الجريمة الالكترونية في المجتمع العربي: المغذيات والانعكاسات

Cybercrime in Arab Society: Drivers and Implications

د/ حنادر عبد الله[1]

Abdellah.hanader@univ-relizane.dz

جامعة أحمد زبانة -غليزان-

قسم علوم الإعلام والإتصال

تاريخ الإرسال: 2025/02/19	تاريخ القبول: 2025/02/22	تاريخ النشر: 2025/03/15

الملخص:

سنحاول في ورقتنا البحثية هذه أن نتطرق إلى جل العناصر الخاصة بمفهوم الابتزاز الالكتروني كنمط خطير من أنماط الجريمة الالكترونية، وانعكاساته الوخيمة على الفرد والمؤسسات والمجتمع، من خلال بعض النماذج الواقعية التي شهدها العالم العربي، فبقدر ما للتكنولوجيا الحديثة من إيجابيات على غرار توفير الجهد والوقت لأداء العديد من الأمور والوظائف، توفير فرص عمل جديدة، تسهيل التواصل الاجتماعي، بقدر ما لها من سلبيات كثيرة أثرت على حياة الأفراد والمؤسسات على حد سواء، وأخذت منحى خطيرا جدا.

توصلنا إلى أن الجريمة بكل أنواعها ولعل ما وجدناه من أخطر الأنواع – حسب اطلاعنا – هو الابتزاز باستخدام مختلف الوسائل الرقمية، لما له من تقويض لحرية الأفراد، وزرع الرعب والهلع في نفوسهم، وإكثار الهواجس باللجوء إلى عديد الممارسات التي تستخدم أسلوب الترهيب والتهديد للمساس بالضحية، وتقييد عمل المؤسسات وإنتاجيتها باختراق الأنظمة وقرصنة المعلومات الدقيقة لها، والدخول في مرحلة المساومة والمفاوضة لتقديم تنازلات أو دفع أموال قصد استرجاع ممتلكاتها (الأموال، الوثائق، المعلومات ...).

الكلمات المفتاحية: الإبتزاز الالكتروني؛ الجريمة الإلكترونية؛ الآثار؛ المجتمع العربي.

Abstract:

This research paper explores cyber extortion as a serious form of cybercrime and its profound impact on individuals, institutions, and society. By examining real-world cases from the Arab world, we highlight how this crime has escalated with the advancement of digital technology. While technology offers numerous benefits, such as efficiency, job creation, and enhanced communication, it also presents significant risks that have taken a dangerous turn.

Cyber extortion poses a major threat by violating personal freedoms, spreading fear, and disrupting institutional operations through digital threats, data breaches, and ransom demands. Our findings emphasize the urgent need for stronger legal frameworks, enhanced cybersecurity measures, and increased public awareness to mitigate its growing risks and protect both individuals and organizations.

Keywords: Cyber extortion; Cybercrime; Impacts; Arab society.

---

[1] المؤلف المرسل: د/ حنادر عبد الله

مقدمة:

أتاح الانتشار الواسع للتكنولوجيات الجديدة توفير شتى سبل الراحة والرعاية للإنسان، سواء من الناحية الاجتماعية، الثقافية، أو حتى الاقتصادية، وأسهم بشكل كبير في تسهيل الحياة اليومية وتعزيز التواصل بين الأفراد. وقد انعكس هذا التطور التقني في تحقيق نجاحات باهرة، خاصة خلال العقود الأولى من القرن العشرين، حيث أحدثت الثورة الرقمية نقلة نوعية في مختلف المجالات. غير أن هذه الطفرة التكنولوجية لم تخلُ من سلبيات خطيرة، كان أبرزها انتشار الجريمة الإلكترونية، التي أخذت أبعادًا غير مسبوقة، وأصبحت تهدد أمن الأفراد والمجتمعات على حد سواء. ومن بين أخطر هذه الجرائم، يبرز الابتزاز الإلكتروني كظاهرة متفشية بشكل لافت، تستغل التطور الرقمي لتصيد الضحايا والتلاعب بهم.

تعتمد جريمة الابتزاز الإلكتروني على التخطيط الممنهج والدقيق الذي يهدف إلى الإيقاع بالضحايا واستغلالهم بطرق مختلفة، حيث يسعى المبتز إلى الحصول على معلومات حساسة تتعلق بالضحية، مثل الصور الشخصية، مقاطع الفيديو، أو بيانات خاصة متاحة عبر الإنترنت أو وسائل التواصل الاجتماعي. وبمجرد امتلاك هذه المعلومات، يبدأ المبتز بممارسة ضغوط نفسية وتهديدات مباشرة على الضحية بغية تحقيق مكاسب مادية أو إشباع رغبات أخرى، غالبًا ما تكون ذات طبيعة غير أخلاقية. وتزداد خطورة هذه الجريمة مع سهولة الوصول إلى بيانات الأفراد عبر المنصات الرقمية، حيث أصبح المستخدمون – وخاصة الفئات الشابة – أكثر عرضة للوقوع في شراك المبتزين دون إدراك مسبق للعواقب الوخيمة التي قد تترتب على ذلك، على مستوى الفرد والمجتمع.

