مجلـة البـاحث للـدراسات الأكاديمية
ISSN: 2352-975X ELBAHITH for Academic Studies EISSN: 2588-2368
المجلد: 12 / العدد: 02 / السنة: 2025 / ص ص: 356 - 381

الجريمة الإلكترونية وانعكاساتها على المنظومة الأخلاقية: الابتزاز الإلكتروني - أنموذجًا-

Cybercrime and Its Impact on the Ethical System: A Case Study of Cyber Extortion

تاريخ الإرسال:2025/03/02 تاريخ القبول:2025/06/01

سامية حمريش *Samia HAMRICHE*
جامعة باتنة1
University of Batna1
samia.hamriche@univ-batna.dz
صليحة رحالي* *Saliha RAHALI*
جامعة باتنة1
University of Batna1
saliha.rahali@univ-batna.dz

ملخص:

تناولت هذه الدراسة الجريمة الإلكترونية، وركزت على الابتزاز الإلكتروني كأحد أبرز أشكالها، وهدفت إلى تحليل ماهية الجريمة الإلكترونية، والابتزاز الإلكتروني، كما استعرضت موقف الشريعة الإسلامية من هذه الجرائم، وناقشت الدراسة الأبعاد الأخلاقية للابتزاز الإلكتروني، مع الإشارة إلى تأثيراته على المنظومة الأخلاقية. إضافة إلى ذلك، تم استعراض تداعياته الأمنية والنفسية والاجتماعية، وطرق مواجهته من خلال تعزيز التشريعات القانونية، التوعية المجتمعية، والتعاون الدولي.

الكلمات المفتاحية: الجريمة الإلكترونية؛ جريمة الابتزاز الإلكتروني؛ المنظومة الأخلاقية؛ الأمن السيبراني؛ الوعي الرقمي.

Abstract:

This study examined cybercrime, focusing on electronic blackmail as one of its main forms. It aimed to analyze the nature of cybercrime and electronic blackmail. The study also reviewed the stance of Islamic law on these crimes and discussed the ethical aspects of electronic blackmail, highlighting its impact on moral values. Additionally, it explored its security, psychological, and social consequences, as well as ways to combat it through stronger legal regulations, community awareness, and international cooperation.

Keywords: *Cybercrime; Cyber Extorsion; Ethical System; Cyber Security; Digital Awareness.*

* - المؤلف المُراسل.

مقدمـة:

في عصر الرقمنة والتقدم التكنولوجي السريع، يشهد العالم انتشارا متزايدا لظاهرة الجريمة الإلكترونية والتي أضحت واحدة من أهم التحديات التي تواجه المجتمعات، حيث تستخدم التكنولوجيا الحديثة في ارتكاب مختلف أنواع الجرائم، وتبرز جرائم الابتزاز الإلكتروني في مقدمة الجرائم الأخلاقية والذي قد يُعد إفرازا عصريا حديثا ولكنه في حقيقة الأمر سلوكا بشريا قديما يتمثل في عدم القدرة على التحكم بالرغبات الشاذة والشعور بالرغبة في السيطرة على الآخرين من خلال تهديدهم وإشعارهم بالخطر، فقد جاء في قوله تعالى على لسان امرأة العزيز: ﴿وَلَئِنْ لَمْ يَفْعَلْ مَا آمُرُهُ لَيُسْجَنَنَّ وَلَيَكُونَنْ مِنَ الصَّاغِرِينَ﴾ (سورة يوسف: الآية 32) فأجابها يوسف - عليه السلام -: ﴿قَالَ رَبِّ السِّجْنُ أَحَبُّ إِلَيَّ مِمَّا يَدْعُونَنِي إِلَيْهِ وَإِلَّا تَصْرِفْ عَنِّي كَيْدَهُنَّ أَصْبُ إِلَيْهِنَّ وَأَكُنْ مِنَ الْجَاهِلِينَ﴾(سورة يوسف: الآية 33)، حيث يشير القرآن في هذه الآية الكريمة إلى القوة النفسية التي يجب أن يتحلى بها الفرد ليكون أكثر قوة في مواجهة الاستغلال من الآخرين، ويؤكد - عليه السلام - على دور الجانب الروحي في دعم القوة النفسية والتي يمكن أن يصد بها الفرد اعتداء الآخرين. ويكتسي هذا الموضوع أهمية خاصة في الوقت الراهن، حيث تزايدت حوادث الابتزاز الإلكتروني بشكل غير مسبوق، مما يتطلب من الباحثين والممارسين تسليط الضوء على الحلول الممكنة لتقليل تداعيات هذه الظاهرة على المجتمع، وتتناول هذه الدراسة الجرائم الإلكترونية بشكل عام، مع التركيز على ظاهرة الابتزاز الإلكتروني باعتبارها نموذجًا حيويًا يعكس التأثيرات المدمرة على المنظومة القيمية والبنية الأخلاقية والسلوكية للأفراد والمجتمعات.

وانطلاقًا من هذه المعطيات، تطرح هذه الدراسة الإشكالية الرئيسية التالية:

EISSN: 2588-2368 ——— ISSN: 2352-975X

ما مدى فعالية الإطار القانوني الجزائري في التصدي لجريمة الابتزاز الإلكتروني ضمن منظومة مكافحة الجريمة الإلكترونية؟

ولتوضيح هذا التساؤل الرئيسي، تطرح هذه الدراسة مجموعة من الأسئلة الفرعية التي ستساعد في استكشاف مختلف جوانب هذه الظاهرة، وهي كالتالي:

- ما المقصود بالجريمة الإلكترونية وما هي أنواعها؟
- ما هي ماهية جرائم الابتزاز الإلكتروني وما هي أبرز أسبابها؟
- ما هو موقف الشريعة الإسلامية من جرائم الابتزاز الإلكتروني؟
- ما هي الأبعاد الأخلاقية المرتبطة بجرائم الابتزاز الإلكتروني؟
- ما هي تداعيات الابتزاز الإلكتروني النفسية، الاجتماعية، والأمنية؟
- ما هي الآليات الممكنة لمواجهة جرائم الابتزاز الإلكتروني والحد من انتشارها؟

- أهمية الدراسة:

- الأهمية العلمية: تساهم في إثراء الدراسات السوسيولوجية حول الجريمة الإلكترونية وعلاقتها بالقيم الأخلاقية، مما يوفر رؤية أعمق حول تأثير التكنولوجيا على السلوك الاجتماعي.

- الأهمية العملية: تساعد في فهم طبيعة الابتزاز الإلكتروني، آلياته، أبعاده الاجتماعية، ما قد يسهم في تطوير استراتيجيات وقائية أكثر فعالية.

- الأهمية التوعوية: تسلط الضوء على مخاطر الابتزاز الإلكتروني، وتقدم توجيهات تساعد الأفراد على حماية أنفسهم من الوقوع ضحايا لهذه الجريمة، وهي مسؤولية مشتركة بين مؤسسات المجتمع.

- الأهمية القانونية والأخلاقية: تبرز التحديات التي تواجه القوانين في التصدي لجرائم الابتزاز الإلكتروني، ومدى تأثيرها على القيم الأخلاقية في المجتمع.

ISSN: 2352-975X ——— EISSN: 2588-2368

- أهداف الدراسة:

1- تحديد مفهوم الجريمة الإلكترونية وبيان سماتها الرئيسية.

2- توضيح مفهوم الابتزاز الإلكتروني، أنواعه والأساليب المستخدمة في استهداف الضحايا

3-توضيح موقف الشريعة الإسلامية من جرائم الابتزاز الإلكتروني والأسس التي يقوم عليها.

4- تحليل الأبعاد الأخلاقية المرتبطة بجريمة الابتزاز الإلكتروني.

