تاريخ الاستلام: 2023/11/05م تاريخ القبول: 2023/11/25 تاريخ النشر: 2023/12/31م

مجلة علمية محكمة نصف سنوية – تصدر عن كلية القانون بجامعة الزاوية
العدد الثالث والعشرون – ديسمبر/ 1445هـ/ 2023
Journal of Legal and Sharia Sciences, Issue (23) (1445 AH/2023م)
National Deposit No. 529 – 2023 رقم الإيداع الوطني529 . 2023

# دور السياسة الجنائية الدولية في مكافحة جرائم الابتزاز الإلكتروني

**عبد الله رمضان بنيني**
**الدرجة العلمية: أستاذ مشارك، قسم القانون العام – كلية القانون – جامعة الزاوية**
**الزاوية – ليبيا**
**Email: : a.bnene@zu.edu.ly**

**الملخص:**

يهدف البحث إلى التطرق لجريمة الابتزاز الإلكتروني وفقاً لما تفتضيه السياسة الجنائية الدولية سواء في جوانبها الموضوعية، أو الإجرائية ولحداثة، وحرصت الكثير من التشريعات الوطنية علي النص عليها وتجريمها، ومن خلال هذه الدراسة توصلت إلى عدة نتائج، أهمها:

1- جريمة الابتزاز الإلكتروني صورة من صور الجريمة الإلكترونية حيث تتم باستخدام شبكات المعلومات، أو الأجهزة الحديثة، وتطبيقاته.
2- لجريمة الابتزاز الإلكتروني طرق مختلفة في ارتكابها كما أن لها وسائل أيضاً خاصة بها تختلف عن الابتزاز التقليدي.
3- جريمة الابتزاز الإلكتروني جريمة عابرة للحدود، فقد يكون المبتز في دولة بالعالم، ويقوم بابتزاز ضحية في أقصى العالم.

**الكلمات المفتاحية:** السياسة الجنائية الدولية، جرائم، الابتزاز الإلكتروني

# The role of international criminal policy in combating cyber-extortion crimes

**Abdullah Ramadan Benini**
**Faculty of Law- Zawia University**
**Azzawia -Libya**
**Email: : a.bnene@zu.edu.ly**

**ABSTRACT**

The research aims to address the crime of electronic blackmail in accordance with what is required by international criminal policy, whether in its substantive or procedural aspects and due to its modernity, and many national legislations were keen to stipulate and criminalize it, and through this study I reached several results, the most important of which are:

1- The crime of electronic blackmail is a form of electronic crime that is carried out using information networks, modern devices, and its applications.
2- The crime of electronic blackmail has different ways of committing it, and it also has its own methods that differ from traditional blackmail.
3- The crime of electronic blackmail is a cross-border crime, as the blackmailer may be in a country in the world, and blackmail a victim in the farthest part of the world.

**Keywords**: international criminal policy, crimes, electronic blackmail

**المقدمة.**

تعد الجريمة الإلكترونية أحدث الجرائم المعلوماتية المعاصرة، والعابرة للحدود، حيث ظهرت مؤخراً، وانتشرت مع تطور التقدم الإلكتروني، وشبكات المعلومات على الانترنت، ومما زاد من أهمية هذه الجريمة على المساحة الدولية اعتمادها على تقنيات عالية التقدم تؤدى إلى صعوبة اكتشافها، ومعرفة مرتكبيها، وإثباتها؛ لأنها تتسم بطابع الحيلة، والدهاء، و تجعل من الصعب الكشف عنها، والوصول إلى الدليل المادي الذى يدين مرتكبيها، لذلك أخذت مدى دولي كبير بدأ بقرار مؤتمر الأمم المتحدة الثامن لمنع الجريمة، ومعاملة السجناء المنعقد في "هافانا" في عام 1990 بشأن الجرائم ذات الصلة بالكمبيوتر حيث حث القرار الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال أجهزة الكمبيوتر، وتجريم هذه الأفعال جنائياً، وأكدت التوصيات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في "البرازيل" في عام 1994على تحديد أنواع

الجرائم التي ترتكب عبر استخدام أجهزة الحاسوب، وظلت الجهود الدولية تبذل مسعاها حتى تم عقد اتفاقية "بودابست" لمقاومة الجرائم المعلوماتية، والاتصالات في 2001 في العاصمة المجرية "بودابست" ، حيث وقع عليها ثلاثون دولة من الاتحاد الأوربي، بالإضافة إلى كندا، واليابان، وجنوب أفريقيا، وأمريكا، ونتج عن هذه الاتفاقية صدور قانون "الأونستيرال" النموذجي في الخامس من يوليو 2001 بتحديد نظام تجارة الإلكترونيات دولياً، ومع غزو الانترنت العالم ارتفعت معدلات الجرائم الإلكترونية، وتعددت أساليبها، وأنواعها من جرائم تجسس، وجرائم القرصنة، وجرائم الإرهاب، وغسيل الأموال، والمخدرات، وغيرها من الجرائم الأخرى، إلى أن ظهرت جريمة ترتكب تعدياً على الحياة الخاصة للمواطنين على مستوى العالم، وتؤدي إلى ابتزازهم، والحصول على مقابل مادي، أو معنوي استغلالاً لهذه التقنية وهى: جريمة الابتزاز ،وبالرغم أنها ليست من الأفعال الإجرامية الجديدة لوجودها قديماً، إلا أنها تطورت لأساليب متقدمة، وفقاً لتقنيات عالية تجعل من الصعب اكتشافها، وإقامة الدليل المادي على مرتكبيها، لذلك أخذت هذه الجريمة حيزاً كبيراً في تشريعات الكثير من الدول، وأصدرت قوانينها لتجريم هذه الجرائم، وغيرها من الجرائم الأخرى التي ترتكب عبر الانترنت، وكانت مصر من الدول الأولى في الشرق الأوسط في تجريم هذه الجرائم بموجب القانون 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، وتضمن هذا القانون تجريم جرائم الاحتيال والاعتداء على بطاقات البنوك، والخدمات، وأدوات الدفع الإلكتروني، وكذلك الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة، والمحتوى المعلوماتي غير المشروع، ولذلك سوف نتناول في هذا البحث السياسة الجنائية التي نظمتها الدول في مكافحة جريمة الابتزاز الإلكتروني كنموذج لمكافحة الجرائم الإلكترونية.

**أولاً:- أهمية البحث:-**

تتمثل أهمية البحث في حداثة جريمة الابتزاز، ولم تتعرض الكثير من التشريعات الوطنية لتجريمها رغم انتشارها، وتهديدها للحياة الخاصة للمواطنين، وآثارها الاجتماعية الخطيرة خاصة في ظل المجتمعات العربية، والإسلامية.

**ثانياً:- إشكالية البحث:-**

تعتمد إشكالية هذا البحث على الوقوف على طبيعة هذه الجريمة القديمة الحديثة، وأساليب ارتكابها والاجراءات الجنائية التي يتعين اتخاذها للحد من انتشارها، وهل تلك الاجراءات كافية للحد منها ومنع انتشارها؟

**ثالثاً:- خطة البحث:-**

سوف نقسم هذا البحث على مبحثين هما:-

المبحث الأول:- السياسية الجنائية الموضوعية في تجريم الابتزاز الإلكتروني.

المبحث الثاني:- السياسية الجنائية الإجرائية في إثبات جرائم الابتزاز الإلكتروني.

