتحادي، أو بالحريق العمد المنصـــوص عليه في المواد (304) ،(305) ، (306) من قانون العقوبات الاتحادي[164]، أو بخطف أحد أبنائه

(163) – المرجع السابق، ص 181.

(164)- المواد (304و305و306) من قانون العقوبات الاتحادي ونصوصها على النحو التالي:

المنصوص عليه في المادة (344) من قانون العقوبات الاتحادي[165]، فهذه الجرائم تدخل في نطاق الجنايات.

الحالة الثانية- التهديد بإسناد أمور خادشه للشرف أو الاعتبار:

يقصد بهذه الحالة نسبة أمور إلى المجني عليه تمس سمعته وشرفه واعتباره، وهي الأمور التي لو صدقت لأوجب توقيع العقاب على من أسندت إليه أو أوجبت احتقاره لدى أهل وطنه[166].

مثال ذلك: أن يقوم الجاني بتهديد المجني عليه بإرسال رسالة إليه بالبريد الإلكتروني للتشهير به، أو إذاعة أمور تمس سمعته، وقد يختلق الجاني مثل هذه الأمور؛ حيث إنها لم تحدث في الحقيقة، أو قد يعلم الجاني هذه الأمور عن الشخص المجني عليه، ويريد إذاعتها ليسيء لشرفه أو اعتباره. وسواء اختلق الجاني هذه الأمور أو أسندها للمجني عليه، فإنه بذلك يسند أمورا لو كانت

المادة (304) يعاقب بالسجن مدة لا تقل عن سبع سنوات كل من أضرم النار عمدا في أبنية أو مصانع أو ورش أو مخازن أو أي عمارات آهلة أو غير أهلة واقعة في مدينة أو قرية، أو في مركبات السكة الحديدية أو عربات نقل شخصا أو أكثر أو تابعة لقطار فيه شخص أو أكثر من شخص أو سفن ماخرة أو راسية في إحدى.

(165)- المادة (344) من قانون العقوبات الاتحادي الإماراتي ويجري نصها على النحو التالي: "يعاقب بالسجن المؤقت من خطف شخصا أو قبض عليه أو حجزه أو حرمه من حريته بأية وسيلة بغير وجه قانوني، سواء أكان ذلك بنفسه أو بوساطة غيره، وتكون العقوبة السجن المؤبد في الأحوال الآتية:

1. إذا حصل الفعل بانتحال صفة عامة أو ادعاء القيام أو التكليف بخدمة عامة أو الاتصال بصفة كاذبة.
2. إذا ارتكب الفعل بطريق الحيلة أو صحبه استعمال القوة أو التهديد بالقتل أو بالأذى الجسيم أو أعمال تعذيب بدنية أو نفسية.
3. إذا وقع الفعل من شخصين فأكثر أو من شخص يحمل سلاحا.
4. إذا زادت مدة الخطف أو القبض أو الحجز أو الحرمان من الحرية على شهر.
5. إذا كان المجني عليه أنثى أو حدثا أو مجنونا أو معتوها.
6. إذا كان الغرض من الفعل المكسب أو الانتقام أو الاغتصاب المجني عليه أو الاعتداء على عرضه أو إلحاق أذى به أو حمله على ارتكاب جريمة.
7. إذا وقع الفعل على موظف عام أثناء تأديته وظيفته أو بسبب ذلك. وإذا أفضى الفعل إلى موت المجني عليه كانت العقوبة الإعدام أو السجن المؤبد ويعاقب بالعقوبة المقررة للفاعل الأصلي كل من توسط في ارتكاب أية جريمة من الجرائم المشار اليها في هذه المادة، وكذلك كل من أخفى شخصا مخطوفا مع علمه بذلك".

(166) - فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، الطبعة الثالثة 2012م.

صـــادقة لأوجبت عقابه بالعقوبات المنصـــوص عليها في القانون، أو ترتب عليها احتقاره لدى أهل وطنه وذويه.