5- دراسة تأثير جرائم الابتزاز الإلكتروني على الجوانب الأمنية والنفسية والاجتماعية.

6- اقتراح آليات فعالة لمواجهة جرائم الابتزاز الإلكتروني والحد من تداعياتها.

- منهج الدراسة: سيتم الاعتماد على المنهج الوصفي التحليلي، كونه الأنسب للموضوع، بوصف الظاهرة المدروسة، أي الابتزاز الإلكتروني، من خلال تحليل خصائصها، أنواعها، ودوافعها وأساليبها، وتأثيراتها وانعكاساتها على المنظومة الأخلاقية، والأسلوب التحليلي: لتحليل العلاقة بين الابتزاز الإلكتروني والقيم الأخلاقية، من خلال مراجعة الأدبيات العلمية المتعلقة بالجريمة الإلكترونية، والقوانين ذات الصلة.

ولمعالجة الموضوع تم تقسيمه إلى المحاور التالية:

المحور الأول: مفهوم الجريمة الإلكترونية:

أولا- الجريمة الإلكترونية: المفهوم، الأشكال:

1- تعريف الجريمة الإلكترونية: عَّرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 الجريمة الإلكترونية بأنها: "أية جريمة

EISSN: 2588-2368 ——— ISSN: 2352-975X

يمكن ارتكابها بواسطة نظام حاسوب أو شبكة حاسوبية، والجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[1].

كما تُعرَّف بأنها: تلك الأفعال التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالإنترنيت، تهدف إلى الاختراق، التخريب، التزوير أو التحريف والقرصنة وكذلك سرقة الملكية الفكرية[2].

عَرَّفها مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[3].

ويرى *Tiedemann* بأنها: "تشمل كل شكل من أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[4].

وعليه، فإن الجريمة الإلكترونية تستند على ممارسات تتسم بعدم الأخلاقية، حيث يقوم مرتكبوها باستغلال مهاراتهم التقنية، دون اعتبار لتأثيراتها السلبية، باعتبارها انتهاكاً صارخاً للقوانين المصممة لحماية الأفراد والمؤسسات من الأضرار الرقمية، مما يفضي إلى تهديد الاستقرار الاجتماعي والاقتصادي على حد سواء.

من خلال عرض التعريفات السابقة الذكر، يمكن استخراج عدة عناصر محورية يتم التركيز عليها عند دراسة مفهوم الجريمة الإلكترونية:

أن جميع التعريفات تؤكد على أن الجريمة الإلكترونية تُرتكب باستخدام الحاسب أو الشبكات الإلكترونية. فقد أشار البعض إلى الإنترنت كوسيط أساسي لارتكاب الجريمة.

طبيعة الأفعال الإجرامية تتنوع بين الاختراق، التخريب، التزوير، التحريف، القرصنة، وسرقة الملكية الفكرية.

وأكدوا على أن المجال الذي تحدث فيه الجريمة هي البيئة الإلكترونية أو الرقمية، بما في ذلك الشبكات الحاسوبية، البيانات الرقمية، وأنظمة المعلومات.

ISSN: 2352-975X ——————————EISSN: 2588-2368

وأن الجريمة الإلكترونية قد تكون غير مشروعة قانونيًا (مخالفة القوانين) أو غير أخلاقية أو غير مصرح بها، وهو ما يوسع نطاق الجرائم ليشمل الأفعال التي قد لا تكون مجرّمة صراحة ولكنها مرفوضة أخلاقيًا أو تنتهك السياسات الرقمية.

وما يلاحظ أيضا أن بعض التعريفات مثل تعريف *Tiedemann* و**منظمة التعاون الاقتصادي والتنمية** تُركز على أي سلوك غير مشروع مرتبط بالحاسوب، مما يعطي الجريمة الإلكترونية نطاقًا واسعًا، أما تعريف الأمم المتحدة فقد كان أكثر تحديدًا، حيث يربط الجريمة الإلكترونية بالجرائم التقليدية لكن في البيئة الرقمية.

- **الفرق بين الجريمة الإلكترونية والجريمة المعلوماتية:** سبق وأن تم التعرف على مفهوم الجريمة الإلكترونية ولمعرفة الفرق بينها وبين الجريمة المعلوماتية وجب أولا التعرف على هذه الأخيرة، والتي عرفها البعض بأنها: "الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية، وأنها سوء استخدام الحاسب، ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه، أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحساب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته، وعليه فإن الجريمة الإلكترونية قد لا تختلف عن الجريمة المعلوماتية في كثير من الأحوال، باستثناء أنها تتم عن طريق جهازي كمبيوتر، أو أكثر متصلة بينها عبر شبكة الإنترنت، والواقع أنه يصعب القول بوجود حدود فاصلة بين الجريمة المعلوماتية والجريمة الإلكترونية، فكلاهما مرتبط بالكمبيوتر، وإن كانت الثانية تجد مكانها في المكان الافتراضي عبر شبكة الإنترنت"[5].

لكن هذا الطرح يظل محل نقاش، نظرًا لأن الجريمة المعلوماتية أيضًا قد تتم عبر الإنترنت، مما يجعل التداخل بين المصطلحين أمرًا متوقعًا وبالتالي، يمكن القول إن

EISSN: 2588-2368 ——— ISSN: 2352-975X

العلاقة بينهما تكاملية أكثر منها تمييزية.

2- أشكال الجرائم الإلكترونية: تتنوع أشكال الجرائم الإلكترونية، نذكر منها على سبيل المثال لا الحصر ما يلي[6]:

أ- الجريمة السياسية والاقتصادية: وهذا ما تستعمله الجماعات الإرهابية، كتحويل الأموال، الاتصال والتنسيق، قرصنة المواقع الحساسة، وسرقة المعلومات.

ب- الجريمة الثقافية: وهي استيلاء المجرم على الحقوق الفكرية للضحية (المؤلفات، البرمجيات، التعدي على القنوات الفضائية).

ج- الجريمة المادية: والتي تسبب أضرارا مالية للضحية.

د- الجريمة الجنسية: من خلال الابتزاز باستعمال صور وفيديوهات الضحية، وكذلك نشر كل ما هو مخل بالآداب على مواقع الإنترنيت.

ثانيا- الأجهزة والمنظمات الدولية لمكافحة الجريمة الإلكترونية:

في ظل تزايد تهديدات الجريمة الإلكترونية، برزت الحاجة إلى تطوير آليات فعالة لمكافحتها، مما أدى إلى ظهور أجهزة ومنظمات دولية متخصصة تعمل على الحد من هذه الظاهرة. وتلعب هذه الأجهزة والمنظمات دورًا محوريًا في وضع السياسات، تعزيز التعاون الدولي، وتنسيق الجهود بين الحكومات لملاحقة المجرمين السيبرانيين. ومن أبرز هذه الهيئات الإنتربول، اليوروبول، والاتحاد الدولي للاتصالات وغيرها، نستعرض أهمها فيما يلي[7]:

1- المنظمة الدولية للشرطة الجنائية: تعتبر المنظمة الدولية للشرطة الجنائية (الإنتربول) إحدى المنظمات الحكومية التي أوكل إليه المجتمع الدولي مهمة التنسيق والبحث والتقصي وتقديم الإرشادات في ميدان مكافحة الإجرام عموما، والجريمة الإلكترونية على وجه الخصوص.

2- الأورجست: تم إنشاء الأورجست في 28 فيفري 2002، بهدف تقوية مكافحة جميع أنواع الإجرام الخطير، وتنعقد اختصاصاته عندما يمس ذلك الإجرام

ISSN: 2352-975X ——— EISSN: 2588-2368

دولتين على الأقل من أعضاء الإتحاد الأوربي أو دولة عضو مع دولة من دول العالم الثالث، أو دولة عضو مع الرابطة الأوربية، وهي في ذلك غير مقتصرة على الأشخاص، فقط وإنما تشمل كافة المؤسسات.

