الأسباب والآثار الاجتماعية للابتزاز الإلكتروني وسبل ومعالجته

Causes and social effects of electronic blackmail and ways and treatment

م.م.أمير علي هادي

جامعة كربلاء/ كلية التربية للعلوم الانسانية

البريد الالكتروني : amer.ali@uokerbala.edu.iq

ملخص البحث

استهدف البحث الحالي دراسة مفهوم الابتزاز الإلكتروني، فضلًا عن معرف أبرز الأسباب والآثار لجريمة الابتزاز الإلكتروني، إلى جانب معرفة واقع حجم مشكلة جريمة الابتزاز الإلكتروني في العراق. ولتحقيق هذه الأهداف وغيرها تكمن أهمية البحث بأن الابتزاز الإلكتروني، يعد من الجرائم المنتشرة في دول العالم بصورة كبيرة مع هيمنة وتغلغل الشبكة المعلوماتية (الإنترنت) في كافة مفاصل الحياة البشرية، حيث أصبح المسيطر وصحاب القوة في كافة الأعمال، وأن طالت آثاره السلبية حياة المواطنين متمثلة بالابتزاز الإلكتروني وغيرها من الجرائم المعلوماتية ومن هذه الأهمية ارتأينا إلى دراسة أسباب وآثار الابتزاز الإلكتروني كونها جريمة دخيلة على المجتمع العراقي.

وتحقيقًا لهذه الأهمية توصل البحث إلى عدة استنتاجات منها:

1) تعد جريمة الابتزاز الإلكتروني إحدى أبرز صور الجرائم الإلكترونية، حيث تُمارس هذه الجريمة عبر شبكة الإنترنت واستخدام الأجهزة الحديثة والتطبيقات المتنوعة، مثل وسائل التواصل الاجتماعي. لقد أصبحت هذه الظاهرة تمثل تهديدًا كبيرًا للأفراد والمجتمعات على حد سواء.
2) إن أساليب ارتكاب هذه الجريمة تتفاوت بشكل ملحوظ عن أساليب الابتزاز التقليدي، حيث يُستخدم الهاتف المحمول المزود بكاميرا للاعتداء على خصوصية الأفراد، سواء من خلال التقاط الصور أو نشر معلومات حساسة أو تسجيلات صوتية ومرئية. تعكس هذه الوسائل خطورة الابتزاز الإلكتروني، إذ تتجاوز الحدود التقليدية، مما يستدعي اهتمامًا أكبر من الأفراد والمجتمعات لمواجهة هذا التحدي.
3) إن التطور التكنولوجي قد ساهم في زيادة وتيرة هذه الجرائم. فسهولة الوصول إلى المعلومات ووسائل الاتصال تجعل من السهل على الجناة تنفيذ مخططاتهم بسرعة وفعالية، مما يتطلب جهودًا أكبر لمكافحة هذه الظاهرة.

وكان من أهم توصيات البحث هي:

1) تحديث النصوص القانونية الإجرائية لتتناسب مع تحديات جريمة الابتزاز الإلكتروني، التي تتطور بشكل مستمر. يجب أن تشمل هذه النصوص آليات جديدة لضبط وتحقيق الجرائم في الفضاء الافتراضي، مع الأخذ في الاعتبار التعقيدات التقنية التي قد تعترض عمليات التحقيق.

4) يجب على الحكومات والجهات التشريعية العمل على تقوية القوانين المتعلقة بالجرائم الإلكترونية، بما في ذلك الابتزاز. يجب أن تكون هناك عقوبات رادعة للجناة، وتحسين آليات الإبلاغ عن هذه الجرائم لتسهيل الوصول إلى العدالة وتوفير الدعم النفسي والقانوني للضحايا.
5) نشر الوعي داخل المجتمع حول أخطار الابتزاز الإلكتروني. يجب أن تشمل هذه المبادرات الإجراءات الاحترازية، مثل عدم مشاركة المعلومات الحساسة على الإنترنت والتأكد من الإبلاغ عن أي محاولة ابتزاز فور حدوثها.
6) يجب على الأفراد الاتصال فورًا بالجهات المتخصصة التي تمتلك الخبرة في التعامل مع قضايا الابتزاز. من الضروري عدم حذف أي محتوى مرتبط بالابتزاز، حيث يعد هذا دليلاً قد يكون حيويًا لملاحقة الجاني.
7) يجب تعزيز التعاون الدولي بين الدول لتبادل المعلومات والتقنيات اللازمة لمكافحة ظاهرة الابتزاز الإلكتروني بفاعلية. فالتعاون المشترك يمكن أن يسهم في تطوير استراتيجيات موحدة لمواجهة هذه الجرائم التي تتخطى الحدود الجغرافية.
8) الكلمات المفتاحية: الاسباب، الآثار، الابتزاز، الابتزاز الإلكتروني.

Abstract

The current research aimed to study the concept of electronic blackmail, as well as to identify the most prominent causes and effects of the crime of electronic blackmail, in addition to knowing the reality of the size of the problem of the crime of electronic blackmail in Iraq. To achieve these goals and others, the importance of the research lies in the fact that electronic blackmail is one of the widespread crimes in the countries of the world in a large way with the dominance and penetration of the information network (the Internet) in all aspects of human life, as it has become the dominant and powerful in all works, and its negative effects have extended to the lives of citizens represented by electronic blackmail and other information crimes. From this importance, we decided to study the causes and effects of electronic blackmail as it is a crime alien to Iraqi society.

To achieve this importance, the research reached several conclusions, including:

1) The crime of electronic blackmail is one of the most prominent forms of electronic crimes, as this crime is practiced via the Internet and the use of modern devices and various applications, such as social media. This phenomenon has become a major threat to individuals and societies alike.
2) The methods of committing this crime differ significantly from traditional blackmail methods, as a mobile phone equipped with a camera is used to violate the privacy of individuals, whether by taking pictures, publishing sensitive information, or audio and video recordings. These methods reflect the seriousness of electronic blackmail, as they exceed traditional boundaries, which requires greater attention from individuals and societies to confront this challenge.
3) Technological development has contributed to the increase in the frequency of these crimes. The ease of access to information and means of communication makes it easy for perpetrators to implement their plans quickly and effectively, which requires greater efforts to combat this phenomenon.

The most important recommendations of the research were:

1) Updating procedural legal texts to match the challenges of the crime of electronic blackmail, which is constantly evolving. These texts must include new mechanisms to control and investigate crimes in virtual space, taking into account the technical complexities that may hinder investigations.
2) Governments and legislative bodies must work to strengthen laws related to electronic crimes, including blackmail. There should be deterrent penalties for perpetrators, and improved reporting mechanisms for these crimes to facilitate access to justice and provide psychological and legal support to victims.
3) Raising awareness within the community about the dangers of cyber-extortion. These initiatives should include precautionary measures, such as not sharing sensitive information online and ensuring that any extortion attempt is reported immediately.
4) Individuals should immediately contact specialized agencies that have experience in dealing with extortion cases. It is essential not to delete any content related to extortion, as this is evidence that may be vital to prosecuting the perpetrator.
5) International cooperation between countries should be enhanced to exchange information and technologies necessary to effectively combat the phenomenon of cyber-extortion. Joint cooperation can contribute to developing unified strategies to confront these crimes that transcend geographical borders.

Keywords: Causes, effects, extortion, cyber-extortion.

