

دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني

The role of digital evidence Criminal in proving the crime of electronic extortionديب أكرم^{1*}، بن بوعبدالله نورة²¹ جامعة باتنة 1، كلية الحقوق والعلوم السياسية (الجزائر)، akram.dib@univ-batna.dz² جامعة باتنة 1، كلية الحقوق والعلوم السياسية (الجزائر)، nora.benbouabdalla@univ-batna.dz

مخبر الحوكمة والقانون الاقتصادي

تاريخ النشر: 2023/03/31

تاريخ القبول: 2023/03/15

تاريخ الاستلام: 2023/02/04

ملخص:

تعد مسألة الإثبات في الجرائم الإلكترونية من المسائل التي شغلت القائمين بالتحقيقات الجنائية، نظرا للطبيعة التقنية الخاصة بالأدلة المتحصل عليها من الشبكة العنكبوتية و الحاسب الآلي، و التي تحتاج إلى دراية بأدوات المعرفة التقنية و خبرة فنية و كفاءة عالية، و لما كانت جريمة الابتزاز الإلكتروني كصورة من صور الجرائم الإلكترونية مسرحها هو الفضاء الإلكتروني، و باعتبارها من جرائم العصر التي تقع خارج إطار الواقع المادي الملموس، فإن إثباتها يكون عن طريق الأدلة الجنائية المعروفة و من بينها الدليل الرقمي الذي يرتبط ارتباطا وثيقا بهذا الفضاء الإلكتروني، إلى جانب كونه الوسيلة التي تمكن من إسناد الجريمة إلى مرتكبها.

وتهدف الدراسة إلى بيان خصوصية الدليل الرقمي الجنائي من الناحيتين الفنية والقانونية، وإبراز دوره في إثبات جريمة الابتزاز الإلكتروني من خلال التعرض إلى قيمته القانونية أمام القضاء الجزائي والإشكالات التي يثيرها في هذه الجريمة ومعالجة تلك الإشكالات بالتقنيات التي تتلاءم وطبيعته الخاصة.

كلمات مفتاحية: الدليل الرقمي، الابتزاز الإلكتروني، الجرائم الإلكترونية، الفضاء الإلكتروني.

Abstract:

The issue of evidence in electronic crimes is one of the issues that preoccupied those conducting criminal investigations, due to the technical nature of the evidence obtained from the world wide web and the computer, which requires familiarity with the tools of technical knowledge, technical experience and high efficiency, and since the crime of electronic extortion is an image among the forms of electronic crimes, the scene of which is the electronic space, and as one of the crimes of the era that falls outside the framework of the tangible physical reality, its proof is through well-known forensic

evidence, including the digital evidence that is related to this electronic space, Also to being the means that enables attribution of the crime to the perpetrator.

The study aims to prove the specificity of the digital evidence from the technical and legal sides, and to highlight its role in proving the crime of electronic extortion by exposing its legal value before the criminal judiciary and the problems it raises in this crime and addressing these problems with techniques that are appropriate to its own nature.

Keywords: digital evidence; electronic extortion; cybercrime; cyberspace.

مقدمة

نتيجة للاستخدام السيء للشبكة العنكبوتية العالمية ووسائل التكنولوجيا والاتصال الحديثة، أضحت البيئة الافتراضية بؤرة لأنماط جديدة من الجرائم تسمى بالجرائم الالكترونية ومن نماذجها جريمة الابتزاز الالكتروني كظاهرة اجتماعية تدق في أعماقها أجراس الخطر على اعتبار أنها توجه للنيل من الحياة الخاصة للأفراد وتطال اعتداءاتها الأشخاص الطبيعية والمعنوية على حد سواء، معتمدة في ذلك على شبكة الإنترنت بدلالاتها التقنية الواسعة كأداة لارتكاب أحد أخطر أصناف الجرائم استفحالاً وأكثرها تعقيداً.

و تثير جريمة الابتزاز الالكتروني عدّة مشكلات من الناحية القانونية تنصب على عملية الإثبات في هذا النوع من الجرائم و مدى قيمة الأدلة المستخلصة من البيئة الافتراضية أمام القضاء الجزائي المختص، ذلك أن الأدلة الجنائية المتحصل عليها من المنظومة المعلوماتية تتسم بطبيعة خاصة يغلب عليها الطابع الفني أو التقني، و هو ما يشكل تحدياً لحكومات الدول و التشريعات الجنائية من أجل العمل على إرساء بيئة قانونية و آليات واضحة المعالم للتعامل مع هذا النوع من الأدلة الرقمية، سواء من طرف المكلفين بالتحقيقات الجنائية فيما يتعلق بإجراءات جمع و استخلاص الدليل الرقمي أو من طرف الهيئات القضائية المختصة عند عرض القضية عليها، و المشرع الجزائري بدوره على غرار التشريعات الأخرى حاول التصدي و احتواء ظاهرة الإجرام الالكتروني بشتى صوره من خلال استحداث نصوص قانونية موائمة لطبيعة هذه الجرائم و كيفية تعامل القاضي الجزائي مع الدليل الرقمي الجنائي من منطلق مبدأ الاقتناع الذي يتمتع به. لذا فإن الدراسة ستجيب على إشكالية رئيسية تتمثل فيمايلي: إلى أي مدى يعبر الدليل الرقمي الجنائي عن الحقيقة التي تصبو إليها الدعوى الجزائية في جريمة الابتزاز الالكتروني؟