**المبحث الأول: السياسية الجنائية الموضوعية في تجريم الابتزاز الإلكتروني**

يعد الابتزاز في حد ذاته جريمة قديمة نوعاً ما، لكنها تطورت لتصبح من أكثر الجرائم قسوة، خصوصاً بعدما اتخذت منحنى أكثر خطورة بسبب الثورة التكنولوجية، والمعلوماتية، حيث استغل البعض هذه التكنولوجيا للاعتداء على خصوصية الآخرين، وتهديدهم بما يحقرهم، أو يضعهم في موقف صعب في المجتمع، حيث يتسلل المجرم إلى تلك الخصوصية ضارباً عرض الحائط أي خطوط حمراء، واستغلال ما وصل إليه كوسيلة للضغط، والتهديد للضحية، ولا يخفى ما لهذا التطور من فوائد من النواحي الاقتصادية، والسياسية، والعلمية إلا أنه لم يخلُ من مواطن الخلل، فقد مهد الطريق لظهور نوع من المجرمين يستخدمون هذه التقنيات لتنفيذ جرائمهم بواسطتها، لهذا فإن الابتزاز الإلكتروني يعد: أي طريقة تستخدم بواسطة وسائل الاتصال التكنولوجية الحديثة، وبالعادة يقوم المجرم باستدراج الضحية عبر التواصل الاجتماعي، أو بعض تطبيقات الهواتف الذكية، لإغرائهم بالظهور في أوضاع غير لائقة، وتصويرهم دون علمهم، وتهديدهم بنشر الصور، ومقاطع الفيديو، وابتزازهم، ولقد أصبحت جريمة الابتزاز الإلكتروني إحدى صور الجرائم الإلكترونية التي تخترق المجتمع، وتهدد دعائمه لذلك سوف نقسم هذا المبحث على مطلبين:-

المطلب الأول:- التعريف بجريمة الابتزاز الإلكتروني، وأهميتها دولياً.

المطلب الثاني:- صور، وأنواع جرائم الابتزاز الإلكتروني.

**المطلب الأول: التعريف بجريمة الابتزاز الإلكتروني، وأهميتها دولياً**

قد انتشرت خلال الفترة الأخيرة جرائم الابتزاز الإلكتروني التي أثرت على جميع أطياف المجتمع ذكوراً، وإناثاً، وهذا يساعد في سرعة انتشارها في كل مكان، وقد ظهرت شكاوى كثيرة في الآونة الأخيرة من عمليات الابتزاز، وخاصة من النساء اللاتي يتعرضن باستمرار لعمليات الابتزاز من قبل الشباب، وذلك من خلال التهديد بعرض صورهن في مواقع التواصل الاجتماعي، ويلاحظ: أن هذه الجرائم في تزايد مستمر بين الشباب، والفتيات وكذلك ضحايا هذه الجرائم، والأمر الذى يتطلب مواجهة، ومكافحة هذه الجريمة، والبحث عن أسباب ظهورها، وانتشارها.(1)

فالتحقيق في الجرائم الإلكترونية يتطلب القيام بإجراءات، وأعمال للتحقيق خارج حدود الدولة مثل تفتيش المواقع الإلكترونية، أو تفتيش الأجهزة الإلكترونية –المادية- للعثور على البيانات، أو المعلومات، أو إلقاء القبض على المطلوبين، أو معاينة مسرح الجريمة، ولذلك يحتاجون إلى تعاون دولي ملموس على أرض الواقع وهذا ما يعطى لهذه الجريمة أهمية دولية.(2)

لا شك أن هذه الجرائم ما ولدت إلا نتيجة إساءة استخدام وسائل الاتصال الإلكترونية التي ظهرت على الساحة الدولية، ولم يكن لها وجود من قبل، ونتعرض تفصيلاً لتعريف، وأهمية هذه الجريمة على النحو التالي:-

**الفرع الأول:- التعريف بجريمة الابتزاز الإلكتروني.**

**أولا :- تعريف الجريمة الإلكترونية:-** تعرف الجريمة الإلكترونية من منظور الفقه القانوني على: أنها سلسلة من الأعمال، والأنشطة التي يعاقب عليها القانون التي تربط السلوك الإجرامي بالثورة التكنولوجية، أو " نشاط إجرامي يمثل هجوماً على برنامج الكمبيوتر " علاوة على ذلك، يعرفها البعض على أنها: "جريمة" ترتكب إذا استخدم شخص ما معرفته بالكمبيوتر لفعل شيء غير قانوني.(3)

الجريمة الإلكترونية هي: فعل غير مشروع ناتج عن" إرادة آثمة يقرر لها القانون عقوبة، وهى أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية، وكما

تعرف الجرائم الإلكترونية بأنها " ذلك النشاط الإجرامي الذى يتم ارتكابه عن طريق استخدام الانترنت، وهى ذلك النوع من الجرائم الذى يهدف إلى التحرش، أو إيذاء الآخرين عن طريق توظيف تكنولوجيا المعلومات، والاتصالات كالكمبيوتر، والهواتف الخلوية، والكمبيوترات اللوحية، وغيرها من التكنولوجيا الحديثة، وهى: الاعتداء غير القانوني الذى يرتكب بواسطة المعلومات الحاسوبية بهدف تحقيق الربح. وهى: أيضاً كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات، أو بنقلها، وقد عُرفت بأنها: الممارسات التي توقع ضد فرد، أو مجموعة مع توفير باعث إجرامي بهدف التسبب بالأذى لسمعة الضحية عمداً، أو إلحاق الضرر النفسي، والبدني به سواءً أكان ذلك بأسلوب مباشر، أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالأنترنت، وما تتبعها من أدوات كالبريد الإلكتروني، وغرف المحادثة والهواتف المحمولة، وقد عرفت بأنها كل اعتداء يقع على نظم الحاسب الآلي، وشبكاته، أو بواسطتها.

**ثانياً:- تعريف جريمة الابتزاز الإلكتروني** :- الابتزاز الإلكتروني: هو الإكراه المعنوي للضحية للحصول على مكاسب مادية، أو معنوية، وذلك بإتباع أساليب الترهيب، والتهديد بنشر أسراره، والكشف عن معلوماته الخاصة أمام الجميع، فهي جريمة الاعتداء على حياة الآخرين الخاصة، حيث يعد الابتزاز الإلكتروني عملية تهديد، وترهيب للضحية بنشر صور، أو مواد فيلميه، أو تسريب معلومات سرية للضحية مقابل دفع مبالغ مالية، أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتز، فالابتزاز الإلكتروني هو: كل تهديد يقوم به الجاني، أو وسيط يتم عبر وسيلة إلكترونية، ويؤثر في نفسية المجنى عليه، أو شخص عزيز لديه، ويدفعه إلى القيام بما طلبه منه الجاني، أو كلفه به سواء أكان مشروعاً، أو غير مشروع، وبتحديد من هو الشخص العزيز لديه قد يكون مصدره القانون، والواقع حيث إن مجرد إحساس الشخص بالمسؤولية ناحيته غير كاف لتوافر الابتزاز، فجريمة الابتزاز الإلكترونية هي: إحدى صور الجرائم الإلكترونية (Cyber-crimes) وهى تتكون من مقطعين هما: الجريمة (Crime)، والمقطع الآخر (Cyber) وهى السيبرانية، أو الفضاء، ويستخدم مصطلح الإلكترونية لوصف فكرة ان الجريمة فهي تلك الأفعال المخالفة للقانون، وقد اصطلح على تعريف الجرائم الإلكترونية بأنها: " المخالفة التي ترتكب ضد

الأفراد أو المجموعات من الأفراد بدافع الجريمة، وبغرض إيذاء سمعة الضحية، أو أذى مادي أو عقلي مباشر، أو غير مباشر باستخدام شبكات الاتصال مثل الانترنت، ويعرف الباحث الابتزاز الإلكتروني بانه: " جريمة من الجرائم التي يحيط بها الغموض يستخدم فيها التهديد بكشف معلومات معينة عن شخص المجنى عليه نفسه، أو من يهمه، وفعل ما يؤدى إلى ايلامه، وتدميره في حالة لم يقوم بالرضوخ، والاستجابة لطلبات الجاني، وكل هذا باستخدام التكنولوجيا في التطبيقات الإلكترونية بالأجهزة الذكية، أو الحواسيب وكل ما يشبهها".

