المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

(دراسة تحليلية للأساليب الإجرامية وقواعد ضبط وتحليل الأدلة الرقمية)

الأستاذ الدكتور/ حسام نبيل الشنراقي

أستاذ علوم الشرطة - رئيس قسم إدارة الشرطة - أكاديمية شرطة دبي

المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي (دراسة تحليلية للأساليب الإجرامية وقواعد ضبط وتحليل الأدلة الرقمية)

الأستاذ الدكتور/ حسام نبيل الشنراقي
أستاذ علوم الشرطة – رئيس قسم إدارة الشرطة – أكاديمية شرطة دبي

المُلخَّص

يتناول البحث المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، مع التركيز على الأساليب الإجرامية المعقدة التي يستخدمها المبتزون لاستغلال ضحاياهم. ويشمل الابتزاز الإلكتروني تهديد الضحية بنشر معلومات شخصية حساسة أو التشهير بها؛ للحصول على مكاسب مادية أو لا أخلاقية أو معنوية، وتبرز الدراسة تحديات عدة في مواجهة هذه الجرائم؛ مثل سهولة ارتكابها، وصعوبة تعقب الجناة، إلى جانب تطور الأدوات الرقمية المستخدمة في هذه الجريمة.

ويشير البحث إلى أهمية التحليل الجنائي الرقمي في مواجهة هذه الجرائم؛ حيث يعتمد على استرجاع الأدلة الرقمية، كالرسائل الإلكترونية والبيانات المخزنة، وفق أسس قانونية وتقنية تضمن قبولها أمام القضاء. كما يؤكد ضرورة تطوير كفاءات أمنية قادرة على التعامل مع الجرائم الرقمية، والتعاون بين الجهات الأمنية والقضائية لضبط الأدلة وتقديمها بطريقة مهنية.

يوفر البحث أيضًا حلولاً واستراتيجيات فعالة لمكافحة الابتزاز الإلكتروني؛ مثل تعزيز الوعي المجتمعي بمخاطر الإنترنت ووسائل التواصل الاجتماعي، وتطوير نظم الحماية الإلكترونية، بالإضافة إلى سن التشريعات القانونية التي تعاقب على هذه الجرائم، وتركز الدراسة على ضرورة تعزيز التعاون الدولي لمكافحة الابتزاز الإلكتروني العابر للحدود.

الكلمات المفتاحية: الابتزاز الإلكتروني – الجرائم السيبرانية – الحلول الأمنية – التحديات الأمنية – الإنترنت المظلم – التحقيقات الجنائية الرقمية – التشريعات السيبرانية – الوقاية من الجرائم الإلكترونية – التكنولوجيا الأمنية – حماية الخصوصية – التهديدات الإلكترونية – الابتزاز عبر وسائل التواصل الاجتماعي – التعاون الأمني الدولي.

ABSTRACT

Police Confrontation of Cyber Blackmail Crimes "Via Social Media" (An Analytical Study of Criminal Methods and Rules for seizing and Analyzing Digital Evidence)

Professor/ Hossam Nabil El-Shenraky
Professor of Police Sciences - Head of Police management Department - Dubai Police Academy

The research "Security Confrontation of Cyber Blackmail Crimes: Challenges and Solutions" deals with a comprehensive study of cyber blackmail crimes via social media, focusing on the complex criminal methods used by blackmailers to exploit their victims. Cyber blackmail includes threatening the victim with publishing sensitive personal information or defaming them in order to obtain material, sexual or moral gains. The study highlights several challenges in confronting these crimes, such as the ease of committing them and the difficulty of tracking down the perpetrators, in addition to the development of digital tools used in the crime. The study indicates the importance of digital forensic analysis in confronting these crimes, as it relies on retrieving digital evidence such as emails and stored data, according to legal and technical foundations that ensure their acceptance before the judiciary. It also emphasizes the need to develop security competencies capable of dealing with digital crimes, and cooperation between security and judicial authorities to seize evidence and present it in a professional manner. The study also provides effective solutions and strategies to combat cyber blackmail, such as enhancing community awareness of the dangers of the Internet and social media, developing electronic protection systems, in addition to enacting legal legislation that punishes these crimes. The study focuses on the need to enhance international cooperation to combat cross-border cyber blackmail.

Keywords: Cyber extortion - Cybercrime - Security solutions - Security challenges - Dark web - Digital forensics - Cyber legislation - Cybercrime prevention - Security technology - Privacy protection - Cyber threats - Social media extortion - International security cooperation

التمهيد:

في عصر يتسم بالتكنولوجيا الرقمية والاتصالات الفورية، أصبح الابتزاز الإلكتروني ظاهرة متزايدة الانتشار والخطورة، وقد أصبح هذا النوع من الجريمة الإلكترونية يمثل تحديًا كبيرًا للأفراد والمؤسسات على حد سواء؛ حيث يستخدم المجرمون التكنولوجيا للضغط على ضحاياهم بهدف تحقيق مكاسب مالية أو شخصية.

ويتضمن الابتزاز الإلكتروني مجموعة واسعة من الأنشطة الضارة؛ مثل التهديد بنشر معلومات خاصة، أو التشهير عبر الإنترنت، أو التهديد بإلحاق الضرر بالأفراد أو المؤسسات إذا لم يتم تلبية مطالب الشخص المبتز، كما يتميز هذا النوع من الجرائم بسهولة التنفيذ وصعوبة تتبع المجرمين، مما يجعله تحديًا كبيرًا أمام أنظمة القانون والأمن الإلكتروني.

وتعد جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي من أخطر الجرائم الإلكترونية في العصر الحديث؛ حيث تستهدف هذه الجرائم الأفراد والمؤسسات عبر استغلال الثغرات الأمنية واستدراج الضحايا بطرق وأساليب إجرامية معقدة. وإن تزايد الاعتماد على التكنولوجيا وانتشار وسائل التواصل الاجتماعي أدى إلى ظهور أنماط جديدة من الجرائم، تتطلب مواجهة أمنية تعتمد على التحليل الدقيق للأساليب الإجرامية، وضبط الأدلة الرقمية وتحليلها بطرق احترافية، لذلك فإن دراسة تلك الجرائم وتحليل أساليبها يمثل ضرورة أمنية مُلِحَّة؛ لفهم طبيعة التهديدات وكيفية التعامل معها بشكل فعال.

كما أن الأساليب الإجرامية في جرائم الابتزاز الإلكتروني متعددة؛ إذ تشمل الاستدراج العاطفي، والتلاعب النفسي، والاحتيال عن طريق خلق هويات وهمية، ولجوء المجرمين إلى استخدام برامج تجسس وتقنيات متطورة لاختراق الخصوصية، مما يعقد عملية جمع الأدلة وضبط الجناة أمام هذه التحديات، لذلك تأتي أهمية التحليل الجنائي الرقمي، الذي يعتمد على تتبع آثار الجريمة في الفضاء السيبراني، واستخدام أدوات متقدمة لاستعادة وتحليل البيانات من الأجهزة والشبكات التي تم استهدافها، ويعتمد نجاح هذه التحليلات على دقة وكفاءة الأدوات المستخدمة، وكذلك على كفاءة الكوادر المؤهلة في هذا المجال.

في هذا السياق، تبرز قواعد ضبط وتحليل الأدلة الرقمية كعنصر أساسي في المواجهة الأمنية لجرائم الابتزاز الإلكتروني، الأدلة التي تشمل الرسائل الرقمية، والصور، والمعلومات المخزنة على الأجهزة الإلكترونية، التي تتطلب معالجة دقيقة وفقًا لمعايير قانونية وتقنية صارمة تضمن قبولها أمام القضاء. ويعتمد ضبط هذه الأدلة على استخدام تقنيات الاسترجاع الرقمي دون المساس بسلامة البيانات، مما يشكل تحديًا في الحفاظ على التسلسل الزمني للأحداث وكشف العلاقات بين الأطراف المتورطة. كما أن التحليل الجنائي الرقمي يجب أن يتم بصورة تحافظ على حقوق الأفراد وخصوصياتهم، مع الأخذ في الاعتبار الجوانب الأخلاقية والقانونية.

وتؤكد هذه الدراسة التحليلية أن المواجهة الأمنية الفعالة لجرائم الابتزاز الإلكتروني تتطلب نهجًا متكاملاً يشمل فهم الأساليب الإجرامية المتجددة، وضبط الأدلة الرقمية بأساليب احترافية تضمن صحتها أمام القضاء، وكذلك فإن التعاون بين الأجهزة الأمنية والجهات القضائية، بالإضافة إلى تطوير قدرات التحليل الجنائي الرقمي، هو السبيل الأنجح لمكافحة هذا النوع من الجرائم. وفي ظل التطور السريع في تقنيات الجريمة الإلكترونية، يصبح من الضروري الاستثمار المستمر في تدريب الكوادر الأمنية، وتطوير أدوات التحليل الرقمي، ورفع مستوى الوعي المجتمعي بطرق الوقاية من هذه الجرائم.

فالانفتاح التقني وما صاحبه من قفزة نوعية في الاتصالات بشكل عام وفي مجال الإنترنت بشكل خاص قد أوجد عدة مظاهر سلبية نجمت عن سوء استخدام الوسائل الإلكترونية التي من المفروض أنها وجدت حتى تخدم بني البشر لا أن تكون سببًا في تعاستهم[1].

أهمية الدراسة:

تعد جرائم الابتزاز الإلكتروني من الجرائم متعددة الأبعاد وشديدة الخطورة، وذلك لما تمثله من قهر للضحية يمارسه الجاني عليها حتى يحصل على مبتغاة، كما أنه قد يؤدي إلى آثار شديدة الخطورة على الأمن؛ حيث قد يؤدي بالضحية إلى الانتحار للتخلص من العار الذي يلحق بها بسبب فضح أسرارها أو هتك ستر خصوصياتها، كما أنها من الجرائم التي تحتاج إلى استراتيجية خاصة في التعامل معها؛ لما تتضمنه من خوف شديد لدى الضحية، وهو ما يتطلب دراسة مستفيضة يمكن من خلالها التوصل إلى آلية مُثلى تحقق مواجهة أمنية مستنيرة وقادرة على فهم التحديات وكيفية مكافحة هذه الجريمة الخطيرة.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في إيجاد آلية متعددة المحاور يمكن من خلالها تحقيق مواجهة أمنية متكاملة لجرائم الابتزاز الإلكتروني بصورها المختلفة وأنماطها المتعددة، وهو ما يحتاج إلى دراسة متكاملة الجوانب يمكن من خلالها فهم الطبيعة شديدة الخطورة للجريمة؛ من خلال فهم وتحليل الأنماط المختلفة للجريمة، وفهم طبيعة الجناة والأدوات التي يستخدمونها للإيقاع بضحاياهم، واستراتيجية الجناة في إجبار ضحاياهم على الاستجابة لهم، وفهم طبيعة الأدلة الرقمية المتخلفة عن الجريمة، وكيفية حفظها وتحصيلها وفقًا للأسس الصحيحة، وتحليلها وصولاً لتحديد شخصية الجناة وإثبات الجريمة عليهم.

(1) د/ سعيد زيوش - ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية – مجلة العلوم الاجتماعية – يناير -2017 العدد 22 – 2017م – ص70ص73

أهداف الدراسة:

تهدف الدراسة إلى تحقيق عدة أهداف تتمثل في:

1. دراسة وتحليل طبيعة جريمة الابتزاز الإلكتروني، وأساليب ارتكابها، وخصائصها، وأنماطها، وسمات مرتكبيها.
2. تحديد وتحليل التحديات الأمنية المرتبطة بجرائم الابتزاز الإلكتروني، وإيجاد حلول لها.
3. فهم وتحليل الطبيعة الخاصة للأدلة الرقمية، وأساليب حفظها وفحصها وتحليلها.
4. إيجاد حلول واستراتيجيات لمكافحة الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

تساؤلات الدراسة:

1. ما المقصود بجرائم الابتزاز الإلكتروني؟
2. ما أنماط الابتزاز الإلكتروني؟
3. ما خصائص ودوافع جريمة الابتزاز الإلكتروني؟
4. كيف نظم القانون القطري والقانون الإماراتي تجريم الابتزاز الإلكتروني؟
5. ما القواعد الإجرائية للتعامل مع الأدلة الرقمية في القانون القطري؟
6. ما القواعد الفنية للتعامل مع الأدلة الرقمية؟

منهج الدراسة:

نتبع في هذه الدراسة المنهج الوصفي التحليلي القائم على وصف جريمة الابتزاز الإلكتروني وأسبابها كافة والآثار المترتبة عليها، وتوضيح أنماطها المختلفة وصولاً إلى فهم الأساليب الإجرامية الحالية كافة، وتحليل كيفية ارتكاب الجاني للجريمة، وفهم دوافعه وكيفية وقوع الضحية في الجريمة، والوصول من خلال التحليل إلى آلية مُثلى للوقاية من الجريمة، وكذلك كيفية التعامل مع الجريمة بأبعادها المختلفة لإقناع الضحايا بالإبلاغ في ظل آلية للحفاظ على سمعة الضحية وسرية المعلومات الخاصة بها، ثم تحقيق مواجهة أمنية فاعلة للجريمة، وضبط الجناة للحد من الجريمة.

نطاق الدراسة:

النطاق الموضوعي: تتضمن الدراسة فهم وتحليل أساليب جريمة الابتزاز الإلكتروني، وسمات مرتكبيها، وكيفية استدراج الضحايا عبر مواقع التواصل الاجتماعي، والإجراءات التي يمكن أن يقو م بها رجال البحث الجنائي لضبط الأدلة الرقمية على الجريمة، وتشريحها للوصول لشخص مرتكبها، وأساليب التحري عن الجريمة.

أدوات الدراسة:

يستخدم الباحث في الدراسة المراجع العلمية المختلفة والدراسات التي أجريت في هذه الجريمة، وكذلك التجارب المختلفة في المكافحة، ودراسات الحالة، وصولاً إلى أفضل التطبيقات والممارسات في مجال التحري عن جرائم الابتزاز الإلكتروني وضبط الأدلة عليها وضبط مرتكبيها.

الدراسات السابقة:

1- أطروحة ماجستير بعنوان: "الابتزاز الإلكتروني للفتاة عبر مواقع التواصل الاجتماعي (الفيسبوك نموذجًا)". وهي دراسة مسحية لعينة من طالبات قسم الإعلام والاتصال بجامعة قاصدي مرباح – تخصص تكنولوجيا الاتصال الجديدة – الجزائر، مقدمة من سمان جويدة، وإيمان مردف 2017م. وقد تناولت الدراسة أهمية منصة (FaceBook) في التواصل الاجتماعي، ومخاطر استخدامه في استدراج الفتيات لابتزازهم إلكترونيًا، ووضحت دوافع واحتياجات الفتيات لاستخدام هذه المنصة؛ كإشباع الحاجة العاطفية، وما يسببه من وقوعهنَّ ضحايا للابتزاز، وكيف يمكن استخدامه بشكل صحيح لعدم الوقوع ضحية للجريمة، واعتمدت الدراسة في توضيح ذلك على إجراء مسح تحليلي لمجموعة فتيات في كلية تكنولوجيا الإعلام في الجامعة من خلال الاستبانة، وتوصلت الدراسة إلى أن السبب الأساسي لوقوع الفتيات ضحايا للجريمة هو عدم كفاية الوعي لديهنَّ بمخاطر هذه المواقع، والتهاون في تبادل البيانات الشخصية عبرها مع غرباء، وعدم اتباع القواعد الصحيحة في هذا الشأن.

2- دراسة محمد حسن مكاوي بعنوان: "الابتزاز الإلكتروني بين التهديد والحماية (دراسة في التشريعات المصرية والأمريكية – Journal of Law and Emerging Technologies issued by the Faculty of Law at the British University in Egypt, Volume 02, Issue 02 October 2022,)

قدَّمت هذه الدراسة تحليلاً شاملاً لظاهرة الابتزاز والتهديد الإلكتروني، وتعريف الابتزاز الإلكتروني وأنواعه وآثاره المجتمعية، وعقدت مقارنة بين القوانين المعمول بها لهذه الجريمة في التشريعين المصري والأمريكي، مع عرض أحدث القضايا الخاصة بتلك الجريمة، وموقف الأحكام القضائية منها، بالإضافة إلى البيانات الإحصائية التي توضح مدى اتساع الظاهرة في المجتمعين المصري والأمريكي. كما أظهرت الدراسة كيف أدى التحول الرقمي إلى زيادة انتهاك الخصوصية عبر الإنترنت، وأظهرت الفجوة بين التشريعات المصرية والتطور الهائل في تكنولوجيا المعلومات والتحول الرقمي، مما أكد حتمية وضرورة سن التشريعات لمواجهة أنواع الجرائم المستحدثة بأشكالها المختلفة وبطرق ارتكابها المتنوعة. وقد حاول الباحث أن يضع بعض الحلول للعقبات الإجرائية التي تؤثر على تطبيق العدالة السريعة والردع العام.

خطة الدراسة:

المبحث الأول: ماهية جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

- **المطلب الأول: التعريف بجريمة الابتزاز الإلكتروني.**
  - الفرع الأول: مفهوم جريمة الابتزاز الإلكتروني.
  - الفرع الثاني: الابتزاز الإلكتروني في الفقه.
  - الفرع الثالث: الابتزاز الإلكتروني في القانون القطري رقم 14 لسنة 2014م والقانون الإماراتي رقم 34 لسنة 2021م.
- **المطلب الثاني: خصائص ودوافع وأنماط ومحاور جريمة الابتزاز الإلكتروني.**
  - الفرع الأول: خصائص جريمة الابتزاز الإلكتروني.
  - الفرع الثاني: دوافع جريمة الابتزاز الإلكتروني.
  - الفرع الثالث: أنماط ومحاور الابتزاز عبر مواقع التواصل الاجتماعي.

المبحث الثاني: إجراءات التحقيق في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

- **المطلب الأول: الإطار الإجرائي القانوني لجريمة الابتزاز الإلكتروني في التشريع القطري.**
  - الفرع الأول: الشكوى في جريمة الابتزاز الإلكتروني.
  - الفرع الثاني: إجراءات ضبط الأدلة الإلكترونية في جريمة الابتزاز الإلكتروني.
  - الفرع الثالث: شروط صحة الدليل الإلكتروني في جريمة الابتزاز الإلكتروني أمام القضاء الجنائي.
- **المطلب الثاني: القواعد الفنية لجمع الأدلة الرقمية في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.**
  - الفرع الأول: مرحلة الإعداد وجمع الأدلة من مواقع التواصل الاجتماعي.
  - الفرع الثاني: توثيق مسرح الجريمة في جرائم الابتزاز عبر مواقع التواصل الاجتماعي.
  - الفرع الثالث: تحليل الأدلة في جرائم الابتزاز الإلكتروني.

مصطلحات الدراسة:

الابتزاز الإلكتروني، الجريمة الإلكترونية، الأدلة الرقمية، التحليل الجنائي الرقمي، التشريح الرقمي للأدلة، تحريز الأدلة الرقمية، الجرائم المستحدثة، التحقيق الجنائي الرقمي.

المبحث الأول
ماهية جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

التمهيد:

تعد جريمة الابتزاز الإلكتروني من الجرائم المستحدثة التي ظهرت مع ظهور التقنيات الحديثة في نقل وتبادل الوسائط الإلكترونية وتطور وسائل التواصل الاجتماعي، وتعاظم تأثيرها على المستخدمين، وسوف نتناول بالدراسة في هذا المبحث التعريف بالابتزاز الإلكتروني وخصائص الجريمة وسمات الجناة في مطلبين: **المطلب الأول:** التعريف بجريمة الابتزاز الإلكتروني، **والمطلب الثاني:** خصائص ودوافع جريمة الابتزاز الإلكتروني.