المبحث الأول: عناصر البحث الأساسية

أولًا/ مشكلة البحث

شهد المجتمع العراقي بعد عام 2003م انفتاحًا كبيرًا على مختلف الجوانب الاقتصادية والاجتماعية والسياسية، وصاحب ذلك دخول وسائل وطرق تقنية وإلكترونية حديثة لم تكن معروفة، وذلك لأن المجتمع العراقي كان مجتمعًا مغلقًا قلما تدخُله الوسائل التقنية المتعلقة بشبكة المعلومات، أما بعد عام 2003، فالواقع يشير إلى تطور هذه الوسائل ودخولها لمختلف مرافق الحياة ونتيجة لنقص الخبرة في التعامل مع أساليب التكنولوجيا الحديثة من حاسوب وإنترنت وغيرها، إلا أن سوء استعمال هذه الوسائل الإلكترونية من قبل ضعاف النفوس وقيامهم بالسرقة والاغتصاب واستغلال بعض الأشخاص كفريسة لهم من خلال الصور أو التسجيلات والفيديو بعد تغييرها باستعمال برامج أخرى لتعديلها بحسب ما يرونه مناسبًا واستغلالهم ماديًا أو معنويًا أو جنسيًا، ومن جانب أخر عدم وجود إطار تشريعي متكامل لتجريم أفعال الابتزاز الإلكتروني والتصدي لها في العديد من الدول، مما أدى إلى تشجيع الجناة على ارتكاب هذه الأفعال دون رادع أو خوف من العقاب، كل ذلك أسهم في تطوير جرائم الابتزاز وزيادة نسب ارتكاب هذه الجرائم في الآونة الأخيرة نتيجة التطور الذي وفر وسائل الرفاهية والرعاية والخدمات للطلبة في كل مجالات الحياة في النواحي الإنتاجية والاجتماعية والثقافية والصحية وغيرها. وإزاء هذا الوضع تحاول السلطات القضائية العراقية تطبيق ما جاء من نصوص في قانون العقوبات لتجريم هذه الأفعال وإنزال العقاب بحق مرتكبيها، ففي بعض الأحيان تلجأ السلطة القضائية إلى تكييف فعل الابتزاز وفقًا للنصوص الخاصة بجريمة التهديد، وفي أحيان أخرى تكيفها وفقًا لنصوص جريمة الاحتيال أو نصوص الخاصة بجريمة اغتصاب الأموال.

علاوة على ذلك تمثل ظاهرة الابتزاز الإلكترونية من المشاكل الحديثة على مجتمعنا وهي إحدى المشاكل الاجتماعي التي تهدد الفرد أو العائلة والمجتمع من خلال التصنت والدخول غير المشروع لمواقع الإنترنت والقيام بالتهديد والابتزاز أو التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنية المختلفة، وفي كثير من الأحيان لا يعلن أو يخبر أحدًا من عالته أو الجهات الأمنية خجلًا أو خوفًا من الفضيحة على سمعته أو سمعة العائلة أو الملاحقة القانونية، كما أن هذا الموضوع لم يلق الدرجة الكافية من البحوث والدراسات التي كتبت عنه كونه موضوع حديث العهد على مجتمعنا إذا ما قورنت بعدد البحوث والدراسات خارج العراق، كما أنه يعد إضافة إلى الدراسات والبحوث العلمية لقلة عددها في المكتبات العراقية، كما أصبحت هذه المشكلة تؤرق المجتمع مما دعت وزارة الداخلية العراقية والوزارة الأخرى إلى ضرورة إجراء البحوث والدراسات لوقاية الأفراد وإيجاد الحلول لتلك المشكلات، لذلك أن الطالب العراقي بحاجة ماسة إلى التوجيه والإرشاد، لأن يمر خلال مراحل النمو المتعددة بمشكلات سلوكية ونفسية وفترات حرجة يحتاج فيها إلى الإرشاد التربوي، لأن التغيرات التي حدثت بما فيها التقدم العلمي والتكنولوجي وما نتج عنه من شبكات التواصل الاجتماعي التي تقوع الطالب في الابتزاز الإلكتروني وتطور المناهج أدى إلى ضرورة وجود مرشدين تربويين ونفسيين في الجامعات العراقية مسلحين بخبرة كافية، لتقديم خدماتهم الإرشادية إلى الطلبة كافة، ومنعهم من الوقع في الابتزازات الإلكترونية. لذا جاءت مشكلة البحث في التساؤلات التالية:

1) ما هي ظاهرة الابتزاز الإلكتروني؟
2) ما هي الآثار الاجتماعية للابتزاز الإلكتروني؟
3) ما الحلول المقترحة لمعاجلة ظاهرة جريمة الابتزاز الالكتروني؟
4) ما هي الطرق التي يتم عن طريقها الابتزاز الإلكتروني؟

ثانيًا/ أهمية البحث

تأتي أهمية البحث من خلال دراسة الأسباب والآثار الاجتماعية للابتزاز الالكترونية وسبل معالجته على طلبة الجامعة للحد من هذه الظاهرة بعد تنوع وتطور وسائل الاتصال الاجتماعي، ويمكن القول أن الابتزاز الإلكتروني، يعد من الجرائم المنتشرة في دول العالم بصورة كبيرة مع هيمنة وتغلغل الشبكة المعلوماتية (الإنترنت) في كافة مفاصل الحياة البشرية، حيث أصبح المسيطر وصحاب القوة في كافة الأعمال، وأن طالت آثاره السلبية حياة المواطنين متمثلة بالابتزاز الإلكتروني وغيرها من الجرائم المعلوماتية ومن هذه الأهمية ارتأينا إلى دراسة أسباب وآثار الابتزاز الإلكتروني كونها جريمة دخيلة على المجتمع العراقي، فضلًا عن أنها تعد من أخطر الجرائم في الوقت الحاضر لما لها من آثار على الفرد والمجتمع، وتحمل في طياتها صفات تجعلها منفردة عن باقي الجرائم التقليدية بكونها جرائم لا يمكن بسهولة الكشف عنها وتكون عابرة للحدود والقارات، فأصبحت مشكلة عالمية يعاني منها جميع المجتمعات، كما هو المجتمع العراقي والذي ساعد على بروز هذه الجريمة عدة أسباب يأتي في مقدمتها ضعف الروابط الأسرية، وضعف الوزع الديني وغيرها من الأسباب. كما يشكل الإعلام دورًا مهمًا في انتشار هذه الجريمة ومن جهة أخرى هناك جمل من التداعيات السياسية والاجتماعية التي تلقي ضلالها على المجتمع العراقي كازدياد حالات الانتحار والسرقة وتصل إلى حد إقصاء شخصيات سياسية من مناصبهم.

ثالثًا/ أهداف البحث

1) يسعى البحث إلى معالجة موضوع جريمة الابتزاز الإلكتروني بشكل أكاديمي وعلمي.
2) عرض مفهوم وأنواع الابتزاز الإلكتروني وطرق استعماله.

3) عرض واقع مشكلة جريمة الابتزاز الإلكتروني في العراق.
4) تحديد أسباب وآثار جريمة الابتزاز الإلكتروني
5) تقديم مجموعة من الحلول المقترحة لمعالجة جريمة الابتزاز الإلكتروني.
6) تقديم بعض التوصيات للمهتمين بالشأن السلطة القضائية التي من شأنها دعم وتقديم أفضل الحلول والمعالجات لمرتكبي جرائم الابتزاز الإلكتروني.

رابعًا/ مفاهيم البحث

1) الأسباب

هي العوامل أو الدوافع التي تؤدي إلى وقوع حدث أو نتيجة معينة، إذ تعبر الأسباب عن العلاقة التي تربط بين حدثين أو فعلين، حيث ينسب الفعل أو النتيجة إلى تأثير هذا العامل، يمكن أن تكون الأسباب مادية، اجتماعية أو نفسية وتساعد في فهم كيفية حدوث الأمور وتفسير الظواهر المختلفة.

2) الآثار

عرف الأثر: هو النتيجة أو التأثير الذي ينتج عن حدث أو فعل معين. يمكن أن يكون هذا الأثر ماديًا أو معنويًا، ويعبر عن التغييرات التي تحدث في الأفراد أو المجتمعات أو البيئة نتيجة لممارسات أو قرارات محددة **(شحاتة، والنجار، 2003 : 7)**.

وعرف الأثر إجرائيًا: بأنه النتيجة أو التأثير الذي ينجم عن فعل أو حدث معين، ويمكن أن يتجلى في شكل تغيير ملموس أو تأثير معنوي. يعكس الأثر كيفية تأثير الأفعال أو القرارات على الأفراد أو المجتمعات أو البيئة، مما يؤدي إلى تغييرات أو نتائج مختلفة.

3) الابتزاز

عرف الابتزاز بأنه: فرض أسلوب التهديد بالفعل أو الترك للحصول على مكاسب من شخص أو جهة ممنوعة شرعًا وعقلًا **(المطلق، 2021: 3-4)**.

عرف الابتزاز كذلك بأنه: محاولة للإكراه وسلب الإرادة والحرية لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو المعنوية **(الصباح وآخرون، 2010 : 14)**.

4) الابتزاز الإلكتروني

يعرف بأنه استخدام التهديد بالإيذاء الجسدي أو النفسي أو الإضرار بالسمعة والمكانة الاجتماعية بتلفيق الفضائح وإلصاق التهم ونشر أغرار مما يجبر المبتز على الدفع مكرهًا لمن يمارس الابتزاز عليه **(الجريش، 2003 : 128)**.