وقد ساوى المشرع بين التهديد بارتكاب جناية والتهديد بإسناد أمور خادشه للشرف أو الاعتبار من حيث التشـــديد. ولا يقبل من الجاني أن يثبت صـــدق الأمور التي أســـندها إلى المجني عليه، فالعقاب المنصـــوص عليه لهذه الجريمة يوقع على الجاني، ســـواء كانت الأمور موضـــوع التهديد صـحيحة أو غير صـحيحة. وإسـناد الأمور الخادشـة للشـرف أو الاعتبار من خلال شـبكة الإنترنت بطريقـة علنيـة، قـد يؤدي إلى تكييف الواقعـة على أنهـا جريمـة قـذف، ومن ثم لا حـاجـة إلى النص عليها، ويمكن تطبيق عقوبة جريمة القذف المنصوص عليها في قانون العقوبات على الحالة المتعلقة بإســناد الأمور الخادشــة للشــرف أو الاعتبار من خلال شــبكة معلوماتية أو إحدى وســائل تقنية المعلومات؛ حيث تعتبر من وسائل العلنية، ولكن النص واجب التطبيق هو نص المادة (16/ 2) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشـــأن مكافحة جرائم تقنية المعلومات)؛** لأن الجريمة مرتكبة بوســيلة إلكترونية والعقوبة المقررة في المرسوم بقانون هي الأشد. فمتى تضمن فعل التهديد إحدى الحالتين السابقتين، كان النص القانوني الواجب التطبيق هو نص المادة (16/ 2) المشار إليها. ويمكن أن يوجه الجاني التهديد إلى شخص طبيعي أو إلى شــخص معنوي [167]، وينبغي أن يرد التهديد في عبارات صــريحة، لذلك يجب على المحكمة أن تبين في حكم الإدانة عبارات التهديد ووسيلته، حتى تستطيع محكمة النقض أو المحكمة الاتحادية العليا أن تتأكد أن ما ورد بتلك العبارات، وبهذه الوسيلة، تتوافر معه أركان جريمة التهديد

(167) – محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق ص1112.

التي يتطلبها القانون.

وقد حدد المشـرع عقوبة جريمة التهديد بارتكاب جناية أو بإسـناد أمور خادشـه للشـرف أو الاعتبار، بالسجن مدة لا تزيد على عشر سنوات، أي أن المشرع شدد العقوبة، وجعلها عقوبة وحيدة ولم ينص على عقوبة الغرامة. ويلاحظ أن المشرع حدد الحد الأقصى للسجن، وترك الحد الأدنى كما هو مقرر في القاعدة العامة التي قررتها المادة (68) من قانون العقوبات الاتحادي بأن لا يقل عن ثلاث سنوات، وللقاضي سلطة تقديرية بين الحدين المنصوص عليهما في المادة سالفة الذكر.

ويتضـح من العقوبة أن المشـرع اعتبر الجريمة جناية حيث عاقب عليها بالسـجن مدة لا تزيد على عشـر سـنوات. ويضـاف إلى العقوبة الأصـلية عقوبات فرعية؛ حيث نصـت المادة (41) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشـــأن مكافحة جرائم تقنية المعلومات)** على المصـــادرة، ومحو أو إعدام المعلومات أو البيانات، وإغلاق المحل أو الموقع الذي ترتكب فيه الجريمة.

كما نصت المادة (42) **من (المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسـنة 2018 بشـأن مكافحة جرائم تقنية المعلومات)** على إبعاد الأجنبي الذي يحكم عليه بالإدانة، وهنا الإبعاد يكون وجوبيا نظرا لأن جريمة الإبتزاز الإلكتروني بوصـفها المشـدد تأخذ وصف الجناية حيث تنص المادة (42) من **(المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسـنة 2018 بشـأن مكافحة جرائم تقنية المعلومات)** على أن: (مع مراعاة حكم الفقرة الثانية من المادة (121) من قانون العقوبات تقضـي المحكمة بإبعاد الأجنبي الذي يحكم عليه في أي من الجرائم الواقعة على العرض، أو يحكم عليه بعقوبة الجناية في أي من

الجرائم المنصوص عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها). بيد أنه وكما سبقت الإشارة إليه فإن نص هذه المادة بصدد الإبعاد مقيد بنص الفقرة الثالثة من المادة (121) من قانون العقوبات التي تقضـــي بعد جواز إبعاد الأجنبي إذا كان زوجا أو قريبا من الدرجة الأولى لمواطن، ما لم يكن الحكم الصادر عليه بصدد جريمة من الجرائم الماسة بأمن الدولة.

ناهيك عن أن المادة (43) **من المرســـوم بقانون اتحادي رقم (5) لســـنة 2012 المعدل بالقانون الاتحادي رقم (2) لســنة 2018 بشــأن مكافحة جرائم تقنية المعلومات،** تضــمنت على مجموعة من التدابير التي يجوز للمحكمة الحكم بها كتدبير وضــع المحكوم عليه تحت الإشــراف أو المراقبة، وتدبير حرمانه من اســتخدام أي شــبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وســـيلة تقنية معلومات أخرى، وتدبير وضـــعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة، ونصت المادة (46) **من المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات،** " يعد ظرف مشدد استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم .

كما يعد ظرفا مشددا ارتكاب أي جريمة منصوص عليها في هذا المرسوم لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة".

وقد اســتحدث المرســوم الجديد هذه المادة التي اعتبرت وســيلة ارتكاب الجريمة ظرفا مشــدداً للعقاب، ففي حالة ارتكاب أي جرائم أخرى غير التي ورد النص عليها في هذا المرســوم ، من خلال استخدام شبكة المعلومات أو الإنترنت أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة

تقنية معلومات، فإن ذلك يعد ظرفا مشددة.

أما الجرائم التي ورد النص عليها في هذا المرسوم فعندما ترتكب لحساب أو لمصلحة دولة أجنبية أو أي جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، فإن ذلك يعد ظرفا مشدداً. وبالتالي تطبق القواعد العامة في التشديد التي تقررها المادة (103) من قانون العقوبات الاتحادي لدولة الإمارات[168] التي تنص على أنه "إذا توافر في الجريمة ظرف مشدد جاز للمحكمة توقيع العقوبة على الوجه الأتي:

أ- إذا كانت العقوبة المقررة أصلا للجريمة هي الغرامة جاز مضاعفة حدها الأقصى أو الحكم بالحبس.

ب- إذا كانت العقوبة المقررة أصلا للجريمة هي الحبس جاز مضاعفة حدها الأقصى.

ت-إذا كانت العقوبة المقررة أصلا للجريمة هي السجن المؤقت الذي يقل حده الأقصى عن خمس عشرة سنة جاز الوصول بالعقوبة إلى هذا الحد.

ث-إذا كانت العقوبة المقررة أصلا للجريمة هي السجن المؤقت الذي يصل إلى حده الأقصى جاز أن يستبدل بها السجن المؤبد.

ونصت المادة (48) **من المرسوم بقانون اتحادي رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (2) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات،** على تطبيق أي عقوبة أشد

(168)- عدل نص المادة (١٠٣) بموجب المادة الأولى من القانون الاتحادي رقم 2006/52.

ينص عليها قانون العقوبات أو أي قانون عقابي آخر[169]. حيث نصت المادة (48): "لا يخل تطبيق العقوبات المنصوص عليها في هذا المرسوم بأي عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر".

حلت المادة (48) محل المادة (26) من القانون القديم وهي بذات المضمون، ويجد الباحث تطبيقا لذلك في المادة (28) التي تنص على أنه يعاقب بالسجن المؤقت والغرامة التي لا تجاوز مليون درهم كل من أنشأ أو أدار موقع إلكتروني أو أشرف عليه أو استخدم معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد التحريض على أفعال أو نشر أو بث معلومات أو أخبار أو أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام.

وتنص المادة (197) مكرر من قانون العقوبات الاتحادي على أن: يعاقب بالسجن المؤقت كل من استعمل أية وسيلة من وسائل الإتصال أو وسائل تقنية المعلومات أو أية وسيلة أخرى في نشر معلومات أو أخبار أو التحريض على أفعال من شأنها تعريض أمن الدولة للخطر أو المساس بالنظام العام[170].

ويلاحظ الباحث على هذين النصين أن العقوبة المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات أشد من العقوبة المنصوص عليها في قانون العقوبات، فلو كان الفرض معكوسا،

---

(169) – عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة" المرسوم بالقانون الاتحادي رقم 5 لسنه 2012"، مرجع سابق، ص 191.

(170)– أضيفت بموجب المادة (2) من القانون الاتحادي رقم 2005/24 تاريخ 2005/12/24م.

أي أنه لو كانت العقوبة المنصـــوص عليها في قانون العقوبات أشـــد فإن النص الوارد في قانون العقوبات يكون الواجب التطبيق.

- موقف المشرع المصري:

شـــهد المجتمع المصـــري في الآونة الأخيرة تزايداً في ظاهرة أطلق عليها تعبير (الإبتزاز الإلكتروني) على نحو لم يكن مألوفاً من قبل في المجتمع بما تتضـــمنه تلك الظاهرة من ترويع للمواطنين وتهديد صارخ لأمنهم وسلامتهم فقد بات لزاماً على المشرع أن يتدخل لمواجهة تلك الظاهرة الخطيرة حفاظاً على أمن المجتمع وســـلامة أفراده. ومن هنا كان مشـــروع القانون المعروض والذي استهدف مواجهة تلك الظاهرة الخطيرة بتغليظ العقاب بعد أن تبين أن النصوص القائمة لم تعد كافية لتحقيق ما هو مستهدف من ردع من تسول له نفسه أن يقدم على ترويع المواطنين على هذا النحو. لذا يجد الباحث أن المشـرع المصـري شـدد العقاب على من يهدد آخر لحمله على شـيء بارتكاب جناية أياً كان نوعها، أو بإسـناد أمور خادشـة للشـرف والاعتبار، والحكمة من تخصـص هذا النوع الأخير من الجرائم يعود لخطورتها الاجتماعية، وما تحدثه من فرقة واضراب بالمجتمع.