إن جريمة الابتزاز الإلكتروني لا تقتصر آثارها على الضحية فحسب، بل تمتد لتشمل المجتمع ككل، لما لها من انعكاسات سلبية على المستويات الأمنية، الاجتماعية، والقانونية. فمن الناحية الشرعية، يعد الابتزاز الإلكتروني انتهاكًا صارخًا للقيم الأخلاقية والدينية التي تحث على صون كرامة الإنسان وحماية خصوصيته. أما من الناحية الاجتماعية، فإنه يؤدي إلى زعزعة الاستقرار النفسي والعاطفي للأفراد، وقد يدفع بعض الضحايا إلى العزلة أو حتى التفكير في إنهاء حياتهم نتيجة الضغوط النفسية الهائلة. ومن المنظور الأمني، يمثل الابتزاز الإلكتروني تهديدًا متزايدًا يستوجب تعزيز آليات الحماية الرقمية وسن تشريعات أكثر صرامة لمكافحته والحد من انتشاره.

وفي هذا السياق، تسلط هذه الورقة البحثية الضوء على جريمة الابتزاز الإلكتروني من مختلف جوانبها، متناولين بالدراسة والتحليل نموذجين بارزين لحالات ابتزاز وقعت عبر موقع فيسبوك في الجزائر، مما يسمح بفهم أعمق لأبعاد هذه الظاهرة وسبل مواجهتها بفعالية.

المحور الأول: الإطار النظري للإبتزاز الإلكتروني والجريمة الإلكترونية

يُعد الابتزاز الإلكتروني تهديدًا متزايدًا في العصر الرقمي، مما يجعل الوعي السيبراني واتخاذ تدابير الحماية أمرًا ضروريًا للأفراد والمؤسسات على حد سواء.

1. تعريف الابتزاز:

هو تلك الأفعال التي تدفع بالفرد إلى التهديد بكشف معلومات معينة عن شخص، أو فعل شيء ليؤذي الشخص المهدد؛ إن لم يقم الشخص المهدد بالاستجابة إلى بعض الطلبات؛ كما يمكن أن تكون هذه المعلومات عادة محرجة أو ذات طبيعة مدمرة اجتماعيا، وهو بمعنى الحصول على أهداف غير مشروعة باستخدام وسائل غير مشروعة أيضا، وقد يستخدم الابتزاز في أي وظيفة مهما كان نوعها للتأثير على الشخص الذي يكون عرضة لهذا الفعل لتحقيق مكاسب نوعية غير مشروعة[1].

2. تعريف الابتزاز الالكتروني:

هو حصول فعل التهديد باستعمال الوسائط الالكترونية، أو عملية ترهيب الضحية بنشر صور وفيديوهات أو تسريب معلومات تخص الضحية مقابل دفع الأخير لمبلغ مالي أو استغلاله للقيام بأعمال غير مشروعة لصالح الجاني، ويتم في حالات كثيرة إسقاط الضحايا من خلال الإيميل أو مواقع التواصل الاجتماعي كونها واسعة الاستعمال والانتشار[2].

3. أشكال الابتزاز الالكتروني:

ثمة العديد من الأشكال للابتزاز الالكتروني، إذ تتغير بتغير الأهداف المرجوة من عملية الابتزاز، وعليه نوجزها كما يلي:

1.3 الابتزاز الالكتروني السياسي:

غايته تحقيق مكاسب سياسية على حساب الضحية، بحيث يبحث المجرم عن الهفوات التي وقعت فيها الضحية ويستخدمها ضدها، وفي حالة الرفض يلجأ المبتز إلى مواقع الانترنت لنشر الوثائق المزورة أو

---

[1] زيوش سعيد، **ظاهرة الابتزاز الالكتروني وأساليب الوقاية منها- قراءة سوسيولوجية وأراء نظرية** .مجلة العلوم الاجتماعية، العدد 22، 2017، ص.71.

[2] الغالبي رامي أحمد، **جريمة الابتزاز الالكتروني وآلية مكافحتها في جمهورية العراق** (ط1)، دار الكتب والوثائق للنشر والتوزيع، بغداد: العراق، 2019، ص.29.

الأخطاء التي صدرت من الضحية، وقد تصل إلى استخدام المبتز لأسماء مستعارة بهدف تدمير السيرة السياسية للضحية.

2.3 الابتزاز الالكتروني المهني:

إذ يعمد المبتز – والذي في العادة يكون مسؤولا عن الضحية في العمل- وبالتالي يملك المجرم الأدلة الكافية عن الضحية، فيشرع في التهديد بإكثار الطلبات أو تحقيق أهداف معينة.

3.3 الابتزاز العاطفي:

يهدف هذا النوع إلى التلاعب بالضحية؛ إذ يعمد المبتز إلى الإساءة للضحية طالبا منه الانصياع لبلوغ هدفه الذي سطره في عملية البحث عن ضحاياه عبر شبكة الأنترنت[1].