ويعرف أيضًا: بأنه جريمة ترتكب ضد شخص لإجباره على تسليم المال أو التوقيع على وثيقة بتهديد لكشف أمر معين أو لصق تهمة بارتكاب جريمة (كرم، **1987: 157)**.

والتعرف النظري للابتزاز الإلكتروني: اعتمد الباحث تعريف نظريًا للابتزاز الإلكتروني على نظرية بالابتزاز الإلكتروني العائد للباحث (فوروارد).

وعرف الابتزاز الإلكتروني إجرائيًا: بأنه شكل من أشكال الجرائم الإلكترونية، يتم من خلاله استخدام التهديدات أو الضغوط للحصول على مكاسب مالية أو غير مالية من الأفراد أو المؤسسات. يعتمد المبتز في غالب الأحيان على استغلال معلومات حساسة أو صور خاصة للضحية، حيث يهدد بنشر هذه المعلومات أو بإلحاق الأذى بها إذا لم تلبِّ الضحية مطالبه. وتُعتبر هذه الجريمة خطيرة، حيث تؤثر سلبًا على الحالة النفسية والاجتماعية للضحايا، مما يستدعي تضافر جهود الأفراد والمجتمع والحكومات لمواجهتها.

المبحث الثاني/ الابتزاز الإلكتروني

أولًا/ نظرية الابتزاز الإلكتروني (فوروارد)

تنطلق هذه النظرية من أن بعض الأفراد الذين يتميزون بالمهارة والنجاح في مجالات كثيرة في حياتهم فأنهم يشعرون بالحيرة وانعدام القوة أمام هؤلاء الأفراد المبتزين، فأنهم يدخلونهم بحالة من الصداقة الحميمة المريحة عندما يريدون شيئًا ولكنهم كثيرًا ما يهددون حتى يحصلوا على ما يريدونه ويشعرونهم بالخوف والالتزام والشعور بالذنب ليتلاعبوا به وربما كان أسوا شيء هو أنه كلما استسلم الضحية للابتزاز الإلكتروني كلما فقد التواصل مع شخصيته المتكامل وبوصلته الداخلية التي تحدد له ما ينبغي أن تكون سلوكياته، كما تشير (فوروارد) إلى الحالة الضبابية التي يمر بها الضحية عن طريق الخوف والالتزام والشعور بالذنب، إذ يعمل المبتز في علاقته مع الضحية في إثارة هذه العوامل، كما يحدث الابتزاز الإلكتروني عندما يعطي بعض الأفراد صورًا خاصة أو مقاطع فيديو أو معلومات سرية أو مكانًا لفرد ما في حياتهم ليكتسبوا منه الحب والاحترام إذ ليس لديهم القدر على أن يؤمنوها لذواتهم فالمبتز الإلكتروني يدرك أهمية وتقدير الضحية لتلك العلاقة مثل هذه العلاقة لا يمكن لها أن تستمر طويلًا (حميد، 2023: 178-179)

ثانيًا/ واقع مشكلة جريمة الابتزاز الإلكتروني في العراق

تشير تقارير وزارة الداخلية العراقية لعامي 2003-2004 إلى تسجيل 4554 قضية تحرش وابتزاز، مما يعكس نسبة مرتفعة تصل إلى 42%. بين عامي 2005-2008، شهدت هذه القضايا ارتفاعًا ملحوظًا، حيث بدأت الجرائم عبر المعاكسات والتحرشات، تلتها علاقات غير شرعية بين الشباب والفتيات عبر وسائل التكنولوجيا الحديثة. عندما ترغب الفتاة في قطع هذه العلاقات، غالبًا ما تتعرض لتهديدات بكشف فضائحها، مما يتطلب تدخل القضاء لمحاكمة مرتكبي هذه الجرائم (عمر، ومحمد، 2019 : 453) وفي تقرير صادر عن مديرية مكافحة إجرام بغداد، يظهر أن عدد جرائم الابتزاز الإلكتروني المسجلة في عام 2018 كان 16 جريمة، مع 19 متهمًا. شهد عام 2019 قفزة في هذه الجرائم، حيث تم تسجيل 213 جريمة مع 101 متهم. واستمر هذا الاتجاه في عام 2020، حيث تم تسجيل 30 جريمة في شهري كانون الثاني وشباط، مع 11 متهمًا. هذا الارتفاع المتواصل يشكل خطرًا يهدد المجتمع (العبادي، 2020 : 540-541). وفقًا لإحصائيات مديرية الشرطة المجتمعية في وزارة الداخلية لعام 2022، تم تسجيل 1950 حالة ابتزاز إلكتروني، غالبيتها تستهدف النساء، بما في ذلك فتيات في سن المراهقة وأطفال دون سن 14 عامًا. وفي مايو 2022، أظهرت إحصائية خاصة أن هناك 2452 جريمة ابتزاز إلكتروني في 15 محافظة. في عام 2023، سجلت وزارة الداخلية العراقية 9384 حالة ابتزاز إلكتروني و7362 ضحية عنف أسري، بالإضافة إلى 567 شخصًا هاربًا تم إعادتهم لذويهم. وقدمت مفارز

الشرطة المجتمعية دعمًا نفسيًا ومعنويًا لعدد كبير من الضحايا، مستندة إلى مبدأ الرعاية اللاحقة لمتابعة أحوالهم (ديجيتال، 2024: 1 https://www.rudawarabia.net).

في عام 2024، انخفضت نسبة جرائم الابتزاز الإلكتروني إلى 3%، مما يعكس جهود الأجهزة الأمنية في كشف هذه الجرائم والقبض على الجناة. هذا الانخفاض يدل على فعالية التدابير المتخذة لمكافحة هذه الجرائم، بالإضافة إلى زيادة الوعي المجتمعي ودور منظمات المجتمع المدني ووزارة الداخلية في نشر المعلومات حول حماية الحسابات وسبل الإبلاغ عن حالات الابتزاز (نيوز، 2024: 1 ، https://shafaq.com) .

بالإضافة إلى ما تم ذكره، هناك عدة عوامل ساهمت في تغيير الوضع المتعلق بالجرائم الإلكترونية، وخاصة الابتزاز، في العراق:

1) تعزيز الوعي المجتمعي: مع تزايد استخدام وسائل التواصل الاجتماعي والتكنولوجيا الرقمية، بدأت جهود التوعية تستهدف المجتمع حول مخاطر الابتزاز الإلكتروني. قامت منظمات المجتمع المدني والجهات الحكومية بتنظيم ورش عمل وندوات تقدم معلومات حول كيفية حماية المعلومات الشخصية والتصرف الصحيح عند التعرض للابتزاز.
2) تطور التكنولوجيا الأمنية: شهدت أدوات وتقنيات الأمن السيبراني تطورًا ملحوظًا، مما عزز من قدرة الأجهزة الأمنية على مواجهة الجرائم الإلكترونية. تم استخدام برامج وتقنيات متقدمة لتعقب المجرمين وتحديد هويتهم، مما ساهم في تعزيز فعالية العمليات الأمنية.
3) التعاون الدولي: مع تزايد انتشار الابتزاز الإلكتروني على مستوى العالم، تم إقامة تعاون دولي بين الدول لتبادل المعلومات والخبرات. هذا التعاون ساعد العراق في تبني استراتيجيات فعالة لمكافحة هذه الجرائم.
4) تحسين الاستجابة القانونية: قامت الأجهزة الأمنية بتقديم الدعم النفسي والمعنوي للضحايا، مما عزز الثقة بين المجتمع والشرطة. كما كانت برامج الرعاية اللاحقة لمتابعة الضحايا خطوة إيجابية لضمان إعادة إدماجهم في المجتمع.
5) دور الإعلام: لعبت وسائل الإعلام دورًا فعالًا في تسليط الضوء على قضايا الابتزاز الإلكتروني وأهمية التصدي لها، مما ساعد في نشر الوعي وزيادة يقظة المجتمع.

يمكن القول إن الجهود المنسقة من قبل الحكومة ومنظمات المجتمع المدني والأفراد أسهمت في تقليل نسبة جرائم الابتزاز الإلكتروني في العراق. ومع ذلك، تبقى التحديات قائمة، حيث إن التكنولوجيا في تطور مستمر، مما يتطلب تحديث الاستراتيجيات والتقنيات بشكل دوري لمواجهة هذه الجرائم. سيبقى الحفاظ على وعي المجتمع وتزويده بالأدوات اللازمة للحماية، بالإضافة إلى تعزيز التعاون بين الجهات المعنية، أمرًا حيويًا لمواجهة هذه الظاهرة.