المطلب الأول: التعريف بجريمة الابتزاز الإلكتروني

الفرع الأول: مفهوم جريمة الابتزاز الإلكتروني

تم تعريف الابتزاز الإلكتروني في القانون القطري كأحد أشكال الجرائم الإلكترونية التي تمثل اعتداءً على حرية الضحية وملكيتها أو خصوصيتها عبر استخدام وسائل تقنية المعلومات مثل الشبكة المعلوماتية، وذلك بهدف تحقيق مكاسب غير مشروعة أو إجبار الضحية على القيام بأفعال لا ترغب بها. كما أن الابتزاز الإلكتروني قد يرتبط بتهديد الضحية بفضح معلومات خاصة أو حساسة، وفي بعض الأحيان قد يشمل تهديدًا بالإضرار بالسمعة أو بالأسرة.

وقد أشار المشرع القطري إلى جريمة الابتزاز الإلكتروني في القانون رقم 14 لسنة 2014 بشأن مكافحة الجرائم الإلكترونية؛ حيث جاء في المادة 9 من هذا القانون أنه: "يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات أو بغرامة لا تزيد على مئة ألف ريال قطري، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات لابتزاز أو تهديد شخص لحمله على القيام بعمل أو الامتناع عنه". وتعتبر هذه المادة أساسًا قانونيًا لتعريف الابتزاز الإلكتروني في قطر؛ حيث يرتكز التعريف على استخدام التهديد بوسائل تقنية المعلومات لتحقيق أهداف غير مشروعة، وقد تبنى المشرع القطري تعريفًا واسعًا لجريمة الابتزاز الإلكتروني؛ إذ لم يحدد بشكل ضيق مضمون التهديد، بل اكتفى بذكر أن التهديد يكون لتحقيق هدف محدد، مثل "حمل الضحية على القيام بعمل أو الامتناع عنه". وبهذا ينظر المشرع إلى الابتزاز الإلكتروني على أنه جريمة متكاملة الأركان إذا تحقق فيها فعل التهديد بواسطة الشبكة المعلوماتية.

ويلاحظ أن القانون رقم 14 لسنة 2014م لم يوضح تعريف جريمة الابتزاز بشكلٍ كافٍ، بينما تناولت المادة 325 من قانون العقوبات القطري جريمة التهديد؛ حيث عرفها المشرع باعتبارها تهديدًا مقترنًا بطلب يلحق ضررًا بالشخص نفسه أو بسمعته أو بماله أو بسمعة شخص يهمه أمره، وذلك لتحقيق مكاسب مادية أو معنوية. وتتنوع الوسائل المستخدمة لتهديد المجني عليه؛ سواء كانت مكتوبة أو شفهية أو باستخدام وسائل أخرى، بشرط أن توحي هذه الأفعال بالعزم على إلحاق الأذى بالشخص أو من يهمه أمره، وعلى ذلك فقد تضمنت المادة 325 تحديد شكل التهديد؛ حيث يمكن أن يكون التهديد مكتوبًا أو شفهيًا أو بأي وسيلة توحي بجدية العزم على إيقاع الضرر، ويستهدف التأثير على إرادة المجني عليه لتحقيق طلب معين من قبل الجاني، وتحديد الغاية من التهديد وهي أن ينصب التهديد على تحقيق غاية معينة، مثل حمل المجني عليه على القيام بعمل ما أو الامتناع عنه؛ حيث تتضح جريمة الابتزاز في هذه الحالة من خلال ربط التهديد بهدف محدد يطلبه الجاني.[2]

كما تعرف جريمة الابتزاز الإلكتروني بأنها: "استخدام التكنولوجيا الرقمية مثل الإنترنت أو الهواتف الذكية لتهديد الأفراد أو المؤسسات بهدف الحصول على المال أو الخدمات أو لغرض آخر بالقوة أو التهديد. ويتضمن الابتزاز الإلكتروني إرسال رسائل تهديدية أو التشهير بالشخص أو نشر معلومات خاصة بهدف إجبار الضحية على القيام بشيء معين؛ مثل دفع مبلغ مالي أو تقديم خدمات أخرى. على أن هذه الأفعال تعتبر غير قانونية وتعرض مرتكبها للمساءلة القانونية بموجب القوانين المحلية والدولية المعمول بها".

إن جريمة الابتزاز الإلكتروني هي شكل من أشكال الجريمة الإلكترونية التي تتمثل في استخدام وسائل الاتصال الإلكتروني؛ مثل الرسائل النصية، والبريد الإلكتروني، والمنصات الاجتماعية، والتطبيقات الرقمية، لتهديد الأفراد أو المؤسسات بهدف الحصول على مال أو خدمات أو لأغراض أخرى بالقوة أو التهديد[3].

وتعتبر جريمة الابتزاز الإلكتروني تطورًا للابتزاز التقليدي؛ حيث تستخدم التكنولوجيا لتوسيع نطاق الضغط على الضحية وتكوين حدود أقل وضوحًا بالنسبة للمرتكب، فعلى سبيل المثال يمكن للمعتدين استخدام الصور أو الفيديوهات الخاصة بالضحية ونشرها عبر الإنترنت كوسيلة للابتزاز المالي أو العاطفي.

(2) جاسم ناصر جاسم المسلماني – التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري – رسالة مقدمة للحصول على درجة الماجستير في القانون العام – كلية القانون – جامعة قطر – يناير 2023م – ص7ص9

(3) Martinez, M., & Anderson, C, "Cyber Extortion: An Emerging Internet-Based Crime", Journal of Cybersecurity, 2021, pp: 126129-

وجريمة الابتزاز الإلكتروني هي استخدام الإلكترونيات وتكنولوجيا المعلومات لتهديد الأفراد أو المؤسسات بأن ينشروا أو يعرضوا معلومات محرجة أو خاصة عبر الإنترنت أو الوسائل الرقمية الأخرى مقابل متطلبات مالية أو أخرى[4].

ويعرف الابتزاز الإلكتروني أيضًا بأنه الأفعال التي تتضمن إساءة استخدام شبكة المعلومات لتحقيق غرض غير مشروع يختلف بحسب ظروف كل فعل وبحسب مرتكب الفعل، ويهدف إلى تحقيق أهداف مالية أو لا أخلاقية أو معنوية.

كما يمكن تحديد الابتزاز الإلكتروني على أنه الأفعال التي يستخدم مرتكبها التقنيات المتقدمة عبر الإنترنت والبرمجيات التي تمكنه من محو آثار الجريمة عقب ارتكابها وصولاً لتحقيق غاياته؛ حيث تختلف الغايات باختلاف مرتكبي الجريمة وباختلاف المؤثرات التي تؤثر عليهم.

ويرى الباحث تعريف الابتزاز الإلكتروني على أنه: "استخدام التكنولوجيا الرقمية؛ مثل الإنترنت والهواتف الذكية، لتهديد الأفراد أو المؤسسات بهدف إجبارهم على تقديم مال أو خدمات أو لتحقيق أهداف أخرى غير مشروعة. ويتم ذلك من خلال التهديد بنشر معلومات خاصة أو محرجة، أو إرسال رسائل تهديدية، ويستغل مرتكب الجريمة وسائل الاتصال الإلكتروني مثل البريد الإلكتروني ومنصات التواصل الاجتماعي لتحقيق غاياته. وتختلف هذه الغايات وفقًا لظروف الجريمة، وتشمل الأهداف المالية أو غير الأخلاقية أو المعنوية، ويستخدم المبتزون تقنيات متقدمة لإخفاء آثار الجريمة" .

الفرع الثاني: الابتزاز الإلكتروني في الفقه

عرَّف بعض الفقهاء الابتزاز بأنه إكراه يمارسه شخص على إرادة آخر ليجبره على فعل جريمة، وعرفه آخرون بأنه: "فعل يرتكبه شخص بتهديد آخر بالقول أو بالكتابة، باستخدام وسائل للتأثير على نفسية الضحية لتخويفه، أو لإزعاجه من خطر لم يحدث بعد، يترتب عليه إلحاق الضرر بماله، أو بشخصه، أو بشخص آخر ذي صلة بالمجني عليه"، وعُرِّف أيضًا بأنه: "تهديد شخص بفضح أمره ما لم يستجب لطلبات الجاني غير المشروعة التي تمس الشرف، أو تتعلق بحرمة الحياة الخاصة للضحية" .

(4) Kasmani, M. F., Ismail, R., Sulong, R. S., & Mahamod, Z. (2018). Cyber blackmailer: Modus operandi and preventive measures. International Journal of Cyber Criminology, 12(2), 334345-

كما عرف بأنه: "الحصول على مستندات أو صور أو معلومات عن الضحية باستخدام وسائل إلكترونية، أو التهديد بالتشهير بمعلومات ووثائق سرية باستخدام التقنيات الإلكترونية لتحقيق أهداف المبتز".[5]

وعرف بأنه: "القيام بالمحاولة للحصول على منفعة مادية أو معنوية من إنسان طبيعي أو شخص معنوي بالإجبار عن طريق تهديده بفضح سره أو استخدام القوة مقابل ضعف الضحية المؤقت أو الدائم"، وعرفه آخرون بأنه سلب إرادة وحرية شخص عن طريق إيذائه بدنيًا أو نفسيًا باستخدام أساليب لا أخلاقية.

كما يعرفه بعض الفقهاء بأنه سلوك غير مشروع يقع باستخدام المواقع الإلكترونية كمنصة (FaceBook)، أو الأجهزة الإلكترونية كالهواتف الذكية وغيرها، وهو أيضًا: "تهديد الجاني للمجني عليه عقب الحصول على معلومات حساسة له كمقاطع الصوت، أو الصور أو المقاطع المصورة أو المحادثات المكتوبة إلكترونيًا لتحقيق منفعة مادية أو معنوية"،[6] كما عرف بأنه: "الحصول على أسرار أو صور، أو مقاطع مصورة لشخص واستخدامها في إجباره على دفع مبالغ مالية للجاني أو إتيان أفعال يجرمها القانون أو تنافي الأخلاق، كتهديد الإناث بنشر صور خاصة لهن على مواقع الإنترنت، أو إبلاغ أقاربهن في حال لم يستجبن لمطالب المبتز".

يتبين من التعريفات السابقة للابتزاز التقليدي أو الإلكتروني أنه وسيلة لإجبار الضحايا أو تهديدهم بواسطة المبتز لتنفيذ إرادته، والابتزاز مرتبط بالتهديد، فلا يمكن أن تتحقق إرادة المبتز دونه.[7]

وعلى ذلك فجريمة الابتزاز الإلكتروني يقوم فيها الجاني باستخدام مهاراته التقنية وبرمجيات متطورة لاختراق المواقع والبيانات المخزنة على الوسائط المتصلة بالإنترنت أو بالشبكات المحلية والدولية، ويمكنه بواسطتها التوصل لبيانات حساسة؛ سواء بواسطة أشخاص أو مؤسسات لاستخدامها للحصول بالتهديد على غاياته الشخصية، أو تحقيق غايات آخرين.

(5) ام د / احمد سبتي احمد، اد/ محمد نعمان عبد النبي – الابتزاز الإلكتروني واثرة في تهديد المجتمع" دراسة فقهية معاصرة " - كانون الثاني 25, 2022 - مجلة جامعة تكريت للعلوم الانسانية المجلد -1 الجزء الاول عدد خاص بالمؤتمر لعام 2022 العدد 29 – ص55ص57 - https://jtuh.org/index.php/jtuh/article/view/1740

(6) شريفة محمد السويدي – د/ زيزيت مصطفي نوفل – اسباب الابتزاز الإلكتروني والاثار الاجتماعية والنفسية المرتبطة به " دراسة كيفية" – مجلة الآداب – العدد 146 – ايلول 2023م – ص616ص618 – Dio: https: //doi.org/10.31973/ 3583/aj.v1i146.4008https://aladabj.uobaghdad.edu.iq/index.php/aladabjournal/article/view/4008

(7) الباحث. باقر غازي حنون، أ.د. حسن حماد حميد - جريمة الابتزاز الإلكتروني (دراسة مقارنة(- مجلة دراسات البصرة - السنة السادسة عشرة / ملحق العدد (42) كانون الأول 2021 – ص53ص54

ويهدف المبتز غالبًا للحصول على مال من الضحية أو علاقة غير مشروعة، أو تلبية طلب طرف آخر تحقيقًا لمنفعة شخصية أو مكاسب مالية يحصل عليها عند تنفيذ المطلوب، كإفشاء أسرار شركة لمنافسيها، أو الحصول على معلومات تمس الأمن القومي لبيعها للأعداء، أو بيع بيانات مؤسسة إذا لم يتم الاستجابة لطلباته، كأن يطلب توظيفه فيها.[8]

ويرى الباحث تعريف الابتزاز الإلكتروني وفقًا لما انتهى إليه رأي الفقه على النحو التالي: "الابتزاز الإلكتروني هو استغلال الجاني للتقنيات الرقمية والبرمجيات المتطورة لاختراق البيانات أو الحصول على معلومات حساسة تخص الضحية؛ سواء كانت شخصًا طبيعيًا أو معنويًا، ثم استخدام تلك المعلومات لتهديد الضحية بنشرها أو استخدامها لتحقيق مطالب غير مشروعة. هذه المطالب قد تكون مالية، أو معنوية، أو غير أخلاقية، وغالبًا ما تكون مدفوعة بمصلحة شخصية أو لتحقيق مكاسب مالية، أو حتى خدمة لأطراف أخرى. ويتم ذلك التهديد عبر وسائل الاتصال الإلكتروني مثل البريد الإلكتروني، أو الرسائل النصية، أو منصات التواصل الاجتماعي، ويعتمد المبتز على التأثير النفسي والتخويف لإجبار الضحية على الامتثال".

الفرع الثالث: الابتزاز الإلكتروني في القانون القطري رقم 14 لسنة 2014م والقانون الإماراتي رقم 34 لسنة 2021م

أولًا: أركان جريمة الابتزاز الإلكتروني في القانون القطري رقم 14 لسنة 2014م:

كي تتحقق جريمة الابتزاز الإلكتروني، يجب أن تتوفر فيها أركان أساسية تشمل:

1. الركن المادي: ويتمثل في فعل التهديد المقترن بطلب معين من الضحية، ويشمل ثلاثة عناصر:

أ- فعل التهديد: هو السلوك الذي يقوم به الجاني لإيقاع الخوف أو الرعب في نفس الضحية، وقد يتم التهديد بطرق مختلفة؛ مثل إرسال رسائل تهديدية عبر البريد الإلكتروني أو الرسائل النصية، أو نشر معلومات خاصة بالضحية على وسائل التواصل الاجتماعي. ويشترط أن يكون التهديد جديًا وليس على سبيل المزاح، وأن يكون قادرًا على التأثير على إرادة المجني عليه.

(8) (Kshetri, N. (2010). "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives." Springer, 2010, pp: 3537-, http: //ndl.ethernet.edu.et/bitstream/12345678950/1/26704/.pdf

ب- الغاية من التهديد: يكون الهدف من التهديد هو إجبار الضحية على القيام بفعل محدد أو الامتناع عنه. والغاية قد تكون تحقيق منفعة مادية مثل المال، أو منفعة معنوية مثل الحصول على معلومات سرية. ويجب أن يكون التهديد مرتبطًا بغاية معينة لاعتبار الابتزاز الإلكتروني مكتمل الأركان.

ج- وسيلة التهديد: يحدد القانون القطري أن تكون وسيلة التهديد عبر تقنية المعلومات أو الشبكة المعلوماتية؛ أي أن الجريمة لا تقع بدون استخدام الوسائل الإلكترونية، مثل البريد الإلكتروني أو وسائل التواصل الاجتماعي.

2. الركن المعنوي: يتطلب الركن المعنوي في جريمة الابتزاز الإلكتروني وجود نية جنائية؛ أي أن الجاني لديه نية واضحة في إلحاق الضرر بالضحية، وتحقيق مكاسب غير مشروعة من وراء ذلك، ويجب أن يكون القصد الجنائي متوفرًا، بحيث يكون الجاني مدركًا وواعيًا لأفعاله ونتائجها، ويعتمد الركن المعنوي على عنصرين:

أ- القصد العام: ويشمل علم الجاني بأن فعله غير قانوني وأنه يستخدم وسيلة التهديد لإلحاق الخوف أو الضرر بالضحية.

ب- القصد الخاص: وهو رغبة الجاني في تحقيق هدف معين من جريمته، مثل الحصول على المال أو المعلومات أو أي منفعة أخرى.

ووفقًا للمادة 9 من القانون القطري لمكافحة الجرائم الإلكترونية (القانون رقم 14 لسنة 2014)، فإن العقوبة المقررة لجريمة الابتزاز الإلكتروني هي الحبس لمدة تصل إلى ثلاث سنوات، وغرامة تصل إلى مائة ألف ريال قطري. وقد يتم الحكم بإحدى هاتين العقوبتين أو بكلتيهما معًا حسب ظروف الجريمة وشدتها.

وتتنوع آراء الفقهاء وشروحاتهم حول المادة 9 من القانون القطري رقم 14 لسنة 2014 بشأن الابتزاز الإلكتروني، كما تعتمد على تفسير مبادئ الشريعة الإسلامية والقوانين الحديثة في مواجهة الجرائم الإلكترونية؛ حيث يتفق الفقهاء على أن الابتزاز الإلكتروني يمثل انتهاكًا للشريعة؛ إذ يقوم على الغش والتهديد والاستيلاء على حقوق الآخرين بغير وجه حق، وهذا العمل يعتبر محرمًا شرعًا لأنه يتضمن الإكراه والضرر، وهو ما حرمه الإسلام صراحة، ويشير العديد من الفقهاء إلى أن الابتزاز الإلكتروني يعد امتدادًا لمفهوم "الابتزاز" في الشريعة، ويشبهه كثيرًا بـ "التهديد" (الوعيد) للحصول على منفعة غير مشروعة. ووفقًا للشريعة يعتبر أي شكل من أشكال الاستغلال أو التهديد للحصول على مكاسب مادية أو

معنوية أمرًا محرمًا، كما يشدد الفقهاء على أن العقوبات المقررة في القانون تتماشى مع مقاصد الشريعة في تحقيق الردع وحماية الناس. ومن منظور إسلامي فإن الشريعة تجيز وضع قوانين حديثة تعاقب على الجرائم التي تهدد أمن الأفراد والمجتمع، بما في ذلك الجرائم الإلكترونية، كما يشير الفقهاء إلى أن الشريعة تحث على إزالة الضرر، فالابتزاز الإلكتروني يسبب ضررًا نفسيًا وماديًا للضحايا. وبالتالي فإن تجريم هذا الفعل يتفق مع مبدأ "لا ضرر ولا ضرار" في الإسلام، مما يعطي القوانين الوطنية الحق في فرض عقوبات لحماية الأفراد، ويوضح بعض الفقهاء أن الابتزاز الإلكتروني يمس العرض والكرامة، وهي أمور يجب حمايتها شرعًا، كما أن استخدام وسائل التهديد والإكراه على الإنترنت لمساس سمعة أو شرف شخص معين يعتبر من المحرمات، لذا فمن الضروري وجود قانون يعاقب على مثل هذه الجرائم لحماية خصوصيات الأفراد، ويرى الفقهاء أن سن قانون يحمي الناس من الابتزاز الإلكتروني يصب في مصلحة المجتمع، ويعزز الأمان والثقة في وسائل التواصل الإلكتروني. وإن الشريعة الإسلامية تبيح التشريعات الوضعية، مثل هذا القانون، إذا كانت تهدف إلى درء المفاسد وجلب المصالح.