4. أسباب الابتزاز الالكتروني:

للابتزاز الإلكتروني عدة أسباب، تختلف باختلاف الأساليب التي يستخدمها المبتزون والوسائل التي يعتمدون عليها لتحقيق أهدافهم. ومن أبرز هذه الأسباب:

1.4 ضعف الوازع الديني.

2.4 انتشار القنوات الفضائية غير المحافظة بحيث ظهرت العديد من البرامج المتدنية ذات الثقافة الهابطة من الافلام والمسلسلات والاغاني التي تعرض في هذه القنوات؛ إذ وفي كثير من الأحيان تبث مشاهد مخلة تؤجج العواطف والمشاعر، الأمر الذي مهد لإقامة علاقات محرمة بين الجنسين.

3.4 تراجع أفراد الأسرة عن تأدية واجباتهم المنوطة بهم (لاسيما الآباء الذين أصبحوا يهملون تربية أبنائهم ويتركونها للوسائل التكنولوجية).

4.4 غياب المعلومات الكافية والصائبة عن المواضيع الحساسة كالأنترنت والهواتف المحمولة.

5.4 غياب التنشئة الاجتماعية السليمة.

6.4 دخول وسائل الاتصال الحديثة بشكل رهيب في حياة الأسر خصوصا الفضائيات وشبكة الانترنت، والتي ألغت كل الحواجز وكسر كل القيود[2].

[1] زيوش سعيد، مرجع سبق ذكره، ص.72.

[2] العيد نوال، **بحوث ندوة الابتزاز: المفهوم- الأسباب- العلاج**. بحث مقدم لمركز باحثات لدراسات المرأة، 1435 ه، الرياض، ص01.

7.4 الإعلام غير الهادف بحيث أضحت وسائل الإعلام المختلفة تقوم بدور خطير في توجيه الرأي وتسويق الأفكار والثقافات، والغالب في الوقت الراهن هو ضلوع الإعلام في توجيه المجتمعات نحو هاوية الانحراف.

8.4 الظروف الاقتصادية التي تلعب دورا مهما في سلوكيات الناس سواء سلبا أو إيجابا، فالجوانب الاقتصادية لها دور على كل من المبتز والضحية كما يظهر تأثيره من جانب الفقر والحاجة والغنى والترف، أما الضحية فإنها كلما كانت فقيرة محتاجة فإن استغلالها من طرف ضعاف النفوس يكون أسهل[1].

9.4 تأخر سن الزواج يعد من الظواهر التي تكون سببا في وقوع الكثير من الضحايا سواء شباب أو فتيات وتعرضهم لعمليات نصب واحتيال وربما يصل الأمر إلى التهديد بالتصفية الجسدية[2].

المحور الثاني: صور الابتزاز الالكتروني وكيفيات ارتكابه

يأخذ الابتزاز الإلكتروني أشكالًا متعددة، حيث يستخدم المجرمون وسائل وتقنيات مختلفة لتهديد الضحايا وإجبارهم على تنفيذ مطالب معينة، ويمكن أن نوجز هذا العنصر في الجدول أدناه:

جدول رقم (01) يوضح صور الإبتزاز الإلكتروني

صور الابتزاز		طرائق ارتكابه	
شخص الضحية	الشخصيات الاعتبارية	الحاسب وملحقاته وبرامجه	
	الأحداث	الأنترنت	البريد الإلكتروني
	النساء		خدمة الدردشة
	الرجال	الهواتف النقالة وبرامجها	
الهدف المرجو	مادي	التسجيلات الصوتية	
	جنسي	التسجيلات المرئية	
	نفعي	اختراقات الحسابات على مواقع التواصل الاجتماعي.	
الوسائل	مادية		
	معنوية		

المصدر: من إعداد الباحث بالإعتماد على (عراب، 2021، ص1210)

[1] بن حميد، صالح، بحوث ندوة الابتزاز: **المفهوم- الأسباب- العلاج**. بحث مقدم لمركز باحثات لدراسات المرأة، الرياض، 1432هـ، ص.01.

[2] الشمري، فلاح، **جريمة ابتزاز النساء ودور جهاز الحسبة في مكافحته**، رسالة ماجستير غير منشورة، جامعة مؤتة، 2008، الأردن، ص.01.

من خلال الجدول يمكن أن نميز بين عدة أشكال من الإبتزاز الإلكتروني:

1. ابتزاز الفدية (Ransomware Blackmail)

يُعد من أكثر أنواع الابتزاز الإلكتروني شيوعًا، حيث يقوم المهاجمون باختراق أجهزة الضحية وتشفير بياناتها، ثم يطالبون بدفع فدية – غالبًا بالعملات الرقمية – مقابل فك التشفير واستعادة البيانات. عادةً ما يتم إرسال رسالة للضحية توضح المبلغ المطلوب والمدة الزمنية المتاحة للدفع. يستهدف هذا النوع من الابتزاز الشركات الكبرى، المؤسسات الحكومية، وحتى الأفراد الذين يمتلكون بيانات حساسة.