**الفرع الثاني:- الأهمية الدولية لجريمة الابتزاز الإلكتروني:-**

لجريمة الابتزاز الإلكتروني أهمية عالمية، ودولية كبيرة حيث تمثل ظاهرة إجرامية عالمية من جانب، ومن جانب آخر تعد هذه الجريمة اعتداء على الحقوق، والحريات العامة المصونة دولياً، ونوضح ذلك تفصيلاً على النحو التالي:-

**أولاً:- جريمة الابتزاز الإلكتروني ظاهرة إجرامية عالمية:-**

تعد جريمة الابتزاز الإلكتروني من نتاج التقدم العلمي والتكنولوجي المعاصر، وتمثل ظاهرة تخترق المجتمع الدولي، وتهدد دعائمه، وتضرب أهدافه، فكافة النظم الدولية تسعى جاهدة إلى تحقيق الأمن، والأمان للأفراد، وتأمين حياتهم، فإذا بهذه الجريمة التي تخترق كافة المجتمعات المتحضرة وتلقى بآثارها السلبية على المجتمع الدولي بأسره لأنها جريمة عابرة للحدود، وارتباطها بالأنترنت، ووسائل التواصل الاجتماعي المنتشر حول العالم فلا يوجد مكان في العالم حالياً لم تدخله خدمات، ونظم الاتصالات الحديثة، بل تتنافس الشركات العالمية ليل نهار على توفير الخدمة، وتطويرها، ومن ثم فإن جريمة الابتزاز الإلكتروني عندما ترتكب تؤثر ليس فقط في الضحية الخاضعة للابتزاز بل بتأثر بها كافة الأفراد في كافة دول العالم سواء كان الضحية معروفاً، أو غير معروف، بالإضافة إلى أن تتبع أدلة إثبات هذه الجريمة تستوجب البحث، والتحري في كافة دول العالم فليس فقط أن كافة دول العالم تتأثر بسلبيات هذه الجريمة، بل تكمن آثارها السلبية في صعوبة معرفة

الفاعل، وإثبات جرمه، بل وتقديمه للقضاء لينال عقوبة عن أفعاله لعدم توافر التجريم في معظم النظم القانونية لدول العالم مما يسهل له الإفلات بجرمه دون عقاب.(4)

**ثانياً:- جريمة الابتزاز الإلكتروني اعتداء على الحقوق، والحريات العامة:-**

تمثل جريمة الابتزاز الإلكتروني انتهاكاً صارخاً للحقوق والحريات العامة للأفراد، والتي تحرص التشريعات الدولية، ومواثيق حقوق الإنسان العالمية، والاقليمية حماية تلك الحقوق، والمحافظة على تلك الحريات حيث يدفع الضحية المجنى عليه تحت تهديد، واكراه مادى، أو معنوي يمارسه الجاني عليه من خلال استغلال التقنيات الحديثة التي توصل إليها التقدم العلمي، وإباحته، فيتم استغلاله للابتزاز غير المشروع للضحية، الأمر الذى يمثل اعتداء على حق الإنسان، وحريته، وحرمة حياته الخاصة، وصيانة عرضه، وجسده، وحياته الشخصية، الامر الذى يترتب على هذه الجريمة إهداراً لحيائه، وكرامته، وخضوعه مسلوباً للإرادة لسيطرة الجاني مسلوباً للإرادة ذليلاً نفسياً ومعنوياً، مما يشكل معه جريمة ضد الإنسانية يستوجب المعاقبة عليها بأغلظ العقوبات، لتحقيق الردع العام والخاص لجميع من تسول له نفسه ارتكابها، واستغلال التقدم الإلكتروني في تنفيذ جريمته، وإخفاء أدلة ثبوتها، وهروب مرتكبها من العقاب، والمسؤولية الجنائية تحت مظلة حرية الرأي، والفكر، والعقيدة، لذلك نادت الأمم المتحدة بتجريم هذه الجريمة في تشريعات الدول الأعضاء في المنظمة، وأطلقت العديد من النداءات من خلال ما تبرمه من اتفاقيات دولية ذات الصلة.(5)

**المطلب الثاني: صور، وأهمية جريمة الابتزاز**

تتعدد صور جريمة الابتزاز الإلكتروني في شكلها النفسي، أو العاطفي، أو كما يطلق عليها البعض جرائم الابتزاز المعنوي، أو العاطفي، أو في شكل آخر أكثر إجراماً، وهى جريمة الابتزاز المادي يكون هدفها مادياً، وليس نفسياً، أو معنوياً، كما تتعدد أنواع هذه الجريمة فهناك أنواع كثيرة يتم ارتكابها لهذه الجريمة من خلال استخدام الحاسوب كأداة جرائم اباحية، أو تزوير للأموال، والمستندات، ونوع آخر يعتمد على استخدام الانترنت، والتقنيات المتقدمة من قرصنة، وتدمير متعمد، ورسائل ضارة، وغيرها، وهذا التعدد للصور، والأنواع نخصص له هذا المطلب تفصيلاً على النحو التالي:-

**الفرع الأول:- صور جريمة الابتزاز الإلكتروني:-**

تتجسد صور جريمة الابتزاز الإلكتروني في صورتين: حسب الهدف الذى ترتكب من أجله فإذا كان هدفها معنوياً عاطفياً فهي تأخذ صورة الابتزاز العاطفي، إذا كان هدفها مادياً فهي تظهر في شكل جريمة الابتزاز المادي ونتعرض لذلك وفقاً التفصيل التالي:-

**أولاً:- الابتزاز العاطفي:-** يقصد به موقف، أو كلام يأخذه ممارس الابتزاز ليسبب لدى الطرف الآخر إحساس بالخجل، أو الخطأ، أو ليحمله مسؤولية لا يتحملها، ويستخدم الابتزاز العاطفي لتحقيق سيطرة عاطفية، ونفسية على الآخرين، وليجعل الآخر يشعر أنه مدين، أو مذنب في حق الشخص الآخر الذى يبتزه وهو أسلوب دنيء في التعامل مع الآخرين، ويتألف الابتزاز العاطفي من خلال ست مراحل هي: الطلب، والمقاومة، والضغط، والتهديد، والإذعان، والتكرار.(6)

**ثانياً: الابتزاز المادي:-** وهو محاولة الحصول على مكاسب مادية عن طريق الإكراه، استغلالاً لحالة الضعف، والابتزاز لضعف العلاقة، وهشاشتها بين ضعاف النفوس، كما يبين تأثير المال على هذه النفوس، وكما يضحى الصديق بصديقه، ويصنف علماء القانون هذه الصورة في جوانبها القانونية التالية:-

أ- جريمة استخدام الوسائل التكنولوجية لارتكاب أعمال إجرامية، بما في ذلك تزوير الأموال عن الماسحات الضوئية، حيث أن لهذا النوع إطاره القانوني في معظم التشريعات الوطنية.