بشكل عام، يثني الفقهاء على جهود الدولة في سن مثل هذا القانون وفرض عقوبات صارمة على جريمة الابتزاز الإلكتروني، ويعتبرونها خطوة ضرورية لحماية الأفراد والمجتمع من أضرار هذا النوع من الجرائم المتطورة التي ظهرت مع انتشار التكنولوجيا.[9]

وقد ركزت محكمة التمييز القطرية في حكم لها في جريمة الابتزاز الإلكتروني على أهمية توفر القصد الجنائي لدى المتهم في مثل هذه القضايا، فقد أكدت أن القصد الجنائي – كعنصر من عناصر الجريمة– يجب استخلاصه من الظروف المحيطة والأدلة المتوفرة، وأنه يدخل ضمن السلطة التقديرية لقاضي الموضوع. وبمعنى آخر، تُقِرُّ المحكمة بأن القصد الجنائي هو نية الجاني في تنفيذ التهديد لتحقيق مصلحة شخصية، ويتم استنتاجه من أفعال الجاني وسلوكه وظروف القضية، كما أكدت المحكمة أن التهديد عبر الوسائل الإلكترونية يعتبر جريمة مكتملة إذا كان التهديد جديًا ومصحوبًا بطلب من الضحية؛ مثل إجبارها على دفع المال أو القيام بأمر معين تحت طائلة تهديد بإيذاء سمعتها أو مصالحها.[10]

ثانيًا: الابتزاز الإلكتروني في القانون الإماراتي رقم 34 لسنة 2021م:

تعد جريمة الابتزاز الإلكتروني من الجرائم الخطيرة التي تهدد المجتمعات، ويعد التهديد والابتزاز سبب تجريمه، فالابتزاز الإلكتروني يمكن تعريفه بأنه: "تهديد شخص لحمله على

(9) جاسم ناصر جاسم المسلماني – التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري - مرجع سابق – ص21ص25

(10) الطعن 63 لسنة 2017 تمييز جنائي

القيام بفعل أو الامتناع عن فعل، ولو كان القيام بالفعل أو الامتناع عنه مشروعًا، وذلك باستخدام نظم المعلومات".

والابتزاز الإلكتروني له عدة أنواع، منها الابتزاز المادي، وهو تهديد الجاني للمجني عليه بالصور والمقاطع المرئية والمستندات على سبيل المثال، ومنها الابتزاز المعنوي، وهو تهديد الضحية بوسائل معنوية كاستخدام العبارات الشديدة لتهديده وتوعده بفضح أمره حتى يعتقد بجدية الجاني في تهديده، وتتنوع أهداف الجناة ما بين مادية و غير أخلاقية ونفعية.

وتتضمن المادة 42 من القانون الإماراتي أن كل من قام بابتزاز أو تهديد آخر لإجباره على إتيان فعل أو الامتناع عن فعل، وذلك باستخدام نظم المعلومات أو إحدى أدواتها، يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن 250000 درهم ولا تزيد على 500000 درهم، أو بإحدى العقوبتين، وتزاد العقوبة للسجن المؤقت الذي لا يزيد عن 10 سنوات إذا كان التهديد يتضمن إجبار الضحية على ارتكاب جريمة أو إسناد مسائل تمس الشرف أو الاعتبار بطلب صريح أو ضمني للقيام بعمل أو الامتناع عنه، وعلى ذلك فقد اعتبرها المشرع جنحة وشددها للجناية إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف والاعتبار .

وتنظم النيابة العامة حملات التوعية بأخطار الابتزاز الإلكتروني والوقاية من السلوكيات التي تعرض المستخدم للابتزاز عبر قنوات التواصل الاجتماعي والرد على الاستفسارات بخصوص الجريمة، كما أطلقت النيابة العامة تطبيق (مجتمعي آمن) الذي يتيح للأفراد الإبلاغ عن الجريمة التي تقع عبر مواقع التواصل الاجتماعي؛ بهدف تعزيز المشاركة المجتمعية في توفير الحماية للمجتمع من الجرائم الإلكترونية.[11]

تعتبر جريمة الابتزاز الإلكتروني ظاهرة تخترق قيم المجتمع المعاصر، كما تهدد أهداف المجتمع في ضمان سلامة أفراده، ولعل الجوهر والسبب في تجريم هذا الفعل هو الابتزاز والتهديد والضغط الذي يتم ممارسته على الضحية بتهديدها بكشف سره، وهو ما يُعَد بدوره أمرًا مشينًا، يجبر المجني عليه على الانصياع لإرادة الجاني والاستجابة لمطالبه كرهًا عنه وخوفًا من الفضيحة، مما دفع المشرع الإماراتي إلى إصدار قوانين تعاقب على هذا السلوك الإجرامي.

ويعتبر الابتزاز صورة من صور تعكير صفو الحياة وزعزعة استقرارها، وهز الشعور بالاطمئنان، الأمر الذي قد ينعكس سلبًا على حياة الفرد المبتز، مما جعل من هذه السلوكيات محلاً للتجريم من جانب المشرع الإماراتي.

(11) د . سعيد بالحاج - جريمة الابتزاز الإلكتروني - https://u.ae/fr/participate/blogs/blog?id=191

لذا فإن العقوبات الرادعة وفرض النظم والقوانين له دور فعال في مكافحة جريمة الابتزاز الإلكتروني، مما يعزز الدور الريادي لدولة الإمارات في مكافحة الجرائم الإلكترونية.[12]

المطلب الثاني: خصائص ودوافع جريمة الابتزاز الإلكتروني

الفرع الأول: خصائص جريمة الابتزاز الإلكتروني

الابتزاز كغيره من الجرائم والأفعال الآثمة الأخرى التي استفاد مرتكبوها من التقدم التقني والإلكتروني، ترتكب بالطرق التقليدية أو بالوسائل الإلكترونية. والابتزاز التقليدي هو الذي يتم من خلال وسائل تقليدية؛ مثل: مواجهة الجاني بالضحية مواجهة مباشرة، أو إرسال خطاب مكتوب بخط اليد يتضمن التهديد الذي يوجهه إليه، أو يتم إرسال التهديد من خلال شخص وسيط.

أما الابتزاز الإلكتروني فيقوم الجاني فيه باستغلال معرفته بالوسائل الإلكترونية؛ كالحاسوب الآلي، والهاتف المحمول بكافة صوره وتطبيقاته، للقيام بجريمته عبر الوسائل الإلكترونية؛ مثل إرسال رسالة تهديد عبر شبكة الإنترنت أو تطبيق الواتس آب، أو نشر الأمور التي يتم التهديد بإفشائها على وسائل التواصل الاجتماعي.[13]

ولجريمة الابتزاز الإلكتروني خصائص عديدة تتميز بها بشكل عام أو ترتبط بالوسائل الإلكترونية، وهو ما سنوضحه من خلال عرض هذه الخصائص على النحو التالي:

- تعد من الجرائم الإلكترونية؛ كونها لا تتم إلا بواسطة استخدام تقنية المعلومات، بالإستعانة بأجهزة متصلة بشبكة الإنترنت، وابتكار برامج معينة من أجل الوصول إلى البيانات الخاصة بالضحية.
- تنوع المصالح التي يلحقها الضرر من جراء ارتكاب جريمة الابتزاز، وهو ما عبر عنه البعض بِـ "تعدد المصلحة محل الحماية الجنائية"، فإذا قمنا بتحليل جريمة الابتزاز نجد من ناحية أنها عدوان على الحرية الشخصية للضحية أو المجني عليه، وقد جرم التهديد في ذاته؛ سواء اقترن بطلب أو تكليف بأمر أو لا، ومن ناحية أخرى نجد أن جريمة الابتزاز تمثل اعتداءً على ملكية المجني عليه وشرفه وسمعته، كما قد تلحق الضرر بكرامته أو بسلامته الشخصية.
- تتنوع جريمة الابتزاز الإلكتروني من حيث وقت ارتكابها إلى:

أ- جريمة وقتية؛ كأن تُهَدد امرأة شفاهةً بفضح سرها لزوجها كي يحصل منها على

(12) https: //www.munasaha.ae/ar/blogs/grym-l-btz-z-l-lktrony

(13) الطوالبة، علي (2008) الجرائم الإلكترونية، جامعة العلوم التطبيقية. مملكة البحرين، ص 60

مبلغ مالي أو منفعة غير أخلاقية، وينتهي التهديد بالتسليم، فغالبًا لا يحتاج ارتكابها إلى فترة طويلة من الزمن، مما يدفع بالجناة دائمًا إلى ارتكاب مثل هذا النوع من الجرائم بحرفية وابتكار؛ باستخدام وسائل التقنية الحديثة بهدف الحصول على المال الوفير في وقت قصير.

ب- جريمة مستمرة أو متتابعة؛ كأن يقوم المجرم بتهديد الضحية كل يوم بإفشاء أسرارها ما لم تسلم له مبلغًا من المال، أو الحصول على منفعة لا أخلاقية مستمرة.

- جريمة الابتزاز الإلكتروني من جرائم الضرر؛ إذ إنه يشترط لاكتمال السلوك الإجرامي المكون للركن المادي لهذه الجريمة أن تتحقق نتيجة معينة، بمعنى أن يقوم المجني عليه بتنفيذ المطلوب منه.
- الجناة في جريمة الابتزاز الإلكتروني غالبًا من الأصدقاء والأقارب؛ لعلمهم بمواطن الضعف لدى المجني عليه، كما أنها قد تمارس من الشريك في الجريمة المهدد بها؛ للحصول منه أو منها على مبلغ مالي، ونظرًا لتوافر هذا الاعتبار في الجناة ففي بعض الأحيان يكونون أحرص على السرية، والضحية يحاول إخفاء ما تعرض له من تهديدات من قبل الجاني خوفًا من انتشار الفضيحة بين الأصدقاء والأهل، والمقابل المطلوب القيام به من قبل المجني عليه قد يكون مشروعًا أو غير مشروع، وقد يكون عملًا أو امتناعًا عن عمل، وتتعدد مراحل الابتزاز الإلكتروني؛ حيث يمر غالبًا – أيًا كانت وسيلته- بست مراحل، هي: الطلب، والمقاومة، والضغط، والتهديد، والإذعان، والتكرار.[14]

ويرى الباحث أن الابتزاز الإلكتروني يتفرد كجريمة ضمن الجرائم الإلكترونية؛ لأنه لا يعتمد فقط على الفعل الإجرامي، بل يعتمد على استخدام التكنولوجيا بشكل متقدم ومبتكر للوصول إلى الضحية، وهذا يضع تحديات جديدة أمام الأجهزة الأمنية والمشرعين الذين يجب عليهم مواكبة تطورات هذه الجريمة التقنية.

الفرع الثاني: دوافع جريمة الابتزاز الإلكتروني

من الأسباب التي تدفع مرتكبي جرائم الابتزاز الإلكتروني لارتكاب جرائمهم تحقيق الربح المادي، أو الرغبة في إثبات الذات، كذلك الدافع في إقامة علاقة غير أخلاقية، وذلك بسبب عدم قدرته على بناء علاقات اجتماعية سوية، كما يمكن أن تكون دوافع الجناة

(14) جاسم ناصر جاسم المسلماني - التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري – مرجع سابق – ص11ص19

خارجية، كأن تدفع الحاجة بعض المنظمات أو الدول للاتصال بشاغلي الأماكن الحساسة في منظماتهم للعمل لدى منظمات أو دول أخرى للحصول على المعلومات والتقنيات المتوفرة لديهم، ويقوم لتحقيق ذلك برشوة أو إقناع أو إغراء الشخص المستهدف، وإذا رفض المغريات تعرض للابتزاز الإلكتروني بالوسائل المختلفة. وبناءً على ما سبق ستتم مناقشة الدوافع المادية وغير الأخلاقية والانتقامية والخارجية، على النحو التالي:

أولاً: دافع الحصول على المال[15]:

إذا كانت دوافع الجاني في جريمة الابتزاز الإلكتروني مالية فإن الجاني يهدد المجني عليه لتسليم نقود له، أو أشياء ذات طابع مادي باستخدام نظم المعلومات المختلفة، فيقوم الجاني بذلك بطريقة مباشرة؛ كأن يطلب الجاني المال مباشرة من المجني عليه، فيطلب منه تحويل مبالغ مالية بشكل مستمر له أو لغيره، أو بطريقة غير مباشرة كأن يطلب من المجني عليه تسديد مبلغ مالي كان قد اقترضه من البنك، أو دفع أقساط سيارة، أو يطلب منه القيام بكشف أسرار الشركة التي يعمل لديها، أو معرفة الأرقام السرية لحسابات الشركة، أو بإطلاق الشائعات ونشرها عنه إذا امتنع عن دفع المبالغ المالية التي يطلبها الجاني، أو عدم تلبية طلباته بهدف تركهم والابتعاد عنهم، مع الوعد بعدم التعرض لهم وعدم تشويه سمعتهم.

ثانيًا: الدوافع غير الأخلاقية[16]:

وقد يكون الدافع غير أخلاقي، وهو ما تتسم به هذه الجريمة في غالب أنماطها؛ حيث يقوم الجاني بتهديد المجني عليه بفضح أمره، أو إفشاء سره، أو الإبلاغ عنه مستغلاً ضعفه أمام تهديداته، وينقسم الابتزاز الجنسي إلى ابتزاز جنسي إلكتروني، ويتحقق عن طريق وسائل الاتصال عبر الإنترنت مثل ماسنجر فيس بوك، أو سكاي بي، أو مواقع الزواج، أو مواقع التوظيف، ويعد الجاني في هذه النوعية من الابتزاز مجرمًا خفيًا يسعى للوصول إلى معلومات حساسة للضحية، أما الابتزاز الواقعي فيتم عندما يقوم الجاني بجمع معلومات عن الضحية مستغلاً علاقته بها كالتقاط صور تسيء للضحية وهي بصحبته، أو أن يحصل على هذه المعلومات أو الوثائق السرية أو المقاطع الصوتية أو المرئية التي تخص المجني عليها بأساليب احتيالية، أو يحصل من الضحية على الأرقام السرية لبطاقات ائتمان ولي أمره دون علمه، ويهدده بفضح أمره في حال عدم تلبية طلباته غير الأخلاقية بتهديده بنشر تلك الوثائق.

(15) Paganini, P. (2018). "Understanding the motives behind cyber extortion: A deep dive into ransomware attacks." Journal of Information Security and Applications, 43, 2332-, DOI: 10.1016/j.jisa.2018.06.004

(16) Holt, T.J., & Smirnova, O. (2014). "Exploring the market for cybercrime tools: Characteristics of buyers and sellers in a digital underground economy." Journal of Criminal Justice, 42(1), 2738-, DOI: 10.1016/j.jcrimjus.2013.11.005

ثالثًا: دافع الانتقام:

يتحقق الدافع الانتقامي بتلذذ الجاني بأذية المجني عليه واستمتاعه بتوسلاته وحتى ببكائه، ومما يزيد الأمر سوءًا أن يقوم الجاني بتصوير المجني عليه ويطلب منه ذكر اسمه أو أي بيانات تتعلق به، كما قد يكون الدافع لدى الجاني هو الانتقام من المجني عليه عن طريق إلحاق الأذى به وإساءة سمعته بنشر صوره؛ إما عن طريق شبكة الإنترنت، أو عن طريق الهواتف الذكية المزودة بكاميرا، أو عن طريق خدمة الواتس آب، والتي تعتبر من أحدث الطرق في الزمن الحاضر لسرعة انتشارها، أو أن يقوم الجاني بابتزاز المجني عليه إذا كان أنثى؛ بمنعها من الزواج بهدف الإضرار بها أو الانتقام منها.

رابعًا: دافع تحقيق الاستفادة:

يتمثل في تصوير بعض الأشخاص في المناصب الحساسة (العسكرية مثلاً) في أوضاع غير أخلاقية، وبعد ذلك يتم اللجوء إلى تهديدهم وإجبارهم على إفشاء معلومات سرية تتعلق بأمن الدولة، أو التصنيع العسكري، والأسرار والتحركات للقطع العسكرية[17].

وقد تلجأ بعض الشركات الكبرى من أجل المنافسة إلى استغلال عاملين لدى شركات منافسة أخرى للحصول على بيانات مالية أو معلومات إدارية حول وضع الشركة المالي أو تعثرها الإداري ومشاكل تعيق استمرار نشاطها في السوق، وتهديدهم وابتزازهم من أجل الحصول على هذه المعلومات عن الشركات المنافسة، لاستغلالها في تحقيق مكاسب سوقية وتعطيل نمو الشركات المنافسة، أو الحصول على معلومات عن أسرارها الصناعية أو التجارية أو مصادر البضاعة فيها أو الأسعار الحقيقية للسلع.

ويرى الباحث أن الدوافع التي قد تدفع المبتز إلى ارتكاب جرائمه تتضمن دوافع مادية، وهي رغبته في الحصول على المال باستغلال أسرار وخصوصيات الآخرين التي ينشرونها عن غير وعي بمخاطر نشرها أو تبادلها مع الآخرين، أو استدراج الضحية إلى إفشاء أسرارها ثم استغلالها بعد ذلك، أو نفسية تتمثل في الرغبة في إذلال الآخرين سواء لدوافع انتقامية أو لأسباب نفسية لدى الجاني، أو اجتماعية بسبب التفكك الأسري، أو الرغبة في إكراه الآخرين على علاقات اجتماعية غير مرغوبة نظرًا لعدم قدرة المبتز على الانخراط في علاقات اجتماعية صحية وسليمة.

(17) أطروحة ماجستير بعنوان "الابتزاز الإلكتروني للفتاة عبر مواقع التواصل الاجتماعي " الفيسبوك نموذجًا" دراسة مسحية لعينة من طالبات قسم الإعلام والاتصال – جامعه قاصدي مرباح " تخصص تكنولوجيا الاتصال الجديدة – الجزائر – مقدمة من سمان جويدة، إيمان مردف 2017م – ص23ص25 - https: //dspace.univ-ouargla.dz/jspui/ samane-mardaf.pdf/1/14448/bitstream/123456789

الفرع الثالث: أنماط ومحاور الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

أولاً: أنماط الابتزاز عبر مواقع التواصل الاجتماعي:

تستخدم مصطلحات الابتزاز والابتزاز الجنسي بانتظام بشكل تبادلي، على الرغم من اختلاف معانيها؛ حيث إن الابتزاز ينطوي على استخدام القوة والعنف أو التهديد باستخدامها للحصول على أموال نقدية أو سلع أخرى ذات قيمة، كما يتضمن الابتزاز الإكراه من خلال التهديد بكشف معلومات حول الضحية للآخرين، وإن الابتزاز الإلكتروني ينطوي على تهديد الضحايا بتدمير الممتلكات أو البيانات[18]، كما ينطوي على الإكراه من خلال التهديد بإفشاء معلومات حساسة عن الضحية يمكن أن تضر بسمعتهم، وتم تعريف المعلومات الحساسة بأنها: "المعلومات التي يمكن استخدامها لتمكين الخصوصية أو الإضرار بالأمان عند وضعها في الأيدي الخطأ"، فيمكن أن يشمل الابتزاز الإلكتروني اختراق جهاز كمبيوتر والتهديد بإتلاف البيانات، كما يتضمن ممارسة السلطة على الضحايا بتهديدهم بنشر معلومات حساسة يمكن أن تضر بسمعتهم إذا لم يمتثلوا لمطالب الجاني.