3- الأوربول: يسمى أيضا بمركز الشرطة الأوربية، وهو أحد الأجهزة المتواجدة على المستوى الأوربي، والتي تتخذ من لاهاي- هولندا مقرا لها، وهي مكلفة بمكافحة الإجرام عن طريق:

- معالجة البيانات المرتبطة بالأنشطة الإجرامية على مستوى الاتحاد الأوربي
- دعم وتشجيع سلطات التحقيق؛ وذلك بتكميل وسائلهم وتحديثها من أجل مكافحة جميع أنواع الإجرام المنظم الدولي الخطير.

تسهيل تبادل تلك المعلومات عن طريق تزويد المحققين بتحاليل عملية وإستراتيجية، وبدعمهم بخبراتهم ومدهم بمساعدته التقنية.

المحور الثاني: ماهية جريمة الابتزاز الإلكتروني:

أولا- مفهوم الابتزاز الإلكتروني:

1- تعريف الابتزاز الإلكتروني: يعرف الابتزاز بأنه: "محاولة تحصيل مكاسب مادية أو معنوية من شخص - أو أشخاص - طبيعي أو اعتباري، بالإكراه بالتهديد بفضح سر من وقع عليه الابتزاز". ويعرف أيضا بأنه: هو "استغلال القوة مقابل ضعف إنسان آخر سواء كان هذا الضعف مؤقتا أو دائما"، أو هو "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 كليهما معا".(8)

إن الابتزاز الإلكترونية يعني أيً نوع من الابتزاز القائم على أساس التهديد بإيقاع الأذى أو التشهير، عن طريق نشر مستندات أو وثائق تضر بالاسم أو السمعة، أو صور فاضحة باستخدام الوسائل الإلكترونية، ولا بد من الإشارة إلى أن جريمة

EISSN: 2588-2368 ——— ISSN: 2352-975X

الابتزاز الإلكتروني تتحقق من خلال نوعان من التهديد، فهناك التهديد الصريح والذي يتم من خلال التلفظ بعبارات التهديد كالتهديد بالنشر أو القتل او الفضح، ويكون صريحا سواء من خلال التخاطب المباشر أو من خلال الهاتف أو من خلال وسائل التواصل الاجتماعي، وقد يكون التهديد ضمني ويتحقق ذلك من خلال إرسال الإشارات والتعبيرات التي تدل على التهديد كإرسال سكين مضرجة بالدم أو إشارة جمجمة أو ضحكة صفراء أو أي أفعال من شأنها أن تسبب تغير ملحوظ في سلوك المجرم دون الإفصاح عنه صراحة وهذا التهديد يُعد تهديدا ضمنيا وبذات الوقت يعد السريان البطيء لارتكاب جريمة الابتزاز.(9)

فالابتزاز الإلكتروني في مضمونه يشبه عملية السطو على المنازل، حيث يُجبر الضحايا على تسليم الأموال تحت تهديد القتل، إلا أن الاختلاف يكمن في الطابع الإلكتروني للعملية. فالابتزاز الإلكتروني يتمثل في تهديد الضحية بنشر صور شخصية أو مقاطع فيديو أو إفشاء معلومات سرية مقابل مبالغ مالية كبيرة. كما قد يُستخدم هذا النوع من الابتزاز للحصول على معلومات حساسة تتعلق بشركات أو أماكن عمل. وغالبًا ما يتم تنفيذ هذه العمليات من خلال استدراج الضحايا عبر البريد الإلكتروني أو منصات التواصل الاجتماعي، التي تُعد وسائل شائعة الاستخدام بين مختلف الفئات العمرية.(10)

فالابتزاز الإلكتروني إذا ليس مجرد تصرف غير أخلاقي، بل هو فعل مجرّم قانونيًا، لما يترتب عليه من انتهاكات وتهديدات وما جاء في التعريفات السابقة يبرز الجوانب الأساسية للابتزاز الإلكتروني ويظهر ذلك من خلال ما يلي:

- جوهره: أنه جريمة تهديد عبر الوسائل الرقمية.
- وسائله: البريد الإلكتروني ووسائل التواصل الاجتماعي.
- أنواعه: صريح ومباشر أو ضمني وغير مباشر.
- أهدافه: مالية، تشويه السمعة، سرقة بيانات حساسة.

ISSN: 2352-975X ——————————EISSN: 2588-2368

- طريقة تنفيذه: استدراج الضحايا عبر الإنترنت.

- يتشابه مع السطو: من حيث الإكراه ولكن باستخدام التكنولوجيا بدلًا من العنف الجسدي.

2- أصناف الابتزاز الإلكتروني: سلك العديد من الباحثين مسالك مختلفة في تصنيفهم لجرائم الابتزاز، نعرضها فيما يلي[11]:

أ - تصنيف الجريمة حسب الفئة المستهدفة:

أ-1- جرائم الابتزاز الإلكترونية الواقعة على الكيانات المالية والاقتصادية والسياسية: وتُستهدف عن طريق التجسس الإلكتروني على أنشطتها واختراق أنظمتها والحصول على معلومات سرية تتعلق بهذه الكيانات، ومن هنا سعت هذه الأخيرة إلى الحفاظ على وثائقها الرسمية السرية والخاصة بكيانها ومخططاتها ونشاطاتها بصورة آمنة ضد تلاعب الأشخاص وعدم الوصول إليها من خلال استخدام التقنيات الحديثة، ونظرا لخطورة هذه البيانات وسريتها سعت العديد من المنظمات الإجرامية للحصول على تلك المعلومات بقصد ابتزاز هذه الكيانات بالحصول على مبالغ مالية نظير عدم نشر بياناتها الخاصة.

أ-2- جرائم الابتزاز الإلكتروني الواقعة على النساء: وتُعد أكثرها انتشارا، حيث يتم تصيد ضحايا الابتزاز الإلكتروني عن طريق الإنترنيت مثل: الفيسبوك، السكايب، واتس آب، البريد الإلكتروني، تويتر، الإنستغرام، يوتيوب، سكايب أو أي وسيلة إلكترونية أخرى يمكن من خلالها الوصول إلى معلومات سرية أو حساسة عن الضحية.

أ-3- جرائم الابتزاز الإلكتروني الواقعة على الأحداث: وتأتي جريمة الابتزاز الإلكتروني للأحداث في المرتبة الثانية بعد **ابتزاز** النساء، حيث يقوم المبتز بالتعرف على الأحداث صغار السن من خلال غرف المحادثات ومواقع التواصل الاجتماعي، ثم يُطلب له صور جنسية مقابل إعطائه مبلغا من المال، ثم يطلب من الحدث

ممارسة الفاحشة مقابل عدم نشر مقاطع الصور الجنسية التي حصل عليها.

أ-4- جرائم الابتزاز الإلكتروني الواقعة على الرجال: حيث يعمد بعض الشباب أو النساء إلى إقامة علاقات غير شرعية مع الرجال ميسوري الحال واستغلال تلك العلاقة في تسجيل مقاطع صوتية أو مقاطع فيديو يتم استغلالها فيما بعد في طلب المال من الضحية نظير عدم نشر هذه المقاطع أو الصور.

ب- تصنيف الجريمة حسب الهدف المقصود:

ب-1- جرائم الابتزاز الإلكتروني بهدف الابتزاز المادي: وهنا يقوم المبتز بطلب الحصول على مبالغ نقدية أو عينية ذات قيمة من المجني عليه في مقابل عدم إفشاء الأسرار التي في حوزته وعدم نشرها على الشبكة المعلوماتية، وتصل هذه المبالغ إلى أرقام فلكية عندما يتم ابتزاز الحكومات والكيانات الاقتصادية الكبرى، حيث تضطر إلى الدفع خوفا من التشهير والمحافظة على سمعتها وعدم فقدان ثقة العملاء بها.