وبناء عليه يجد الباحث أن المشـــرع المصـــري نص بالمادة375 مكرر من قانون العقوبات المصري المضافة بالقانون رقم 10 لسنه 2011 م على أنه: "مع عدم الإخلال بأية عقوبة أشد واردة في نص آخر، يعاقب بالحبس مدة لا تقل عن سنة كل من قام بنفسـه أو بواسطة الغير باستعراض القوة أو التلويح بالعنف أو التهديد بأيهما أو استخدامه ضد المجنى عليه أو مع زوجه أو أحد أصوله أو فروعه، وذلك بقصـــد ترويعه أو التخويف بإلحاق أي أذى مادي أو معنوي به أو الإضـــرار بممتلكاته أو سـلب ماله أو الحصـول على منفعة منه أو التأثير في إرادته لفرض السـطوة عليه أو

إرغامه على القيام بعمل أو حمله على الامتناع عنه أو لتعطيل تنفيذ القوانين أو التشـــريعات أو مقاومة الســـلطات أو منع تنفيذ الأحكام أو الأوامر أو الإجراءات القضـــائية واجبة التنفيذ أو تكدير الأمن أو السكينة العامة، متى كان من شأن ذلك الفعل أو التهديد إلقاء الرعب في نفس المجنى عليه أو تكدير أمنه أو سكينته أو طمأنينته أو تعريض حياته أو سلامته للخطر أو إلحاق الضرر بشيء من ممتلكاته أو مصالحه أو المساس بحريته الشخصية أو شرفه أو اعتباره. وتكون العقوبة الحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات إذا وقع الفعل من شخصين فأكثر، أو باصطحاب حيوان يثير الذعر أو بحمل أية أســـلحة أو عصـــى أو آلات أو أدوات أو مواد حارقة أو كاوية أو غازية أو مخدرات أو منومة أو أية مواد أخرى ضـــارة، أو إذا وقع الفعل على أنثى، أو على من لم يبلغ ثماني عشرة سنة ميلادية كاملة. ويقضى في جميع الأحوال بوضع المحكوم عليه تحت مراقبة الشرطة مدة مساوية لمدة العقوبة المحكوم بها".

وتنص المادة 375 مكررا (أ) من قانون العقوبات على أن:" يضاعف كل من الحدين الأدنى والأقصـــى للعقوبة المقررة لأية جنحة أخرى تقع بناء على ارتكاب الجريمة المنصـــوص عليها في المادة السابقة، ويرفع الحد الاقصى لعقوبتي السجن والسجن المشدد إلى عشرين سنة لأية جناية أخرى تقع بناء على ارتكابها. وتكون العقوبة السجن المشدد أو السجن إذا ارتكبت جناية الجرح أو الضرب أو إعطاء المواد الضارة المفضي إلى موت المنصوص عليها في المادة (236) من قانون العقوبات بناء على ارتكاب الجريمة المنصوص عليها في المادة السابقة، فإذا كانت مسبوقة بإصرار أو ترصـــد تكون العقوبة الســـجن المؤبد أو المشـــدد. وتكون العقوبة الإعدام إذا تقدمت الجريمة المنصوص عليها في المادة 375 مكررا أو اقترنت أو ارتبطت بها أو تلتها جناية القتل العمد

المنصوص عليها في الفقرة الأولى من المادة (234) من قانون العقوبات".

وأحيانا يتوافر التعدد المعنوي بين الرشـوة والابتزاز[171]؛ فالموظف الذي يهدد بالامتناع عن القيام بعمل إلا بعد الحصول على مبلغ مالي معين تنعقد مسؤوليته عن الفعل الأشد؛ لأن طلبه اقترن بتهديد.

(171)– غنام محمد غنام، شرح قانون العقوبات " القسم الخاص"، جرائم الاعتداءعلى المصلحة العامة والأموال، بدون دار نشر، 1999– 2000م، ص 119، 120.