2. الابتزاز الجنسي (Sextortion)

يحدث هذا النوع عندما يتمكن المبتزون من الحصول على صور أو مقاطع فيديو حساسة للضحية، سواء عن طريق الاختراق أو الخداع، ثم يهددون بنشرها إذا لم يتم تنفيذ مطالبهم. قد تشمل هذه المطالب دفع المال أو إرسال المزيد من المحتوى الشخصي. غالبًا ما تتم هذه الجرائم عبر وسائل التواصل الاجتماعي أو تطبيقات المواعدة، حيث يستغل المجرمون ثقة الضحايا أو قلة وعيهم بالمخاطر الأمنية.

3. الابتزاز بالمعلومات الشخصية (Doxxing and Information Blackmail)

في هذا النوع، يجمع المبتزون بيانات شخصية حساسة عن الضحية، مثل العناوين، الحسابات البنكية، أو رسائل البريد الإلكتروني، ثم يهددون بنشرها علنًا ما لم يتم دفع فدية. يُستخدم هذا النوع من الابتزاز بشكل شائع ضد الشخصيات العامة، الصحفيين، ورجال الأعمال، بهدف تشويه سمعته.

4. ابتزاز وسائل التواصل الاجتماعي (Social Media Blackmail)

يعتمد المبتزون هنا على اختراق حسابات الضحايا في مواقع التواصل الاجتماعي مثل فيسبوك، إنستغرام، أو تويتر، ثم يطلبون فدية مقابل استرجاع الحساب. في بعض الحالات، يقوم المبتزون بنشر محتوى مزيف أو محرج لإجبار الضحية على الاستجابة لمطالبهم. يستهدف هذا النوع من الابتزاز المشاهير والمؤثرين الرقميين بشكل خاص، نظرًا لأهمية حساباتهم على الإنترنت.

5. الابتزاز عبر البريد الإلكتروني التجاري (Business Email Compromise - BEC)

يستهدف هذا النوع من الابتزاز الشركات والمؤسسات، حيث يقوم القراصنة باختراق البريد الإلكتروني الرسمي لموظفي الإدارة المالية أو التنفيذيين، ثم يستخدمونه لإرسال طلبات مزيفة لتحويل الأموال. في بعض الحالات، يهدد المهاجمون بنشر معلومات حساسة عن الشركة ما لم يتم دفع الفدية.

6. الابتزاز بالأدلة المزيفة (Fake Evidence Blackmail)

يعتمد هذا النوع على التلاعب النفسي، حيث يدعي المبتزون امتلاكهم لمعلومات أو أدلة محرجة عن الضحية، حتى وإن كانت غير حقيقية. يتم إرسال رسائل بريد إلكتروني أو رسائل عبر وسائل التواصل تتضمن أدلة مزيفة، مع تهديد بنشرها إذا لم يتم دفع المال. يعتمد هذا الأسلوب على خوف الضحايا وعدم قدرتهم على إثبات العكس.

7. ابتزاز تعطيل الخدمة الموزع (DDoS Extortion)

في هذا النوع، يهدد المبتزون بإيقاف موقع إلكتروني أو خدمة رقمية من خلال إغراقها بعدد هائل من الزيارات غير الشرعية، مما يؤدي إلى تعطيلها. تستهدف هذه الهجمات عادةً الشركات التي تعتمد على الإنترنت في أعمالها، حيث يُجبر أصحاب المواقع على دفع المال مقابل عدم تنفيذ التهديد.

المحور الثالث: إنعكاسات و آثار الابتزاز الالكتروني على الفرد والمجتمع

يعد الابتزاز الإلكتروني من أخطر الجرائم السيبرانية التي تؤثر على الأفراد والمجتمعات بشكل عميق. فهو لا يقتصر على الخسائر المالية فقط، بل يمتد ليشمل أضرارًا نفسية واجتماعية وأمنية قد تكون لها عواقب بعيدة المدى. فيما يلي أبرز التأثيرات التي يخلفها الابتزاز الإلكتروني على الأفراد والمجتمع

1. الانعكاسات:

هناك الكثير من **النتائج الوخيمة** التي تنجم عن عمليات الابتزاز الالكتروني سواء على الفرد أو على المجتمع؛ والتي نلخصها في العناصر التالية:

1.1 ارتفاع نسب الانتحار:

ففي حال كان الضحية غير قادر على تنفيذ ما يطلب منه، يلجأ إلى وضع حد لحياته خوفا من تحمل العواقب الوخيمة الناجمة عن المضمون الابتزازي الذي يحاوره المجرم.

2.1 التفكك الأسري:

أدت عمليات الابتزاز في حالات كثيرة إلى تدمير الروابط الأسرية؛ كأن يطلق الرجل زوجته أو يضربها أو يقتلها أو يعذب ابنته أو ابنته... الخ بسبب فضيحة ما؛ كانت بذنب أو من دون ذنب، وهذا مرده إلى الاستعمال الخاطئ لوسائل التواصل الاجتماعي.