ب-2- جرائم الابتزاز الإلكتروني بهدف الابتزاز الجنسي: وهو أكثر أنواع الابتزاز شيوعا، حين يكون المجني عليه امرأة أو حدثا صغيرا أو رجلا ميسور الحال، وهنا يقوم المبتز بالتعرف على الضحية عن طريق مواقع التواصل الاجتماعي أو غرف الدردشة، ثم يقوم بالتحدث مع الضحية والتواصل معها وأخذ صور لها بموافقتها، ثم يطلب إشباع رغباته الجنسية أو التهديد بنشر الأسرار التي حصل عليها، فتضطر الضحية للامتثال لرغباته خشية الفضيحة ويتواصل مسلسل الابتزاز.

ب-3- جرائم الابتزاز الإلكتروني بهدف المنفعة: وينتشر هذا النوع من الابتزاز لدى العصابات الإجرامية، وذلك بقصد تنفيذ مخططاتهم الإجرامية والتوسع في تنفيذها، واستغلال الضحايا لتكون وسائل لارتكاب الجرائم.

ISSN: 2352-975X ——— EISSN: 2588-2368

3- الأبعاد الأخلاقية للابتزاز الإلكتروني وموقف الشريعة الإسلامية منه:

أ- الأبعاد الأخلاقية للابتزاز الإلكتروني: تُعَدُّ جرائم الابتزاز من أبرز الجرائم الأخلاقية لما تنطوي عليه من ممارسات مركبة تشمل الإكراه على ارتكاب المنكر، الاستمرار في ممارسته، والتهديد بالفضيحة، وقد تتفاقم تداعياتها لتصل إلى إنشاء أوكار للدعارة من خلالها. وتُشكِّل الجرائم الأخلاقية بمختلف أشكالها أحد العوامل الرئيسة التي تُسهم في انحدار المجتمعات، إذ تؤدي إلى ظهور أنماط متعددة من الانحرافات التي تُضعف بنية المجتمع وتهدد نسيجه الأخلاقي وقيمه السلوكية.

وقد أولى الإسلام اهتماماً كبيراً بمبدأ الخصوصية، حيث تمثل ركيزة أساسية لحفظ كرامة الإنسان وصيانة حقوقه. وقد جاءت النصوص الشرعية لتؤكد على أهمية احترامها وعدم انتهاكها سواء على المستوى الشخصي أو الاجتماعي، مما يعكس منظومة متكاملة من القيم والتشريعات التي تُعزز الاستقرار المجتمعي وتُرسِّخ الأخلاقيات السامية، فقد ورد النهي الصريح عن التجسس على الآخرين، كونه انتهاكا لحرمة الحياة الخاصة للأفراد وسببا في نشر الفتن وإفساد العلاقات، يقول الله ﷻ ﴿يَا أَيُّهَا الَّذِينَ آَمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا﴾ (سورة الحجرات: الآية 12)، كما يحرص الإسلام على حماية الخصوصية في المواقف الحوارية ومنع انتهاكها بغير إذن، يقول ﷺ: "من استمع إلى حديث قوم وهم له كارهون صبَّ في أذنيه الآنك يوم القيامة" رواه البخاري، كما حثت الشريعة على قيمة الستر وحفظ أسرار الناس وعدم إفشائها ونفرت من تتبع أخطاء الآخرين ونشر عيوبهم، يقول ﷺ: "من ستر مسلما ستره الله في الدنيا والآخرة" رواه مسلم، وقوله ﷺ: "من تتبع عورة أخيه تتبع الله عورته، ومن تتبع الله عورته فضحه في بيته". رواه البخاري

فاحترام الخصوصية في الشريعة الإسلامية ليس مجرد قيمة دينية، بل هو واجب شرعي وأخلاقي يستمد مشروعيته من نصوص القرآن والسنة، ويتعين على المجتمعات

EISSN: 2588-2368 ——— ISSN: 2352-975X

الإسلامية والأفراد الحرص على الالتزام بهذه القيمة لحفظ كرامة الإنسان وتعزيز التعايش السلمي في ظل احترام الحقوق والواجبات، ومع تطور وسائل الاتصال وتقنيات المعلومات في العصر الحديث، أصبح الحفاظ على الخصوصية تحدياً كبيراً، تُبرز الشريعة الإسلامية بوضوح منهجية شاملة يمكن تطبيقها في هذا السياق، من خلال تطوير قوانين لحماية البيانات الشخصية ومنع التعدي عليها استناداً إلى المبادئ الشرعية التي تنادي بالعدل وصون الحقوق.

ب- موقف الشريعة الإسلامية من الابتزاز الإلكتروني: تمثل الشريعة الإسلامية نموذجًا متكاملًا في معالجة الظواهر الاجتماعية والتحديات المستجدة، حيث تتسم بمنهجية شاملة تجمع بين الجانبين الوقائي والعلاجي لمواجهة التطورات المعاصرة، ومنها جرائم الابتزاز الإلكتروني، ومع تزايد هذه الجرائم في ظل التقدم التقني، برزت الحاجة لفهم الأسس الشرعية التي تُسهم في تحقيق المقاصد العليا للشريعة الإسلامية والمتمثلة في حفظ الدين، النفس، النسل، المال، والعقل.

حيث ترتكز الشريعة الإسلامية على استراتيجية وقائية تهدف إلى منع وقوع الجرائم الإلكترونية، من خلال سد الذرائع المؤدية إليها عبر تقنين الممارسات وتشريع الحدود التي تنظم العلاقات الاجتماعية بكل مجالاتها، وتعزيز المنظومة الأخلاقية والتربوية، والتي تعكس حرص الشريعة الإسلامية على البعد الأخلاقي والتربوي في نهج الوقاية، فقد حرص الشرع الحكيم كل الحرص على ستر عورات المسلمين وحفظ خصوصياتهم الشرعية بعيدا عن أعين الناس، وشرع لذلك تشريعات عديدة منها: أحكام الاستئذان والنظر وغض البصر واللباس ونحو ذلك.. وفي المقابل نهى عن التجسس والاطلاع على العورات والدخول من غير استئذان، ويلاحظ أن هذه الأحكام الشرعية عبارة عن سياج يحمي الإنسان ويحيطه بمزيد من الحماية والأمن والخصوصية والستر، خاصة مع توسع الناس في الاشتراك في شبكات التواصل الاجتماعي وانتشار تكنولوجيا الاتصال، ولا شك أن أي سلوك أو عمل

ISSN: 2352-975X ——————————EISSN: 2588-2368

يكسر هذه الحواجز أو يحاول اختراق هذا السياج فهو مدان في الشرع، بل ويطبق عليه أحيانا مع تماديه حد الحرابة لإفساده في الأرض بهذا السلوك المشين[12].

أما عند وقوع الجريمة، فإن الشريعة الإسلامية تتبنى منهجًا متوازنًا يجمع بين العدل والرحمة لتحقيق الردع والإصلاح، عن طريق سن عقوبات تتراوح بين الحدود والتعزيزات، والتي تهدف إلى تحقيق الردع والإصلاح مع مراعاة حقوق الجاني في التوبة، وحقوق المجتمع في الحماية من الضرر، حيث تُظهر الشريعة الإسلامية قدرة عالية على التكيف مع المستجدات، من خلال اعتمادها على مبادئ مرنة وشاملة في مكافحة الجرائم الإلكترونية، بما في ذلك جرائم الابتزاز الإلكتروني، ويظل المنهج الإسلامي متفرداً في تحقيق التوازن بين حماية حقوق الفرد وأمن المجتمع، مع الحفاظ على مقاصد الشريعة التي تهدف إلى تحقيق العدالة والأمن الفردي والاجتماعي.