ب- باستخدام التكنولوجيا الحديثة لارتكاب جرائم، يمكنك إنشاء مواقع إباحية، والانضمام إلى الجمعيات الإرهابية، وشراء وبيع الأسلحة، وشراء وبيع المخدرات، وشراء وبيع أسرار الآخرين عن طريق اختراق مواقع الويب، أو أجهزة الكمبيوتر، أو استخدام بطاقة ائتمان لانتحال شخصية شخص آخر، وفى عالم افتراضي رقمي تفرضه التطورات التكنولوجية، قد يفاجئ الشخص نفسه في بيئة إجرامية حيث تسرق أمواله دون أي دليل ملموس.(7)

ج- انتهاكات الملكية الفكرية للغير من خلال عرض المنتجات الفكرية باستخدام مغاير لاسم المؤلف الحقيقي، وتشويه السمعة وهو نوع من الجرائم الإلكترونية يسعى القائم على تلك

الجرائم في تحقيقها من خلال نشر بعض التعليقات، أو الصور التي تعمل على إهانة الطرف الآخر ما يجعله في حالة اضطراب، أو قلق يؤدى به الحال إلى الانعزال عن الأسرة، والأصدقاء.(8)

**الفرع الثاني:- أنواع جريمة الابتزاز الإلكتروني:-**

لجرائم الابتزاز الإلكتروني أنواع كثيرة يصعب حصرها لتنوع السلوك الإجرامي، وتطور التقنيات الحديثة، واختلاف ثقافة الشعوب، ودرجة تقدم الدول، وحيازتها لوسائل التقنية الحديثة لذلك سوف نتناول الأنواع الأكثر شيوعاً في العالم، والكثير من دول المجتمع الدولي على النحو التالي:-

**أولاً:- الجرائم التي يتم استخدام الكمبيوتر كأدوات لتنفيذها:-** وهى تنتمى إلى الجرائم المادية مثل استخدام الأطفال في عرض المواد الإباحية من خلال عرض كتب ونصوص أو مواد مرئية تحتوى على مواد مخلة الغرض منها إثارة الرغبات الجنسية لدى الآخرين من خلال عرض المواد غير الأخلاقية المتعلقة بالأطفال وهي تأخذ إحدى الصور التالية كما قدمنا:-

أ- جريمة استخدام الوسائل التكنولوجية لارتكاب أعمال إجرامية، بما في ذلك تزوير الأموال عن الماسحات الضوئية، حيث أن لهذا النوع إطاره القانوني في معظم التشريعات الوطنية.

ب- استخدام التكنولوجيا الحديثة لارتكاب جرائم، يمكنك إنشاء مواقع إباحية، والانضمام إلى الجماعات الإرهابية، وشراء وبيع المخدرات، وشراء، وبيع الأسلحة، وشراء وبيع أسرار الآخرين عن طريق اختراق مواقع الويب، أو أجهزة الكمبيوتر، أو استخدام بطاقة ائتمان لانتحال شخصية شخص.

**ثانياً:- الجرائم التي يكون فيها الكمبيوتر هو الهدف الذى يسعى إليه مرتكبو الجرائم الإلكترونية:-** هناك نوعية جديدة من الجرائم المرتبطة بشكل أساس بالكمبيوتر والانترنت على سبيل المثال القرصنة، والاستخدام غير مرخص لبرامج، وتطبيقات الكمبيوتر، والقيام بنشر الفيروسات الضارة بأجهزة الآخرين، أو التجسس على محادثات الآخرين على الانترنت وغيرها من السلوكيات غير اللائقة التي تضر بالغير معنوياً، ومادياً وهى:-

أ- القرصنة الرقمية:- إن تطوير الكمبيوتر أدى إلى الانتشار الواسع في استخدام الانترنت، الذى سمح بتبادل المعلومات بين الناس، مما أدى لاحقاً إلى بعض السلوكيات الإجرامية من بينها القرصنة الرقمية.

ب- التدمير المتعمد:- ويقصد به استخدام الانترنت للولوج إلى الشركات، والمنظمات، ومن ثم القيام بمسح، أو نسخ بعض المعلومات المهمة التي تضر بالمنظمة، وعملائها.

ج- الرسائل الضارة:- وهي تعد من أهم أشكال الجرائم الإلكترونية، وأكثرها انتشاراً والتي يمكن من خلالها اختراق كمبيوتر الضحية عن طريق تلك الرسائل التي تكون في ظاهرها أنها رسائل إعلانية، وعند القيام بفتحها يتم إصابة كمبيوتر الضحية بزرع الفيروسات وبرامج التجسس.(9)

بالإضافة إلى وجود جرائم ملحقة وناتجة عن الجرائم السابقة وهى:-

1. جرائم الحاسوب الاقتصادية وتشمل:- الاحتيال المعلوماتي، التجسس المعلوماتي في قطاع الأعمال، قرصنة برامج الحاسوب، الإتلاف المعلوماتي، جريمة الدخول غير المصرح به إلى نظام الحاسوب، سرقة الخدمات، الجرائم المتعلقة باستخدام الحاسوب في إخفاء تلاعب مديري المؤسسات المالية.
2. الجرائم المتعلقة بانتهاك حرمة الحياة الخاصة، باستخدام بيانات شخصية غير صحيحة، جمع وتخزين بيانات صحيحة على نحو غير مشروع، الإنشاء غير المشروع وإساءة استخدام البيانات الشخصية، مخالفة القواعد الشكلية التي تدخل في نطاق الحماية التشريعية لخصوصية المعلومات.
3. الجرائم المعلوماتية التي تهدد المصالح القومية، أو السلامة الشخصية للأفراد، معلومات تتعلق بالأمن القومي، الجرائم المعلوماتية التي تهدد السلامة الشخصية للأفراد

**المبحث الثاني: السياسة الجنائية في إثبات جرائم الابتزاز الإلكتروني**

يقصد بالسياسة الجنائية: مجموع السياسات العامة التي يتبناها المجتمع لمكافحة الإجرام، والجريمة، والمجرم، بلا إفراط، ولا تفريط في حقوق الفرد (البريء والمدان)، وبالتالي فإن السياسة الجنائية هي نتاج عمل جماعي، تسهم فيه سلطات المجتمع الرسمية (السلطة التنفيذية والسلطة التشريعية والقضائية)، وتسهم فيه كذلك منظمات المجتمع، وتساهم السياسة

الجنائية في كشف الجريمة، ومرتكبها ولما كانت الجرائم الإلكترونية من الجرائم التي لا تترك آثاراً خارجيةً ماديةً، فهي لا تترك بقع دماء كما في جرائم الاعتداء، والقتل، ولا إتلاف كما في جرائم السطو، فالجريمة الإلكترونية جريمة نظيفة أي لا تترك آثاراً ماديةً ملموسةً، ولذلك كانت هذه الجريمة صعبة الاكتشاف، والإثبات.