الخاتمة:

إن التقدم التقني والمعلوماتي في الارتباط والإتصـال، كان معجزة هذا العصـر الذي دخل به كنوع من التحدي لمرحلة انتقالية حاسمة في حياة البشرية. حيث استطاعت هذه التقنية أن ترفع جميع الحواجز وتقرب المســـافات إلى حد جعل العالم وكأنه قرية صـــغيرة. وبقدر ما أصـــبح نقمة نظرا للتجاوزات العديدة والمختلفة من اختراقات وســطو وتعد صــريح على حرية الأفراد والمؤســســات، والمساس بأمن خصوصياتهم؛ فقد حققت التكنولوجيا الحديثة للإنسان منافع لا حصر لها، وبقدر هذه المنافع جرت عليه مشـــاكل لم يكن يتخيلها، ومن أخطرها جريمة الابتزاز الإلكتروني؛ حيث يجد الإنسان نفسه مهددا بإلحاق الأذى به في سمعته، أو نفسه، أو ماله، أو بشخص عزيز لديه ما لم يقم بتنفيذ المطلوب منه؛ لذا عملت العديد من التشـــريعات على تجريم الابتزاز الإلكتروني انصـــياعا للوضع الحالي.

و تباينت صـــور الابتزاز الالكتروني الاجرامية وتشـــعبت أنواعها، فلم تعد تهدد المصـــالح التقليدية التي تحميها القوانين والتشـريعات منذ عصـور قديمة، بل أصـبحت تهدد المصـالح والمراكز القانونية التي اسـتحدثتها التقنية المعلوماتية بعد اقترانها بثورة الاتصـالات. والتهديد بالإيذاء بوصـفه ســـلوكا إجراميا في الابتزاز الإلكتروني لابد أن يكون مقترنا بطلب، وأن يكون الجاني قاصـــدا إياه. والتهديد قد يكون موضوعه ماديا، من خلال التهديد بالعنف، أو معنويا من خلال إفشاء الأسرار، أو التشـهير بالشـخص. كما أنه قد يكون بطريقة مباشـرة، أو غير مباشـرة عبر وسـيط. وتكتمل جريمة الابتزاز الإلكتروني بقيام المجنى عليه بتنفيذ المطلوب منه أيا كانت طبيعته ماديا، أم عاطفيا،

مشـــروعا، أم غير مشـــروع، مما اســـتدعى بيان المســـؤولية الجنائية للفاعل في جريمة الابتزاز الإلكتروني، والظروف المشددة لها.

هذا وقد توصل الباحث إلى مجموعة من النتائج والتوصيات يمكن إجمالها في الآتي:

أولًا- النتائج:

1. الابتزاز الإلكتروني أحد نتائج التقدم التكنولوجي، والاســـتخدام المُذهل لوســـائل التواصـــل الاجتماعي، وقد بلغت خطورته على الأفراد والمجتمعات حدا كبيرا؛ ورغم ذلك لم تكن العقوبات الواردة في كل من التشريعين الإماراتي والمصري كافية لهذه الجريمة.
2. الابتزاز الإلكتروني انتهاك لحق الفرد في الخصـــوصـــية، والكرامة والحرية، والملكية، والســـلامة الجسـدية، والروحية (الرفاه العاطفى)، لأنه تهديد بإيقاع إيذاء على النفس، أو المال، أو السـمعة والشرف.
3. الجناة في جريمة الابتزاز الإلكتروني يكونون أحيانًا من الأقارب والأصدقاء، والمجنى عليهم فيها أغلبهم من النساء والشباب، إضافة إلى بعض الأشخاص المعنوية سواء العامة أو الخاصة.
4. يختلف الابتزاز الإلكتروني عن غيره من صور السلوك الإجرامي التي تتشابه معه مثل الابتزاز الذي يقع بالوسـائل التقليدية، أو جريمة اسـتغلال نفوذ، أو انتهاز احتياج أو ضـعف هوى نفس القاصر.
5. الابتزاز الإلكتروني أحد مظاهر المعاملات الاقتصـــادية غير المشـــروعة، كما أنه أحد المظاهر التي تشـــكل خروجا على حرية التعبير، فهو يُعد أحد مظاهر التعبير الممقوت الذي لا تضـــمنه حرية التعبير.