ثانيا- دوافع وأساليب وتحديات الابتزاز الإلكتروني:

1- دوافع (أسباب) الابتزاز الإلكتروني: من أسباب الابتزاز الإلكتروني التهاون بإرسال الصور عبر الوسائل، أو عبر البريد الإلكتروني، أو حفظ الصور في ذاكرة الجوال وعدم إزالتها عند بيع الجهاز، فيلجأ المبتز حين يملك هذه الصور إلى الضغط على صاحبها، وابتزازه من أجل تحقيق الغايات التي يبتغيها، ليفضحه بما يملك من صور أو أصوات. ولا يقف عند هذا الحد بل قد يقوم بتصوير أحوال وأوضاع ربما كانت مشينة، ومن ثم يزداد التهديد كما يزداد الوضع سوءا إذا طلب مع ذلك أموالا بل ربما أشرك معه غيره.

وبشكل عام يمكننا تسليط الضوء على أبرز الأسباب التي تسهم في حدوث الابتزاز، وذلك من خلال تحليل العوامل المتنوعة التي تساهم في ظهوره وانتشاره:[13]

EISSN: 2588-2368 ——— ISSN: 2352-975X

أ- مشكلات سلوكية: نتيجة للممارسات الخاطئة في مراحل التنشئة المختلفة ما قد يؤدي إلى اختلال منظومة القيم وبالتالي الاتجاه والسلوك، فالتربية الخاطئة أو عدم التربية وفق المرجعية الشرعية أدى إلى تطوير مفاهيم مشوهة عن العلاقة بين الجنسين، كما أثرت بعض الموروثات المجتمعية وبعض زوايا الثقافة الشعبية في صورة البطل والضحية، والذي يدفع إلى ممارسة بعض أنواع السلوك الإجرامي بدعم هذه الثقافة السلبية خاصة مع توفر الوسائل الإلكترونية ذات المخاطر الأقل.

ب- طبيعة الوسيلة الإلكترونية: توفر الوسائل الإلكترونية الحديثة العديد من المزايا للمنحرفين سلوكيا وهذا ما شجع على ظهور العديد من الجرائم الإلكترونية خلال العقد الماضي، ومن هذه الظواهر الإجرامية برزت مشكلة الابتزاز الإلكتروني، حيث توفر البيئة الإلكترونية لمستخدمها درجة عالية من التحكم في الوسيلة، فقد وجد المجرم العديد من المزايا ومن أهمها:

- **الفرصة:** إذ أن من أهم أركان الجريمة بشكل عام توفر الفرصة وفي عالم إلكتروني كبير، فإن فرصة غفلة الضحية أو عدم وعيها أو ضعف مقاومتها تُعد أهم مقومات بناء الفرصة المناسبة لارتكاب الجريمة.

- **التخفي:** توفر الإنترنيت والوسائل الإلكترونية عموما لمسيء استخدامها فرصة كبرى للتخفي لممارسة الجريمة والانحراف وابتزاز الضحايا من وراء الشاشات ولوحات المفاتيح أو الأرقام المجهولة المصدر للهواتف وميض البلوتوث الأزرق في الزوايا المظلمة.

- **المخاطرة:** لكل الجرائم في حسابات مرتكبيها درجة من المخاطرة قد تجعل المجرم يتراجع عن ارتكاب الجريمة إذا ارتفعت درجة المخاطرة مثل السطو المسلح على المصارف واختطاف الطائرات وغيرها، أما البيئة الإلكترونية فتقدم للمجرم فرصة كبرى لممارسة جرائمه بدرجة أقل من المخاطرة.

ISSN: 2352-975X ——————————EISSN: 2588-2368

ب-1- أسباب عاطفية: قد يقوم بعض المراهقين بالعديد من الممارسات على شبكة الإنترنيت نتيجة مشكلات عاطفية يعانيها المراهق في حياته الطبيعية، ويمارس مراهقون كشفت عنهم القضايا الأمنية عن درجة من الحرمان العاطفي في بيئته الخاصة ما يدفعه للبحث عن الإشباع العاطفي من خلال علاقات منشؤها الإنترنيت والهواتف النقالة، ومن دوافع المبتز في المظهر العاطفي تجريب مهاراته في السيطرة عاطفيا ونفسيا على الآخرين.

ب-2- أسباب اقتصادية: قد يؤدي الحرمان الاقتصادي - في مختلف المجتمعات - بالكثيرين إلى ممارسات قد تصل إلى حد الانحراف إلى الجريمة بشكل أو بآخر، حيث تم رصد الكثير من الحالات التي كان دافع المبتز فيها هو تحقيق مكاسب مالية مبررا ذلك بأنه نتيجة معاناته من البطالة والفقر، وقد يهيئ الضحية (خاصة الفتيات) المجال للمبتز لدخول عالمها وأسرارها نتيجة حاجتها المادية التي لم تشبعها الأسرة ومن ثم تصبح عرضة للابتزاز.

ب-3- أسباب ثقافية: في بعض المجتمعات يختلف ويتفاوت مفهوم الجريمة والانحراف بحسب جنس الشخص (ذكر وأنثى) وبحسب الضحية وقد تجد بعض الموروثات الثقافية مبررات تسهم في عدم ردع المراهقين، وترسخ بعض جوانب الثقافة السلبية مظاهر

ب-4- التعزيز الإعلامي: يقضي الشباب اليوم ساعات طويلة أمام شاشات التلفزيون يشاهدون تدفقا عالميا حرا من المعلومات والمواد الترفيهية التي لا تعزز كلها بالضرورة القيم والأخلاق المجتمعية، وتعد الجريمة الإلكترونية على رأس قائمة الأفلام الأكثر رواجا في السنوات الأخيرة والتي أظهرت المجرم الإلكتروني بمظهر البطل الذكي المحترف الذي عجزت المصالح الأمنية الإطاحة به.

ومن هذه الثقافات نشأت ظاهرة الذكاء الإلكتروني المرتبط بالإجرام الإلكتروني مهملة الجوانب الانحرافية في الموضوع، ومن جهة أخرى أظهرت وسائل الإعلام من

EISSN: 2588-2368 ——— ISSN: 2352-975X

خلال الدراما والأغاني المصورة (الفيديو كليب) نماذج متعددة لبناء العلاقات العاطفية والجنسية بين الشباب والفتيات، كلها تتم خارج السياقات الاجتماعية المعتبرة ما دفع بعض الشباب من الجنسين للمغامرة في هذا الاتجاه ومن ثم تتكشف نهاية العلاقات بطريقة مؤلمة للطرفين لعدم نشوئها في بيئة طبيعية.

2- أساليب الابتزاز الإلكتروني والفئات المستهدفة: تتنوع أساليب الابتزاز الإلكتروني كما يلي[14]:

- الابتزاز المقترن بجريمة سرقة المعلومات والتهديد باستخدامها وتبدو أكثر وضوحا في المجالات التجارية وامتدت إلى الشباب والفتيات.

- الابتزاز جراء الحصول على وثائق من خلال اختراق الأجهزة والاستيلاء على محتوياتها ومن ثم استغلالها.

- الابتزاز جراء بيع وتداول معلومات سرية وتتضح هذه العملية حينما يتم تداول معلومات شخصية ثم المتاجرة بها، كبيع وتداول صور خاصة من قاعات الأفراح ومحتويات الهواتف الجوالة في مناطق يسهل التعرف على صاحب هذه الصور والمعلومات.