فالإثبات: هو كل ما يؤدي إلى كشف الحقيقة، أما في معناه القانوني فهو كل ما يؤدي إلى كشف الحقيقة، وإقامة الدليل علي وجود قاعدة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون، ويعد الاثبات من أهم التحديات التي تواجه الأجهزة الأمنية، ويزداد صعوبة في الجريمة الإلكترونية بصفة عامة، لأن اكتشاف الجريمة الإلكترونية بصفة عامة، وجريمة الابتزاز الإلكتروني ليس بالسهل، بل وحتى عند اكتشاف الجريمة والإبلاغ عنها يبقى عبء الاثبات به الكثير من الصعاب، فالجريمة الإلكترونية تتم في بيئة غير تقليدية لأنها تقع في إطار ملموس، لأن أركانها تقوم بين بيئة حاسب آلي، أو جهاز الكتروني تقنى، واستخدام الانترنت وسيلة أخرى، مما يزيد من الصعوبات التي تواجه رجال الضبط الجنائي، والقضائي لأن العمل في هذه البيئة تكون فيها البيانات والمعلومات عبارة عن نبضات إلكترونية ترسل عبر نظام إلكتروني، مما يسهل من محو الأدلة الإلكترونية من قبل الجاني أمراً يسيراً.(10)

كما أن وسائل الاثبات التقليدية دائماً في اثبات مثل هذا النوع من الجرائم نظراً لاختلافها بطبيعتها الخاصة عن الجريمة التقليدية، ولاختلاف العناصر المادية التي تقوم عليها الجريمة الإلكترونية، وفكرة مسرح الجريمة في الجرائم الإلكترونية يتضاءل دورها في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة، ولتوضيح ذلك تفصيلاً نقسم هذا المبحث على مطلبين:-

المطلب الأول:- قواعد وأحكام جريمة الابتزاز الإلكتروني.

المطلب الثاني:- إجراءات الاستدلال والتحقيق والمحاكمة لجرائم الابتزاز الإلكتروني.

**المطلب الأول: قواعد وأحكام جريمة الابتزاز الإلكتروني**

لقد بذلت الأمم المتحدة جهوداً كبيرة لحث الدول على التجريم، والعقاب لجرائم الابتزاز الإلكتروني وتم عقد الاتفاقيات الدولية بالخصوص على نحو ما قدمنا لذلك، حرصت الكثير من الدول على النص صرامة في تشريعاتها العقابية على تجريم جريمة الابتزاز الإلكتروني، والعقاب عليها بنصوص صحيحة، وتوجد دول أخرى ومنها ليبيا لم تتناولها بالتجريم والعقاب وبقيت جريمة الابتزاز التقليدية على وضعها التقليدي، ولما كانت السياسة الجنائية الإجرامية تقضى دراستها تحديد سياسة التجريم، والعقاب للجرائم قبل الخوض في الإجراءات التي حددتها التشريعات الإجرائية للكشف عن الجريمة، ومرتكبيها، والتحقيق معه، وتقديمه إلى المحاكمة لذلك يتعين بداية أن نتعرض لسياسة التجريم والعقاب الدولية لهذه الجريمة من خلال تناول تجريم جريمة الابتزاز الإلكتروني، والعقوبة المقررة لها في بعض تشريعات الدول التي جرمتها، وعاقبت عليها مثل فرنسا، ومصر، والكويت، والإمارات وغيرها من دول أخرى، ثم يتبين مدى صحة الحكم الصادر بشأن هذه الجرائم لتنفيذه دولياً باعتبار أن هذه الجريمة عابرة للحدود ويمكن ارتكابها خارج اقليم الدولة، وهذا ما سوف نتعرض له تفصيلاً على النحو التالي:-

**الفرع الأول:- التجريم، والعقاب لجرائم الابتزاز الإلكتروني في مصر، وفرنسا:**

يعد التهديد سنداً مثبتاً أو موجداً لدين، او تصرف، او براءة، أو سند، ذا قيمة أدبية، أو اعتبارية، أو أوراقاً تثبت وجود حالة قانونية، أو اجتماعية، أو أكراه أحدٍ بالقوة، أو التهديد على إمضاء ورقة مما تقدم، أو ختمها يعاقب السجن المشدد، وتنص المادة 326 من ذات القانون على أنه: كل من حصل بالتهديد على اعطائه مبلغاً من النقود، أو أي شيء آخر يعاقب، فالمشرع المصري في بعض النصوص الأخرى لجأ إلى العقاب على الابتزاز محدداً مضمون التهديد في الابتزاز دون تحديد الغرض من التهديد، وبالتالي يقع الابتزاز طالما تم التهديد بالإفشاء مثلاً للقيام بعمل أو الامتناع عن عمل، حيث تنص المادة 309 (أ) على أن: " يعاقب بالحبس كل من أذاع، أو سهل إذاعة، أو استعمل ولو في غير علانية تسجيلاً، أو مستنداً متحصلاً عليه بإحدى الطرق المبينة في المادة السابقة، أو كان ذلك بغير رضاء صاحب الشأن، ويعاقب بالسجن مدة لا تزيد عن خمس سنوات كل من هدد

بإفشاء أمر من الأمور التي تم التحصيل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل، أو الامتناع عنه، ويعاقب بالحبس إذا لم يكن التهديد مصحوباً بطلب، أو بتكليف بأمر، وكل من هدد غيره شفهياً بواسطة شخص آخر بمثل ما ذكر يعاقب بالحبس مدة لا تزيد عن سنتين، أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوباً بتكليف بأمر، أو لا.(11)

وقد أخذت بذلك بعض التشريعات منها: المادة 4/3 من القانون الكويتي رقم 13 لسنة 2010م المتعلق بمكافحة جرائم تقنية المعلومات التي تنص على أن: " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار، ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: استعمل الشبكة المعلوماتية، أو استخدام وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي، أو اعتباري لحمله على القيام بفعل، أو الامتناع عنه، فإذا كان التهديد بارتكاب جناية، أو بما يعد ماساً بكرامة الأشخاص، أو خادشاً للشرف، والاعتبار، او السمعة كانت العقوبة الحبس مدة لا تجاوز خمس سنوات، والغرامة التي لا تقل عن خمسة آلاف دينار، ولا تجاوز عشرين ألف دينار، أو بإحدى هاتين العقوبتين. ويذهب المشرع الإماراتي إلى ذات الاتجاه، حيث تنص المادة 16 من القانون رقم 5 لسنة 2012 المتعلق بمكافحة جرائم تقنية المعلومات على أن يعاقب بالحبس مدة لا تزيد عن سنتين، والغرامة التي لا تقل عن مائتين، وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل، أو الامتناع عنه، وذلك باستخدام شيكه معلوماتية، أو وسيلة تقنية معلومات، وتكون العقوبة السجن مدة لا تزيد عن عشر سنوات إذا كان التهديد بارتكاب جناية، أو بإسناد أمور خادشه للشرف، أو الاعتبار.