أما مصطلح Sextortion فيشمل أحد أنماط الابتزاز الإلكتروني الذي يقوم على استخدام البيانات غير الأخلاقية للضحايا [19] على مواقع التواصل الاجتماعي، فيتمكن الجناة من الحصول على معلومات حساسة من خلال تحليل محتوى حسابات وسائل التواصل الاجتماعي، أو إهمال المستخدم، أو الاستيلاء على هذه البيانات من الضحايا عن عمد ووعي. ومن الملاحظ أن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي صار أكثر شيوعًا؛ حيث يتم جمع المعلومات عادةً من الملفات الشخصية على وسائل التواصل الاجتماعي أو الاستيلاء عليها بخداع المستخدمين؛ فَقَد أفادت بعض الإحصاءات أن 6 إلى 8 بالمائة من الشباب التشيكي (الذين تتراوح أعمارهم بين 8 و17 عامًا) تعرضوا للابتزاز على مواقع التواصل الاجتماعي؛ حيث طلب المبتزون الأموال وعلاقات غير أخلاقية أو صور فاضحة للضحية وأشياء أخرى من الضحايا، وفي حالات ابتزاز أخرى عبر مواقع التواصل الاجتماعي انتحر الضحايا بسبب الابتزاز، كما أفادت دراسة بزيادة حالات الابتزاز على مواقع التواصل الاجتماعي في دول مجلس التعاون الخليجي؛ إذ يتم الإبلاغ عن 30 ألف حادثة من هذا القبيل سنويًا من قبل دول مجلس التعاون الخليجي، و80 بالمائة من هذه الحوادث تتعلق باستهداف النساء بمحتوى غير أخلاقي. كما أن ابتزاز الأطفال على وسائل

(18) Wang, Y., & Stefanone, M. A., "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality", New Media & Society, 2022., pp: 535541-

(19) Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525540-. https: //doi.org/10.1057/s412842-00246-020-

التواصل الاجتماعي يتم فيه استخدام الأدلة أو الصور المثيرة للحصول على فوائد حسية أو أموال نقدية، وقد ارتفع هذا الأمر أيضًا بشكل كبير في العقد الماضي.

ومن أنماط الابتزاز الإلكتروني ما تتعرض له المؤسسات عبر مواقع التواصل الاجتماعي؛ حيث يهدد الأفراد بتشويه سمعتها فيطلب المبتزون الأموال أو الخدمات غير الأخلاقية أو أداء خدمة مشروعة أو غير مشروعة، ولا شَكَّ أن الوقوع ضحية للابتزاز يمكن أن يشوه اسم الضحية وسمعة عائلته، كما قد يؤدي إلى ضائقة نفسية قد تصل إلى الانتحار، ويمكن أن يساهم هذا الأمر في ازدياد مشاعر القلق أو الخوف أو الاكتئاب أو اضطرابات التكيف الاجتماعي التي قد تؤدي إلى العزلة الاجتماعية والخوف من مواجهة الناس.

وبالنسبة للأطفال، يمكن أن تشمل الآثار الجانبية لوم الذات، والذكريات أو المشاعر الغازية، والتعاسة، وتدني احترام الذات، والأحلام السيئة، والأرق، والعصبية، ونوبات القلق، والصعوبات التعليمية. وعلى الرغم من هذه العواقب، تشير الأبحاث إلى أن الناس غالبًا ما يكونون عرضة لأن يصبحوا ضحية للابتزاز على وسائل التواصل الاجتماعي؛ بسبب ميلهم إلى الكشف عن معلومات حساسة عبر الإنترنت.[20]

الإفصاح عن الشخصية الحقيقية عبر مواقع التواصل الاجتماعي يتضمن مشاركة معلومات حساسة مع أشخاص آخرين فهو نشاط متعمد يشارك فيه الشخص ممارساته الشخصية وصوره وعواطفه مع الآخرين، وتم تعريف الكشف عن الذات عبر الإنترنت على أنه الكشف عن الذات الذي يحدث عبر الإنترنت، ويتم الترويج للإفصاح الذاتي عبر الإنترنت من خلال منصات وسائل التواصل الاجتماعي نظرًا لقيمته التجارية.

ويركز المجرمون وأعضاء جماعات الجريمة المنظمة على استخدام مواقع التواصل الاجتماعي لابتزاز المستخدمين بسبب الميل الأكبر لمستخدمي مواقع التواصل الاجتماعي للكشف عن شخصياتهم الحقيقية على مواقع التواصل الاجتماعي، وقد سعت جهود مكافحة الابتزاز على مواقع التواصل الاجتماعي للحد من هذه الجرائم من خلال رفع مستوى الوعي بمخاطر استخدام الإنترنت، وتقديم المشورة حول كيفية تجنب الوقوع ضحية لهذا الجرائم، وتسعى هذه الحملات للحد من مشاركة المعلومات الشخصية الحساسة على مواقع التواصل الاجتماعي، ومع ذلك يستمر المستخدمون في تبادل هذه المعلومات.

(20) Authors. Alma Spaniardi, Janki Modi Avari, Teens, Screens, and Social Connection An Evidence-Based Guide to Key Problems and Solutions, 2023, Jenna Margolis and Dinara Amanbekova, Social Media and Cyberbullying, pp: 81: 83, https: //doi.org/10.10077-24804-031-3-978/

إنَّ بعض الأسباب المطروحة لتفسير الإفصاح عن الشخصية والبيانات عبر مواقع التواصل الاجتماعي تتضمن الفشل في فهم مخاطر مشاركة المعلومات الحساسة، والتركيز على متعة الانخراط في هذا النشاط وإمكانية السماح للعلاقات بالتطور[21].

ويرى الباحث أن أنماط الابتزاز الإلكتروني أصبحت أكثر تعقيدًا وانتشارًا مع تزايد استخدام وسائل التواصل الاجتماعي، وأن الجرائم التي تستهدف الضحايا عبر الإنترنت ليست مادية أو غير أخلاقية فقط، بل لها تداعيات نفسية واجتماعية خطيرة قد تصل إلى الانتحار، وإنَّ الجهود المبذولة للحد من هذه الجرائم تحتاج إلى تعزيز الوعي حول مخاطر الكشف عن الذات عبر الإنترنت، وتعليم الأفراد كيفية حماية خصوصياتهم على هذه المنصات.

ثانيًا: محاور الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي:

1- التعرض للإيذاء:

تم تحديد العمر والجنس والميل إلى الكشف عن الذات عبر الإنترنت والرغبة في استخدام وسائل التواصل الاجتماعي لإرسال صور حميمة كعوامل خطر للوقوع ضحية للابتزاز على وسائل التواصل الاجتماعي. وكان الشباب أكثر عرضة لخطر الوقوع ضحية لهذا النشاط من كبار السن، ويعتقد أن الأشخاص الذين تتراوح أعمارهم بين 15 و25 عامًا هم الأكثر عرضة للخطر[22]، ويعتقد أيضًا أن الإناث أكثر عرضة للخطر من الذكور بسبب ميل الإناث إلى التعرض لضغوط أكبر لنشر صور حميمة لأنفسهن على وسائل التواصل الاجتماعي.

كما لوحظ وجود علاقة بين الانخراط في الإفصاح عن البيانات الشخصية والوقوع ضحية للابتزاز على مواقع التواصل الاجتماعي؛ حيث إن الذين يكشفون عن معلوماتهم الشخصية أكثر عرضة للوقوع ضحية للابتزاز، كما أن مشاركي الصور الشخصية الجنسية معرضون لخطر الوقوع ضحية للابتزاز على مواقع التواصل الاجتماعي[23]، كما أن عدم الوعي بمخاطر استخدام مواقع التواصل الاجتماعي فيما يتعلق بالتبعات القانونية لإنشاء ومشاركة صور غير أخلاقية للأطفال، فضلاً عن تصميم وسهولة استخدام تطبيقات الوسائط الاجتماعية، يزيد من احتمالية إنشاء مثل هذه الصور ومشاركتها، وبالتالي الوقوع

(21) Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats" by Will Gragido, John Pirc, Nicholas Hoffman, & Daniel Molina, Syngress, 2011, pp: 2022-

(22) Cybercrime and Digital Forensics: An Introduction" by Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Routledge, 2017,

(23) Abdullah Al Habsi · Michelle Butler · Andrew Percy, Blackmail and the self-disclosure of sensitive information on social media: Prevalence, victim characteristics and reporting behaviours amongst Omani WhatsApp users", Security Journal, 2023, pp: 250: 252, https: //doi.org/10.1057/s412843-00376-023-

ضحية للابتزاز. ويمكن أن يؤدي تصميم تطبيقات الوسائط الاجتماعية وسهولة استخدامها أيضًا لزيادة التعرض للابتزاز من خلال الترويج لمزيد من الإفصاح عن الهوية الحقيقية للمستخدمين، وسهولة إنشاء الصور غير الأخلاقية وتوزيعها، ودوام الصور ومستوى الأمان بإنشاء حسابات الوسائط الاجتماعية، فالتطبيقات التي شجعت ميزاتها على الكشف عن المعلومات والصور، وجعلت إنشاء الصور وتوزيعها أسهل، واحتفظت بالصور وسمحت بإنشاء حسابات بمعلومات كاذبة، يمكن أن تسهل حدوث الابتزاز.

2- التباين الثقافي في الوعي:

إنَّ الدليل على الدور المهم الذي يمكن أن تؤديه المعايير الثقافية في تشكيل مواقف الناس ودوافعهم للانخراط في الكشف عن الذات على وسائل التواصل الاجتماعي واضح أيضًا، فضلاً عن وعيهم باحتمال أن يصبحوا ضحية للابتزاز على وسائل التواصل الاجتماعي. وقد أشارت الدراسات التي أجريت في الدول الغربية إلى أن الناس غالبًا ما يشعرون بأن المعايير الثقافية تشجع على نشر المحتوى غير الأخلاقي على حسابات وسائل التواصل الاجتماعي؛ حيث يسعى الناس إلى زيادة جاذبيتهم وتفاعلاتهم مع المستخدمين الآخرين على وجه الخصوص، وأبلغت الإناث أنه طلب منهن مشاركة صور حميميَّة؛ حيث ذكر البعض أنهن شعرن بالضغط لمشاركة مثل هذه الصور من أجل الحفاظ على تفاعلاتهن، ومع ذلك أفاد مستخدمو وسائل التواصل الاجتماعي في الدول الغربية بأنهم أقل وعيًا باحتمال حدوث ابتزاز أو الإضرار بالسمعة نتيجة لمشاركة مثل هذه المعلومات على وسائل التواصل الاجتماعي، في المقابل تميل المعايير الثقافية في البلدان العربية إلى الحد من نشر المحتوى غير الأخلاقي على مواقع التواصل الاجتماعي وخاصة بالنسبة للنساء؛ حيث تميل النساء إلى مواجهة ضرر أكبر بسمعتهن ومكانة اجتماعية منخفضة إذا انخرطن في مثل هذا السلوك، ونتيجة لذلك فإنهن أكثر وعيًا باحتمال حدوث ابتزاز وإلحاق الضرر بالسمعة إذا شاركوا معلومات شخصية حساسة على وسائل التواصل الاجتماعي، وقد أدت هذه المعايير الثقافية والعواقب الاجتماعية المحتملة التي قد تتبع مثل هذا الإفصاح إلى التعبير عن مخاوف جدية بين النساء العربيات بشأن خصوصيتهن على وسائل التواصل الاجتماعي، وكيف يمكن استخدام المعلومات التي شاركنها لابتزازهن من قبل مستخدمي وسائل التواصل الاجتماعي الآخرين، وعلى الرغم من هذه المخاوف، تم اقتراح المعايير الثقافية التي تقيد تطور العلاقات خارج الإنترنت في الثقافات العربية، وخاصة بالنسبة للنساء، لتحفيز الناس على الانخراط في الكشف عن الذات بشكل أكثر حرية وانفتاحًا على

وسائل التواصل الاجتماعي؛ حيث استخدموا وسائل التواصل الاجتماعي لتطوير علاقات جديدة، متحررين من القيود التي يواجهونها في تعاملاتهم الاجتماعية في المجتمع.[24]

وعلى الرغم من الوعي المتزايد باحتمال حدوث الابتزاز وعواقبه الخطيرة، فقد استمر الناس في الثقافات العربية في تعريض أنفسهم لخطر الابتزاز على وسائل التواصل الاجتماعي أثناء سعيهم لبدء علاقات جديدة مرغوبة، وتثير مثل هذه الأبحاث تساؤلات حول مدى نجاح حملات التوعية في تغيير السلوك وتقليل مخاطر الابتزاز على وسائل التواصل الاجتماعي، فضلاً عن إظهار الحاجة إلى مزيد من البحث لفهم كيفية تفاعل الأعراف والمواقف والمعتقدات الثقافية مع بعضها البعض للتأثير على السلوك.

3- استخدام الإكراه في الابتزاز:

تم استخدام أسلوبين رئيسين من المبتزين للحصول على معلومات حساسة من ضحاياهم، الأول حيث قام الضحايا بمشاركة معلومات أو صور حساسة مع المبتز أو قام المبتز بتسجيلها أثناء مشاركتهم طوعًا في نشاط حساس عبر كاميرا الويب فقط، وعندما انهارت هذه العلاقات أو عندما لم يعد الضحايا على استعداد لمشاركة المعلومات أو الصور أو مقاطع الفيديو الحساسة مع مرتكب الجريمة، بدأ الابتزاز مع إجبار الضحايا على إعادة بدء العلاقة أو الاستمرار في الكشف عن معلومات حساسة.

الثاني هو الصور أو مقاطع الفيديو؛ حيث يقوم المبتز بالتلاعب عاطفيًا بالضحية للكشف عن معلوماتها الحساسة بالادعاء بأنه مكتئب أو لديه ميول انتحارية ومحاولة إثارة الشعور بالذنب أو الالتزام لدى الضحية لمساعدتها من خلال مشاركة هذه البيانات، وقد تبين أن البالغين والشباب - على حد سواء- كانوا ضحايا لهذه الأساليب الإكراهية.

وتبين أيضًا من الحالات العديدة أن الشباب الذين يقعون ضحايا للابتزاز على مواقع التواصل الاجتماعي هم أكثر عرضة للإبلاغ عن استخدام هذه الأساليب الإكراهية ضد الآخرين، مما يؤدي إلى إدامة الانتهاكات، ومع ذلك فمن غير الواضح ما إذا كان البالغون يواجهون دورة مماثلة من الضحية إلى الجاني، أو ما هي الآليات التي قد تسبب هذا التحول.[25]

(24) Tommy K.H. Chan, Christy M.K. Cheung, Zach W.Y. Lee, Cyberbullying on Social Networking Sites : A Literature Review and Future Research Directions" , Information & Management, Volume 58, Issue 2, March 2021, 103411, pp: 12: 14 https: //www.sciencedirect.com/science/article/pii/S0378720620303499?via%3Dihub

(25) Nash, M. (2020). "Coercion, Consent, and the Criminal Law: Understanding the Limits of Criminal Liability." Criminal Law Review, 1, 2439-. DOI: 10.2139/ssrn.3563456

4- الكشف عن الذات على وسائل التواصل الاجتماعي:

تم التحقيق في الكشف عن الذات على وسائل التواصل الاجتماعي من بين 67 دراسة تمت مراجعتها، فحصت الأغلبية (41 من أصل 67) بشكل مباشر سبب مشاركة الأشخاص في الكشف عن أنفسهم على وسائل التواصل الاجتماعي أو العوامل التي يمكن أن تزيد من احتمالية انخراط الفرد في هذا السلوك، وركز الباقي على استخدام وسائل التواصل الاجتماعي بشكل عام، مع الإشارة إلى الكشف عن الذات ضمن النتائج التي توصلوا إليها.

وقد بينت الدراسات أن الإفصاح عن الذات مرتبط بالوقوع ضحية للابتزاز عبر مواقع التواصل الاجتماعي؛ حيث أشارت إلى أن الإفصاح عن الهوية الحقيقية عند التواصل عبر مواقع التواصل الاجتماعي يزيد من مخاطر الوقوع ضحية للابتزاز، وسلطت الضوء على قدرة المعايير الثقافية على تشكيل المواقف ودوافع الانخراط في الكشف عن الذات على وسائل التواصل الاجتماعي.

وحددت الدراسات في هذا المجال ثلاثة مواضيع رئيسة: الحاجة إلى العلاقات والكشف عن الشخصية، والانفصال بين المخاوف المتعلقة بالخصوصية والكشف عن الشخصية عبر الإنترنت، وتأثير ميزات المنصة على الكشف عن الشخصية. وإنَّ الحاجة إلى العلاقات والتعبير عن الشخصية هو أحد أكبر العوامل التي تؤثر على الكشف عن الشخصية على وسائل التواصل الاجتماعي، وهو الدافع لدى الشخص لاستخدام وسائل التواصل الاجتماعي. كما قرر العديد من مستخدمي مواقع التواصل ممن يفصحون عن شخصياتهم الحقيقية عبر الإنترنت برغبتهم في استخدام وسائل التواصل الاجتماعي للحفاظ على العلاقات، وهو ما دعاهم للتواصل مستخدمين هوياتهم الحقيقية لتعميق صداقاتهم واكتساب المكانة الاجتماعية أو القبول أو الدعم والتحقق من الصحة[26].

كما تبين بعض الدراسات أن مستخدمي مواقع التواصل يقومون بالإفصاح عن معلوماتهم الشخصية لإدارة الانطباع الذي تولد لدى الآخرين؛ حيث يكشف المستخدمون عن المعلومات التي تساعدهم في تحقيق أهداف علاقتهم، بينما يرغب مستخدمو مواقع التواصل الاجتماعي في التعبير عن الذات للإفصاح التلقائي أثناء تعبيرهم عن أنفسهم عبر الإنترنت.[27] على وجه الخصوص، الأشخاص الذين عاشوا في البيئات التي أيدت

(26) "Coercion and Responsibility in Criminal Law: A Study of the Limits of Criminal Liability" by Douglas Husak, Oxford University Press, 2020, pp: 22: 24

(27) Pemberton, A., Winkel, F.W., & Groenhuijsen, M.S. (2007). "Taking victims seriously in restorative justice: A crime victim and human rights perspective." European Journal of Crime, Criminal Law and Criminal Justice, 218220-.

العادات الاجتماعية التي تفرض ضوابط سلوكية وأخلاقية في المجتمع خارج الإنترنت، كانوا يستخدمون مواقع التواصل الاجتماعي للتعبير عن ذواتهم "الحقيقية" والانخراط في الكشف عن الذات عبر الإنترنت كوسيلة لتلبية احتياجاتهم التعبيرية والعاطفية، كما هو الحال مع الدراسات التي تبحث في الابتزاز عبر مواقع التواصل الاجتماعي، فقد سعت العديد من الدراسات أيضًا إلى تحديد مخاطر كشف مستخدمي مواقع التواصل الاجتماعي لشخصياتهم الحقيقية؛ حيث توصلت هذه الدراسات إلى أن العمر والانفتاح وضبط النفس والكفاءة الذاتية أثرت على كمية ونوعية البيانات الشخصية والمعلومات التي يقوم مستخدمو مواقع التواصل الاجتماعي بالإفصاح عنها.

أما الذين كانوا أصغر سنًّا وأكثر انفتاحًا، فقد كانت لديهم مستويات أقل، بينما كان ضبط النفس وزيادة الكفاءة الذاتية في استخدام وسائل التواصل الاجتماعي والتلاعب بها أكثر عرضة لكشف معلوماتهم على وسائل التواصل الاجتماعي، وبالتالي فإن الدوافع الكامنة وراء استخدام مواقع التواصل الاجتماعي، بالإضافة إلى الخصائص الفردية مثل العمر والشخصية والسمات النفسية، يمكن أن تؤثر على مقدار ونوع الكشف عن الذات الذي يشارك فيه الأشخاص على وسائل التواصل الاجتماعي، وكشفت الدراسات أيضًا أن الناس كانوا قلقين بشأن خصوصيتهم على وسائل التواصل الاجتماعي.[28]

أما معظم الدراسات التي تبحث في كيفية تأثير المخاوف المتعلقة بالخصوصية على الميل إلى الانخراط في الكشف عن الذات على وسائل التواصل الاجتماعي، فلم تتوصل إلى أي دلائل على أن المخاوف المتعلقة بالخصوصية تؤثر بشكل مباشر على سلوك الكشف عن الذات، وعند تحديد موعد الكشف عن المعلومات على وسائل التواصل الاجتماعي كان الناس يميلون إلى الانخراط في تحليل التكلفة والعائد للإيجابيات والسلبيات التي يعتقدون أنها مرتبطة بالمشاركة في الكشف عن الذات عبر الإنترنت.[29]

ثم توصل هذا التحليل إلى تقليل الجوانب السلبية عند اتخاذ القرار بشأن ما إذا كان سيتم الكشف عن المعلومات على وسائل التواصل الاجتماعي أم لا؛ حيث تم التقليل من أهمية السلبيات المترتبة على الإفصاح عن الشخصية عبر الإنترنت، في حين تمت المبالغة

(28) د. هشام رشدي خير الله – ادراك المراهقات لمخاطر الابتزاز الإلكتروني عبر الانترنت وتأثيره على اتجاهاتهم نحو استخدام تطبيقات التواصل الاجتماعي عبر الهواتف الذكية "دراسة في ضوء مجتمع المخاطر" – المجلة العلمية لبحوث الصحافة – عدد 24 – الجزء الاول – يوليو 2022 – ص123

(29) "The Impact of Self-Disclosure on Social Media on Personal Relationships: A Cross-Cultural Analysis" by Bazarova, N. N., & Choi, Y. H., Journal of Communication, 2020., DOI: 10.1093/joc/jqz052

فـي تقديـر الـمنفعة الـمترتبة على الإفصـاح عـن الشـخصية الحقيقيـة فـي العلاقـات والتعبيـر عـن الـذات، ومـع ذلـك يمكـن أن تؤثـر الـمخاوف الـمتعلقة بالخصوصيـة على موقـع التواصـل الاجتماعـي الـذي يسـتخدمه الشـخص ومـدى تفعيـل ضوابـط الخصوصيـة فـيها، فـيمكن أن تشـجع الـمخاوف الـمتعلقة بالخصوصية الـمستخدمين على الحد من ظهور ملفاتهم الشـخصية على وسـائل التواصـل الاجتماعـي، وتقييـد تفاعلاتهـم مـع مسـتخدمين غيـر معروفـين.