3.1 ارتفاع منسوب الجريمة بشتى أشكالها:

(السرقة، القتل، الاختطاف،... الخ) فالمبتز عادة ما يطلب من الأشخاص مبالغ مالية تدفعهم إلى اختلاس هذه الأموال وهو ما يؤدي إلى القتل وارتكاب الجرائم.

4.1 تحطيم العلاقات الاجتماعية وتشويه سُمَع الأشخاص:

إذ أصبح من السهل صناعة محتوى ابتزازي عن طريق برامج الكترونية متطورة هدفه تلطيخ الصورة الإيجابية للشخص المبتز وتشويه سمعته مما يؤدي إلى آثار سلبية اجتماعية خطيرة جدا.

5.1 الوقوع في الخيانة:

بجميع اشكالها فقد يخون الرجل دولته بسبب ويصبح عميلاً لدولة أخرى أو لأي جهاز أمني معادي أو غير معادي يهدف إلى جمع المعلومات عن شخص معين، فلطالما سمعنا قصصاً عن الموساد الإسرائيلي

وكيف يوقع بالشباب في وحل العمالة عن طريق ابتزازهم جنسياً وتصويرهم في وضعيات غير لائقة ومن خوفهم الشديد يدفعهم ذلك الى الانجرار لمستنقع العمالة والاستجابة خوفاً من النتائج[1].

2. الآثار الناجمة عن الابتزاز الالكتروني[2]:

يُعد الابتزاز الإلكتروني خطرًا يهدد الأفراد والمجتمعات على مستويات متعددة، مما يستدعي تكاتف الجهود للتوعية بمخاطره وتعزيز سبل الحماية منه. ومن خلال اتخاذ التدابير المناسبة، يمكن الحد من تأثير هذه الجريمة وضمان بيئة إلكترونية أكثر أمانًا للجميع.

1.2 الآثار الشرعية:

وهي من أعظم الآثار والنتائج السالبة التي تؤثر على المجرم وهي معصية الله تعالى والتعرض لسخطه وعقوبته سبحانه عز وجل.

2.2 الآثار النفسية:

إن الابتزاز الجنسي ينجر عنه عدة آثار نفسية تلازم الضحية طوال حياته، وقد تتطور لتستحيل ديمومة حياته؛ مما يفقده الثقة بنفسه وبالآخرين، ويجعل من الضحية شخصية غريبة الأطوار ، مضطربة وغير سوية، وقد تصاب بالأمراض النفسية المستعصية كالاكتئاب والقلق الحاد والانهيار العصبي.

ويؤثر الابتزاز الجنسي على المجني عليه بشكل خاص وعائلته بشكل عام والذين يصابون كذلك بالاضطرابات النفسية وينعكس ذلك على المجتمع وعلاقة الأفراد مع بعضهم البعض، ويكون لديهم ردة فعل أو الرغبة في الانتقام، ويحقق لها تطورا في الامراض النفسية ويدفعهم إلى الرغبة في الانتحار.

3.2 الآثار الاجتماعية:

تتنوع المخلفات الاجتماعية التي تحققها جرائم الابتزاز، وهي على مراتب وأنواع منها ما يترتب على الفرد خاصة إن كانت الضحية فتاة؛ فإن فرصها في الزواج تصبح قليلة بل شبه منعدمة لإعراض الناس عنها وربما هي من ترفض الزواج؛ إضافة إلى صعوبات التعامل مع الآخرين ورغبتها في الانتقام من المجرم ومن

[1] سايبر ون، **أضرار الابتزاز الالكتروني**،2021، متاح على: www.Cyberone.co :

[2] الغديان سليمان عبد الرزاق، وآخرون، **صور جرائم الابتزاز الالكتروني ودو افعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين** .مجلة البحوث الأمنية، المجلد 27، العدد 69، 2018.

نفسها، والشعور بنقد الذات، وشعورها بالإهانة والامتعاض والخجل والإحباط وسيطرة الأفكار السلبية عليها، وكثرة الشكوك والوساوس، وعدم القدرة على التركيز والاستقرار.

4.2 الآثار الأمنية:

يؤدي الابتزاز الالكتروني إلى زعزعة الأمن في المجتمعات ويحول المجتمع إلى غابة ملآى بالوحوش؛ بحيث لا يستطيع الفرد أن يأمن على نفسه وعائلته، فالإجرام بكل أنماطه يؤدي إلى انهيار القيم والأخلاق في المجتمع العربي والمسلم؛ ويؤدي إلى خلخلة كيانه وانتشار الفساد والرذيلة وسوء الأخلاق.

5.2 آثار الابتزاز الالكتروني على المجتمع كافة:

إن انتشار هذه الجرائم وتوسعها في ضوء التطورات التكنولوجية تؤثر على أسس وركائز بناء الأسر والمجتمعات؛ مما يجعل المجتمعات سلاحا بيد المجرمين الراغبين بهتكها وهدمها على أهلها، كونها تمس أولى حلقات المجتمع المدني وهي الأسرة وتنتقل لبقية المؤسسات التي تصبوا إلى تكوين إطار اجتماعي مسلم ومحافظ قادر على التصدي لمثل هذه الجرائم ومكافحتها.