- الابتزاز من خلال العلاقات التي تبدأ بريئة عبر المواقع وأجهزة الألعاب الإلكترونية، وتنتهي محزنة بالابتزاز وأحيانا بالجريمة.

- الابتزاز باستخدام البريد الإلكتروني وغرف الدردشة، وهذه الصور الأشهر إذ يسمح نظام البريد الإلكتروني والمسنجر بخصوصية أكبر بين طرفين ومن ثم يسمح النظام بتبادل الملفات والوثائق لتتيح فيما بعد الفرصة للمبتز لاستغلالها بغية الحصول على مكاسب مادية أو معنوية وأحيانا إيذاء الضحية.

- الابتزاز باستخدام المنتديات والمواقع، والتي تتشكل من خلالها علاقات وحوارات تؤدي في نهاية الأمر إلى نوع من الود الافتراضي لمن يحمل ذات الأفكار ويظهر قدرا من الثقة أمام الطرف الآخر، ومن خلال المشاركة اليومية في هذه

ISSN: 2352-975X ——— EISSN: 2588-2368

المنتديات والمواقع تنشأ علاقات تبدأ شبه رسمية ثم تتكشف فيما بعد عن شخصيات وهمية وأهداف قد تنتهي إلى أنماط انحرافية منها الابتزاز.

- الابتزاز باستخدام الشبكات الاجتماعية: حينما ظهرت موجة الشبكات الاجتماعية لم يتوقع الخبراء أن تكتسح الكثير من النشاطات الاتصالية على شبكة الإنترنيت، وقد رافق العلاقات التي نشأت عبر هذه الشبكات مظاهر ابتزاز تطورت إلى قضايا وفضائح مدوية.

3- الابتزاز الإلكتروني: تداعياته الأمنية والنفسية والاجتماعية: تنطوي جريمة الابتزاز على جرائم متعددة، والتي يترتب عليها آثار سلبية جسيمة تؤثر بشكل مباشر على الأفراد والمجتمعات على حد سواء نستعرضها فيما يلي:

أ- الآثار الأمنية: يُعد الإيمان بالله والالتزام بشرائعه، من أعظم أسباب تحقيق الأمن والاستقرار في المجتمعات، وهو ما أكده قول قول الله ﷻ ﴿الَّذِينَ آمَنُوا وَلَمْ يَلْبِسُوا إِيمَانَهُمْ بِظُلْمٍ أُولَئِكَ لَهُمُ الْأَمْنُ وَهُمْ مُهْتَدُونَ﴾ (سورة الأنعام الآية 82)، ومن أسباب اختلال الأمن وإحلال الخوف هو الكفر بالله والوقوع في معصيته وانتهاك محارمه، لا سيما إذا جاهروا بالمعاصي وأعلنوها، يقول ﷻ: ﴿وَضَرَبَ اللَّهُ مَثَلًا قَرْيَةً كَانَتْ آمِنَةً مُطْمَئِنَّةً يَأْتِيهَا رِزْقُهَا رَغَدًا مِنْ كُلِّ مَكَانٍ فَكَفَرَتْ بِأَنْعُمِ اللَّهِ فَأَذَاقَهَا اللَّهُ لِبَاسَ الْجُوعِ وَالْخَوْفِ بِمَا كَانُوا يَصْنَعُونَ﴾ (سورة النحل الآية 112).

ومن أبرز الجرائم التي تؤدي إلى زعزعة الأمن المجتمعي جرائم الابتزاز، التي تؤثر بشكل مباشر على الشعور بالأمان لدى الأفراد، وغالباً ما تكون هذه الجريمة مدخلاً لارتكاب جرائم أخرى مثل الاغتصاب والزنا، إلى جانب تعاطي المسكرات والمخدرات، وقد تتطور إلى الدعارة والاعتداء على ممتلكات الآخرين، فضلاً عن ذلك، قد ترتبط جرائم الابتزاز بارتفاع معدلات جرائم القتل، ففي بعض الحالات، تلجأ الضحية أو أحد أفراد أسرتها إلى قتل المبتز انتقاماً لشرفها، خاصة في المجتمعات التي ترتبط فيها قضايا الشرف بمفاهيم "غسل العار". وقد شهدت بعض الحوادث

EISSN: 2588-2368 ——— ISSN: 2352-975X

ظهور جماعات تتبنى الانتقام من المبتزّين بصورة مباشرة، كما حدث في إحدى الحالات حيث أنشأت جماعة تُسمى "سيوف الأعراض" موقعاً إلكترونياً يحمل شعاراً يدعو إلى التصدي لهذه الجرائم(15).

وعليه فإن الالتزام بشريعة الله والوقوف عند حدوده يعدان أساسا لتحقيق الاستقرار والأمن والسلام المجتمعي، في حين أن ارتكاب المعاصي، والتي يمثل الابتزاز الإلكتروني واحدا منها هو مدعاة لتهديد الأمن والسلام وتفكيك البنية الأخلاقية والقيمية للمجتمع.

ب- الآثار النفسية: تؤثر جريمة الابتزاز بشكل كبير على الأفراد المستهدفين، حيث تتسبب في تدهور صحتهم النفسية والعاطفية، والتي تؤدي إلى مجموعة من الاضطرابات النفسية والجنسية، كالإقبال على الإباحية أو التفلت الجنسي، إلى جانب اضطرابات في الرغبة والوظيفة الجنسية بسبب الجرح النفسي الكبير المرتبط بالموضوعات الجنسية، كما قد يعاني الشخص من الشعور المستمر بالقلق والاكتئاب، والإرهاب الاجتماعي أو الوسواس القهري، فضلاً عن الاضطرابات الجسمية التي تنشأ بسبب الضغوط النفسية، فقد يصاب الأفراد بانهيارات عصبية ونوبات من الغضب الشديد والقلق والتوتر، والبكاء المستمر، والشعور الدائم بالذنب واضطرابات النوم، وتكرار الكوابيس الليلية، وعدم التركيز، والخوف، وترك العمل أحيانا رغم الحاجة إلى المال، والعصبية التي تنعكس على العمل والبيت، وقلة الإنتاج في العمل، كما قد يعانون من نوبات هلع بسبب استرجاع العلاقة السابقة والتهديدات المرتبطة بها، بالإضافة إلى الشعور بتوتر مستمر نتيجة لهذه التجارب.

إضافة إلى تعرض المبتز أيضًا لمشاعر تدني قيمة الذات والاضطرابات الفصامية، والضغوطات النفسية المستمرة التي قد تؤدي إلى اضطرابات نفسية مثل النكوص، وأحيانًا تصل إلى التفكير في الانتحار. وفي بعض الحالات، قد تظهر رغبة في الانتقام أو العدوان، وتزداد المحاولات لإيذاء الذات.، ويعاني الضحايا أيضًا من

ISSN: 2352-975X ——————————EISSN: 2588-2368

معاناة انفعالية وسلوكية، تشمل الشعور بالانطوائية والعزلة، وعدم الرغبة في إقامة علاقات اجتماعية، وصعوبة التعامل مع الآخرين، والخجل من الإفصاح عن مشاكل صحية مرتبطة بالجهاز التناسلي أو الالتهابات المختلفة[16]، كما أن التعرض لهذا النوع من الابتزاز قد يؤدي إلى تدمير صورة الفرد في محيطه الاجتماعي والمهني. حيث يجد الضحايا أنفسهم في مواجهة مع المجتمع بعد أن يتم نشر معلومات أو صور خاصة بهم على الإنترنت، مما يخلق حالة من النفور الاجتماعي تجاههم. وفقًا للعديد من الدراسات، يُظهر الأفراد الذين تعرضوا للابتزاز الإلكتروني صعوبة في استعادة سمعتهم الشخصية في محيطهم الاجتماعي أو في أماكن العمل، مما يعزز من الشعور بالعزلة والاغتراب داخل المجتمع.[17]

ج- الآثار الاجتماعية: تؤثر جريمة الابتزاز الإلكتروني بشكل مباشر على العلاقات الاجتماعية والتفاعل بين أفراد المجتمع، مما يقوض ويهدد تماسكه واستمراره، حيث تتولد حالة من الخوف وانعدام الثقة، وهنا تتوقف كثير من عمليات التفاعل الاجتماعي تحت ضغط الخوف وانعدام الثقة بالآخر.