وعلـى الرغـم مـن الـمخاوف الـمتعلقة بالخصوصيـة، لا يـزال الـمستخدمون يكشـفون عـن معلوماتهـم الشـخصية علـى مواقـع التواصـل، ممـا يمكنهـم مـن عـرض ملفاتهـم الشـخصية للـمتفاعلين معهـم، ممـا يعـزز مـن تأثيـر الـمخاوف الـمتعلقة بالخصوصيـة علـى مـا كان مرئيًـا للعامـة ومـع تفاعـل الـمستخدمين، وليـس نوعيـة أو كـم الـمعلومات التـي كشـفوا عنهـا.

كمـا أنـه بـدلاً مـن أن تؤثـر مخـاوف انتهـاك الخصوصيـة علـى كـم الـمعلومات الشـخصية التـي يتـم مشـاركتها عبـر مواقـع التواصـل الاجتماعـي، فـإن مـدى الكشـف عـن البيانـات الشـخصية عبـر الإنترنـت مقبـول اجتماعيًـا، فـإذا كان الإفصـاح عـن الشـخصية الحقيقيـة للـمستخدم مقبـول اجتماعيًـا بيـن الـمستخدمين، فإنهـم يكونـون أكثـر ميـلاً لذلـك.

وقـد أكـدت الدراسـات العديـد مـن الـمخاوف بشـأن فعاليـة رفـع الوعـي للحـد مـن التعـرض للابتـزاز، فركـزت علـى تزايـد مخـاوف انتهـاك خصوصيـة الـمشاركين كوسـيلة لتقليـل احتمـال تعرضهـم للوقـوع ضحايـا لجرائـم الابتـزاز الإلكترونـي، وقـد حققـت هـذه التـدخلات نجاحًـا محـدودًا بسـبب اخـتلاف مخـاوف الخصوصيـة وبيـن الـمشاركة فـي الإفصـاح عـن الشـخصية عبـر الإنترنـت فـي هـذه الدراسـات.[30] بـل يمكـن أن تحقـق التـدخلات نجاحًـا أكبـر مـن خـلال العمـل علـى تغييـر التقاليـد الاجتماعيـة التـي تقبـل وتشـجع الكشـف عـن الـذات علـى مواقـع التواصـل الاجتماعـي.

وفـي تأثيـر ميـزات النظـام الأساسـي على الكشـف عن الذات، كان الـموضوع الرئيسـي الأخيـر الـذي بـرز مـن هـذه الدراسـات هـو التأثيـر الـذي يمكـن أن تحدثـه ميـزات النظـام الأساسـي لتطبيقـات الوسـائط الاجتماعيـة علـى الـميل إلـى الـمشاركة فـي الكشـف عـن الذات على وسـائل التواصـل الاجتماعـي.[31]

(30) Self-Disclosure and Psychological Well-Being in the Age of social media: A Meta-Analysis" by Nguyen, M. H., Bin, Y. S., & Campbell, A., Cyberpsychology, Behaviour, and Social Networking, 2021., DOI: 10.1089/cyber.2020.0329

(31) "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality" by Wang, Y., & Stefanone, M. A., New Media & Society, 2022., DOI: 10.1177146144482110451 48/

وقد تبين أن مقدار وطبيعة ضوابط الخصوصية المتاحة في تطبيقات الوسائط الاجتماعية المختلفة تعمل على توليد الثقة، فكلما شعر المستخدمون بثقة أكبر في هذه التطبيقات، زاد ميلهم إلى الإفصاح عن أنفسهم عبر الإنترنت، بالإضافة إلى ذلك فإن مدى شعور الأفراد بأنهم يستطيعون الثقة في المستخدمين الآخرين لتطبيقات وسائل التواصل الاجتماعي أثر على سلوكهم في الكشف عن الذات، مع ارتباط مشاعر الثقة الأكبر بمزيد من الإفصاح عن الذات.

إن مدى إمكانية تشفير المحتوى، وسهولة التقاط الصور ومشاركتها مع الآخرين، وما إذا كان المحتوى مؤقتًا أو دائمًا بطبيعته، أثر أيضًا على مدى الكشف عن الذات على وسائل التواصل الاجتماعي، فإذا كان المحتوى مشفرًا، فهذا يسمح للمستخدمين بالشعور بالتحكم في الأشخاص الذين يشاركون معلوماتهم معهم، ويمكن أن يؤدي إلى مزيد من الاتصال عبر الإنترنت الكشف عن الذات، وكان هذا على الرغم من إمكانية قيام مستخدمين آخرين بمشاركة هذا المحتوى دون موافقتهم. وبالمثل إذا كانت تطبيقات الوسائط الاجتماعية سهلة الاستخدام ومجانية وتسهل مشاركة الصور، فإن ميزات التصميم هذه تميل إلى تشجيع المزيد من الكشف عن الذات ومشاركة الصور.

بالإضافة إلى ذلك، إذا اعتقد الأفراد بأن صورهم وبياناتهم ستتم مشاركتها مع الآخرين مؤقتًا مثل Snapchat، فإنهم يميلون إلى أن يكونوا أكثر حرمانًا من الإفصاح عن أنفسهم عبر الإنترنت، ويمكن أن تؤثر أيضًا ميزات التصميم والمنصة المختلفة لتطبيقات الوسائط الاجتماعية على الغرض الذي يستخدمه الأفراد لتطبيقات الوسائط الاجتماعية، وبالتالي مقدار ونوع الكشف الذاتي عبر الإنترنت الذي يشارك فيه المستخدمون في هذا التطبيق.[32]

أخيرًا، إذا كان الأفراد راضين عن التصميم وميزات النظام الأساسي لتطبيقات الوسائط الاجتماعية، فمن المرجح أيضًا أن يقوموا بالإفصاح عن أنفسهم بهذه الطريقة، ومن الضروري النظر في كيفية تأثير ميزات التصميم والمنصة لتطبيقات الوسائط الاجتماعية بشكل مختلف على الإفصاح عن الذات، ونتيجة لذلك قد تختلف قابلية تعرض مستخدمي الوسائط الاجتماعية لأن يصبحوا ضحية للابتزاز على وسائل التواصل الاجتماعي، اعتمادًا على تطبيق الوسائط الاجتماعية الذي يستخدمونه.[33]

(32) Utz, S., Muscanell, N., & Khalid, R., "Self-Disclosure on Social Media: The Role of Intrinsic versus Extrinsic Motivations", Computers in Human Behaviour, 2021, pp: 1214-

(33) Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525540-. https: //doi.org/10.1057/s412842-00246-020-

ويرى الباحث أن محاور الابتزاز الإلكتروني عبر وسائل التواصل الاجتماعي تسلط الضوء على عوامل متعددة تسهم في وقوع الأفراد ضحية لهذه الجريمة، وهناك تأثير واضح للثقافة، والعمر، والجنس، والدوافع الشخصية على احتمالية التعرض للابتزاز. ومع ذلك يظهر أن مشكلة الابتزاز الإلكتروني لا تتعلق فقط بالوعي بالمخاطر، بل أيضًا بالرغبة في استخدام وسائل التواصل الاجتماعي لتحقيق أهداف شخصية وعاطفية. وبناءً على ذلك قد تحتاج حملات التوعية إلى معالجة هذا التناقض بين المخاوف المتعلقة بالخصوصية والرغبة في التعبير عن الذات عبر الإنترنت.

المبحث الثاني
إجراءات التحقيق في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

التمهيد:

تمثل جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي تحديًا متزايدًا في العصر الرقمي؛ حيث تتنوع أشكال وأساليب هذه الجرائم لتشمل التهديد بنشر معلومات شخصية أو صور خاصة مقابل الحصول على المال أو غيره من المكاسب. وتستغل هذه الجرائم التواصل المفتوح عبر الإنترنت للوصول إلى ضحايا من جميع الفئات العمرية، مما يزيد من صعوبة ضبط مرتكبيها وتقديمهم للعدالة. وتتطلب إجراءات التحقيق في هذا النوع من الجرائم تجهيزات خاصة وفهمًا عميقًا لتقنيات التحقيق الرقمي وأدواته، بهدف جمع الأدلة الإلكترونية وتوثيقها، وتتبع المجرمين، وتقديمهم للمحاكمة. من هنا، تبرز أهمية تطوير المهارات التقنية والقدرات التحليلية لدى جهات إنفاذ القانون، وتبني استراتيجيات متقدمة للتصدي لهذه الظاهرة المتنامية، وتعزيز وعي الأفراد حول حماية معلوماتهم الشخصية على منصات التواصل الاجتماعي،[34] وهو ما سنتناوله في هذا المبحث.

المطلب الأول: الإطار الإجرائي القانوني لجريمة الابتزاز الإلكتروني في التشريع القطري

الفرع الأول: الشكوى في جريمة الابتزاز الإلكتروني

إن مراجعة الشكوى في جريمة الابتزاز الإلكتروني تتطلب فحص مفهوم الشكوى في قانون الإجراءات الجنائية القطري والشروط الإجرائية اللازمة لتقديمها.

(34) ALJI Mohamed and CHOUGDALI Khalid, Digital Investigation of a Cybercrime: Sextortion as a Case Study, Proceedings of the Digital Privacy and Security Conference 2019 10.11228/dpsc.01.01, Electronics and Telecommunication Systems Research Group, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, p: 13

أولاً: مفهوم الشكوى:

عرف بعض الفقهاء الشكوى بأنها تعبير المجني عليه عن إرادته في اتخاذ الإجراءات الجنائية الناشئة عن الجريمة، وهناك رأي آخر في الشكوى مفاده أنها تعبير عن إرادة الضحية يترتب عليه أثر قانوني بموجب اختصاص الدعوى الجنائية كما يتبين من إزالة القيود المفروضة على النيابة العامة فيما يتعلق بالقدرة على تحريك الدعوى الجنائية، والتفسير الأكثر ترجيحًا هو: "البيان الذي أدلى به الضحية أو الضحايا للسلطة المختصة للشكوى رسميا بشأن جريمة ارتكبت ضده أو ضد آخرين، وبالتالي طلب بدء إجراءات جنائية في الحالات التي لا يمكن فيها للنيابة العامة بدء مثل هذا الإجراء دون هذه الشكوى". ويشمل هذا الإجراء بالضرورة تلك الأفعال التي يقوم بها الضحية أو ممثله القانوني والتي توجه إلى ضابط الشرطة القضائية، أو إلى عضو في النيابة العامة، أو محكمة مختصة، بهدف تحريك الإجراءات القانونية اللازمة ضد مرتكب الجريمة المعنية فيما يتعلق بتلك الجرائم التي تم تأسيسها فقط بموجب أحكام قانونية، كما تنص المادة (3) من قانون الإجراءات الجنائية القطري على أنه: "لا يجوز تحريك الدعوى الجنائية إلا بناء على شكوى من المجني عليه أو من يمثله في الجرائم المنصوص عليها في المواد (331)، (330)، (329)، (326)، (325/1)، (323/1)، (309)، (308)، (308)، (293)، (332)، (333)، (357)، (389/1)، (393/1)، (394)، و(395) من قانون العقوبات، وكذلك في الجرائم الأخرى المنصوص عليها في القانون، ويجب أن تقدم الشكوى شفاهة أو كتابة من المجني عليه أو من يمثله قانونًا إلى النيابة العامة أو إلى أحد مأموري الضبط القضائي، وإذا وقعت الجريمة متلبسًا بها وجب تقديم الشكوى إلى من يكون حاضرًا من رجال السلطة العامة".

ثانيًا: ميعاد تقديم الشكوى:

أوجب المشرع القطري تقديم الشكوى خلال مدة محددة؛ حيث تنص المادة (7) من قانون الإجراءات الجنائية القطري على أنه: "لا تقبل الشكوى بعد ثلاثين يومًا من اليوم الذي علم فيه المجني عليه بالجريمة ومرتكبها، أو من اليوم الذي علم فيه من ينوب عنه بها، ما لم ينص القانون على خلاف ذلك". وقد أوضحت محكمة النقض القطرية ما يترتب على هذه المهلة لتقديم الشكوى، وقد قضت المحكمة بأنه: "لا يجوز تقديم الشكوى بعد انقضاء ثلاثين يومًا من علم المجني عليه بوقوع الجريمة وهوية مرتكبها". ويشير هذا النص إلى أن سريان هذه المدة قد نص عليه المشرع قرينة قانونية لا تقبل أي دليل ينفي افتراض التنازل. وقد نص المشرع على أن سكوت المجني عليه في هذا الصدد خلال هذه المدة يعد تنازلاً عن حق الشكوى. وبالتالي، فإذا ظل حق الشكوى قائمًا أو مستمرًا، فلا يجوز استخدامه كأداة للترهيب أو الابتزاز أو الانتقام. وبالمثل، فإن تقديم الشكوى في غضون المدة التي ينص عليها القانون يزيل مجرد افتراض التنازل وينقذ العواقب القانونية لهذا الإجراء.

ثالثًا: مقدم الشكوى:

تقدم الشكوى من المجني عليه أو وكيله القانوني، وفي حالة تعدد المتضررين يكفي أن يتقدم أي منهم بالشكوى، أما في حالة تعدد المتضررين وكانت الشكوى ضد شخص واحد فإنها تعتبر قد قدمت ضد الآخرين جميعًا، ولا بد من الإشارة إلى أنه إذا لم يكمل المتضرر السادسة عشرة من عمره أو كان مصابًا بعاهة عقلية تقدم الشكوى من الشخص الذي له الولاية عليه، أما إذا كان المتضرر شخصًا اعتباريًا تقدم الشكوى من ممثله القانوني أو من يفوضه. وفي هذا الصدد قضت محكمة التمييز القطرية بقولها: "إن الدفوع التي ساقها الطاعن لرفض إسقاط حق المجني عليه في تقديم الشكوى من الميعاد المنصوص عليه في المادة (3) من قانون الإجراءات الجنائية مرفوضة لأن المشرع نص في المادة (3) من قانون الإجراءات الجنائية على أنه لا يجوز تحريك الدعوى الجنائية بناء على شكوى المجني عليه أو من يمثله إلا عن جرائم معينة واردة في قائمة شاملة وليست من الجرائم التي ارتكبها الطاعنون، وبناء على ذلك فإن الدفوع المتعلقة بالشكوى تصبح غير ذات قيمة، ولا يغير من هذا ما ساقه الطاعن الثاني من ضرورة تطبيق القياس في هذه الدعوى؛ إذ يتبين من نص المادة (3) أعلاه أن جميع الجرائم المنصوص عليها في تلك المادة تدخل في نطاق الباب السابع من الكتاب الثاني -الجرائم الاجتماعية- والجرائم الواردة في الكتاب الثالث من قانون العقوبات، والتي لا تتعلق إلا بحقوق فردية خاصة، بحيث يكون لكل منهما أهلية تقديرية للتنازل عن حقوقه".

وفي جميع الأحوال ينتهي حق المجني عليه في الشكوى بوفاته، أما إذا توفي المجني عليه بعد تقديم الشكوى فلا أثر لذلك على استمرار الدعوى، وقد نص المشرع القطري على أن صاحب الشكوى أو الطلب يجوز له التنازل عنها في أي وقت قبل صدور حكم نهائي في الدعوى، والشروط المفروضة على مقدم التنازل هي الشروط نفسها المفروضة على مقدم الشكوى أو الطلب، وهي توافر الشروط المذكورة أعلاه فيما يتعلق بمؤهلات المشتكي وقبوله، أما إذا تعدد المشتكون فلا يكون التنازل ملزمًا إلا إذا وقع عليه جميع المشتكين. ومن الجدير بالذكر أن التنازل الصادر من أحد المتهمين يعتبر تنازلاً من جميع المتهمين، وهذا يعني انتهاء الدعوى الجنائية، أما إذا مات المشتكي فلا ينتقل هذا الحق في التنازل إلى خلفائه، وفي هذا الصدد قضت محكمة التمييز القطرية بأنه: "لما كان من المقرر أن الطلب يختلف اختلافًا جوهريًا عن الشكوى من حيث إنه قرار إداري لا يعتمد على الإدارة الشخصية بل وفقًا لمعايير موضوعية في الدولة ولا يثبت إلا بالكتابة، في حين أن التشابه الوحيد بين الطلب والشكوى هو التنازل عنهما وفقًا للمادة (10) من قانون الإجراءات الجنائية، ونظرًا لهذا الوضع، ولما كان القانون لم يشترط تقديم الطلب خلال مدة معينة

من تاريخ الجريمة -ولم يرد نص في هذا الشأن فيما يتعلق بالشكوى- فإن الحق في تقديمه يستمر إلى أن تصبح الدعوى الجنائية باطلة بعد انقضاء المدة المنصوص عليها في المادة (14) من قانون الإجراءات الجنائية، والاعتراض في هذا الصدد يعد خطأ في تطبيق القانون.

رابعًا: تقديم الشكوى:

في قانون مكافحة الجرائم الإلكترونية أصدر المشرع القطري في القانون رقم (14) لسنة 2014 قانون مكافحة الجرائم الإلكترونية، والذي لم يقيد صراحة حرية النيابة العامة في تحريك الدعوى عن كافة الجرائم المشمولة به، بتقديم شكوى من المجني عليه، كما فعل في بعض الجرائم المنصوص عليها في المادة (3) من قانون الإجراءات الجنائية، وهذا يعني أن قيد الشكوى لا يسري على الجرائم المنصوص عليها في المادة (3) من قانون الإجراءات الجنائية إذا ارتكبت عن طريق شبكة الإنترنت؛ أي أنها أصبحت جرائم إلكترونية، وبالتالي يجوز تحريكها من قبل النيابة العامة، ولا يجوز للمجني عليه التنازل عنها، ولذلك قضت محكمة التمييز القطرية بأن: "المادة 3 من قانون الإجراءات الجنائية تنص على أنه: لا يجوز رفع الدعوى الجنائية إلا بناء على شكوى من المجني عليه أو من يمثله في الجرائم المنصوص عليها في قانون العقوبات، وكذلك في الجرائم الأخرى المنصوص عليها في القانون". كما نصت المادة (10) من القانون ذاته على أنه يجوز لمن قدم الشكوى التنازل عنها في أي وقت إلى أن يصدر حكم نهائي في الدعوى، وبالتالي تنقضي الدعوى الجنائية بالتنازل. وحيث إنه يتبين من الأوراق أن الجريمتين اللتين أقامت النيابة العامة من أجلهما المحكوم عليه وأدين من أجلهما معاقب عليهما بمقتضى المادة (89) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وقد خلا القانون المذكور صراحةً من تقييد حرية النيابة العامة في تحريك الدعوى عنهما وعن سائر الجرائم الواردة فيهما بمجرد تقديم شكوى من المجني عليه، كما فعل في بعض الجرائم المنصوص عليها في المادة (3) من قانون الإجراءات الجزائية المذكور، والتي لم يقم المحكوم عليه بعقوبة عنها بمقتضى أي منها، وإن ما يثيره المحكوم عليه في هذا الشأن بخصوص تحريك الدعوى أو انقضائها بالتنازل غير مقبول، ولا تكون المحكمة مسؤولة إذا لم تتطرق إلى دفاعه في هذا الشأن، ولو تطرق إليه الحكم المطعون فيه ورفضه على نحو يتفق مع هذا الرأي السابق.