6.2 آثار الابتزاز الالكتروني على القيم والمعتقد:

تعد القيم الميثاق الأخلاقي الذي يسير المجتمع؛ ومجتمعنا العربي الجزائري يستمد قيمه من الشريعة الاسلامية، ولما كانت عمليات الابتزاز مجرمة شرعا، تصبح عمليات الابتزاز سببا في انهيار معايير التسامح والتكافل واحترام حقوق الآخرين والستر؛ الأمر الذي ينتج عنه قيم اجتماعية مضادة وسلبية لما هو مرجو، ومنها الحقد والضغينة والكراهية وانتهاك الحرمات.

إن انتشار هذه الجرائم وتوسعها في ضوء التطورات التكنولوجية يُلقي بظلاله الثقيلة على أسس وركائز بناء الأسر والمجتمعات، حيث أصبحت هذه الجرائم تهديدًا مباشرًا للنسيج الاجتماعي، مما يجعل المجتمعات أكثر عرضة للاستغلال والاختراق من قِبل المجرمين الذين يسعون إلى تفكيكها وهدمها من الداخل. فبما أن الأسرة تُشكّل اللبنة الأولى في بناء المجتمع المدني، فإن استهدافها يُعدّ مقدمة لضرب الاستقرار الاجتماعي، إذ تنتقل تداعيات هذه الجرائم من الأفراد إلى المؤسسات الاجتماعية الأخرى، مما يُضعف قدرتها على أداء دورها في تعزيز القيم الأخلاقية وترسيخ المبادئ التي تحمي المجتمع من الانحرافات السلوكية المضرة به في كافة جوانبه.

ومع تزايد اعتماد الأفراد على التكنولوجيا في مختلف جوانب الحياة، تتعاظم خطورة هذه التهديدات، ما يفرض على المجتمعات ضرورة تطوير آليات حماية فعّالة لمواجهة هذه الجرائم، سواء من خلال التوعية

الرقمية، أو تعزيز الرقابة الأسرية، أو عبر سنّ تشريعات قانونية صارمة تضمن ردع المجرمين وحماية الضحايا. فالهدف الأساسي هو بناء مجتمع مسلم ومحافظ، قادر على التصدي لمثل هذه التحديات، من خلال ترسيخ ثقافة الاستخدام الآمن للتكنولوجيا، وتعزيز التعاون بين المؤسسات القانونية والتعليمية والاجتماعية، لضمان بيئة رقمية أكثر أمانًا واستقرارًا

المحور الرابع: نماذج من الواقع العربي (الجزائري بشكل خاص)

يعد الابتزاز الإلكتروني من الجرائم الرقمية المتزايدة في العالم العربي. فيما يلي بعض النماذج الواقعية التي عرفت انتشارًا واسعًا وأثارت الرأي العام:

1- النموذج الأول:

" **حياة** " فتاة جزائرية تبلغ من العمر 23 سنة تعرضت للقرصنة، التهديد والابتزاز بغية الوصول على الأموال. أحداث القضية تعود **إلى 2016/02/17** حينما تلقت حياة دعوة صداقة عبر الفيسبوك من طرف حساب مجهول (مستعار تحت مسمى كريم كريمو).

حاول المدعو كريم التقرب من حياة بكل الطرق بالرغم من رفضها قبول الصداقة، لكنه ظل مُصِرًا على التقرب منها فأرسل طلب صداقة مرة أخرى؛ غير أن حياة رفضت طلب الصداقة بعد مرور عدة أيام، لتقبل صداقته لاحقا بعدما أوهمها بنية التقرب منها وخطبتها.

بعد ذلك فشل كريم في كسب ثقة الفتاة والتقرب منها؛ إذ شرع هذا الأخير بالتخطيط للإيقاع بالفتاة والانتقام منها بكل الطرق والوسائل الممكنة.

كانت خطة المسمى كريم الحصول على الصور الشخصية لحياة بهدف ابتزازها وسلبها أموالها، فاقترح على صديقه المسمى سمير خطة العمل لمساعدته في العملية فوافق، ليتمكن بعد دقائق معدودات من قرصنة حساب الفتاة أين استولى على بياناتها الشخصية وصورها الخاصة.

انتهز المدعو كريم الفرصة وبدأ في تهديد حياة بنشر صورها على مختلف مواقع التواصل الاجتماعي إن لم ترضخ لطلبه، والمتمثل في إعطائه المال. أمام هذا التهديد، شعرت حياة بالخوف والارتباك، فسارعت إلى الاتصال بصديقتها لإعلامها بالأمر وطلب النصيحة.