كما تؤثر بشكل عميق على كيان الأسرة وبنيانها في حال تعرض أحد أفرادها لجريمة الابتزاز، لما لها من تأثير على العرض والشرف، حيث تعتبر هذه الجريمة عارا اجتماعيا توصم به الأسرة، وقد أشار الزهراني إلى أن العديد من الضحايا أبلغوا عن شعورهم بالذنب تجاه أسرهم بسبب الأضرار التي قد تلحق بهم نتيجة للابتزاز، مما يعزز من حالة الانعزال الداخلي داخل الأسرة[18].

وباعتبار المنظومة الأخلاقية هي الميثاق الذي يحكم المجتمع، تصبح عملية الابتزاز سببا في اهتزاز معايير الأخلاق، كالستر واحترام حقوق الآخرين وخصوصياتهم، الأمر الذي ينتج عنه قيم اجتماعية مضادة وسلبية، كالحقد والضغينة والكراهية والعدوانية وانتهاك الحرمات.

وللحد من تفشي ظاهرة الابتزاز الإلكتروني لابد من اتخاذ التدابير والسياسات

EISSN: 2588-2368 ——— ISSN: 2352-975X

اللازمة والمتمثلة فيما يلي:

ج-1- الإطار القانوني: تعتبر التشريعات والقوانين من أبرز الآليات لمكافحة الابتزاز الإلكتروني، حيث تساهم القوانين الصارمة في تحديد العقوبات المقررة لمرتكبي هذه الجرائم. على سبيل المثال، ينص قانون مكافحة الجرائم الإلكترونية في مصر على فرض عقوبات قاسية على مرتكبي الابتزاز الإلكتروني، بحيث قد تصل العقوبة إلى السجن لمدة تصل إلى خمس سنوات، فضلاً عن فرض غرامات مالية كبيرة[19]، بالإضافة إلى ذلك، ساهمت بعض الدول العربية في تأسيس محاكم متخصصة في الجرائم الإلكترونية، مما يساعد في تسريع الإجراءات القضائية وإنصاف الضحايا بشكل أكثر فعالية، ومن أجل تحقيق فعالية هذه التشريعات، يجب أن يتم تكامل الجهود بين الجهات القضائية والأمنية، وتطوير الأنظمة التقنية التي تساهم في حماية الأفراد. يجب أن تركز السياسات على تعزيز التعاون بين القطاعين الحكومي والخاص لضمان توفير بيئة قانونية آمنة.

ولقد قام المشرع الجزائري بوضع مجموعة من النصوص القانونية لمكافحة الجريمة الإلكترونية، منها:

القانون رقم 09-04 لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ويعد الإطار العام لمكافحة الجريمة الإلكترونية.

قانون العقوبات، لا سيما المادة 303 مكرر و303 مكرر1، التي تجرم الأفعال المتعلقة بانتهاك الحياة الخاصة عن طريق الوسائل الإلكترونية، كالنشر دون إذن أو التهديد بنشر معلومات أو صور.

المرسوم التنفيذي رقم 20-311 لسنة 2020، المتعلق بإنشاء الهيئة الوطنية لحماية المعطيات الشخصية، والذي يعزز حماية الأفراد من الاستغلال الإلكتروني والابتزاز.

تعديل قانون الإجراءات الجزائية لتشمل وسائل التحقيق الرقمي كالتفتيش

ISSN: 2352-975X ——— EISSN: 2588-2368

الإلكتروني والتنصت على المراسلات الرقمية.

ورغم ذلك، لا تزال الحاجة قائمة لتعزيز الإجراءات الوقائية والردعية، وتطوير القدرات التقنية للجهات الأمنية والقضائية، لمواكبة تطور هذه الجريمة.

ج-2- التقنيات الحديثة: حيث تلعب التقنيات الحديثة دوراً مهماً في الحد من الابتزاز الإلكتروني، وتعد برامج الحماية من الفيروسات والبرمجيات الخاصة بالأمن الرقمي من الأدوات الأساسية التي يستخدمها الأفراد والمؤسسات لحماية معلوماتهم الشخصية من التسريب أو الاستغلال، حيث تساعد هذه البرامج على التعرف المبكر على محاولات اختراق البيانات وحمايتها من التهديدات المحتملة[20] .

إضافة إلى ذلك، يُعد التشفير من الأدوات التقنية المحورية في تعزيز الأمان الرقمي، حيث يقوم بتحويل البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح فك التشفير المناسب، مما يجعل الوصول إلى المعلومات الشخصية شبه مستحيل على المخترقين. كما أن استخدام المصادقة الثنائية يعد من أبرز وسائل الحماية التي يمكن أن تقلل من مخاطر اختراق الحسابات الشخصية، وبالتالي يقلل من احتمالات الابتزاز الإلكتروني.

ج-3- الوعي المجتمعي والتثقيف الرقمي: يُعد تعزيز الوعي المجتمعي حول قضايا الأمان الرقمي أحد العناصر الأساسية في مكافحة الابتزاز الإلكتروني. يجب أن تتعاون المؤسسات الحكومية والتعليمية لنشر ثقافة الأمان الرقمي من خلال برامج توعوية تهدف إلى تعريف الأفراد بأهمية حماية بياناتهم الشخصية عند استخدام الإنترنت. ويجب التركيز على أهمية الخصوصية الرقمية والابتعاد عن مشاركة المعلومات الحساسة أو الصور في وسائل التواصل الاجتماعي إلا في بيئات آمنة[21].

وتلعب المؤسسات التعليمية دوراً مهماً في هذا السياق، حيث يمكنها تنظيم ورش عمل ودورات تدريبية تهدف إلى تعليم الطلاب كيفية حماية أنفسهم من المخاطر الرقمية. ويجب أن تشمل هذه الأنشطة التوعية بأساليب استخدام الإنترنت بشكل

EISSN: 2588-2368 ——— ISSN: 2352-975X

آمن، وتقديم إرشادات حول كيفية التعامل مع حالات الابتزاز الإلكتروني في حال حدوثها.

ج-4- التعاون الدولي في مواجهة الابتزاز الإلكتروني: تعتبر مشكلة الابتزاز الإلكتروني قضية عالمية لا تتوقف عند حدود الدول، مما يستدعي التعاون الدولي لمكافحتها. لذا من المهم تبادل المعلومات بين الدول المختلفة وتعزيز التنسيق بين الأجهزة الأمنية لملاحقة المجرمين الإلكترونيين. ساهمت الاتفاقيات الدولية مثل "اتفاقية بودابست" بشأن الجرائم الإلكترونية في وضع إطار قانوني للتعاون بين الدول في مكافحة الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني.[22]

إن تعزيز التعاون بين الدول يتطلب تبادل الخبرات والأدوات التقنية المتقدمة لملاحقة المجرمين على الصعيدين الإقليمي والدولي، مما يمكن الدول من ملاحقة الجرائم عبر الحدود الإلكترونية وتقديم الجناة إلى العدالة بشكل فعال.