ثالثًا/ أنواع الابتزاز الإلكتروني

ذكر (الرياحي، 2024 : 384-385) أن هناك أربعة أنواع من الابتزاز الإلكتروني وهي:

1) الابتزاز الجنسي: يحدث عندما يتمكن الجاني من الحصول على صور أو مقاطع فيديو تحتوي على محتوى فاضح أو جنسي للمجني عليه. يقوم الجاني بعد ذلك بتهديد الضحية بنشر تلك المواد، مما يجعله تحت ضغط شديد للامتثال لرغباته. هذا الابتزاز غالبًا ما يتضمن طلبات لأفعال غير أخلاقية أو أنشطة جنسية، وهو يمثل اعتداءً نفسيًا وجسديًا خطيرًا على الضحية.

2) الابتزاز المادي: يركز الجاني في هذا النوع على شخصيات بارزة في المجتمع، حيث يقوم بجمع معلومات حساسة عنهم من خلال الإنترنت. يستغل الجاني هذه المعلومات لتهديد الضحية، طالبًا منه المال أو غيره من الفوائد المادية مقابل عدم نشر تلك المعلومات أو استخدامها بطريقة تضر بسمعته.
3) الابتزاز الاجتماعي: يتعلق هذا النوع باستغلال الجاني لخوف الضحية على سمعته في المجتمع، لا سيما إذا كانت الضحية امرأة. يحصل الجاني على صور أو معلومات حساسة ويتعهد بالاحتفاظ بها سراً ما لم يستجب الضحية لمطالبه. يمكن أن تشمل هذه المطالب الحصول على أموال أو الانخراط في أفعال غير أخلاقية.
4) الابتزاز الديني: يستغل الجاني الدين كوسيلة للسيطرة على الضحية، حيث يزرع في ذهنه شعورًا بالذنب ويهدده بالعقاب من الله إذا لم يستجب لمطالبه. يتسبب ذلك في شعور الضحية بالعجز والخوف، مما يجعله أكثر عرضة للاستجابة للابتزاز. قد يطلب الجاني أفعالًا تتعلق بالمال أو النشاطات الأخرى، مستغلًا الضعف النفسي للضحية.

رابعًا/ وسائل وطرق استعمال الابتزاز الإلكتروني

لخص الباحثين في مجال الإعلام وعلم الاجتماع وسائل الابتزاز الإلكتروني منها (صالح، 2018: 100):

1) الهواتف الذكية: تعد الهواتف الذكية وسيلة رئيسية للابتزاز، حيث يمكن للمبتزين إرسال رسائل تهديد عبر تطبيقات المراسلة. بالإضافة إلى ذلك، يمكنهم تسجيل مكالمات أو التقاط صور من كاميرا الهاتف دون علم الضحية، مما يزيد من ضغط الابتزاز.
2) البريد الإلكتروني: يستخدم المبتزون البريد الإلكتروني لإرسال رسائل تهديد أو طلبات فدية. قد يتضمن البريد الإلكتروني روابط ضارة أو مرفقات تحتوي على برامج خبيثة تهدف إلى جمع بيانات المستخدم.
3) إنشاء مواقع على شبكة الأنترنت: يمكن للمبتزين إنشاء مواقع وهمية لنشر المعلومات الحساسة أو الصور الخاصة بالضحايا. هذه المواقع قد تكون مصممة لتبدو قانونية لجذب المزيد من الزوار، مما يتيح لهم الضغط على الضحايا.
4) إنشاء غرفة محادثة أو دردشة: تُستخدم غرف الدردشة كوسيلة لجذب الضحايا وتكوين علاقات معهم، حيث يتم استدراجهم لمشاركة معلومات شخصية. بعد ذلك، يُستخدم ما تم جمعه في عملية الابتزاز.
5) تركيب أو حذف صور خالفة للواقع ونشرها باسم آخر يراد به ابتزازه: تعد هذه الطريقة من أسوأ وسائل الابتزاز، حيث يقوم المبتز بتعديل صور الضحية أو إنشاء صور وهمية ثم نشرها عبر الإنترنت. هذه الصور تُستخدم لتشويه سمعة الضحية أو للإضرار بمكانتها الاجتماعية.
6) أما طرق استعمل جريمة الابتزاز الإلكتروني فقد ذكرها (طه، 2022) بالتالي:
7) التهديد: يعد التهديد أحد أهم صور الابتزاز الإلكتروني الذي يعرف بأنه كل فعل أو سلوك من شأنه أن يبعث الخوف في نفس المجني عليه، بهدف الأضرار به، أو بأي شخص أخر يهمه أمره، مما يحمل المجني عليه إلى أن ينفذ ما يريده الجاني.
8) التشهير: يعد التشهير أحد أهم الصور المتعلقة والمستخدمة للابتزاز الإلكتروني، ويعرف بأنه الإعلان عن أسرار أو أخطاء إنسان، ونشرها بين الناس، فالابتزاز فيه تشهير للمجني عليه شخصًا طبيعيًا أو معنويًا من خلال نشر المعلومات على الشبكة الأنترنت.
9) الإكراه: يتمثل الإكرار بوصفه أحد صور جريمة الابتزاز الإلكتروني في أين يهدد المكره قادر على الإكراه بعاجل من أنواع العقاب، يؤثر العاقل لأجله الإقدام على ما أكره عليه، وغلبت على ظنه أنه يفعل ما هدد به، إذ امتنع مما أكرهه عليه (طه، 2022 : 573-574).
10) خامسًا/ أسباب الابتزاز الإلكتروني

11) لخص الباحثين في علم الاجتماع والجريمة أسباب الابتزاز الإلكتروني في النقاط الآتية:

12) أسباب اجتماعية: وتتمثل في الآتي:

أ) التنشئة الأسرية الخاطئة: تلعب الأسرة دورًا حاسمًا في تشكيل شخصية الفرد. إذا كانت التنشئة غير صحيحة، مثل غياب الدعم العاطفي أو التعزيز الإيجابي، قد ينشأ الفرد مع قيم ضعيفة، مما يجعله عرضة للسلوكيات المنحرفة مثل الابتزاز. فالأطفال الذين ينشؤون في بيئات غير صحية قد يفتقرون إلى القدرة على تقييم العواقب السلبية لأفعالهم.

ب) جماعة رفقاء السوء: تؤثر جماعات الأقران بشكل كبير على سلوك الأفراد. الانخراط مع أصدقاء يشجعون على السلوكيات السلبية مثل الابتزاز يمكن أن يؤدي إلى ضغط اجتماعي قوي يدفع الفرد لتبني تلك السلوكيات. هذه الديناميكية قد تجعل من الصعب على الأفراد اتخاذ خيارات صحيحة أو الابتعاد عن الأفعال غير الأخلاقية.

1) أسباب نفسية: وتتمثل في

أ) ضعف الوازع الديني والأخلاقي: يعزز الوازع الديني من الإحساس بالمسؤولية والأخلاق. عندما يكون ضعيفًا، قد ينعدم الوعي بعواقب السلوكيات الضارة. الأفراد الذين يفتقرون إلى التوجيه الروحي قد يجدون في الابتزاز وسيلة لتحقيق أهدافهم دون اعتبار للأخلاق أو التأثيرات على الآخرين، كما أن غياب الدافع الأخلاقي الذي من أبرز مظاهره هو ما يجري في عالم الإنترنت وما يحدث في مواقع التواصل الاجتماعي من عمليات خدع وسرقة واحتيال فلا حدود للعلاقات والتواصل، وهذا ما أكدته وزارة الداخلية العراقية عن وجود 14 حالة لجريمة الابتزاز الإلكتروني خلال عام 2023 (عمر، 210 : 41).

ب) الفراغ العاطفي: الأفراد الذين يعانون من فراغ عاطفي أو نقص في العلاقات الإنسانية قد يسعون لتعويض هذا الشعور بطرق غير صحية، مثل الابتزاز. يمكن أن تكون هذه السلوكيات وسيلة للحصول على القوة أو السيطرة أو حتى مجرد جذب الانتباه، مما يؤدي إلى انخراطهم في ممارسات سلبية تؤثر على الآخرين (أبو عليان، 2013 : 122).