**الفرع الثاني:- تنفيذ الأحكام الصادرة في جريمة الابتزاز الإلكتروني دولياً.**

القاعدة التقليدية: هي تلازم السيادتين التشريعية، والقضائية في المجال الجنائي، بما يعني أن كل دولة لا تعترف سوى بأحكام قانونها الجنائي الوطني، ولا تعتد ولا تنفذ على إقليمها سوى الأحكام الجنائية الصادرة عن إحدى محاكمها الوطنية، ويجد ذلك سنده في أن تطبيق القانون الجنائي يعد تعبيراً عن سيادة الدولة بوصفه يحمي المصالح الأساسية

للمجتمع، والدولة، والحقوق الجوهرية لأفراده، إضافة إلى أن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، وهو ما يحول دون الخضوع لحكم قانون أجنبي، وتطبيقه.(12)

أما فيما يتعلق بحجية الأحكام الجنائية الأجنبية في شقها الإيجابي، فإنه يجب أن يفسح لها مكان بين أحكام المعاهدات الدولية ذات الصلة، وهكذا يمكن أن يؤخذ في الاعتبار بالآثار الجنائية غير المباشرة للأحكام الجنائية الأجنبية لاسيما في مجال العود، ووقف التنفيذ، وتقدير العقوبة في ضوء ما يثبت من الخطورة الإجرائية للجاني، أما بالنسبة لحجية الأحكام الجنائية في شقها السلبى فقد اعترف بها بعض المشرعين إذ يمتنع إقامة الدعوة الجنائية ضد من ارتكب جريمة في الخارج متى ثبت أن المحاكم الجنائية الأجنبية قد برأته، أو أدانته نهائياً واستوفى عقوبته، فكأن هؤلاء المشرعين يعترفون بقوة الشيء المحكوم فيه ولو تعلق الأمر بحكم أجنبي تطبيقاً لقاعدة امتناع محاكمة الشخص عن ذات الفعل مرتين.(13)

أرى أنه حان الأوان لتجاوز بعض المفاهيم التقليدية، وخاصة فيما يتعلق بتلازم السيادتين التشريعية، والقضائية في المجال الجنائي في الجرائم الإلكترونية، وذلك بالتوجيه نحو الاعتراف في بعض الحالات وعلى نحو ما بحجية التشريع الجنائي غير الوطني، وبحجية الحكم الجنائي الصادر عن محاكم دولة أخرى، وتتجلى أهمية ذلك على وجه الخصوص في مجال الجرائم الإلكترونية التبعية التي تفترض ارتكاب جريمة أصلية على إقليم دولة ما، ثم وقوع الجريمة التابعة على إقليم دولة أخرى.

**المطلب الثاني: إجراءات الاستدلال، والتحقيق، والمحاكمة في جرائم الابتزاز الإلكتروني**

الجرائم الإلكترونية كغيرها من جرائم تمر بثلاثة إجراءات لا غنى عنها، وتتمثل الاجراءات في: إجراءات جمع الاستدلالات، وإجراءات التحقيق الابتدائي، وإجراءات التحقيق النهائي (المحاكمة)، إلَّا إن هذه الإجراءات تختلف بعض الشيء عن إجراءات الجرائم التقليدية، كما أنها تتطلب خبراء تقنيين، وأجهزة إلكترونية لكشف ملابسات الجريمة قد لا نجد هذه الأشياء في الجرائم الإلكترونية، ومثل هذه الصعوبات صعوبة الحصول علي الأدلة في الجرائم الإلكترونية وهو على الجناة خاصة، وأن الجرائم الإلكترونية لا حدود جغرافية لها، فمن الصعب البحث عن الجناة والقبض عليهم إذا كانوا خارج إقليم الدولة، كما أن

الجهاز الشرطي، والقضائي قليل الخبرة في مثل هذه الجرائم مما يؤدي إلي صعوبة المهمة، لذلك تعد إجراءات جمع الأدلة تمثل أساس جوهري للتحقيق، والمحاكمة في جرائم الابتزاز الإلكتروني لذلك سوف نركز في هذا المطلب على إجراءات جمع الاستدلالات من حيث أهميتها في إثبات جريمة الابتزاز الإلكتروني، والسلطة المختصة بالقيام بها، وحدود اختصاصات هذه السلطة، وذلك وفقاً للتفصيل التالي:-

**الفرع الأول:- أهمية جمع الاستدلالات في إثبات جريمة الابتزاز الإلكتروني:**

تقوم مرحلة إجراءات الاستدلال: علي أساس أنها جمع للمعلومات المتعلقة بالجريمة، والمجرم، وذلك بهدف التحضير للدعوى الجنائية، و مباشرتها، لذا فمن حسن السياسة التشريعية أن تحدد هذه الإجراءات على سبيل الحصر بنصوص قانونية حتى لا يكون ذلك عقبة أمام القائمين في سبيل كشف الجريمة، والمحافظة علي الآثار المتخلفة عنها، وسماع من يروي ضرورة لسماعه.

أن فحوى الاستدلال، وهدف إجراءاته هو مجرد جمع المعلومات المتعلقة بالجريمة، والمساهمين فيها، وغايته توضيح الأمور لسلطة التحقيق لكي تتصرف علي وجه معين، وهي قد تكون سابقة فيكون غرضها الكشف عنها، وقد تكون لاحقة لظهور الجريمة فيكون غرضها الوصول إلي معرفة الشخص المتهم (13) .

ويهدف إلي تبصير السلطة المكلفة بالتحقيق بالمعلومات التي تمكنها من التصرف علي نحو أو آخر، فهو ليس تحقيقاً بالمعنى الفني، وليس مرحلة من مراحل الدعوى الجنائية بل هو إجراء أولى يسبق تحريكها وله طبيعة شبه إدارية، و كما عرف بأنه عبارة عن مجموعة من الإجراءات تباشر خارج إطار العمومية، وقبل البدء فيها لقصد التثبيت من وقوع الجريمة عن مرتكبها، وجمع الأدلة، والعناصر اللازمة للتحقيق فيها.(14)

هذه المرحلة وبحق من المراحل الخطيرة، والمهمة، فهي وإن كانت ليست من مراحل الدعوى العمومية إلا أنها تعد خط الدفاع الأول ضد الجريمة، وترجع أهميتها إلى أنها من جهة تسمح بحفظ الشكاوى والبلاغات غير المدعمة، والتي لا يجدي تحقيقها لإثبات الجريمة بما يوفي التحقيق الابتدائي، ومن جهة ثانية تتيح لسلطة التحقيق أن تتصرف بشأن تحريك الدعوى الجنائية، وهي علي بينة وعلم كافيين بحقائق الأمور، ومن جهة ثالثة تفيد

فـي تهيئـة أدلـة الـدعوى إثباتـاً أو نفيـاً، وتسـهل مهمـة التحقيـق الابتـدائي، أو المحاكمـة فـي الكشف عن الحقيقة، ومن جهة رابعة نجدها تقرر علي أثر المعلومات المتوفرة، والمستقاة من عدة مصادر مصير الدعوى الجنائية، مما يعنى استبعاد الاتهامات الكيدية، وغير الجدية.(15)