6. يتخذ الســلوك الإجرامي في الابتزاز الإلكتروني شــكل التهديد بإيذاء المقترن بطلب، وبذلك فهو يختلف عن جريمة التهديد غير المقترن بطلب من المجني عليه.
7. تطلب المشــرع الإماراتي ضــرورة أن يكون موضــوع التهديد جريمة، مشــددا العقاب إذا كان موضوعه جناية على النفس، أو المال، أو نسبة أمور مخلة بالشرف.
8. تتعدد أشــكال التهديد الذي يقع به الابتزاز الإلكتروني، فقد يكون مباشــرا أو من خلال وســيط، شفويا أو مكتوبا.
9. الابتزاز الإلكتروني من جرائم الضرر؛ حيث تتطلب قيام المجني بتنفيذ المطلوب منه، فإذا لم يقم بذلك تكون الجريمة في حالة شروع.
10. أخذت بعض التشريعات بالمصــادرة بوصــفها عقوبة إضــافية لجريمة الابتزاز الإكتروني مع ضمان حقوق الغير حسن النية.
11. تنعقد المسئولية الجنائية للجاني عن جريمة الابتزاز الإلكتروني، كما تنعقد عن الجريمة التي يطلب من المجني عليه تنفيذها؛ لكون المجني عليه غير مسئول جنائيا لخضــوعه لإكراه معنوي إن توافرت شروط توافره.

ثانيًا- التوصيات:

خرج الباحث بجملة من التوصيات أهمها:

1. يوصـــي الباحث بالأخذ بالمفهوم الواســـع في تعريف الابتزاز الإلكتروني المتمثل في: كل تهديد يقوم به الجاني، أو وســيط عنه يتم عبر وســيلة إلكترونية، ويؤثر في نفســية المجنى عليه، أو

شـخص عزيز لديه، ويدفعه إلى القيام بما طلبه منه الجاني، أو كلفه به سـواء أكان مشـروعا أم غير مشروع.

2. زيادة التوعية الأخلاقية والقانونية بأهمية الحفاظ على السرية بالنسبة للمعلومات التي يتعين حظر نشرها، أو إتاحتها لصـاحب الشـأن فقط، والتوعية بخطورة إسـاءة اسـتخدام الوسـائل الإلكترونية، وتبصير الأفراد بوسائل تشفير بياناتهم الشخصية وآلياته.
3. تشجيع التبليغ عن جريمة الابتزاز الإلكتروني على أن يكون في سرية تامة، والقضـاء على ثقافة العار التي تهيمن على الضحية.
4. إدراج جريمة الابتزاز الإلكتروني، في قانون مكافحة جرائم تقنية المعلومات على أن يكون النص كالآتي: يعاقب بالسجن مدة لا تتجاوز خمس سنوات كل من هدد غيره بالعنف، أو بإفشاء أمور أو نسـبتها إليه لا يرغب في اطلاع أحد عليها، وكان التهديد مصـحوبا بطلب أو بتكليف بأمر سواء أكان مشروعا أم غير مشروع.

ويعاقب بالسجن المؤقت كل من توافر في حقه أحد الأمور الآتية دون الإخلال بأي عقوبة أشد:

(أ) من كان موظفا عاما وتوصل إلى هذه الأمور بحكم وظيفته.

(ب) من وضع تهديده موضع التنفيذ.

(ج) من لحقه ضرر مادي عند تنفيذ التهديد.

(د) إذا كان المجني عليه موظفا عاما.

(هـ) إذا كان المجنى عليه من الفئات المستضعفة؛ مثل: النساء، أو الأطفال، أو ذوي الاحتياجات الخاصة.

(و) إذا كان الجاني مؤتمنا على أسرار المجنى عليه بحكم عمله، أو بطلب المجني عليه.

(ز) إذا تم ارتكاب الفعل من قبل جماعة إجرامية.

(ح) إذا كان التهديد بجناية أو بإفشاء أو نسبة أمور مخدشة بالشرف.

(ط) إذا اتخذ السلوك الإجرامي صورة الاعتياد أو تكرر أكثر من مرة.

5. يوصـــي الباحث بالعقاب على تلقى عائدات الابتزاز والإفادة منها، أو إخفائها بنص خاص كالآتي: يعاقب بالحبس مدة لا تقل على سنة كل من حصل على أو امتلك أو أخفي أو تصرف باي أموال أو ممتلكات أخرى تم الحصول عليها من ارتكاب جريمة الابتزاز الإلكتروني، مع العلم بأنه تم الحصول عليها بصورة غير مشروعة".
6. رد كل ما يمكن رده لصاحب الشأن وتم التحصل عليه نتيجة الابتزاز الإلكتروني، دون الإضرار بحقوق الغير حسن النية.
7. يقترح الباحث إضـافة نص خاص للمرسـوم رقم (5) لسـنة 2012 بشـأن مكافحة جرائم تقنية المعلومات يقرر امتناع المســؤولية الجنائية للمجنى عليه، يكون كالأتي:" لا يعد المجنى عليه مسـؤولا مسـئولًا جنائيًا عن أي جريمة نشـأت أو ارتبطت مباشـرة بكونه مجنيا عليه في جريمة الابتزاز الإلكتروني).
8. تطبيق نظام التدابير الاحترازية في مواجهة مرتكبي جرائم الابتزاز الإلكتروني كوضـع الجاني في مركز تأهيل نفسي لمدة لا تقل عن ستة أشهر.