الفرع الثاني: الطبيعة الخاصة للأدلة الإلكترونية وإجراءات ضبطها في جريمة الابتزاز الإلكتروني

أولاً: الطبيعة الخاصة للأدلة الرقمية في جرائم الابتزاز الإلكتروني:

الأدلة الرقمية بما فيها أجهزة الحاسوب والأجهزة الإلكترونية التي تتواجد فيها تلك

الأدلة، أدلة هشة وحساسة لدرجات الحرارة العالية والرطوبة والصدمات الكهربائية والكهرباء الساكنة والمجالات المغناطيسية، وينبغي لمن يقوم بعمليات جمع الأدلة الرقمية باتخاذ الاحتياطات اللازمة عند التوثيق والتصوير والتغليف والنقل والتخزين لتلك الأدلة الرقمية وأجهزتها لتجنب تغيير أو إتلاف أو تدمير البيانات.

كما أن الأدلة الرقمية في جرائم الابتزاز الإلكتروني لها خصائص فريدة تميزها عن الأدلة التقليدية في الجرائم الأخرى، وتفرض مجموعة من التحديات التي يجب معالجتها بعناية خلال التحقيقات. وفي هذا السياق يجب أن تفهم الطبيعة الخاصة لهذه الأدلة من خلال عدة جوانب رئيسة :

1- القابلية للتعديل والتغيير:

الأدلة الرقمية، مثل الرسائل الإلكترونية والصور والفيديوهات والمحادثات على وسائل التواصل الاجتماعي، تتمتع بقدرة عالية على التعديل أو التغيير، فيمكن بسهولة تعديل المحتوى الرقمي أو حذفه، مما يجعل من الضروري توثيق الأدلة وحمايتها فور اكتشافها. ويساهم استخدام تقنيات التجزئة (Hashing) مثل MD5 أو SHA في ضمان سلامة البيانات وعدم تعديلها بعد جمعها.

2- التوقيت الحرج للأدلة الرقمية:

الأدلة الرقمية تتغير بسرعة خصوصًا في الجرائم التي تحدث عبر الإنترنت، فعلى سبيل المثال: قد تختفي رسائل الابتزاز أو يتم تعديل المنشورات والصور في أي لحظة، لذلك يتطلب جمع الأدلة الرقمية في جرائم الابتزاز الإلكتروني سرعة كبيرة واتباع إجراءات قانونية دقيقة لضمان الحفاظ على الأدلة قبل تعديلها أو إخفائها.

3- التوزيع المتعدد للأدلة:

في حالات الابتزاز الإلكتروني، قد تكون الأدلة موزعة عبر منصات متعددة مثل وسائل التواصل الاجتماعي، والبريد الإلكتروني، وتطبيقات المراسلة، مما يجعل من الضروري تحديد جميع المصادر الممكنة للأدلة، واستعمال أدوات متخصصة لجمع هذه البيانات من منصات مختلفة مثل Facebook أو WhatsApp، مع ضمان الحفاظ على توثيق كامل لها.

4- القدرة على استعادة الأدلة المحذوفة:

من أبرز سمات الأدلة الرقمية هي قدرتها على الاستعادة حتى إذا تم حذف البيانات يمكن للأدلة الرقمية أن تسترجع باستخدام تقنيات تحليل البيانات الجنائية، مثل "استعادة الملفات

المحذوفة" باستخدام أدوات مثل EnCase و FTK Imager، هذه الأدوات تمكن المحققين من استرجاع البيانات المحذوفة من الهواتف الذكية أو أجهزة الكمبيوتر.

5- التوثيق والتسلسل الزمني:

الأدلة الرقمية تتطلب توثيقًا دقيقًا لكل خطوة من خطوات جمعها وتغليفها ونقلها، ويجب توثيق توقيت جمع الأدلة، وتوضيح الأدوات المستخدمة في جمع الأدلة وتغليفها، كما أن التسلسل الزمني للأدلة الرقمية يعد أمرًا بالغ الأهمية لإثبات العلاقة بين الجريمة والفاعل.[35]

6- الحفاظ على سلامة الأدلة:

أحد أبرز التحديات في التعامل مع الأدلة الرقمية هو الحفاظ على سلامتها من التلاعب، فعملية نقل الأدلة تتطلب تأمينها وحمايتها باستخدام تقنيات مثل التشفير أثناء النقل والتخزين، وأي تغيير في البيانات يمكن أن يؤدي إلى رفض الأدلة في المحكمة.

والأدلة الرقمية بجميع مصادرها المختلفة متطورة ومتنوعة، كما أن هناك أدلة رقمية يمكن الحصول عليها مباشرة أثناء التواجد في مسرح الجريمة دون الحاجة للنقل والتغليف، والبعض يحتاج إلى النقل، والبعض يحتاج إلى التغليف والنقل والتخزين، وبغض النظر عن نوع الدليل فإن هناك إرشادات بناءً على أفضل الممارسات خاصة بإجراءات تغليف ونقل وتخزين ما تم ضبطه وجمعه من الأدلة الرقمية ومصادرها المختلفة، ويحتاج للتغليف أو النقل أو التخزين أو لهم جميعًا، وينبغي أن يتم تطبيق إجراءات التغليف والنقل والتخزين بطريقة دقيقة وموثوقة؛ لتجنب تغيير أو تدمير أو إتلاف البيانات الرقمية. وعملية التغليف يقصد بها وضع الأجهزة والمكونات التي تحتوي على دليل رقمي داخل أوعية خاصة أو تغليفها بأغلفة خاصة، ولذلك فإنه في هذا السياق نعني بالتغليف أيضًا تعبئة الأجهزة في حاويات أو أكياس خاصة، وفيما يلي سنقوم بذكر الخطوات المهمة التي ينصح باتباعها عند تنفيذ أي من تلك الإجراءات.[36]

(35) Ahmed A. Abd El-Latif, Lo'ai Tawalbeh, Manoranjan Mohanty, Brij B. Gupta, Konstantinos E. Psannis, igital Forensics and Cyber Crime Investigation Recent Advances and Future Directions, 2025, pp: 4346-, https: //www.routledge.com/Digital-Forensics-and-Cyber-Crime-Investigation-Recent-Advances-and-Future-Directions/AbdEl-Latif-Tawalbeh-Mohanty-Gupta-Psannis/p/book/9781032075396

(36) Jeremy Leighton John, Digital Forensics and Preservation, DPC Technology Watch Report 1203- November 2012, Series editors on behalf of the DPC, Published in association with Charles Beagrie Ltd., pp: 915-, https: //www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-reports-1810-/dpctw1203--pdf/file

ثانيًا: إجراءات ضبط الأدلة الرقمية في جرائم الابتزاز الإلكتروني:

لا تختلف جريمة الابتزاز الإلكتروني عن غيرها من الجرائم التقليدية والجرائم الإلكترونية من حيث إجراءات الدعوى المرتبطة بها والمراحل التي تمر بها، وإن كان من الصعب في الجرائم الإلكترونية المرتكبة عن طريق الوسائل الإلكترونية أو شبكة الإنترنت - كما هو الحال في جريمة الابتزاز الإلكتروني- إثبات مسؤولية مرتكبيها. ويتولى مأمورو الضبط القضائي التحقيق في الجرائم والبحث عن مرتكبيها وجمع الأدلة اللازمة للتحقيق والمحاكمة. كما يجوز لمأموري الضبط القضائي الاستعانة بالخبراء في جريمة الابتزاز الإلكتروني، وطلب رأيهم شفاهةً أو كتابة. وقد نصت المادة (63) من القانون القطري رقم (23) لسنة 2004 بإصدار قانون الإجراءات الجنائية على أن: "تجري النيابة العامة التحقيق في الجنايات والجنح التي ترى لزوم التحقيق فيها". ولذلك فإن النيابة العامة – أو من تفوضه من مأموري الضبط القضائي– تقوم بتفتيش الأشخاص والأماكن ونظم المعلومات المتعلقة بالجريمة، على أن يكون أمر التفتيش مسببًا ومحددًا، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة، وإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل تتعلق بالجريمة، وجب على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ اللازم بشأنها. وإن نص المادة (15) من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة جرائم تقنية المعلومات (14/2014)، المتضمن حظر استبعاد أي دليل ناتج عن وسائل تقنية أو أنظمة معلومات أو شبكات معلومات أو مواقع إلكترونية أو بيانات ومعلومات إلكترونية بسبب طبيعة تلك الأدلة، وتنص المادة (16) على أنه: "لا يجوز استبعاد أي دليل حصلت عليه الجهة المختصة أو جهات التحقيق من دول أخرى لهذا السبب، ما دام قد تم الحصول عليه وفقًا للإجراءات القانونية والقضائية للتعاون الدولي"، يتفقان مع المادة (204) من قانون الإجراءات الجنائية القطري رقم (23) لسنة 2004، التي تنص على أنه: "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه ضروريًا لظهور الحقيقة". وفي جميع الأحوال يجوز للنيابة العامة أن تأمر بجمع الأدلة والتسجيل الفوري لأي بيانات أو معلومات إلكترونية أو بيانات مرور أو معلومات محتوى تراها ضرورية لمصلحة التحقيقات في جريمة الابتزاز.

وللنيابة العامة أن تأمر جميع الجهات ذات العلاقة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو معلومات المحتوى المتعلقة بموضوع الجريمة أو ما يفيد في كشف الحقيقة، كما لها أن تأمر بضبط الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة، ولها أن تأمر باتخاذ التدابير والإجراءات الكفيلة بالمحافظة على هذه الأجهزة أو الأدوات أو أنظمة المعلومات أو البيانات أو المعلومات

الإلكترونية، وذلك لحين صدور قرار من الجهات القضائية المختصة بشأنها. وباستثناء الالتزامات المهنية المنصوص عليها في القانون، لا يجوز لأي شخص أن يستند إلى الأسرار المهنية أو متطلباتها للامتناع عن تقديم المعلومات أو الوثائق المطلوبة وفقًا لأحكام هذا القانون.

الفرع الثالث: شروط مشروعية ضبط الدليل الإلكتروني في جريمة الابتزاز الإلكتروني أمام القضاء الجنائي

لقد تبنى المشرع القطري في إثبات الجرائم ما يعرف بنظام الأدلة الحرة أو ما يسمى بالقناعة الذاتية أو الشخصية للقاضي؛ أي أن للقاضي في جريمة الابتزاز الإلكتروني حرية قبول كل ما يشكل قناعته ويبني عليها، وكذلك حرية تقدير قيمة هذا الدليل، ولا يحدد هذا النظام طرقًا أو أدلة معينة للإثبات، بل إن للخصوم الحرية التامة في تقديم الأدلة التي تؤدي إلى قناعة القاضي، ويتمتع القاضي بسلطة واسعة في البحث عن الحقيقة واتباع طرق مختلفة تؤدي إلى تكوين قناعته دون التقيد بأساليب معينة. ولذلك قضت محكمة التمييز القطرية بما يلي: "ومن المقرر أنه وإن كان يكفي أن يشك القاضي في ثبوت التهمة حتى يحكم لصالح المتهم بالبراءة، فإن حد ذلك أن يكون قد فحص الدعوى فحصًا شاملاً ثاقبًا، وأن يكون على علم بأدلتها، وأن يكون حكمه خاليًا من عيوب التعليل. ومن الضروري أيضًا في أصول الفقه أن يؤدي الدليل الذي يستند إليه الحكم إلى النتائج التي استند إليها من دون تعسف في النتيجة أو تعارض مع قاعدة العقل والمنطق. ولما كان الأمر كذلك، فإن الحكم في مبرراته للحكم بالبراءة من التهمة... لم يعرض أقوال شهود الإثبات ويبدي رأيه فيها بما له من سلطة تقديرية في تقدير أقوال الشهود، ورفضها تارة لأسباب لا تتفق مع القانون الصحيح وبتأويل غير صحيح للنصوص التي قدمها للتفسير في ضوء وضوحها وبجهد غير مقبول ينطوي على خلط بين قواعد الإثبات في المواد المدنية والجزائية وتطبيق أحكام الشريعة الإسلامية في غير محلها، وتارة أخرى لأسباب غير مقبولة لا تصلح مبررًا لاستبعاد أقوال هؤلاء الشهود، فإن ما ذكره الحكم على النحو المذكور أساس تبرئته غير سليم، لأنه يشير إلى عدم إحاطة المحكمة الكاملة بالواقعة وأدلتها، مما يؤدي إلى معرفة حقيقة التهمة ومدى ثبوتها بهذه الأدلة، ويكشف عن قيام المحكمة بواجبها في الموازنة بين أدلة الإثبات والنفي، مما يؤدي إلى النتيجة التي توصلت إليها، مما يجعل حكمها محل نظر".[37] ويتضح مما تقدم أن تقدير كفاية الأدلة وتوافر الشروط القانونية فيها في جريمة الابتزاز الإلكتروني من الأمور التي تخضع للسلطة التقديرية للقاضي؛ ولذلك قضت محكمة التمييز القطرية بأن: "المقرر أن المعيار في المحاكمات الجنائية هو اقتناع القاضي بناء على

(37) حكم محكمة التمييز القطرية – تمييز جنائي – الطعن رقم 510/ 2015 – جلسة 15 فبراير 2016م

الأدلة المقدمة إليه بإدانة المتهم أو تبرئته، وأن وزن وتقدير أقوال الشهود متروك لمحكمة الموضوع التي تضعهم في المكانة التي تراها وتقدرهم بالقدر الذي تقتنع به. وكانت المحكمة قد أبدت ثقتها واطمئنانها إلى أقوال شهود الإثبات التي تضمنت ما يؤدي إلى ما استندت إليه. وطبقًا للحكم فإن ذلك لشوته وسلامة حكمها فيما يتعلق بجريمة الاشتراك في تزوير المحررات الرسمية التي أدين بها المستأنفون. ويصبح ما يشكو منه المستأنف في هذا الشأن محل خلاف حول سلطة محكمة الموضوع في تقدير أدلة الدعوى، وهو ما لا يجوز الرجوع إليه لإثارته أمام محكمة التمييز. ولا يتغير ذلك بما ذهب إليه في أسباب طعنه بشأن تجاهل المحكمة لأقوال شهود النفي؛ حيث إنه من المقرر أن للمحكمة تجاهل أقوالهم ما دامت لم تقتنع بها".[38] ويمكن توضيح شروط صحة وحجية الأدلة الإلكترونية في جريمة الابتزاز الإلكتروني أمام المحكمة الجزائية من خلال استعراض ما يسمى بالشرعية الإجرائية في جريمة الابتزاز الإلكتروني، والتي ترتكز على عدد من العناصر تتمثل فيما يلي:

أولًا: يجب أن يكون الدليل في جريمة الابتزاز الإلكتروني مشروعًا؛ أي يجب الحصول عليه بطريقة مشروعة، فلا يجوز استعمال أي وسيلة غير مشروعة للتأثير على المتهم للحصول على اعترافه، ومن الوسائل غير المشروعة سوء المعاملة والتهديد بالإيذاء والإغراء والوعود والترهيب والتأثير النفسي واستعمال المخدرات والكحول والأدوية، ويعتبر باطلاً كل دليل تم الحصول عليه عن طريق التعذيب أو الإكراه أو المساس بالسلامة البدنية أو المعنوية للفرد عن طريق التدخل التعسفي، وقد نص قانون الإجراءات الجزائية القطري على أنه: ".. ولا يجوز له أن يحكم على أي دليل لم يعرض عليه في الجلسة أو تم الحصول عليه بطريقة غير مشروعة...، وأن يكون الإجراء الذي حصل به القاضي على الأدلة متفقا مع الإجراءات المشروعة التي تحترم فيها الحريات وتوفر الضمانات المقررة في القانون".

وفي هذا الصدد قضت محكمة النقض المصرية – بشأن إحدى جرائم الابتزاز الإلكتروني– بما يلي: "لما كان الحكم المطعون فيه قد تبين من وقائع الدعوى، أن المتهم استأجر بارًا في العقار الذي يقيم فيه وحصل على ترخيص بمزاولة نشاط ما يسمى "نت كافيه"، وأبلغه في مجال شبكة المعلومات الدولية والحاسبات الآلية، وتوافرت لديه الرغبة في تهديد النساء وابتزازهن للحصول منهن على ما يريد من أموال أو ممارسات غير أخلاقية عبر الإنترنت بعد تصويرهن في ممارسات غير أخلاقية وهمية، وتهديدهن بإرسال تلك الصور إلى أقاربهن أو بيعها ونشرها على الشبكة المذكورة. ومن أجل ذلك أنشأ موقعين إلكترونيين أحدهما باسمه الحقيقي والآخر باسم وهمي، واستخدم الأخير في التعرف على المجني

(38) حكم محكمة التمييز القطرية – المواد الجنائية – الطعن رقم 116 جلسة 5 ديسمبر 2016م

عليها، وإيهامها بأنه يعمل مدعيًا عامًا وأنه يحبها ويريد الزواج منها، وأنه يريد رؤيتها عارية. وعندما رفضت في البداية بدأ يلح عليها تارة بإغرائها بالزواج وتارة أخرى بالتهديد بعدم الزواج منها حتى استجابت لطلبه ومكنته من رؤيتها عارية تماما وفي ممارسات غير أخلاقية، وذلك بإجبارها على القيام بهذه الوضعيات أمام كاميرا الكمبيوتر الخاصة بها والاتصال بجهاز الكمبيوتر الخاص بالمتهم الذي قام بتصوير هذه المشاهد وتسجيل هذه الصور، ثم بدأ يهددها ويحاول ابتزازها بطلب خمسة آلاف جنيه منها وتهديدها بإرسال تلك الصور لأقاربها أو بيعها لآخرين ونشرها على الإنترنت إذا لم تستجب له، وعندما رفضت في البداية أرسل بعض صورها العارية لشقيقتها التي عرضتها على المجني عليها التي أصابها الرعب والخوف من الفضيحة كونها محامية فأبلغت الإدارة المختصة بوزارة الداخلية، وأكدت التحقيقات صحة الواقعة، وتم استخراج عدد من الرسائل المرسلة للمجني عليها على جهاز الكمبيوتر الخاص بها والتي ثبت أنها مرسلة لها من البريد الإلكتروني للمتهم وتتضمن تهديدات بنشر صورها وطلبات مبالغ مالية. وتنفيذًا لإذن النيابة العامة تم القبض على المتهم وضبط جهاز الحاسب الآلي الخاص به المستخدم في ارتكاب الواقعة بمقر إقامته وتبين أنه يحتوي على صور عارية للمجني عليها، مما يؤكد قيامه بإرسال رسائل تهديد من بريده الإلكتروني وإرسال صور المجني عليها لشقيقتها كما يحتوي على صور وأفلام لفتيات أخريات عاريات مكتوب على كل واحدة منهن اسمها وعنوانها ويحوي محادثات مع المتهم وصحة انتحاله اسمين وادعائه للمجني عليها أنه وكيل نيابة وقد استند الحكم إلى أدلة ثبوت الواقعة على هذا النحو في حق المستأنف والتي استند إليها من أقوال المجني عليها وشقيقتها وضباط الشرطة القضائية والتقارير الفنية التي فحصت الحاسب الآلي، وهو دليل جائز يؤدي إلى ما نص عليه الحكم".[39]

ومن هذا الحكم يتبين ما يلي:

1- أن المتهم استأجر محلًا تجاريًا وحصل على ترخيص بمزاولة نشاط "نت كافيه"، واستغل نشاطه في تهديد وابتزاز النساء للحصول منهن على ما يريد من أموال أو ممارسات غير أخلاقية عبر الإنترنت بعد تصويرهن عاريات في ممارسات غير أخلاقية وهمية وتهديدهن بإرسال تلك الصور إلى ذويهن أو بيعها ونشرها على الشبكة المذكورة، وبذلك تتضح أركان الجريمة.