**الفرع الثاني:- السلطات، والاختصاصات في مرحلة جمع الاستدلالات لجريمة الابتزاز الإلكتروني.**

إن تحديد سلطة الضبط القضائي ينطوي حتماً ولزوماً على منح أصحاب هذه الصفة الاختصاص بمباشرة إجراءات جنائية تحوي في بعضها مساساً بالحرية الشخصية، وكانت قواعد الاختصاص هي من صميم قواعد الإجراءات الجنائية، فإن ذلك يقتضى أن يكون القانون وحده هو الأداة الصالحة لتخويل سلطة الضبط القضائي، لذا نجد المادة 31 من قانون الإجراءات الجزائية تنص علي أن " مأموري الضبط القضائي في دائرة اختصاصهم وهم أعضاء الادعاء العام، ضباط الشرطة، والرتب النظامية الأخرى بدءاً من رتبة شرطي، جهات الأمن العام الذي يصدر بتحديدهم قرار من رئيس الجهة، الولاة ونوابهم، كل من تخوله القوانين هذه الصفة، ويجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص تخويل الموظفين صفة الضبطية القضائية بالنسبة إلى الجرائم التي تقع في دائرة اختصاصهم وتكون متعلقة بأعمال وظائفهم، وفى المؤتمر الدولي لجرائم الحاسب الآلي والذي انعقد في " اوسلو " بالنرويج أثير موضوع عدم إمكانية البنية التحتية لشبكة الانترنت من التوصل إلى تحديد شخصية مرتكب الجريمة والمصدر الحقيقي لها، وموقعه علي وجه التحديد، حيث أن ما قامت بها تقنية الانترنت حتي الآن هي إمكانية التعرف علي عنوان الحاسب الآلي فقط، وهو ما يعرف بمصطلح بروتوكول الانترنت IP الذي يشير إلى رقم يعين جهاز الحاسب الآلي على الوصول إلى شبكة الانترنت مثل هذا الرقم الذى يحدد هوية الحاسب الآلي الذي استخدم في ارتكاب جرائم الانترنت إنما يفيد حالة التوصل إليه واتخاذ إجراءات التحفظ بقصد ضبطه، مع ملاحظة أمر علي قدر من الأهمية وهو أن هذا الرقم ليس موحدا علي مستوى العالم، وتعويلاً علي ما تقدم فإن رجال الضبط القضائي يحتاجون في هذا النوع المستحدث من الجرائم إلي صلاحيات معينة أكثر مما يعرفه القانون الآن، إذ

كيف يمكن لرجال الضبط القضائي القيام بتحديد الشخص مرتكب الجريمة الإلكترونية أو المعلوماتية، سيما أنه لا توجد حدود إلكترونية في هذا الشأن؟ فمن الممكن أن يقوم شخص ما بارتكاب حريمته في احدى دول الخليج عبر مزود من الولايات المتحدة الأمريكية لتتحقق النتيجة الإجرامية في دول أفريقية هنا تزداد الحاجة إلى معرفة الصلاحيات التي يمكن أن يحتاجها رجال الضبط القضائي لكي يمكنهم التوصل إلى الجاني وتطبيق القانون عليه، ولاسيما إذا كانت الجريمة قد تحققت في أكثر من دولة من دول المعمورة، ومن أجل ذلك قامت دول كثيرة بإعداد قوات خاصة للتعامل مع الجريمة التي تتم عبر شبكة الانترنت، قوات لا تعتمد على التدريبات المادية والعضلية التقليدية التي يتلقاها رجال الشرطة، و إنما تعتمد علي البناء العلمي والتكنولوجي لإفرادها من أجل التعامل مع نظم الحاسب الآلي، والإنترنت بحيث يمكنهم القيام بأنشطة تخصصية كمطاردة الهاكرز، ومخترقي الأنظمة، وغيرها، فمثلاً الولايات المتحدة الأمريكية تطورت في وقت لاحق وأصبحت قسماً.(16)

وهناك أيضاً مركز الشكاوى الخاص بجرائم الانترنت التابع لمكتب التحقيقات الفيدرالي الذي يعد إطار مقاصة لفرز، وتصفية عمليات التبليغ الفردية عن نشاطات غير المشروعة، حيث يقوم بالربط بين المعلومات التي يتلقاها من ضحايا نفس العملية غير المشروعة الذي قد يصل عددهم المئات، فيعد منها ملف قضية مهمة يسلمها لحاجات تطبيق القانون، وفى "هونج كونج" تأسست وحدة خاصة لمكافحة قرصنة الانترنت، والتي أمكنها القبض علي 12 شخصاً في خمس قضايا خلال مدة ستة أشهر من تاريخ إنشائها، وفى "فرنسا" تم إنشاء مكتبٍ مركزيٍ لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات تابعة لوزارة الداخلية، وفى إطار بحثنا للجرائم المتعلقة بشبكة الانترنت فإنها تثار مدى إمكانية تلقي البلاغات، والشكاوى، والتحقيق منها، والحصول علي الإستيضاحات بشأنها، وإجراء المعاينات عبر شبكة الانترنت، لاسيما في الوقت الحاضر أصبح من السهل جداً الولوج إلى موقع خاص بالبلاغات وكتابة البلاغ حول الجريمة، ثم إرساله إلى الجهات المختصة، كما هو الحال في بعض المواقع الأمريكية كموقع المباحث الفيدرالية، ووزارة العدل الأمريكية، وموقع البلاغات الخاص بالمخابرات المركزية الأمريكية، وموقع حماية البرمجيات الأوروبية، وغيرها من المواقع التي أصبحت تقدم خدماتها في هذا المجال بشكل

حديث جداً، حيث أن الأمر يمتد بشكل قوى، ومتميز إلى إمكانية إدخال الحاسب الآلي في مجال الاستدلال على الجرائم حيث أنه بمجرد كتابة بلاغ عبر الانترنت وإرساله إلى الجهات المختصة فإن الانترنت سوف تتولى عملية رصد التحريات الكاملة حول الواقعة، وأشخاصها، وامداد كل من له علاقة مهنية بالجريمة يكافه البيانات اللازمة لسير الاستدلال، والتحقيق، ولذالك ومن أجل توافق النظم الإجرائية مع نظم التكنولوجيا شرعت بعض النظم الإجرائية إلى توسيع قاعدة الإرشاد الجنائي فيما يتعلق بالبحث عن الجرائم، ومرتكبيها لكي تشمل أحقية السلطات المختصة في الاتصال بمزود الانترنت ISP لكي يتولى التحفظ علي السجلات المخزونة في الخادم المضيف، ومن تلك الأنظمة التشريع الأمريكي، فصفوة القول إذ على رجال الضبط القضائية قبول البلاغات القضائية، والشكاوى، وفحصها، والتحقق منها، وعدم رفضها سواء كانت تلك البلاغات، أو الشكاوى بالطريق العادية، أو تمت بالطرق المستحدثة خاصة وأن غالبية النظم الإجرائية لا تشترط وسيلة معينة بذاتها لتقديم البلاغ، والشكوى، وإن إجراءات جمع الاستدلالات من الإجراءات التي تسبق التحقيق ورفع الدعوى الجزائية، والتي يختص بها مأموري الضبط القضائي، والتي يكون عليهم النائب العام مشرفاً، ومسؤولاً عن أعمالهم، حيث يحق للنائب العام الإشراف على أعمال الضبط القضائية، كما يحق له مطالبة الجهات المختصة مساءلة مأموري الضبط القضائي تأديبياً على تقصيرهم أو مخالفتهم لواجبات عملهم، وإجراءات جمع الاستدلالات ينطوي فيها عملية البحث، والتحري حول الجريمة والتمهيد للتحقيق فيها، دون التوغل في عملية التحقيق التي تختص بها النيابة العامة دون غيرها كما أن قواعد الإجراءات الجزائية تهم كل فرد في المجتمع سواء كان بريئاً أو مذنباً، فالمجتمع ينشد الحقيقة ولا يرغب في إفلات أي مذنب من العقاب، وذلك لا يتم إلا باتخاذ الإجراءات الجزائية المناسبة.(17)