يُعد الابتزاز الإلكتروني نموذجًا للجريمة الإلكترونية التي تفرض تحديات أخلاقية معقدة على الأفراد والمجتمع. إذ تؤدي هذه الجريمة إلى انتهاك القيم الأخلاقية مثل الأمانة، الخصوصية، والاحترام، ما يساهم في زعزعة المنظومة الأخلاقية القائمة. فمع تزايد استخدام التكنولوجيا الرقمية، أصبحت فرص استغلال الأفراد عبر الإنترنت أكثر انتشارًا، مما يفرض تهديدًا مباشرًا على أخلاقيات التفاعل الرقمي، ويجعل من الضروري تعزيز الوعي الأخلاقي والأمني للحد من هذه الظواهر.

خاتمة:

تُعد الجريمة الإلكترونية إحدى التحديات الكبرى التي تواجه المجتمعات الحديثة، حيث تتخطى آثارها حدود الأضرار المادية لتطال القيم الأخلاقية والاجتماعية، ويؤدي الابتزاز الإلكتروني إلى خلل كبير في المنظومة الأخلاقية، مما يستدعي تضافر الجهود القانونية، الاجتماعية، والأمنية لمواجهته. كما أن تعزيز القيم الأخلاقية والوعي الرقمي يشكلان ركيزة أساسية للحد من هذه الجرائم وحماية الأفراد من

ISSN: 2352-975X ——————————EISSN: 2588-2368

مخاطرها.

ويمكن ذكر أهم **النتائج** المتوصل إليها:

1- الجريمة الإلكترونية هي أي فعل غير قانوني يتم باستخدام الوسائل الإلكترونية، وتهدف إلى الإضرار بالأفراد أو المؤسسات. تشمل أنواعها الاحتيال الإلكتروني، الاختراق، سرقة الهوية، التجسس الرقمي، ونشر البرمجيات الخبيثة.

2- الابتزاز الإلكتروني هو نوع من أنواع الجريمة وأبرز أسبابه ضعف الوعي الأمني، الاستغلال العاطفي، التساهل في مشاركة البيانات الشخصية، وضعف القوانين الرادعة.

3- أن الشريعة الإسلامية تتبنى موقفًا حازمًا ضد الابتزاز، إذ تعتبره نوعًا من الظلم وأكل أموال الناس بالباطل، وهو محرم شرعًا. كما تحث الشريعة على حماية الحقوق الشخصية وتحريم الإكراه والتعدي على خصوصيات الآخرين.

4- يؤدي الابتزاز الإلكتروني إلى انهيار قيم الثقة بين الأفراد، وانتشار الخوف والشك، كما يعزز سلوكيات غير أخلاقية كالكذب والخداع والتلاعب، ما يسهم في تآكل المنظومة الأخلاقية في المجتمع.

كما يترتب على الابتزاز الإلكتروني تداعيات أهمها:

- نفسية: كالشعور بالخوف، القلق، الاكتئاب، وقد يصل الأمر إلى الانتحار في بعض الحالات.

- اجتماعية: كانعدام الثقة في العلاقات الاجتماعية، تفكك الأسر، والعزلة الاجتماعية.

- أمنية: كزيادة جرائم الإنترنت، صعوبة تتبع المجرمين، وزيادة الأعباء على الجهات الأمنية والقضائية.

5- ولمواجهة الابتزاز الإلكتروني يتطلب الأمر توفر آليات منها:

- تعزيز الوعي الرقمي بين الأفراد حول مخاطر مشاركة المعلومات الشخصية.

EISSN: 2588-2368 ——— ISSN: 2352-975X

- سن قوانين صارمة تعاقب مرتكبي هذه الجرائم.

- تطوير تقنيات الحماية الإلكترونية مثل التشفير والذكاء الاصطناعي لمكافحة الجرائم الرقمية.

- دعم الضحايا نفسيًا وقانونيًا لمساعدتهم على تجاوز آثار الابتزاز.

- تعزيز دور المؤسسات الدينية والتربوية في نشر ثقافة الاستخدام الأخلاقي للتكنولوجيا.

وعليه: يمكن تقديم **المقترحات** التالية:

1- العمل على ترسيخ الوعي المجتمعي من خلال حملات توعوية حول مخاطر الابتزاز الإلكتروني وكيفية تجنبه.

2- إدراج التربية الرقمية في المناهج التعليمية لتعريف الشباب بأساليب الحماية الإلكترونية.

3- تطوير التشريعات والقوانين لردع المبتزين وحماية الضحايا قانونيا.

4- تشجيع الضحايا على التبليغ دون الخوف من الوصمة الاجتماعية.

5- تعزيز دور المؤسسات التعليمية والدينية والإعلامية في مكافحة الابتزاز الإلكتروني عبر برامج خاصة.

الهوامش والمراجع:

(1)- محمود إبراهيم الغازي: الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الإسكندرية: ط1، 2014، ص118.

(2)- حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية – التسريبات، التجسس الإلكتروني، الإرهاب، دار فكر وفن للطباعة والنشر والتوزيع، ط1، 2015، ص16.

(3)- نهلا عبد القادر المومني: الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص49.

(4)-*K. Tiedemann, Fraudes et autre délies d'affaires commis à l'aide d'ordinateurs éléctroniques, Revus de droit pénal et criminologie, N7, Bruxelle 1984, p612.*

(5)-هشام بشير: الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والإستراتيجية، العدد 90، 2012، ص10

(6)- حسنين شفيق: مرجع سابق، ص 17-18

ISSN: 2352-975X ——— EISSN: 2588-2368

(7)- هشام بشير: مرجع سابق، 22-23.

(8)- صالح بن عبد الله بن حميد: الابتزاز - المفهوم والواقع - مركز باحثات لدراسات المرأة، الرياض، 1432ه، ص14

(9)- خالد حسن لطفي: جرائم الإنترنيت، بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني، دار الفكر الاجتماعي، الإسكندرية، ط1، 2018، ص136.

(10)- حسين يونس، خليل الجندي: الابتزاز الإلكتروني والجرائم الإلكترونية: المفهوم والأسباب، دار كفاءة المعرفة، ط1، 2021، ص50.

(11)- المرجع نفسه، ص138-139.

(12)- خالد لطفي، مرجع سابق، ص110-111.

(13)- فايز بن عبد الله الشهري: دور مؤسسات المجتمع في مواجهة ظاهرة الابتزاز وعلاجه – الابتزاز الإلكتروني نموذجا– مركز باحثات لدراسات المرأة، الرياض، 1432، ص 18

(14)- فايز بن عبد الله الشهري: مرجع سابق، ص154.

(15)- عبد العزيز الحمين: الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، الرياض، 1432ه)، ص64.

(16)- *Martin, L. "Le chantage émotionnel et ses conséquences sur la psychologie des victimes." Psychologie clinique et sociale, vol. 12, no. 3, 2020, pp. 35-48.*

(17)- علي الزهراني: "الابتزاز الإلكتروني في العالم العربي: التحديات والحلول"، مجلة الأمن السيبراني، 15-30، 2021.

(18)- عادل الزهراني: أثر الجرائم الإلكترونية على المجتمع العربي، دار الكتاب العربي، الرياض، 2019، ص114.

(19)- علي عبد الله: الجرائم الإلكترونية: التحديات والحلول، القاهرة، دار المعارف، 2020، ص32.

(20)- هالة الشامي: القوانين العربية لمكافحة الجرائم الإلكترونية- دراسة مقارنة- مجلة القانون والسياسة، 2021، م10، ع4، ص 55.

(21)- مصطفى الطيب، "الابتزاز الإلكتروني وأثره على الأمن الاجتماعي"، مجلة الأمن الرقمي، م15، ع 3، 2022، ص47.

(22)- سامي عبد الله منصور: التعاون الأمني الدولي في مكافحة الجرائم الإلكترونية- الواقع والتحديات-مؤسسة العلوم القانونية، القاهرة، 2021، ص 92.