2- أن الجهات المختصة اعتمدت في إثبات الجريمة على استخراج عدد من الرسائل المرسلة إلى المجني عليها من الجاني على جهاز الكمبيوتر الشخصي الخاص بها، والتي ثبت أنها مرسلة إليها من البريد الإلكتروني للمتهم، تهددها بنشر صورها وطلب مبالغ مالية.

(39) مجموعة أحكام النقض المصرية – الطعن 3981 لسنة 80 قضائية – الصادر بجلسة 17 أكتوبر 2011م -

3- بناءً على إذن صادر من النائب العام المختص تم القبض على المتهم وحصلت الأدلة التالية بالطريق القانوني: تم ضبط جهاز الحاسب الآلي الخاص بالمتهم الذي استعمل في ارتكاب الواقعة بمقر إقامته وتبين أنه يحتوي على صور عارية للمجني عليها، مما يؤكد قيامه بإرسال رسائل تهديد من بريده الإلكتروني وإرسال صور المجني عليها لشقيقتها، كما تبين أنه يحتوي على صور وأفلام لفتيات أخريات عاريات مكتوب على كل واحدة منهن اسمها وعنوانها، إلى جانب محادثات مع المتهم وصحة اتخاذه لاسمين وادعائه للمجني عليها أنه وكيل نيابة.

4- استند حكم الاستئناف إلى ثبوت الواقعة على هذا النحو في حق المستأنف، وذلك بناءً على ما حصل عليه من أدلة من أقوال المجني عليها وشقيقتها وضباط الشرطة القضائية والتقارير الفنية التي فحصت الحاسب الآلي، وهو دليل صحيح يؤدي إلى ما نص عليه الحكم.

ثانيًا: عند تناول جريمة الابتزاز الإلكتروني يراعى مبدأ براءة المتهم، وضرورة إشراف القضاء على الإجراءات كافة باعتباره الحارس الطبيعي للحقوق والحريات، فضلاً عن ضمان حق المتهم في الدفاع عن نفسه ونفي التهمة المنسوبة إليه. وفي هذا الصدد قضت محكمة التمييز القطرية بأنه: "من المقرر أن نفي التهمة وكيدية الاتهام دفاعان موضوعيان لا يستحقان الرد ما دام الرد عليهما مستمدًا من أدلة الإثبات التي استند إليها الحكم. هذا فضلاً عن أن الحكم لكي يثبت ويكون سليمًا يجب عليه أن يورد الأدلة التي قدمها والتي تصح على ما خلص إليه من وقوع الجريمة المنسوبة إلى المتهم، ولا يلزمه أن يلاحقه في كل تفصيل من تفاصيل دفاعه، لأن ما يترتب على تجاهله لها هو رفضه لها، وعليه فإن ما يثيره الطاعن في هذا الشأن لا يعدو أن يكون جدلاً موضوعيًا في تقدير الأدلة وفي سلطة محكمة الموضوع في ترجيح عناصر الدعوى واستنباط اعتقادها، وهو ما لا يجوز إثارته أمام محكمة التمييز."[40]

ثالثًا: تجدر الإشارة إلى أن المشرع القطري قد اشترط في التوقيع الإلكتروني كدليل إثبات أن يتوافر فيه الآتي:

1- أن تكون معلومات إنشاء التوقيع مرتبطة بالموقع وليس بأي شخص آخر.
2- أن تكون معلومات إنشاء التوقيع وقت التوقيع تحت سيطرة الموقع وليس أي شخص آخر.
3- إمكانية اكتشاف أي تغيير يطرأ على التوقيع الإلكتروني بعد حدوث التوقيع.
4- إمكانية اكتشاف أي تغيير يطرأ على معلومات رسالة البيانات بعد وقت التوقيع إذا كان الغرض من اشتراط التوقيع – قانونًا– هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع.

(40) محكمة التمييز القطرية – تمييز جنائي – الطعن رقم 63 لسنة 2017م – جلسة 16 أكتوبر 2017م

المطلب الثاني: القواعد الفنية لجمع الأدلة الرقمية في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

الفرع الأول: مرحلة الإعداد وجمع الأدلة من مواقع التواصل الاجتماعي

جمع الأدلة الرقمية من مواقع التواصل الاجتماعي في حالات جرائم الابتزاز الإلكتروني يتطلب خطوات دقيقة ومتخصصة؛ إذ يجب الحفاظ على مصداقية الأدلة وحمايتها من التلاعب لضمان قبولها في المحاكم. وفيما يلي شرح تفصيلي لهذه الخطوات، مع التركيز على ممارسات جمع الأدلة الرقمية من مواقع التواصل الاجتماعي: [41]

أولاً: تحديد نطاق الأدلة المطلوبة وتخطيط عملية الجمع:

- الخطوة الأولى: تحديد الأدلة التي قد تكون متاحة على الحسابات أو الصفحات المتورطة في عملية الابتزاز، وتتضمن هذه الأدلة الرسائل النصية، والصور، ومقاطع الفيديو، والتعليقات، وسجلات النشاط المرتبطة بالابتزاز.
- الخطوة الثانية: التخطيط الشامل، فمن الضروري وضع خطة لجمع الأدلة بناءً على نوع الجريمة وطبيعة الحسابات المتورطة، على سبيل المثال: إذا كان الابتزاز يتضمن صورًا أو تهديدات مباشرة، يجب التركيز على محتوى الرسائل المباشرة وسجلات المحادثات.

ثانيًا: حفظ الأدلة باستخدام تقنيات التصوير الرقمي والتوثيق المباشر:

- التصوير الرقمي: تستخدم تقنية "لقطة الشاشة" أو "تصوير الشاشة" كطريقة أولية لتوثيق الرسائل، والصور، أو غيرها من المحتويات المعروضة على الحسابات المعنية، ويفضل استخدام برامج تصوير متقدمة تتضمن معلومات عن وقت وتاريخ أخذ اللقطة لضمان المصداقية. [42]
- حفظ الروابط والتفاصيل التقنية: يتم تسجيل الروابط الخاصة بالمنشورات أو الرسائل لضمان القدرة على الرجوع إليها لاحقًا، ويتضمن ذلك تسجيل أسماء المستخدمين، ومعرف الحساب (ID)، والتاريخ المحدد لأي تفاعل ذي صلة. [43]

(41) هند نجيب – ضبط الأدلة الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة – المجلة الجنائية القومية – المجلد 61 – العدد 3 – نوفمبر 2016 – ص102 - https: //ncj.journals.ekb.eg/article_208596_34d8c5ea5267de cb20915a2587933a12.pdf

(42) Valentin Gazeau; Khushi Gupta; Min Kyung An, Enhancing Social Media Data Collection for Digital Forensic Investigations: A Web Parser Approach, 2024 International Conference on Computer, Information and Telecommunication Systems (CITS), Girona, Spain, 1719- July 2024, https: //ieeexplore.ieee.org/xpl/conhome/10608004/proceeding , DOI: 10.1109/CITS61189.2024.10607983

(43) د/ إبراهيم الحسيني، جرائم الحاسوب والتحقيقات الرقمية، 2020.

ثالثًا: الحصول على بيانات الاتصال والموقع الجغرافي إذا كانت متاحة:

العديد من شبكات التواصل الاجتماعي تقدم معلومات محدودة حول الموقع الجغرافي أو عنوان الـ IP للمستخدمين، ومع ذلك ففي بعض الحالات يمكن استنتاج بعض البيانات الجغرافية أو التقنية التي تدل على موقع المبتز إذا كانت المنصة تحتفظ بتلك البيانات.

ويمكن للمحققين الاعتماد على هذه البيانات لتحديد موقع المبتز الجغرافي المحتمل أو على الأقل استبعاد بعض المواقع غير المحتملة.[44]

رابعًا: التواصل مع مزودي خدمات التواصل الاجتماعي:

- طلب البيانات الرسمية: يتطلب جمع الأدلة المتعمقة في الجرائم الإلكترونية – مثل الابتزاز– التواصل مع مزودي الخدمة (كمنصات "FaceBook"، و"X"، و"Instagram") لطلب بيانات إضافية، ويتم إرسال طلبات رسمية بموافقة قضائية للحصول على معلومات دقيقة تتضمن سجلات النشاط وسجلات الدخول إذا كانت متاحة.
- الاستجابة للطلبات الطارئة: في الحالات الحرجة يمكن للمحققين إرسال طلبات طارئة للحصول على بيانات في أسرع وقت ممكن، وخاصة إذا كانت هناك حاجة لحماية الضحية.[45]

خامسًا: التحليل الفني للأدلة الرقمية من مواقع التواصل الاجتماعي:

بعد جمع البيانات الأولية يتم تحليلها باستخدام برامج متخصصة مثل أدوات التحليل الجنائي الرقمي، وتشمل هذه التحليلات فحص الرسائل المتبادلة لتحديد نمط التهديدات والضغط المستخدم، وتحديد أي قرائن تدل على هوية المبتز.

ويمكن تحليل الوسائط المتعددة – مثل الصور والفيديوهات – بحثًا عن بيانات تعريفية (Metadata) قد تشير إلى معلومات إضافية حول وقت ومكان تسجيلها.[46]

سادسًا: حفظ النسخ الأصلية للأدلة الرقمية في قواعد بيانات آمنة:

يتم الاحتفاظ بنسخ من الأدلة الرقمية في قواعد بيانات آمنة، ويفضل أن تكون محمية

(44) James R. Lyle, Barbara Guttman, Digital Investigation Techniques: A NIST Scientific Foundation Review, NIST Internal Report, NIST IR 8354, November 2022, pp: 3740-, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf

(45) Digital Forensics and Cybercrime Investigations, https: //criminal-justice.iresearchnet.com/criminal-justice-process/impact-of-technology/digital-forensics-and-cybercrime-investigations/

(46) Kausik Maitra , Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation and Evidence Collection, International Journal of Innovation and Applied Studies ISSN 20289324- Vol. 43 No. 2 Aug. 2024, pp. 261271-, Innovative Space of Scientific Research Journals http: //www.ijias.issr-journals.org/,

ببرامج خاصة للحفاظ على النسخ الأصلية دون تعديل، وذلك بهدف استيفاء المعايير القانونية وضمان قبول الأدلة في المحكمة.

وتستخدم برامج مثل برامج تشفير الملفات وخوارزميات "التجزئة" (Hashing) لحماية البيانات وضمان ثباتها.[47]

سابعًا: إعداد تقرير الأدلة الرقمية لعرضه أمام المحكمة:

إعداد تقرير شامل وموثق يصف كل خطوة في جمع الأدلة، بدءًا من جمع الرسائل حتى تحليلها وحفظها، ويتضمن التقرير توثيقًا زمنيًا للأدلة وأي تفاصيل إضافية تم جمعها من المنصات الاجتماعية.

ويعتبر هذا التقرير وثيقة رسمية يتم استخدامها من قبل المحققين والقضاء كمرجع للتأكد من أن الأدلة جمعت وحللت وفق الإجراءات القانونية المعترف بها.[48]

الفرع الثاني: توثيق مسرح الجريمة في جرائم الابتزاز عبر مواقع التواصل الاجتماعي

توثيق مسرح الجريمة عملية مهمة وتعد سجلاً مهمًا في عملية التحقيق، فمن المهم توثيق مسرح الجريمة بدقة بما في ذلك حالة أجهزة الكمبيوتر ووسائط التخزين وأجهزة الشبكة اللاسلكية والهواتف المحمولة والهواتف الذكية والمساعدات الرقمية الشخصية، وغيرها من أجهزة تخزين البيانات ومكونات الوصول إلى شبكة الإنترنت والأجهزة الإلكترونية الأخرى. ونظرًا لتنوع مصادر الأدلة الرقمية في الحجم والشكل والتقنية، يجب ألا يغيب عن إدراك رجل الأمن المختص بتوثيق مسرح الجريمة أن الأدلة الرقمية لا تكون واضحة أو ظاهرة في جهاز الحاسوب أو الأجهزة الأخرى، بل قد توجد مبعثرة في أجهزة متعددة؛ لذا فإن توثيق مسرح الجريمة ينبغي أن يكون مفصلاً باستخدام الفيديو والتصوير الفوتوغرافي وكتابة الملاحظات والرسومات، ليمكن إعادة أو نقل تفاصيل المسرح لاحقًا، كما ينبغي أن يشمل توثيق الأنشطة والعمليات المعروضة على شاشات الأجهزة توثيقًا كاملاً.

ومن خصائص الأدلة الرقمية اتساع مسرحها، ولذلك فإنه في حال امتد مسرح الجريمة إلى مكان أوسع فيجب توثيق المكونات الرئيسة لتقنية الارتباطات (سلكية أو لاسلكية) بين

(47) The Essential Evidence Collection Guide for Websites, Social Media, and Team Collaboration Tools How to Collect and Preserve Evidence on Websites, Social Media Platforms, and Enterprise Social Networks, 2020, pp: 39- https: //f.hubspotusercontent10.net/hubfs/1818760/PDFs/2020%20The%20Essential%20Evidence%20Collection%20Guide%20for%20Websites%20Social%20Media%20and%20Team%20Collaboration%20Tools%20_%20Guidebook.pdf

(48) مجلة التحقيقات الجنائية الرقمية، العدد 4، 2022

أجهزة الحاسوب والأجهزة التقنية الأخرى في جميع مواقع مسرح الجريمة. وعادةً ما يدل وجود مكونات شبكية - سواء من نقاط وصول سلكية أو لاسلكية- على احتمال وجود أدلة إضافية خارج نطاق مسرح الجريمة الرئيسي أو الذي يتم معاينته حاليًا، وفي حال وجود مثل هذه المكونات الشبكية في مسرح الجريمة فيجب توثيقها توثيقًا مفصلاً أيضًا.

وقد يكون هناك بعض الظروف التي قد لا تسمح لرجال الضبط بجمع جميع المكونات أو الأجهزة الإلكترونية في مسرح أو موقع الجريمة، مما يجعل توثيقها ذا أهمية قصوى، وأيضًا إذا كانت هناك قوانين أو محاذير معينة أو أي عوائق أخرى تمنع أو تحول دون تفتيش أو جمع الأجهزة في مسرح الجريمة فيجب على الأقل توثيقها. (49)

توثيق مسرح الجريمة في جرائم الابتزاز عبر مواقع التواصل الاجتماعي يتطلب إجراءات دقيقة تضمن تسجيل جميع الأدلة الرقمية المرتبطة بالجريمة بشكل موثوق، وإليك الخطوات الأساسية لتوثيق هذه الأدلة في مسرح الجريمة الرقمي:

1- التقاط صور أو لقطات شاشة للمحادثات والمحتوى:

أول خطوة في توثيق مسرح الجريمة هي التقاط صور أو لقطات شاشة للمحادثات كافة، والرسائل، والمنشورات، والصور المرتبطة بالابتزاز على مواقع التواصل الاجتماعي، ويفضل أن يتم التقاط لقطات كاملة تتضمن اسم الحساب، وتاريخ ووقت الرسائل، والتفاصيل المرتبطة بالحادث، بحيث يتم عرض المحادثة بشكل كامل ودقيق.

2- توثيق عنوان الإنترنت (URL):

يجب توثيق عنوان URL للصفحات أو المنشورات أو الملفات التي تحتوي على الأدلة، وذلك لتسهيل الوصول إلى المحتوى الأصلي لاحقًا، ويمكن نسخ عنوان URL ولصقه في ملف توثيق خاص بالقضية، مع مراعاة توثيق تاريخ ووقت الدخول إلى كل رابط.

3- تسجيل معلومات المستخدم والأجهزة:

يتم توثيق جميع المعلومات المتاحة حول المستخدمين المتورطين في الجريمة، مثل أسماء الحسابات، وعناوين البريد الإلكتروني، وعناوين IP إن توفرت، ويمكن الحصول على بعض هذه البيانات من إعدادات الحسابات أو طلبها بشكل قانوني من منصة التواصل الاجتماعي في حال كانت مسجلة.

(49) Barbara Guttman, Douglas R. White, Tracy Walraven, Digital Evidence Preservation Considerations for Evidence Handlers, NIST Interagency Report, NIST IR 8387, September 2022, p: 12, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf

4- استخدام أدوات التحليل الجنائي الرقمي:

يفضل استخدام أدوات تحليل جنائي متخصصة لتوثيق الأدلة بشكل احترافي، مثل **En-Case** أو**FTK Imager** ، فهذه الأدوات تتيح حفظ البيانات وتوثيقها دون تعديلها، كما تقوم بحساب قيمة التجزئة للأدلة (hash value) ، مما يضمن عدم تعديلها.

5- حفظ النسخ الأصلية ونسخ احتياطية مؤمنة:

من المهم إنشاء نسخة أصلية من الأدلة المحفوظة ونسخة احتياطية على وسائط تخزين مؤمنة، ويفضل أن تكون الوسائط مشفرة وأن توضع في مكان آمن لمنع الوصول غير المصرح به إليها وضمان حماية الأدلة من الفقدان.

6- التوثيق الزمني للأدلة:

يجب أن يتم تسجيل توقيت وتاريخ جميع الأدلة، بما في ذلك وقت التقاط كل لقطة شاشة أو حفظ ملف معين، فالتوثيق الزمني عامل مهم في المحاكمات؛ حيث يظهر تسلسل الأحداث ويعزز من موثوقية الأدلة الرقمية.[50]

7- إعداد تقارير مفصلة وشاملة:

يتم إعداد تقرير شامل يوضح كل خطوة تم اتخاذها في توثيق الأدلة، بما في ذلك الأدوات المستخدمة، وتفاصيل عن الأشخاص الذين قاموا بجمع الأدلة، وأي تعديل قد يحدث على الأدلة الأصلية، ويعد هذا التقرير جزءًا أساسيًا لتقديم الأدلة للمحكمة بطريقة مهنية.[51]

الفرع الثالث: تحليل الأدلة في جرائم الابتزاز الإلكتروني

يستهدف تحليل الأدلة استخلاص الاستنتاجات التي تستند إلى الأدلة التي عثر عليها وتم فحصها، ويتم هنا استخدام مجموعة من التقنيات والأدوات التي سنتحدث عنها لاحقًا، والفحص والتحليل عمليتان مختلفتان، لكن يحدث نوع من الخلط في المسمى، فالفحص يقوم بالمراجعة التقنية للأدلة من خلال تحديد وفحص واستخراج جميع الأدلة المحتملة من جميع وسائط الأدلة الرقمية التي تم جمعها وضبطها، أما التحليل فيتم فيه تحليل جميع البيانات التي أعدت في الخطوات السابقة بشكل مفصل وبناء الاستنتاجات.[52]

(50) د/ سلمان بن على القحطاني – علوم الأدلة الجنائية الرقمية "المفاهيم وطرق المعالجة " في ضوء التطور التقني الحديث" مرجع سابق - ص 147

(51) د/ أحمد لطفي السيد مرعي - الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني، دراسة مقارنة، بحث منشور في مجلة الدراسات القانونية والاقتصادية - كلية الحقوق - جامعة مدينة السادات، المجلد الثامن، العدد الثاني - يونيو 2022، ص 306ص310

(52) د/ سلمان بن على القحطاني – علوم الأدلة الجنائية الرقمية "المفاهيم وطرق المعالجة " في ضوء التطور التقني الحديث" مرجع سابق - ص 160

وعند التحليل، يقوم المحلل بربط جميع النقاط بما فيها ما تم التوصل إليه من نتائج في مرحلة الفحص، ورسم صورة كاملة للمعني بالقضية، وبعد إعداد قائمة بالأدلة الرقمية ذات العلاقة بالقضية، يقوم المحلل بالبحث عن الإجابة عن جميع التساؤلات المتعلقة بجميع بنود قائمة الأدلة الرقمية؛ مثل: من؟ وماذا؟ ومتى؟ وأين؟ وكيف؟ لإيضاح هوية المستخدم أو التطبيق الذي قام بإنشاء أو تحرير أو إرسال كل بند من بنود قائمة الأدلة، وكيفه جاء هذا الدليل أصلاً إلى الوجود، كما أن المحلل يفسر أيضًا أين تم العثور على الدليل، ويشرح لماذا كل هذه المعلومات مهمة، وماذا تعني بالنسبة للقضية المعنية.