فبمقتضى هذه المرحلة تجمع الدلائل التي تفيد في كشف الحقيقة والتي قد تصلح أساساً للمحاكمة في الجنح، والمخالفات، أو أساساً للتحقيق الابتدائي في الجنايات، والجنح، وتعد المعاينة في الجرائم الإلكترونية مهمة، حيث قد تتطلب معاينة العالم الافتراضي، ويستطيع عضو سلطة التحقيق، أو مأمور الضبط القضائي الانتقال إلى العالم الافتراضي من خلال حاسوبه الشخصي، أو إحدى مقاهي الانترنت، أو من خلال جهاز الخبير، أو

عن طريق اللجوء إلى مقر مزود الخدمة والذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة، وهناك خطوات يجب اتباعها في معاينة العالم الافتراضي وهى تصوير شاشة الحاسب الآلي وعدم نقل أي مواد معلوماتية من مسرح الجريمة قبل التأكد من عدم اختراق الجهاز الذى قد يتسبب في محو البيانات المسجلة، ويجب تعطيل حركات الاتصالات والتحفظ علي سلسلة المهملات في النهاية يجب الاستعانة بأهل الخبرة متى دعت الحاجة لذلك، ومن إجراءات جمع الاستدلالات سماع أقوال المشتبه بهم، ويقتصر هذا الإجراء بإعلامهم بهم بالتهم المسنودة إليهم، ومجمل الأدلة الموجهة ضدهم دون مناقشتهم تفصيلياً في الواقعة، وسماع أقوالهم دون مواجهتهم، ويعد من المشتبه فيهم كل شخص كان متواجداً في مسرح الجريمة أو يحوم حولها أو هناك أدلة أخرى ضده، ويجب على مأمور الضبط القضائي سماع أقواله، وتدوينها مع إرسالها لوكيل النيابة المختص خلال أربع وعشرين ساعة، إذا دعت الحاجة لذلك، ونص القانون البلجيكي في ذلك علي أنه: " يجوز لقاضى التحقيق، والشرطة القضائية أن يستعين بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطى القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة، أو المحمولة، أو المنقولة، علي أن يتم ذلك بالطريقة التي تريدها جهة التحقيق.(18)

**الخاتمة**

تعرضنا في هذا البحث إلى جريمة الابتزاز الإلكتروني وفقاً لما تفتضيه السياسة الجنائية الدولية سواء في جوانبها الموضوعية، أو الإجرائية ولحداثة، وأهمية هذه الجريمة حظيت باهتمام كبير في العديد من الاتفاقيات الدولية، وحرصت الكثير من التشريعات الوطنية علي النص عليها وتجريمها، من خلال هذه الدراسة توصلت إلى عدة نتائج، وتوصيات نوجزها في التالي:

**أولاً:- النتائج::**

1. جريمة الابتزاز الإلكتروني صورة من صور الجريمة الإلكترونية حيث تتم باستخدام شبكات المعلومات، أو الأجهزة الحديثة، وتطبيقاته.
2. لجريمة الابتزاز الإلكتروني طرق مختلفة في ارتكابها كما أن لها وسائل أيضاً خاصة بها تختلف عن الابتزاز التقليدي.
3. جريمة الابتزاز الإلكتروني جريمة عابرة للحدود، فقد يكون المبتز في دولة بالعالم، ويقوم بابتزاز ضحية في أقصى العالم.
4. جريمة الابتزاز جريمة قد تتسبب في حدوث جرائم بعدها، كالزنا، أو القتل، أو جريمة عنف، أو سرقة.
5. وأخيراً جريمة الابتزاز الإلكتروني جريمة يصعب إثباتها، حيث من السهل أن تمحى آثارها بسهولة، وتحتاج لعمل شاق حتي يتم إثباتها.

**ثانياً:- التوصيات.**

1. الحاجة إلى التنسيق، والتعاون القضائي، والإجرائي الدوليين في مكافحة جريمة الابتزاز الإلكتروني، وتنفيذ التعاون الدولي بنشاط، وإفساح المجال لدور المعاهدات الدولية، والالتزام بمبدأ المساعدة القانونية المتبادلة.
2. تفعيل الأحكام القانونية الوطنية، والدولية المتعلقة بالتعاون الدولي في مكافحة الجرائم، والعمل القضائي، مثل مكافحة مرتكبي هذه الجرائم ومحاكمتهم بسرعة، حيث لا يمكن مكافحة هذه الجرائم بفعالية إلا من قبل جميع البلدان، والمنظمات الدولية، والإقليمية.
3. العمل علي توفير المعلومات بشكل مستمر عن الجرائم، وسرعة التعامل معها بكل شفافية.
4. نشر الوعى المجتمعي عن الخطر الذي يمكن أن تشكله الجرائم الإلكترونية التي يتعرض لها الفرد عبر وسائل الإعلام الرقمي، وذلك من خلال إقامة الندوات، والمنشورات التي تهدف إلى التوعية بخطر هذه الجرائم.

**الهوامش**

1- عبدالله العجمي- المشكلات العملية والقانونية للجرائم الإلكترونية- دراسة مقارنة رسالة ماجستير- جامعة الشرق الأوسط- لبنان2014 ص18.

2- عبدالله العجمي:- المرجع نفسه ص19.

3- محمد عمران السرجى- الجريمة الإلكترونية في المجتمع الخليجي، وكيفية مواجهتها- مجمع البحوث والدراسات- أكاديمية السلطان قابوس لعلوم الشرطة- سلطنة عمان 2014 ص28 وما بعدها.

4- محمد عبدالله سلامة- موسوعة جرائم المعلوماتية- المكتب العربي الحديث- الإسكندرية 2007 ص149.

5- محمد عبدالله سلامة- المرجع نفسه ص 151.

6- محمد عبدالله سلامة- المرجع نفسه ص153.

7- سليمان عبدالمنعم- الجريمة الإلكترونية- بحث مقدم في المؤتمر الخامس عشر- للجمعية الدولية لمكافحة الجرائم- القاهرة 2019ص8.

8- سليمان عبدالمنعم- المرجع نفسه ص9.

9- خالد وليد محمود- الجرائم الإلكترونية كظاهرة عالمية- بحث مقدم لمجلة القانون الجنائي- كلية الحقوق- جامعة الكويت العدد 12 المجلد الثاني في 5/8/2023 ص 6.

10- خالد وليد محمود- المرجع نفسه ص 12.

11- خالد وليد محمود- المرجع نفسه ص 13.

12- نبيلة هبه هدوال- الجوانب الجنائية لجرائم الانترنت- دار الفكر الجامعي- الإسكندرية 2013 ص 18 وما بعدها.

13- نبيلة هبه هدوال- المرجع نفسه ص 126.

14- عبدالقادر جرادة- دستور الاستدلال والتحقيق الجنائي- مكتبة آفاق غزة فلسطين 2012 ص 18.

15- عبدالقادر جرادة- المرجع نفسه ص 19.

16- عبدالقادر جرادة- المرجع نفسه ص 21.

17- محمد خليل بحر- التحقيق الجنائي- دار النهضة العربية- القاهرة 2022 ص 116.

18- محمد خليل بحر- المرجع نفسه ص 118.