قائمة المراجع

1. ابن منظور، لسان العرب، مادة بز، ج1، دار المعارف.
2. أحمد أبو الروس بسيوني، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، منشورات المكتب الجامعي الحديث، الإسكندرية، الطبعة الثانية، 2014.
3. أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2009.
4. أحمد فؤاد عبد المجيد، الحجية القانونية لوسائل التقدم العلمي، الدار العلمية الدولية للنشر والتوزيع، عمان، الطبعة الثانية، 2012.
5. أشرف توفيق شمس الدين، الجنائية للحرية الشخصية من الوجهة الموضوعية، دراسة مقارنة، دار النهضة العربية، 2007م.
6. أميرة محمود الفقي، الإثبات الجنائي للجرائم المرتكبة عبر الإنترنت، رسالة دكتوراة، جامعة عين شمس.
7. بندر عقاب الدرويش، الإثبات في رائم الإرهاب الإلكتروني" دراسة مقارنة"، عمان، الأردن، 2017.
8. تامر محمد صالح، الإبتزاز الإلكتروني" دراسة تحليلية مقارنة"، جامعة المنصورة، الطبعة الأولى، 2018.
9. جميل الصغير، الجوانب الإجرائية المتعلقة بالإنترنت، دار النهضة العربية، 1998.
10. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، 2002 .
11. جندي عبد الملك، موسوعة الأحكام الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2011.
12. جيرار كورنو، ترجمة منصور القاضي، معجم المصطلحات القانونية، المؤسسة الجامعية للدراسات والنشر والتوزيع، 1998.
13. حسن صادق المرصفاوي، قانون العقوبات الخاص- منشاة المعارف- الإسكندرية مصر،1991.
14. حسن علي السمني، شرعية الأدلة المستمدة من الوسائل العلمية ، رسالة دكتوراة، جامعة القاهرة، 1983.
15. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراة، كلية القانون، جامعة عين شمس، 2005.

16. خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، دار الفكر الجامعي، 2020م.

17. خالد حسن أحمد لطفي، آليات التحقيق الجنائي في جرائم تقنية المعلومات، دار الفكر الجامعي، الإسكندرية، 2018.

18. خالد حسن أحمد، جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دار الفكر الجامعي، 2019.

19. خالد حسن لطفي، التقاضي الإلكتروني كنظام قضائي معلوماتي، دار الفكر الجامعي، 2020.

20. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، 2011.

21. خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، 2020م.

22. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، لإسكندرية، 2008.

23. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

24. رمسيس بهنام، قانون العقوبات جرائم القسم الخاص، الطبعة الأولى، منشأة المعارف، 1999م.

25. رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي – الطبعة الثامنة 1985م.

26. سامي الشوا، الغش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، 2003.

27. سعد عاطف عبد المطلب، الحماية الجنائية للمصنفات الرقمية" دراسة مقارنة"، دار الفكر الجامعي، 2019م.

28. سعيدي سليمة، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، 2017م.

29. سيد حسن عبد الخالق ، النظرية العامة لجريمة إفشاء الأسرار في التشريع الجنائي المقارن، رسالة دكتوراة، جامعة عين شمس، 1987.

30. صالح أحمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في إطار اتفاقية بودابست، 2017.