ويمكن للمحللين إعطاء قيمة للنتائج التحليلية، وذلك من خلال البحث عن متى حدثت الأشياء، وكذلك بإنتاج الجدول الزمني الذي يعيد بناء مسرح الجريمة بشكل متماسك، ففيما يخص الأدلة الرقمية يحاول المحللون دائمًا شرح وتفسير متى تم إنشاء هذا الدليل والدخول إليه وتعديله واستقباله وإرساله والاطلاع عليه وإطلاقه، كما أنهم يقومون بملاحظة وتفسير سلسلة الأحداث وتدوينها التي حدثت في الوقت نفسه.

كما أن عمليات التحليل التي يمكن أداؤها تشمل على سبيل المثال: الإطار الزمني، والبيانات المخفية، والملفات، والتطبيقات، والملكية، والحيازة، ويمكن شرح هذه العناصر كالتالي:

1- **تحليل الإطار الزمني**: تحليل الإطار (الجدول) الزمني يمكن أن يكون مفيدًا في تحديد متى وقعت الأحداث على نظام الحاسوب مثلًا، والتي يمكن أن تستخدم كجزء من الربط بين استخدام الحاسوب والأفراد في ذلك الوقت من وقوع الأحداث، وهذا يشمل – على سبيل المثال– تحليل البيانات الوصفية للملفات والخاصة بأوقات وتواريخ التحديث والإنشاء والوصول والتحديث، وكذلك تواريخ وأوقات السجلات المخزنة في ملفات تسجيلات الدخول والخروج والأخطاء وغيرها.[53]

2- **تحليل البيانات المخفية**: من المعلوم أنه يمكن إخفاء البيانات داخل الأجهزة الحاسوبية باستخدام طرق عديدة، منها التشفير والضغط أو بتغيير امتداد الملف. وعليه فإن تحليل البيانات المخفية التي تم استخراجها بواسطة عمليات الفحص ستكون مفيدة جدًّا في كشف واستعادة هذه البيانات، التي قد تشير إلى معارف أو ملكيات أو معنى معين، ومن تلك الطرق على سبيل المثال: محاولة فك كلمات المرور أو التشفير أو عمليات الضغط للتمكن من دخول محتوى الملف المحمي أو المخفي بهذه الطرق، وكذلك التأكد من

(53) Albert j.Marcella, jr.doug menendez, cyber forensics "a field manual for collecting ,examining, and preserving evidence of computer crime", second edition , CRC press , 2008,P: 22

صحة امتداد الملف بالأدوات المناسبة، لذلك فإنَّ محاولة التلاعب بامتدادات الملف وتغيير امتداده الصحيح قد يوحي بأن هناك محاولة لإخفائه. (54)

3- **تحليل التطبيقات والملفات:** العديد من التطبيقات البرمجية والملفات التي تم تحديدها واستخراجها قد تحتوي على معلومات ذات صلة بالتحقيق، كما أنها يمكن أن تعطي نظرة ثاقبة على قدرات النظام ومستوى المعرفة لدى المستخدم، ونتائج هذا التحليل قد تشير إلى وجوب اتخاذ خطوات إضافية في مجال عمليات الاستخراج والتحليل، وهي:

أ- فحص محتويات الملف.

ب- تحديد عدد ونوع نظام (أنظمة) التشغيل.

ج- إيجاد الرابط ما بين الملفات والتطبيقات المثبتة على الجهاز.

د- النظر في العلاقات بين الملفات، على سبيل المثال: ربط تاريخ الدخول للإنترنت إلى ذاكرة التخزين المؤقت وملفات البريد الإلكتروني إلى مرفقات البريد الإلكتروني وغيرها.

ه- تحديد أنواع الملفات ذات الامتدادات غير المعروفة لتحديد قيمتها في التحقيق.

و- فحص مواقع تخزين المستخدمين الافتراضية (default user document) للتطبيقات وهيكلة توزيع الملفات (file structure) في القرص الصلب لتحديد إن كان تم تخزين الملفات في المواقع الافتراضية الخاصة بهم أو في مواقع بديلة. (55)

(54) K. Manivannan and V. Ramanan, Conventional Forensic Approach to Computer Crime Detection, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 22780661-,p-ISSN: 22788727-, Volume 22, Issue 3, Ser. I (May - June 2020), P: 43, DOI: 10.97902203014345-0661/ https: //www.researchgate.net/publication/341371489_Conventional_Forensic_Approach_to_Computer_Crime_Detection

(55) MARCUS K. ROGERS, enterprise Incident Response and Digital Evidence Management and Handling, Information Security Management Handbook, Sixth Edition, VOLUME 2pp: 398403-, https: //engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf

النتائج والتوصيات

أولاً: النتائج:

1- تبين من خلال تحليل الأنماط المختلفة لجرائم الابتزاز الإلكتروني وسمات الجناة وخصائص الجريمة أن الجناة يعتمدون بشكل كبير على عنصر المفاجأة للضحية، مع الضغط الشديد على الضحية للاستجابة لرغبات الجناة وعدم السماح لهم بالتفكير أو الاستعانة بآخرين لدعمهم.

2- من خلال دراسة وتحليل خصائص الجريمة والجناة تبين أن الجريمة تتميز بالتأثير الشديد على الضحية؛ حيث إنها قد تؤدي إلى انتحار الضحية أو الإقدام على أفعال خطيرة، أو قد تؤدي إلى آثار اجتماعية خطيرة كانتشار الفاحشة وهدم الروابط الأسرية، بالإضافة إلى آثار اقتصادية خطيرة على قطاع الأعمال عبر ارتكاب أنماط الابتزاز وغيرها من الأنماط التي تمس المؤسسات والشركات والهيئات الحيوية.

3- غالبًا ما يسعى الجناة في هذه الجريمة إلى الحصول على منفعة مالية أو معنوية أو غير أخلاقية، ويعتمدون في استدراج الضحايا على الوقوع تحت سيطرتهم على مواقع التواصل الاجتماعي بشكل كبير؛ حيث يمكنهم استغلال نقاط الضعف الخاصة بالضحايا من خلال دراسة حساباتهم على مواقع التواصل، والنفاذ إليهم من خلال تحليلهم لمحتوى تلك المواقع، وهو ما يتطلب من المستخدمين الحذر الشديد عند التعامل مع الآخرين عبر تلك المواقع.

4- تؤدي الأدلة الرقمية دورًا كبيرًا في إثبات هذه الجريمة، وهو ما يتطلب الحرص على جمع تلك الأدلة والتحفظ عليها وتحليلها وفقًا للقواعد المرعية؛ حتى تعد حجة على الجاني وتوصل المحققين إلى تحييد هوية الجناة وضبطهم.

ثانيًا: التوصيات:

1- يوصي الباحث بعقد الدورات التدريبية للعاملين في مجال إنفاذ القانون في الجرائم الإلكترونية؛ لتطوير معارفهم بشأن الأساليب الإجرامية والأنماط الجديدة من جرائم الابتزاز الإلكتروني والحيل التي يستخدمها الجناة في استدراج ضحاياهم، وفهم كيفية الحفاظ على الأدلة في مسرح الجريمة الرقمي وطبيعته الخاصة.

2- تعزيز القدرات الخاصة بالمعامل الجنائية الرقمية والفاحصين الرقميين في مجال الطب الشرعي الرقمي والمعمل الجنائي، وتطوير معارفهم بشأن أنماط الجرائم التي تستجد حتى يمكنهم فهم الطبيعة المتجددة لمسرح الجريمة الرقمي وكيفية التحفظ على الأدلة الرقمية في جرائم الابتزاز عبر مواقع التواصل الاجتماعي.

3- إيجاد آلية إلكترونية يمكن من خلالها تلقي البلاغات بشكل آلي ودون تدخل بشري ودون طلب بيانات المجني عليهم في جرائم الابتزاز الإلكتروني، وذلك لتشجيع الإبلاغ عن هذه الجرائم، ويمكن من خلالها القيام بالتحقيقات دون تطلب حضورهم أو تواجدهم في جلسات المحاكمة أو الإفصاح عن شخصياته.

4- إبرام اتفاقية مع مزودي خدمات الإنترنت ومواقع ومنصات التواصل الاجتماعي المختلفة؛ لإيجاد آلية تعمل بالذكاء الاصطناعي لرصد عمليات استدراج الضحايا عبر مواقع التواصل الاجتماعي، وحظرهم بمجرد ارتكابهم للأنشطة التي تعد من قبيل الاستدراج للإفصاح عن أسرار أو معلومات سرية أو صور أو غيرها.

5- تعزيز التعاون مع مواقع التواصل الاجتماعي في إطار الاتفاقية الأممية المبرمة مؤخرًا في أغسطس 2024 من الجمعية العامة للأمم المتحدة؛ بشأن مكافحة الإجرام عبر الإنترنت، والعمل على تفعيل بنودها في إطار الحد من جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

قائمة المراجع

أولاً: المراجع العربية

- أطروحة ماجستير بعنوان: "الابتزاز الإلكتروني للفتاة عبر مواقع التواصل الاجتماعي "الفيسبوك نموذجًا" دراسة مسحية لعينة من طالبات قسم الإعلام والاتصال – جامعة قاصدي مرباح"، تخصص تكنولوجيا الاتصال الجديدة، الجزائر، مقدمة من سمان جويدة، إيمان مردف 2017م، ص23ص25 – https: //jspui/dz.ouargla-univ.dspace/pdf.mardaf-samane/1/14448/123456789/bitstream
- أحمد سبتي أحمد، محمد نعمان عبد النبي، الابتزاز الإلكتروني وأثره في تهديد المجتمع "دراسة فقهية معاصرة"، كانون الثاني 25, 2022، مجلة جامعة تكريت للعلوم الإنسانية، المجلد 1، الجزء الأول (عدد خاص بالمؤتمر) لعام 2022، العدد 29، ص55ص57 – https://jtuh.org/index.php/jtuh/article/view/1740
- باقر غازي حنون، وحسن حماد حميد ، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، مجلة دراسات البصرة، السنة السادسة عشرة، ملحق العدد (42)، كانون الأول 2021، ص54-53.
- جاسم ناصر جاسم المسلماني، التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري، رسالة مقدمة للحصول على درجة الماجستير في القانون العام، كلية القانون – جامعة قطر ، يناير 2023م، ص9-7.
- هشام رشدي خير الله، إدراك المراهقات لمخاطر الابتزاز الإلكتروني عبر الإنترنت وتأثيره على اتجاهاتهم نحو استخدام تطبيقات التواصل الاجتماعي عبر الهواتف الذكية "دراسة في ضوء مجتمع المخاطر "، المجلة العلمية لبحوث الصحافة، العدد 24، الجزء الأول، يوليو 2022، ص3-1.
- سعيد زيوش، ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الاجتماعية، العدد 22، 2017م، ص73-70.
- شريفة محمد السويدي، وزيزي مصطفى نوفل، أسباب الابتزاز الإلكتروني والآثار الاجتماعية والنفسية المرتبطة به "دراسة كيفية"، مجلة الآداب، العدد 146، أيلول 2023م، ص618-616
- Doi: https: //doi.org/10.31973/aj.v1i146.4008 https://aladabj.uobaghdad.edu.iq/index.php/aladabjournal/article/view/4008/3583
- هند نجيب، ضبط الأدلة الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة، المجلة الجنائية القومية، المجلد 61، العدد 3، نوفمبر 2016، ص102
- https://ncj.journals.ekb.eg article___208596___34d8c5ea5267decb20915a2587933a12.pdf

ثانيًا: المراجع الأجنبية:

- "Coercion and Responsibility in Criminal Law: A Study of the Limits of Criminal Liability" by Douglas Husak, Oxford University Press, 2020, pp: 22: 24
- "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality" by Wang, Y., & Stefanone, M. A., New Media & Society, 2022., DOI: 10.1177/14614448211045148
- "The Impact of Self-Disclosure on Social Media on Personal Relationships: A Cross-Cultural Analysis" by Bazarova, N. N., & Choi, Y. H., Journal of Communication, 2020., DOI: 10.1093/joc/jqz052
- Abdullah Al Habsi · Michelle Butler · Andrew Percy, Blackmail and the self-disclosure of sensitive information on social media: Prevalence, victim characteristics and reporting behaviours amongst Omani WhatsApp users", Security Journal, 2023, pp: 250: 252, https: //doi.org/10.1057/s41284-023-00376-3
- Ahmed A. Abd El-Latif, Lo'ai Tawalbeh, Manoranjan Mohanty, Brij B. Gupta, Konstantinos E. Psannis, igital Forensics and Cyber Crime Investigation Recent Advances and Future Directions, 2025, pp: 43-46, https: //www.routledge.com/Digital-Forensics-and-Cyber-Crime-Investigation-Recent-Advances-and-Future-Directions/AbdEl-Latif-Tawalbeh-Mohanty-Gupta-Psannis/p/book/9781032075396
- Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525-540. https: //doi.org/10.1057/s41284-020-00246-2
- Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525-540. https: //doi.org/10.1057/s41284-020-00246-2
- Albert j.Marcella, jr.doug menendez, cyber forensics “a field manual for collecting ,examining, and preserving evidence of computer crime”, second edition , CRC press , 2008,P: 22
- ALJI Mohamed and CHOUGDALI Khalid, Digital Investigation of a Cybercrime: Sextortion as a Case Study, Proceedings of the Digital Privacy and Security Conference 2019 10.11228/dpsc.01.01, Electronics and Telecommunication Systems Research Group, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, p: 13

- Authors. Alma Spaniardi, Janki Modi Avari, Teens, Screens, and Social Connection An Evidence-Based Guide to Key Problems and Solutions, 2023, Jenna Margolis and Dinara Amanbekova, Social Media and Cyberbullying, pp: 81: 83, https: //doi.org/10.1007/978-3-031-24804-7
- Barbara Guttman, Douglas R. White, Tracy Walraven, Digital Evidence Preservation Considerations for Evidence Handlers, NIST Interagency Report, NIST IR 8387, September 2022, p: 12, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf
- Cybercrime and Digital Forensics: An Introduction" by Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Routledge, 2017,
- Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats" by Will Gragido, John Pirc, Nicholas Hoffman, & Daniel Molina, Syngress, 2011, pp: 20-22
- Digital Forensics and Cybercrime Investigations, https: //criminal-justice.iresearchnet.com/criminal-justice-process/impact-of-technology/digital-forensics-and-cybercrime-investigations/
- Holt, T.J., & Smirnova, O. (2014). "Exploring the market for cybercrime tools: Characteristics of buyers and sellers in a digital underground economy." Journal of Criminal Justice, 42(1), 27-38, DOI: 10.1016/j.jcrimjus.2013.11.005
- https: //ieeexplore.ieee.org/xpl/conhome/10608004/proceeding , DOI: 10.1109/CITS61189.2024.10607983
- James R. Lyle, Barbara Guttman, Digital Investigation Techniques: A NIST Scientific Foundation Review, NIST Internal Report, NIST IR 8354, November 2022, pp: 37-40, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf
- Jeremy Leighton John, Digital Forensics and Preservation, DPC Technology Watch Report 12-03 November 2012, Series editors on behalf of the DPC, Published in association with Charles Beagrie Ltd., pp: 9-15, https: //www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-reports-1/810-dpctw12-03-pdf/file
- K. Manivannan and V. Ramanan, Conventional Forensic Approach to Computer Crime Detection, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 3, Ser. I (May - June 2020), P: 43, DOI: 10.9790/0661-2203014345 https: //www.researchgate.net/publication/341371489_Conventional_Forensic_Approach_to_Computer_Crime_Detection
- Kasmani, M. F., Ismail, R., Sulong, R. S., & Mahamod, Z. (2018). Cyber blackmailer: Modus operandi and preventive measures. International Journal of Cyber Criminology, 12(2), 334-345

- Kausik Maitra , Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation and Evidence Collection, International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 43 No. 2 Aug. 2024, pp. 261-271, Innovative Space of Scientific Research Journals http: //www.ijias.issr-journals.org/,
- Kshetri, N. (2010). "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives." Springer, 2010, pp: 35-37, http: //ndl.ethernet.edu.et/bitstream/123456789/26704/1/50.pdf
- MARCUS K. ROGERS, enterprise Incident Response and Digital Evidence Management and Handling, Information Security Management Handbook, Sixth Edition, VOLUME 2pp: 398-403, https: //engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf
- Martinez, M., & Anderson, C, "Cyber Extortion: An Emerging Internet-Based Crime", Journal of Cybersecurity, 2021, pp: 126-129
- Nash, M. (2020). "Coercion, Consent, and the Criminal Law: Understanding the Limits of Criminal Liability." Criminal Law Review, 1, 24-39. DOI: 10.2139/ssrn.3563456
- Paganini, P. (2018). "Understanding the motives behind cyber extortion: A deep dive into ransomware attacks." Journal of Information Security and Applications, 43, 23-32, DOI: 10.1016/j.jisa.2018.06.004
- Pemberton, A., Winkel, F.W., & Groenhuijsen, M.S. (2007). "Taking victims seriously in restorative justice: A crime victim and human rights perspective." European Journal of Crime, Criminal Law and Criminal Justice, 218-220.
- Self-Disclosure and Psychological Well-Being in the Age of social media: A Meta-Analysis" by Nguyen, M. H., Bin, Y. S., & Campbell, A., Cyberpsychology, Behaviour, and Social Networking, 2021., DOI: 10.1089/cyber.2020.0329
- The Essential Evidence Collection Guide for Websites, Social Media, and Team Collaboration Tools How to Collect and Preserve Evidence on Websites, Social Media Platforms, and Enterprise Social Networks, 2020, pp: 3-9 https: //f.hubspotusercontent10.net/hubfs/1818760/PDFs/2020%20The%20Essential%20Evidence%20Collection%20Guide%20for%20Websites%20Social%20Media%20and%20Team%20Collaboration%20Tools%20_%20Guidebook.pdf
- Tommy K.H. Chan, Christy M.K. Cheung, Zach W.Y. Lee, Cyberbullying on Social Networking Sites: A Literature Review and Future Research Directions" , Information & Management, Volume 58, Issue 2, March 2021, 103411, pp: 12: 14 https: //www.sciencedirect.com/science/article/pii/S0378720620303499?via%3Dihub

- Utz, S., Muscanell, N., & Khalid, R., "Self-Disclosure on Social Media: The Role of Intrinsic versus Extrinsic Motivations", Computers in Human Behaviour, 2021, pp: 12-14
- Valentin Gazeau; Khushi Gupta; Min Kyung An, Enhancing Social Media Data Collection for Digital Forensic Investigations: A Web Parser Approach, 2024 International Conference on Computer, Information and Telecommunication Systems (CITS), Girona, Spain, 17-19 July 2024,
- Wang, Y., & Stefanone, M. A., "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality", New Media & Society, 2022., pp: 535-541