بدورها، اقترحت سيرين – صديقة حياة – أن تتعامل مع الموقف بحذر، حيث نصحتها بتحديد موعد مع صاحب الحساب بحجة تسليمه المبلغ المالي، وذلك بهدف كشف هويته والتأكد من شخصيته. كان

الهدف من هذه الخطة هو جمع أدلة ملموسة تساعد على اتخاذ الإجراءات اللازمة ضد المبتز، سواء عبر الإبلاغ عنه للجهات المختصة أو إيجاد طريقة لردعه وإيقاف تهديداته المتكررة

في حدود الساعة 15:30 قررت حياة الذهاب للمكان المتواجد فيه كريم بمعية صديقتها لمنحه المال، حين وصولها إلى المكان المحدد، اختبأت – سيرين – لتراقب صديقتها من بعيد. بعد وصول كريم وافقت حياة منحه المال شريطة حذفه لصورها الشخصية.

ابتزاز الشاب للفتاة أدخلها في حالة هستيرية وضغوطات نفسية؛ بحيث لم يكتف بهذا بل زاد طمعه في الحصول على مبالغ مالية أخرى؛ وهنا قررت الفتاة تقديم شكوى للسلطات الأمنية للقيام بمهامها.

2- النموذج الثاني:

انتحل المسمى محمد صفة المدعوة حياة وراح يتحدث مع صديقتها ريما عبر الفيسبوك، طالبا من ريما منحه مبلغا ماليا بحكم أن والد الفتاة في حال حرجة بالمشفى. كانت حياة في منزلها رفقة زوجها يتبادلان أطراف الحديث؛ وبعد خروجه من المنزل تلقت اتصالا هاتفيا من ريما بخصوص إرسالها المبلغ المالي الذي طلبته منها عبر الفيسبوك؛ لتتفاجأ حياة مما قالته ريما، وراودتها شكوك أن حسابها القديم عبر الفيسبوك تعرض للقرصنة، فقامت بمحاولة فتحه للتأكد من الأمر.

حاولت حياة الدخول إلى حسابها إلا أن الرقم السري قد تغير، قامت بعدها بتشكيل رقمها القديم للاتصال بصاحبه قصد مساعدتها لاسترجاع الرقم السري الخاص بالفيسبوك، عندئذ قام صاحب الشريحة (محمد) بقطع المكالمة وطلب من حياة عدم الاتصال به مجددا. في نفس اليوم قامت حياة بشرح الوقائع بأكملها لزوجها أين طالبها برقم هاتفها القديم للاتصال به إلا أن محمد لا يجيب.

المدعو سفيان هو الآخر انتحل صفة حياة عبر الفيسبوك وراح يتكلم مع لينا بحساب حياة، وفي كل مرة كان سفيان يطلب من لينا إرسال صورها الشخصية بغرض ابتزازها، وبعد حصوله على الصور عاود الاتصال بها طلبا للمال، لتتفاجأ لينا أن المتصل شاب وليس صديقتها حياة مما جعلها تدخل في حالة هستيرية ونفسية صعبة.

3- النموذج الثالث من بعض الدول العربية:

في مصر، انتشرت عدة قضايا تتعلق بابتزاز المشاهير والشخصيات العامة. في إحدى القضايا الشهيرة، تم تسريب بيانات شخصية لممثلة معروفة، حيث هددها المبتزون بنشر معلومات حساسة إن لم

تدفع لهم مبلغًا ضخمًا. بعد تقديم بلاغ رسمي، تمكنت وحدة مكافحة الجرائم الإلكترونية من القبض على العصابة، وتبين أنها كانت تستهدف شخصيات مشهورة أخرى بنفس الأسلوب.

في العراق، تصاعدت حوادث الابتزاز الإلكتروني، حيث يتم استهداف الفتيات بشكل خاص عبر مواقع التواصل الاجتماعي. في إحدى الحالات، تعرضت فتاة جامعية للابتزاز بعد أن أرسلت صورًا شخصية لصديق تعرفت عليه عبر الإنترنت. قام الصديق المزعوم بتهديدها بنشر الصور إذا لم تدفع له المال. وبعد أن حاولت الضحية الانتحار بسبب الضغط النفسي، تدخلت عائلتها وقدمت بلاغًا رسميًا، مما ساهم في القبض على الجاني.

في السعودية، تم تسجيل العديد من حالات الابتزاز عبر تطبيق "سناب شات"، حيث يقوم المبتزون بإيهام الضحايا بأنهم أصدقاء موثوقون، ثم يحصلون على صور أو معلومات شخصية لاستغلالها لاحقًا. في إحدى القضايا، تم استدراج فتاة عبر "سناب شات"، وبعد أن أرسلت صورًا خاصة، بدأ المبتز بتهديدها بنشرها إن لم تدفع له المال. لجأت الضحية إلى الجهات الأمنية التي تمكنت من تحديد هوية الجاني والقبض عليه متلبسا مع مصادرة جميع حساباته المزعومة.