2) أسباب تقنية (التكنولوجيا الحديثة):

توفر التكنولوجيا الحديثة سهولة في الاتصال، لكن هذا يجعل الأفراد أيضًا عرضة للاستغلال. نقص الوعي بكيفية حماية المعلومات الشخصية يعرض الأفراد لخطر الابتزاز. كما أن سهولة الوصول إلى الآخرين عبر الإنترنت تعزز فرص الاعتداء، حيث يمكن للمرء استخدام وسائل التواصل الاجتماعي أو الرسائل النصية في تهديد الضحايا (لطيف، 2024 : 572). كما يمثل الإعلام عنصرًا معقدًا في انتشار الابتزاز الإلكتروني، حيث يؤثر على البيئة الرقمية التي يعيش فيها الأفراد بطرق متعددة. توفر وسائل الإعلام الحديثة، وخصوصًا منصات التواصل الاجتماعي، فرصًا للأشخاص لمشاركة معلوماتهم الشخصية، مما يعرضهم لمخاطر الاستغلال من قبل المبتزين الذين يمكنهم بسهولة جمع البيانات عن ضحاياهم المحتملين. وتسلط وسائل الإعلام الضوء على حالات الابتزاز بشكل مكثف، مما يسهم في زيادة الوعي حول هذه الظاهرة. لكن في بعض الأحيان، يمكن أن تؤدي هذه التغطيات إلى تحفيز الفضول أو تقليد السلوكيات الإجرامية، حيث تُقدم أعمال الابتزاز كنوع من القوة، مما قد يشجع البعض على الانغماس فيها. حيث تُسهل التقنيات الحديثة أيضًا طرق تواصل المبتزين مع ضحاياهم عبر الرسائل النصية أو تطبيقات الدردشة، مما يجعل الابتزاز يحدث بشكل سري وسريع، ويزيد من تفشي المشكلة. ويعزز نقص الوعي بالأمان الرقمي من فرص نجاح المبتزين، حيث يفتقر الضحايا إلى المعرفة الضرورية لحماية أنفسهم. لا يمكن تجاهل الأثر النفسي للإعلام، حيث قد يؤدي المحتوى السلبي إلى شعور بالخوف والقلق لدى المستخدمين، مما يدفعهم إلى الاستهتار بممارساتهم الرقمية أو فقدان الحذر (الغديان وآخرون، 2018، 179-180).

3) أسباب اقتصادية:

فالجوانب الاقتصادي تؤدي دورًا على سلوكيات الناس أما سلبًا أو إيجابًا، حيث نجد أن الجوانب الاقتصادية لها دور على كل من المبتز والضحية كما يظهر تأثيره من الجانبين جانب الفقرة والحاجة والغني والترف، حيث ترتبط معدلات الابتزاز الإلكتروني ارتباطًا وثيقًا بالفقر والبطالة. فكلما كانت الظروف الاقتصادية صعبة، زادت الضغوط على الأفراد للبحث عن وسائل غير مشروعة لتأمين احتياجاتهم، لذلك تعد الظروف الاقتصادية الصعبة من العوامل الرئيسية التي تدفع الأفراد إلى اتخاذ قرارات غير محسوبة. عندما يواجه الأفراد صعوبات مالية، قد يبحثون عن وسائل لكسب المال بطرق غير قانونية، مثل الابتزاز. الإحباط الناتج عن الفقر والبطالة يمكن أن يزيد من قابلية الأفراد للانخراط في سلوكيات ضارة. وتشير إحصائيات وزارة العمل أن معدلات الفقرة ارتفعت في العراق، حيث تزايد نسبة الفقر في عام 2018 بلغت النسب أكثر من 20% بمعدل 7370 مليون نسمة تحت خط الفقرة، وقد تزايدت هذه النسبة في العام الذي يليه لتبلغ أكثر من 31% إذ أصبح عدد الفقرات 12680 مليون نسمة، ووفقًا لمصادر في وزارة التخطيط ونتيجة الأزمة الاقتصادية والصحية والسياسية الناتجة عن أزمة كورونا العالمية والتي أثرت على المستوى المعيشي للفرد العراقي لتصل النسبة من 26,7 % في عام 2020 إلى 29,7 عام 2021 ومن المتوقع أن يزداد نسبة الفقر لتصل إلى أكثر من 31 في السنوات اللاحقة (حافز، 2023 : 94)، وهذا الحال ينطبق على البطالة وما تسببه من مشاكل للأفراد ودفعهم إلى الابتزاز فالجاني يبتز الضحية رغبة في حصوله على المال، في حين نجد أن الضحية بسبب حاجتها للمال تخضع للابتزاز كأن يبتز المدير أخلاقيًا الموظفة التي تعمل لديه بسبب حاجتها إلى العمل،، كما تلعب البطالة أيضًا دورًا مؤثرًا في جذب الشباب نحو هذه السلوكيات بالإضافة إلى عدم وجود الرقابة الذاتية عليهم (أبو زيد، 2022 : 14-15).

4) أسباب سياسية:

تتعدد الأسباب السياسية التي تسهم في تفشي جريمة الابتزاز الإلكتروني، حيث تلعب البيئة السياسية دورًا محوريًا في تعزيز أو تقليص هذه الظاهرة، يمكن أن تؤدي الأوضاع السياسية المضطربة، مثل الحروب والأزمات الاقتصادية، إلى زيادة نسبة الابتزاز الإلكتروني. فخلال هذه الفترات، يواجه الأفراد ضغوطًا نفسية وفوضى، مما يجعلهم فريسة سهلة للمبتزين الذين يستغلون نقاط ضعفهم. من ناحية أخرى، يشكل ضعف التشريعات المتعلقة بالأمن السيبراني عاملًا رئيسيًا في تفشي هذه الجريمة. في الدول التي تفتقر إلى قوانين صارمة أو آليات فعالة لمواجهة الجرائم الإلكترونية، يشعر المبتزون بالجرأة، حيث يعتقدون أنهم بعيدون عن العقاب. علاوة على ذلك، تلعب السياسات الحكومية دورًا مهمًا في تعزيز الوعي المجتمعي حول الأمان الإلكتروني. عندما تكون الحكومات غير ملتزمة بتوعية الناس أو بتوفير الدعم الكافي، تنشأ بيئة مواتية لانتشار جريمة الابتزاز. أيضًا، تسهم التكنولوجيا الحديثة في تمكين المبتزين من استخدام أدوات وتقنيات متقدمة. في سياق سياسي يفتقر إلى الاستثمار في التعليم والتكنولوجيا، يمكن أن يتفاقم الوضع ويؤدي إلى زيادة هذه الجريمة (شعيب، 2023: 46).

سادسًا/ آثار الابتزاز الإلكتروني

1) آثار نفسية:

يترك الابتزاز الإلكتروني آثارًا نفسية عميقة على المجني عليهم، تتجلى في مشاعر الخوف والقلق والتوتر، وهي ردود فعل طبيعية للشعور بالخطر حيث تجعل الضحية شخصية غريبة الأطوار وغير سوية وتصاب بالأمراض

النفسية المستعصية كالاكتئاب والانهيار العصبي، والتوتر والشعور الدائم بالذنب والأرق والسهر، وصعوبات النوم، وتكرار الكوابيس الليلية، كما يمكن أن يؤدي الضغط النفسي إلى محاولات انتحار من قبل المبتزين بسبب الخوف من العار، خاصة بين المراهقين والنساء. بالإضافة إلى ذلك، يعاني الأفراد من ضعف الثقة بالنفس، مما يؤثر سلبًا على قدراتهم ووجهة نظرهم تجاه الحياة (عبد الحميد، 2008 : 39). كما وتشمل الآثار النفسية أيضًا الإهمال العاطفي، حيث يشعر الفرد بحرمان من الحب والحنان، مما يزيد من شعوره بالنقص وعدم التقدير. هذه المعاملة قد تؤدي إلى مشكلات مثل التأخر الدراسي أو الهروب من المدرسة. كما قد يعاني الأطفال من العنف النفسي عند شعورهم بتفضيل أحد الوالدين لأخواتهم، مما يؤدي إلى إحباط ومرارة، وتزايد مشاعر العداء تجاه الآخرين (قنبر، 2008 : 24-25).