31. عبد الرازق الموافي عبد اللطيف، حكم قضائي بشأن الاختصاص الجنائي بجرائم الإنترنت، "مجلة معهد دبي القضائي" العدد الأول مايو 2012م.
32. عبد الرازق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة " المرسوم بالقانون الاتحادي رقم 5 لسنه 2012، الكتاب الأول، إصدار معهد دبي القضائي، 2014
33. عبد الرزاق الموافي عبد اللطيف، شرح قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة" المرسوم بالقانون الاتحادي رقم 5 لسنه 2012"، الكتاب الثاني، 2014.
34. عبد الرزاق سندالي، التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر، 19-20 يونيو، المملكة المغربية، 2009.
35. عبد العظيم مرسي، جرائم الاعتداء على الأموال، دار النهضة العربية، القاهرة، مصر، 1993م، ص126.
36. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006 .
37. عبد القادر عودة، التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي، مؤسسة الرسالة ناشرون، لبنان، بيروت، ط1، 2008م.
38. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، الإسكندرية، 2002.
39. عبد الوهاب المعمري، جريمة الاختطاف الأحكام العامة والخاصة والجرائم المرتبطة، دار الكتب القانونية، القاهرة، مصر، 2010م.
40. عمر سالم، المراقبة الإلكترونية، دار النهضة العربية، القاهرة، 2000.
41. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن إستخدام الإنترنت ، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية 2004.
42. عمر محمد بن يونس، الإجراءات الجنائية عبر الإنترنت، المرشد الفيدرالي للتفتيش وضبط الحواسيب، بدون جهة نشر، وبدون مكان نشر.
43. فخري عبد الرزاق الحديثي، شرح قانون العقوبات القيم الخاص، الجرائم الواقعة على الأموال، الطبعة الثانية، منشورات دار الثقافة، عمان، 2011.

44. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية – الطبعة الثالثة 2012م.
45. قاسم محمد عبد الله، الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، 2010.
46. كامل حامد السعيد، شرح قانون العقوبات– الجرائم الواقعة على الأموال، ط3، منشورات دار الثقافة للنشر والتوزيع، 2014، ص169.
47. محمد الألفي، بحث في الدليل الرقمي وحجيته في الإثبات، بحث منشور على الإنترنت.
48. محمد الأمين البشري، التحقيق في جرائم الأنترنت، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، 2000.
49. محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الألي والأنترنت، بحث مقدم في الحلقة العلمية بعنوان " الإنترنت والإرهاب" المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، دبي، 2008.
50. محمد الدسوقي، الحماية الدولية لسرية المعلومات، دار الفكر العربي، 2003.
51. محمد تيمور عبد الحسيب، ط2، الحاسبات الإلكترونية وتكنولوجيا الاتصال، دار الشروق، القاهرة، 2014.
52. محمد زكي أبو عامر، الحماية الجنائية للحريات الشخصية ، منشآة المعارف ، الإسكندرية . 1979
53. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1998.
54. محمد صبحي نجم، قانون أصول المحاكمات الجزائية الأردني، منشورات الجامعة الأردنية، عمان، الأردن، الطبعة الأولى.
55. محمد صبحي نجم، قانون العقوبات القسم الخاص، الجرائم المخلة بالمصلحة العامة والثقة العامة والواقعة على الأموال وملحقاتها، منشورات دار الثقافة للنشر والتوزيع، 2014.
56. محمد علي سويلم، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية" دراسة مقارنة"، دار المطبوعات الجامعية، 2018م.
57. محمد علي سويلم، الحماية الجنائية للمعاملات الإلكترونية الجرائم المعلوماتية والإلكترونية.
58. محمد محمد عبد اللطيف، مبدأ الأمن القانوني، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد السادس والثلاثون، أكتوبر 2004م.

59. محمود أحمد طه ، التنصت والتلصص على سرية الإتصالات الشخصية بين التجريم والمشروعية ، دار الفكر والقانون ، المنصورة.
60. محمود نجيب حسنى، شرح قانون العقوبات القسم الخاص، ط8، منشورات دار العربية، مصر،1984.
61. مصطفى مجدي هرجة، التعليق على قانون العقوبات في ضوء الفقه والقضاء، ط2، منشورات روز اليوسف، القاهرة، 1992.
62. ممدوح خليل البحر، حماية الحماية الخاصة في القانون الجنائي، دراسة مقارنة ، مكتبة دار الثقافة للنشر والتوزيع عمان، الأردن 1996.
63. ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، الجريمة عبر النت، مكتبة دار الحقوق، الشارقة، 2010.
64. ميللر آثر، الحماية القانونية لبرامج الكمبيوتر والبيانات، منشورات سويت ماكسويل، لندن، ترجمة الدار العربية للعلوم، نقوسيا، 1985.
65. ندوة بعنوان" الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية"، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 يونيو 2007، المملكة المغربية.
66. نوال عبد العزيز العيد، آثار جريمة الابتزاز الإلكتروني الابتزاز المفهوم، والأسباب، والعلاج، بحث منشور على الشبكة العنكبوتية في موقع: نوال عبد العزيز العيد، تحت العنوان: http://nawalaleid.com/cnt/lib/768.
67. هشام فريد رستم، الحماية الجنائية لحق الإنسان في صورته، مكتبة الآلات الحديثة بأسيوط، 1986.
68. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، 1994.

والله ولي التوفيق.