خاتمة:

في ختام هذا البحث، يمكن التأكيد على أن الابتزاز الإلكتروني لم يعد مجرد جريمة فردية عابرة، بل أصبح ظاهرة متفاقمة تتطلب استجابة جماعية وحلولًا متكاملة. فالمبتزون لا يستهدفون فقط الأموال، بل يسعون إلى تدمير حياة الضحايا على المستويات النفسية، والاجتماعية، وحتى الجسدية، مما يجعلهم يعيشون تحت وطأة الضغوط والتهديدات المستمرة. إن نماذج مثل "حياة" و"لينا" ليست سوى حالات محدودة ضمن شبكة واسعة من الضحايا الذين وقعوا فريسة لهذه الجريمة، مما يؤكد الحاجة إلى تدخلات أكثر صرامة وإجراءات وقائية أكثر كفاءة.

لقد أصبح الابتزاز الإلكتروني من أخطر الجرائم السيبرانية بسبب سهولة انتشاره، وعدم حاجة المجرم إلى التواجد المادي بالقرب من الضحية، فضلًا عن استخدام تقنيات متطورة تتيح له التخفي والتهرب من الملاحقة الأمنية. هذه العوامل جعلت الابتزاز الرقمي يشكل تهديدًا مباشرًا ليس فقط للأفراد، بل للمجتمعات بأكملها، حيث يسهم في نشر الخوف وانعدام الثقة في الفضاء الإلكتروني، وهو ما يؤثر سلبًا على تفاعل الأفراد مع التكنولوجيا وعلى استقرار العلاقات الاجتماعية والمهنية.

ومن هذا المنطلق، أصبح من الضروري إعادة النظر في الأطر القانونية لمكافحة الابتزاز الإلكتروني، بحيث يتم تحديث القوانين لتشمل جميع أشكال هذه الجريمة، وتحديد عقوبات صارمة للمجرمين، إلى جانب تسهيل عملية الإبلاغ عن الجرائم الرقمية دون خوف من الوصمة الاجتماعية. كما يجب على الحكومات تطوير وسائل أكثر تطورًا لمكافحة هذه الجرائم، من خلال دعم وحدات مكافحة الجرائم الإلكترونية، وتعزيز التعاون الدولي في تتبع المبتزين.

ولا يقتصر الحل على التشريعات فقط، بل يجب أن يشمل أيضًا **تعزيز الوعي الرقمي** لدى مختلف الفئات المجتمعية، خاصة الشباب والمراهقين الذين يشكلون الفئة الأكثر عرضة للاستهداف. فمن خلال برامج التوعية والتثقيف الرقمي، يمكن تعزيز ثقافة الاستخدام الآمن للإنترنت، وتعليم الأفراد كيفية حماية معلوماتهم، والتعامل مع أي محاولات ابتزاز بطريقة صحيحة دون الوقوع في فخاخ المجرمين.

وختامًا، فإن القضاء على الابتزاز الإلكتروني أو على الأقل الحد من آثاره، يتطلب **تكاتفًا مشتركًا بين الحكومات، والمؤسسات الأمنية، والمجتمع المدني، والأفراد أنفسهم**. فبقدر ما يمكن أن تكون التكنولوجيا وسيلة للابتزاز والاستغلال، يمكن أيضًا أن تكون أداة للحماية والتوعية وتعزيز الأمن السيبراني. إن مواجهة هذه الجريمة تتطلب يقظة مستمرة، وجهودًا متواصلة لضمان بيئة رقمية أكثر أمانًا، تحمي الأفراد وتحفظ حقوقهم وكرامتهم في العالم الرقمي المتسارع الذي نعيش فيه.

قائمة المراجع:

أولًا: الكتب

1. الغالبي، رامي أحمد، **جريمة الابتزاز الالكتروني وآلية مكافحتها في جمهورية العراق** (ط1)، دار الكتب والوثائق، بغداد: العراق، 2019.

ثانيًا: الرسائل الجامعية

1. الشمري، فلاح، **جريمة ابتزاز النساء ودور جهاز الحسبة في مكافحته**، رسالة ماجستير غير منشورة، جامعة مؤتة، 2008، الأردن.

ثالثًا: المقالات العلمية

1. الغديان، سليمان عبد الرزاق، وآخرون، **صور جرائم الابتزاز الالكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين** .مجلة البحوث الأمنية، المجلد 27، العدد 69، 2018.
2. زيوش، سعيد، **ظاهرة الابتزاز الالكتروني وأساليب الوقاية منها- قراءة سوسيولوجية وأراء نظرية** . مجلة العلوم الاجتماعية، العدد 22، 2017.
3. عراب، مريم .(2021) .**جريمة التهديد والابتزاز الالكتروني** .*مجلة الدراسات القانونية المقارنة*، *7*(1)، 1210-1213.

رابعًا: بحوث المؤتمرات والندوات

1. العيد، نوال، **بحوث ندوة الابتزاز؛ المفهوم- الأسباب- العلاج** .بحث مقدم لمركز باحثات لدراسات المرأة، 1435 هـ، الرياض.
2. بن حميد، صالح، **بحوث ندوة الابتزاز؛ المفهوم- الأسباب- العلاج** .بحث مقدم لمركز باحثات لدراسات المرأة، الرياض، 1432هـ.

خامسًا: المصادر الإلكترونية

1. سايبر ون .(2021) .**أضرار الابتزاز الالكتروني** .متاح على.www.Cyberone.co :