2) الآثار الاجتماعية: تتنوع الآثار الاجتماعية التي تحققها جرائم الابتزاز وهي على عدم تراتب وأنواع منها

أ) آثار على مستوى الفرد: إن تعرض الأفراد للابتزاز الإلكترونية يترتب عليه آثار خطيرة وسلبية منها الاضطرابات النفسية والصدمات التي تعاني منها الضحية بعد تعرضها للابتزاز، فغالبًا ما تعاني من الاكتئاب والانهيار العصبي والقلق والتوتر، وأحيانًا تلجأ إلى العزلة الاجتماعية وانقطاعها عن التواصل مع الآخرين والخوف من مواجهتهم وغيرها من الاضطرابات التي يعاني منها الضحية، كما وتصبح الضحية رهينة بيد المبتز، وذلك لأنها لا تملك القدرة على اتخاذ قراراتها ولا تتحكم بسلوكياتها بل تنفذ قرارات المبتز وأوامره، كما يترك الابتزاز آثارًا كبيرة وأضرارًا عميقة في نفسية وشخصية المرأة فقد يستدعي ذلك لجؤها إلى العلاج النفسي من اجل التخلص من خوفها ومواجهة مشاكلها، كما يستهدف الابتزاز تشويه سمعة الفرد، ولا سيما أن كانت الضحية امرأة فيولد لها الكثير من المشكال بعد اكتشاف أمرها ومعرفة المجتمع به، وبما أن المجتمع العراقي بكونه مجتمع شرقي نجده يتهم بسمعة المرأة وأن كانت ضحية ابتزاز، فتقل فرص الزواج أمامها وغيرها من المشكلات المجتمعية التي يمكن أن تواجهها، كما يترك الابتزاز أثارًا عميقة على الضحية بأن يكون دافعًا للقتل، إذ تلجأ بعض الأسر إلى التخلص من أبنتهم حفاظًا على سمعتهم بعد أن اتخذ الابتزاز منح أخلاقيًا وفي حالات أخرى تلجأ الضحية للانتحار نتيجة الضغط النفسي الهائل الذي تعاني منه ولاسيما أن معظم الضحايا من المراهقين وغيرها من الآثار المترتبة للابتزاز الإلكتروني كالضرر المادي للضحية الذي يخسر جزء كبير من أموالهِ بغية التخلص من تهديد المبتز (لطيف، 2024 : 576).

ب) آثار على مستوى المجتمع: تتمثل الآثار الاجتماعية نتاج مجموعة من المواقف والتفاعلات مع بعض الأفراد من مستخدمين وسائل التواصل الاجتماعي، والذي يتعدى تأثيرها الفرد ليشمل الأسرة، والمجتمع ككل، مما قد يترتب على ذلك خلل في العلاقات بين الفرد وأسرته وتمزق للنسيج والبناء الاجتماعي وتعاظم أثرها لسنوات لاحقة بسبب انتشار الخلافات والمنازعات وفقدان الثقة مما يعمل على تدمير كيان المجتمع وهشاشته، وفي سياق أوسع، يؤدي انتشار الابتزاز الإلكتروني إلى زعزعة الاستقرار الاجتماعي. فقد تشعر المجتمعات بالخوف من الإفصاح عن المعلومات، مما قد يعيق التواصل الفعال ويعطل التطورات الاجتماعية والاقتصادية. وفي النهاية، تُعتبر هذه الجريمة تهديدًا حقيقيًا للقيم والمبادئ التي تُحافظ على تماسك المجتمع، مما يستدعي الحاجة الملحة لمواجهة هذه الظاهرة والتوعية بمخاطرها (الرويس، 2020 : 107-108). كما يترتب أيضًا على هذه الجريمة آثارًا وخيمة على منظومة الدين والقيم، حيث إن جريمة الابتزاز الإلكتروني تؤثر بشكل عميق على القيم والمبادئ الأخلاقية والدينية في المجتمع. من الناحية القيمية، يمكن أن تزعزع هذه الجرائم أسس الثقة والأمان بين الأفراد. فالابتزاز يتنافى مع القيم الإنسانية الأساسية التي تشجع على الاحترام والتعاون، مما يؤدي إلى خلق مناخ من الخوف والقلق، وعندما يُبتز الأفراد، يشعرون بالعجز وفقدان السيطرة، مما قد يدفعهم إلى اتخاذ قرارات

غير أخلاقية أو اللجوء إلى سلوكيات غير قانونية لمحاولة استعادة شعورهم بالتحكم. وهذا يُظهر كيف يمكن أن تتعرض الأخلاق العامة للتآكل نتيجة لضغوط الابتزاز (الزيدي، 2019 : 76). أما من المنظور الديني، فإن الابتزاز يُعتبر جريمة تُناقض تعاليم معظم الأديان التي تحث على الصدق والرحمة والتعاون. تؤدي هذه الأفعال إلى شعور بالذنب والعار لدى الضحايا، مما يؤثر سلبًا على علاقتهم بالذات وبالإله، ويزيد من مشاعر القلق والاكتئاب، وبما أن المجتمع العراقي يستمد قيمة من الدين الإسلامية وبما أن الابتزاز هو جريمة محرمة شرعًا تصبح هذه الجريمة سببًا في انهيار القيم الأخلاقية والتسامح واحترام حقوق الآخرين، الأمر الذي يؤدي إلى إنتاج قيم اجتماعية سلبية ومضادة لها هو متعارف عليه مجتمعيًا كالحقد والخيانة وانهاك الحرمات (البهادلي، وآخرون، 2013 : 103).

3) الآثار الأمنية: إن للابتزاز الإلكترونية تُعَدّ جريمة الابتزاز الإلكتروني من التحديات الأمنية الخطيرة التي تؤثر سلبًا على استقرار المجتمع. فقد سهلت وسائل التواصل الاجتماعي على مرتكبي هذه الجرائم اكتساب مهارات احترافية في تنفيذها، مما أدى إلى ظهور عصابات إجرامية عابرة للحدود يصعب تتبعها وكشفها. بعض هذه العصابات يساهم في دعم الإرهاب والتطرف، كما يتضح من استخدام تنظيم القاعدة وعناصر داعش للمنصات الاجتماعية لنشر أفكارهم وجذب مجندين جدد، وتتجاوز آثار الابتزاز الإلكتروني البعد الفردي لتطال النسيج الاجتماعي برمته، مما يؤدي إلى تدهور الأمن والخصوصية. حينما يشعر الأفراد بعدم الأمان على حياتهم وأسرهم، ينعكس ذلك سلبًا على ثقة المجتمع في نفسه، ويتحول إلى بيئة تفتقر إلى القيم الأخلاقية الأساسية. هذا التدهور في القيم يعزز من انتشار السلوكيات السلبية ويجعل المجتمع عرضة لزعزعة الاستقرار، مما يتطلب استجابة جماعية لمكافحة هذه الظاهرة الخطيرة (الخالدي، 2020: 2065).

المبحث الثالث/ الحلول المقترحة لمعالجة ظاهرة جريمة الابتزاز الإلكتروني

تعد جريمة الابتزاز الإلكتروني من الجرائم الخطيرة التي تتطلب جهودًا مشتركة من الأفراد والمجتمع والحكومات للحد منها والقضاء عليها، نذكر منها

الجانب الوقائي الداخلي: ويتمثل فيما يلي (زيوش، 2017 : 84-85):

يجب على الأشخاص الذين يستخدمون شبكة الأنترنت في الأماكن العامة والأماكن الخاصة أن يكونوا على قدر كافٍ من الحيطة والحذر، كأن يحذروا عندما يكتبون اسم المستخدم وكلمة السر لموقع ما وبحيث يطالبهم الموقع المعني بحفظ كلمة المرور فبمجرد كبسة زر واحدة على زر موافق يكون الموقع قد احتفظ بكلمة السر حتى ولو تم مسح بيانات المتصفح في نهاية العمل، لذا يجب أن يكون حفظ كلمات السر للمواقع المسجل فيها في الأجهزة الشخصية الموجودة في البيت فقط.

قبل شراء جهاز الكمبيوتر وجب على أفراد الأسرة أن يكونوا على اطلاع تام وواسع بمجال شبكة الأنترنت ومخاطرها وسلبياتها وبفوائدها وإيجابياتها، وأن يكون جهاز الكمبيوتر المتصل بشبكة الأنترنت الموجود بالبيت تحت رقابة الأسرة.

يجب أن يكون الجهاز أو الأجهزة المتصلة في البيت تحتوي على برامج لمكافحة الفيروسات، هذه البرامج يجب أن تكون خاضعة لنظام التحيين اليومي.

الجانب الخارجي: ويتمثل فيما يلي (زيوش، 2017 : 86):

يجب على الضحية التقرب من أقرب مصلحة أمنية (مقر شرطة، مفرزة للدرك الوطني) وتقديم شكوى مؤسسة على وقائع مبينة.

يجب على الضحية عدم التمادي مع المبتز كأن يحاول أن يستعطفه أو يحاول أن يلبي رغباته، نتيجة ما يملكه هذه المبتز من ملفات شخصية (قد تكون صوتية، أو صور، أو فيديو)

يجب على الضحية إخبار أفراد الأسرة بما وقع له من مشكل، حيث سيجد كل المساندة والدعم.

يجب عمل نسخة احتياطية عن كل البرامج والملفات التي يراها الفرد مهمة، وهذا حتى يسهل الوصول إليها فيما بعد، خاصة إذا عمل مسح تام للجهاز وللأقراص الصلبة التي تحتوي على المعلومات.

وفيما يلي توضيح شامل لمستويات العمل المختلفة اللازمة لمواجهة هذه الظاهرة:

على مستوى الفرد: وتتمثل في

يجب على الأفراد، وخاصة الشباب والأطفال، أن يكونوا على دراية بخطورة الابتزاز الإلكتروني. من الضروري تنظيم ورش عمل وحملات توعوية في المدارس والجامعات لشرح مخاطر هذه الجريمة وطرق الوقاية منها.

يتعين على الأفراد تجنب مشاركة المعلومات الحساسة على الإنترنت. يجب استخدام كلمات مرور قوية وفريدة لكل حساب، وتفعيل خيارات الأمان المتاحة مثل المصادقة الثنائية.

من الضروري أن يتعرف الأفراد على أهمية الإبلاغ عن أي حالة ابتزاز يتعرضون لها. ينبغي عليهم التوجه فورًا إلى الجهات المختصة، مع الحرص على حفظ جميع الأدلة مثل الرسائل والصور.

في حالة التعرض للابتزاز، ينبغي على الأفراد عدم الاستجابة لمطالب المبتز والحفاظ على هدوئهم. يمكن أن يؤدي الاستجابة إلى زيادة الضغوط والمطالب (أحمد، 2019 : 145).

على مستوى المجتمع:

يجب أن تُعطى الأسر أهمية كبيرة في توعية الأطفال والمراهقين حول مخاطر الأمن الإلكتروني. يمكن تنظيم ندوات في الأحياء أو المدارس لتثقيف الأسر.

يلعب الإعلام دورًا حيويًا في تسليط الضوء على جرائم الابتزاز الإلكتروني. ينبغي أن تقدم وسائل الإعلام نصائح وقائية وتعرض قصصًا تعليمية تعزز الوعي.

يجب أن تكون هناك مؤسسات مدنية تقدم الدعم النفسي والقانوني للضحايا. يمكن أن تساعد هذه المؤسسات في معالجة آثار الابتزاز وتقديم الاستشارات اللازمة.

تنظيم برامج توعية تستهدف جميع فئات المجتمع، خاصة الشباب والأطفال، مع التركيز على تعزيز المعرفة حول مخاطر الابتزاز الإلكتروني وسبل الوقاية.

يمكن استغلال منصات التواصل الاجتماعي لنشر رسائل توعوية وتفاعل مباشر مع الجمهور، مما يعزز من فعالية الحملة التوعوية (الدين، 1973 : 94).

على مستوى الحكومة:

يتعين على الحكومات سن قوانين صارمة تعاقب مرتكبي جرائم الابتزاز الإلكتروني. يجب أن تكون العقوبات رادعة وأن تشمل كافة أشكال الابتزاز.

من المهم تدريب الأجهزة الأمنية على كيفية التعامل مع جرائم الإنترنت. ينبغي تزويدهم بالتقنيات اللازمة للكشف عن الجناة وجمع الأدلة.

يجب أن يكون هناك تعاون بين الدول لمكافحة الجرائم الإلكترونية عبر الحدود. يمكن إنشاء تحالفات دولية لتبادل المعلومات والخبرات في هذا المجال.

يتطلب الأمر تطوير وتأمين البنية التحتية الرقمية ضد الهجمات الإلكترونية. ينبغي العمل على تحسين أمان الشبكات والمعلومات لحماية الأفراد والمؤسسات (العتيبي، 2010 : 52).

على مستوى التقنية

يجب أن تُستخدم برامج حماية فعالة لحماية الأجهزة من الفيروسات والبرامج الضارة. ينبغي تشجيع الأفراد على تحديث برامج الحماية بشكل دوري.

من الضروري استخدام تقنيات التشفير لحماية البيانات الشخصية والمعلومات الحساسة من الوصول غير المصرح به.

يجب تطبيق إجراءات تحقق صارمة من هوية المستخدمين على منصات التواصل الاجتماعي والمواقع الإلكترونية. هذا يساعد في تقليل فرص الانتحال والابتزاز.

يتعين على الحكومات والشركات الاستثمار في الأمن السيبراني لحماية البنية التحتية الرقمية. يمكن أن يشمل ذلك إنشاء فرق متخصصة لمراقبة التهديدات.

ينبغي أن تتم تغطية جرائم الابتزاز الإلكتروني بطريقة مسؤولة، تركز على توعية الجمهور دون نشر تفاصيل قد تضر بالضحايا (المويشر، 2013 : 145).

المبحث الرابع/ الاستنتاجات والتوصيات

أولًا/ الاستنتاجات

تعد جريمة الابتزاز الإلكتروني إحدى أبرز صور الجرائم الإلكترونية، حيث تُمارس هذه الجريمة عبر شبكة الإنترنت واستخدام الأجهزة الحديثة والتطبيقات المتنوعة، مثل وسائل التواصل الاجتماعي. لقد أصبحت هذه الظاهرة تمثل تهديدًا كبيرًا للأفراد والمجتمعات على حد سواء.

يتميز الابتزاز الإلكتروني بكونه يتضمن سلوكًا ماديًا يترافق مع تأثيرات نفسية عميقة على الضحايا.

إن أساليب ارتكاب هذه الجريمة تتفاوت بشكل ملحوظ عن أساليب الابتزاز التقليدي، حيث يُستخدم الهاتف المحمول المزود بكاميرا للاعتداء على خصوصية الأفراد، سواء من خلال التقاط الصور أو نشر معلومات

حساسة أو تسجيلات صوتية ومرئية. تعكس هذه الوسائل خطورة الابتزاز الإلكتروني، إذ تتجاوز الحدود التقليدية، مما يستدعي اهتمامًا أكبر من الأفراد والمجتمعات لمواجهة هذا التحدي.

إن التطور التكنولوجي قد ساهم في زيادة وتيرة هذه الجرائم. فسهولة الوصول إلى المعلومات ووسائل الاتصال تجعل من السهل على الجناة تنفيذ مخططاتهم بسرعة وفعالية، مما يتطلب جهودًا أكبر لمكافحة هذه الظاهرة.

يُمكن أن تؤدي هذه الجرائم إلى تدمير سمعة الضحايا بشكل كبير، حيث يمكن أن تُستخدم المعلومات المُبتزة ضدهم في حياتهم المهنية والشخصية، مما يسبب آثارًا نفسية واجتماعية طويلة الأمد.

ثانيًا/ التوصيات

تحديث النصوص القانونية الإجرائية لتتناسب مع تحديات جريمة الابتزاز الإلكتروني، التي تتطور بشكل مستمر. يجب أن تشمل هذه النصوص آليات جديدة لضبط وتحقيق الجرائم في الفضاء الافتراضي، مع الأخذ في الاعتبار التعقيدات التقنية التي قد تعترض عمليات التحقيق.

على وزاره الداخلية والجهات ذوات الصلة على رفع الوعي العام حول مخاطر الابتزاز الإلكتروني، وتعليم الأفراد كيفية حماية أنفسهم. يتطلب ذلك إطلاق حملات توعية تشمل ورش عمل، ندوات، وموارد إلكترونية تهدف إلى توضيح أساليب الحماية والتصرف السليم عند التعرض لهذه الجرائم.

من الضروري توفير المعلومات اللازمة للأفراد حول سبل الحماية والتصرف في حال التعرض للابتزاز.

ينبغي تطوير برامج تثقيفية رقمية تشمل معلومات حول الخصوصية، الأمن الرقمي، وأهمية الحفاظ على البيانات الشخصية، مما يساهم في بناء مجتمع أكثر أمانًا.

يجب على الحكومات والجهات التشريعية العمل على تقوية القوانين المتعلقة بالجرائم الإلكترونية، بما في ذلك الابتزاز.

يجب أن تكون هناك عقوبات رادعة للجناة، وتحسين آليات الإبلاغ عن هذه الجرائم لتسهيل الوصول إلى العدالة وتوفير الدعم النفسي والقانوني للضحايا.

نشر الوعي داخل المجتمع حول أخطار الابتزاز الإلكتروني. يجب أن تشمل هذه المبادرات الإجراءات الاحترازية، مثل عدم مشاركة المعلومات الحساسة على الإنترنت والتأكد من الإبلاغ عن أي محاولة ابتزاز فور حدوثها.

يجب على الأفراد الاتصال فورًا بالجهات المتخصصة التي تمتلك الخبرة في التعامل مع قضايا الابتزاز. من الضروري عدم حذف أي محتوى مرتبط بالابتزاز، حيث يعد هذا دليلاً قد يكون حيويًا لملاحقة الجاني.

يجب تشجيع الضحايا على عدم الشعور بالعزلة والبحث عن الدعم المادي والمعنوي من أشخاص موثوقين، سواء كانوا أصدقاء، عائلة، أو متخصصين نفسيين. يمكن أن يساعد الدعم في تجاوز الصدمة النفسية المترتبة على هذه التجربة.

من الضروري تدريب وتأهيل العاملين في جهات التحقيق والجهات القضائية على استخدام أساليب التحقيق الحديثة وفهم الدليل الرقمي. يمكن أن يسهم هذا التدريب في ضمان تحقيق العدالة وعدم إفلات الجناة من العقاب بسبب قلة الخبرة.

يجب تعزيز التعاون الدولي بين الدول لتبادل المعلومات والتقنيات اللازمة لمكافحة ظاهرة الابتزاز الإلكتروني بفاعلية. فالتعاون المشترك يمكن أن يسهم في تطوير استراتيجيات موحدة لمواجهة هذه الجرائم التي تتخطى الحدود الجغرافية.

قائمة المصادر والمراجع

أولًا/ الكتب العربية والمترجمة

صالح، تامر محمد (2018): الابتزاز الإلكتروني (دراسة تحليلية مقارنة)، مطبعة الإسكندرية، مصر.

المويشر، تركي (2013): بناء نموذج أمني لمكافحة الجرائم المعلوماتية لقياس فاعليتها، جامعة نايف العربية للعلوم الأمنية، الرياض.

شحاتة، حسن، و النجار، زينب (2003) : معجم المصطلحات التربوية والنفسية (عربي – إنكليزي)، القاهرة، مصر، الدار المصرية اللبنانية.

أحمد، خالد حسن (2019): جرائم الأنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني دراسة مقارنة، دار الفكر الجامعي، الإسكندرية.

الجريش، سلمان (2003): الفساد الإداري وجرائم وإساءة استعمال السلطة الوظيفية، مكتبة العبيكان للنشر والتوزيع، الرياض.

العتيبي، سليمان (2010) : دور أجهزة البحث الجنائي في الكشف عن الجرائم المعلوماتية دراسة تطبيقية على شرطة منطقة مكة المكرمة، جامعة نايف العربية للعلوم الأمنية، الرياض.

كرم، عبد الواحد (1987) : معجم المصطلحات القانونية، مكتبة النهضة العربية، القاهرة.

الدين، علي صباح (1973) : الخدمة الاجتماعية، مؤسسة المطبوعات الحديثة، القاهرة.

الصباح، علي عبد الله شديد وآخرون (2010) : الابتزاز المفهوم والأسباب والعلاج، مركز باحثات لدراسة المرأة، الرياض.

الزيدي، كاظم عبد جاسم (2019): جريمة الابتزاز الإلكتروني (دراسة مقارنة)، مكتبة القانون المقارن، بغداد، العراق.

أبو عليان، محمد بسام (2013) : الانحراف الاجتماعي والجريمة، دار البشر للنشر والتوزيع، عمان، الأردن.

عمر، معن خليل (2010): التنشئة الاجتماعية، دار الشروق، عمان.

عبد الحميد، نبيه نسرين (2008): الإجرام الجنسي، دار الجامعة الجديدة، الإسكندرية، مصر.

المطلق، نورة بنت عبد الله بن محمد (2021): ابتزاز الفتيات أحكامه وعقوبته في الفقه الإسلامي، جامعة الإمام محمد بن سعود الإسلامية، كلية الشريعة.

ثانيًا/ المجلات والدوريات

لطيف، أماني هاشم (2024): الابتزاز الإلكتروني وتداعياته على الواقع السياسي والاجتماعي العراقي، مجلة دراسات دولية، العدد (98)، العراق.

عمر، جيهان حسين ، ومحمد، سعيد محمد (2019): الابتزاز العاطفي لدى طلبة الجامعة، مجلة أبحاث كلية التربية الأساسية، المجلد (15)، العدد (3)، جامعة دهوك، كلية التربة الأساسية، العراق.

حافظ، حنان يونس (2023): واقع الفقر في العراق التحديات والمقترحات، المجلة العراقية للعلوم الاقتصادية، العدد (76)، العراق.

الرياحي، رفيف عبد الحافظ محمد تقي(2024): دور المرشد التربوي في مواجهة الابتزاز الإلكتروني في مدارس محافظة البصرة، المؤتمر العلمي السنوي الرابع والعشرون، مجلة كلية التربية الأساسية، العدد خاص، العراق.

زيوش، سعيد (2017): ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الاجتماعية، العدد (22)، جامعة الشلف، الجزائر.

الغديان، سليمان بن عبد الرزاق وآخرون (2018): صور جرائم الابتزاز الإلكتروني وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، دار المنظومة رواد في قواعد المعلومات العربية، مجلد (27)، العدد(69).

طه، صابرين ناجي (2022): السبل القانونية في مكافحة الابتزاز الإلكتروني، مجلة كلية التراث الجامعة، المجلد (1) العدد (33)، قسم القانون، العراق.

البهادلي، عبد الرضا ناصر ، وآخرون (2021): آثار الابتزاز الإلكتروني كعقوبة بين الفقه الأمامي والقانون العراقي، مجلة أبحاث ميسان، المجلد (17)، العدد (43)، جامعة الأديان والمذاهب، إيران.

الخالدي، عبير نجم عبد الله (2020) : دور الوعي الاجتماعي في مواجهة الابتزاز الإلكتروني للمرأة، مجلة كلية التربية، المجلد (4)، العدد (38)، جامعة صلاح الدين، كلية التربية، العراق.

الرويس، فيصل بن عبد الله (2020): الوعي الاجتماعي بظاهرة الابتزاز الإلكتروني لدى الأسرة في المجتمع السعودي دراسة ميدانية للعوامل والآثار، مجلة كلية الآداب والعلوم الإنسانية، الجزء (2)، العدد(33)، جامعة شقراء، المملكة العربية السعودية.

أبو زيد، محمد صابر (2022): إسهامات الخدمة الاجتماعية في الحد من مخاطر الابتزاز الإلكتروني للشباب وتصور مقترح من منظور الأزمن في طريقة خدمة الفرد، مجلة القاهرة للخدمة الاجتماعية، المجلد (1)، العدد (36)، مصر.

العبادي، هديل سعد أحد (2020): جريمة الابتزاز الإلكتروني للنساء دراسة مقارنة، مجلة جامعة الأنبار للعلوم القانونية والسياسية، المجلد (10)، العدد (2)، جامعة النهرين، كلية العلوم السياسية، العراق.

ثالثًا/ الرسائل والأطاريح

الحسن، بوشعير (2023): حداد شعيب: جريمة الابتزاز الإلكتروني دراسة مقارنة، رسالة ماجستير (منشورة)، جامعة محمد البشير الإبراهيمي برج بوعريريج، كلية الحلول والعلوم السياسية، الجزائر.

قنبر، فراس يوسف قنبر(2008): العنف ضد الأطفال الإناث "دراسة ميدانية في مدينة بغداد"، رسالة ماجستير " غير منشورة"، جامعة بغداد، كلية الآداب، قسم علم الاجتماع.

رابعًا/ مصادر الإنترنيت

ديجيتال، روداو (20024): 9384 حالة ابتزاز إلكتروني وعنف أسري وهروب بالعراق خلال 2023، مقال منشور بتاريخ 10/20/ 2024 رابط المقال https://www.rudawarabia.net .

نيوز، شفق (2024): كواليس الابتزاز الإلكتروني في العراق.. "هكر صالح" و"ابتزاز الأزواج" وتفاؤل أمني، مقال منشور بتاريخ 5/18/ 2024، رابط المقال : https://shafaq.com .