وللإجابة على الإشكالية المطروحة أعلاه، ستم معالجة الموضوع من خلال تقسيمه إلى مبحثين، يخصص أولهما للتعرض إلى الدليل الرقمي الجنائي في جريمة الابتزاز الالكتروني، ويخصص الثاني لبيان القيمة القانونية للدليل الرقمي الجنائي في إثبات جريمة الابتزاز الالكتروني.

وختمنا هذه الدراسة باستعراض أهم النتائج المتوصل إليها مع إيراد مجموعة من الاقتراحات القابلة للتجسيد.

المبحث الأول: الدليل الرقمي الجنائي في جريمة الابتزاز الإلكتروني

إن الأدلة الجنائية تتواجد في مسرح الجريمة بتواجد هذه الأخيرة التي انتقلت بدورها من الوسط المادي إلى الوسط الرقمي الذي تنفذ فيه الجرائم الإلكترونية عموماً، و من بينها جريمة الابتزاز الإلكتروني كظاهرة مستحدثة اخترقت المجتمعات في ظل التطور التقني الذي يشهده العالم، و بالموازاة لذلك ظهرت الأدلة الرقمية كوسيلة يستند إليها في إثبات الجريمة الواقعة في البيئة الافتراضية، و عليه سوف نتطرق من خلال تفاصيل هذا المبحث إلى مفهوم الدليل الرقمي الجنائي في **المطلب الأول**، ثم التعرض لموضوع جريمة الابتزاز الإلكتروني في **المطلب الثاني**.

المطلب الأول: مفهوم الدليل الرقمي الجنائي

من منطلق الأهمية البالغة التي يوليها فقهاء القانون الجنائي والتشريعات الجنائية الحديثة بالأدلة الرقمية، فإنه بداية يتعين علينا تحديد تعريف للدليل الرقمي من خلال **الفرع الأول**، وبيان خصائصه بالتفصيل في **الفرع الثاني**.

الفرع الأول: تعريف الدليل الرقمي الجنائي

قبل التطرق لتعريف الدليل الرقمي، لابد من تحديد تعريف للدليل بوجه عام باعتبار الدليل الجنائي الأصل العام للدليل الرقمي.

أولاً: المدلول العام للدليل الجنائي

يشير لفظ الدليل في اللغة إلى البينة أو الحجة، إذ هو ما يؤدي إلى استقرار الحق لصاحبه و تأكيد الحق بالبينة¹، و يعرف مجموعة من الباحثين المختصين الدليل بأنه أي شيء يميل منطقياً إلى إثبات أو دحض مسألة معينة في قضية أو خلاف معروض أمام القضاء².

والدليل الجنائي عموماً يقصد به الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي انتهى إليه، أو هو الوسيلة التي يبحث عنها في التحقيق بغرض إثبات صحة واقعة الجريمة ونسبتها للمتهم أو البحث عن ظرف من ظروفها المادية أو الشخصية³.

¹ _ عبد الرحمن خلفي، الإجراءات الجزائية في القانون الجزائري والمقارن، الطبعة السادسة، دار بلقيس، الجزائر، سنة 2022، ص 492.

² _charles R. swanson, Neil C. Chamelin, Leonard Territo, Robert W. Taylor, **Criminal investigation**, 11th edition. McGraw-Hill. United Kingdom, London, a business Unit of the McGraw-Hill Companies, New York, United States, 2011, P656.

³ _ عمر زودة، الإثبات في المواد الجزائية، دون طبعة، دار هومة، الجزائر، سنة 2021، ص 12.

ثانيا: المدلول الضيق للدليل الجنائي الرقمي

تعتبر المنظمة الدولية لأدلة الحاسوب IOCE المرجع الأساسي التي كان لها السبق في تعريف الدليل الرقمي سنة 2000، حيث عرفته بأنه: " المعلومات المخزنة والمتنقلة بشكل ثنائي والتي يمكن الاعتماد عليها أمام المحكمة"¹، ومن جهة أخرى عرفت مجموعة العمل العلمية للأدلة الرقمية SWEGDE الدليل الجنائي الرقمي بأنه: " مجموعة المعلومات القيمة التي تخزن أو ترسل في شكل رقمي"².

وقصد استيعاب هذا النوع المستحدث من الأدلة، يذهب بعض الباحثين والمفكرين في الحقل القانوني إلى تبني تعريف يأخذ بالوسيلة المستعملة في استخراج الدليل الرقمي، حيث يعرفه البعض بأنه: " الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء"³.

والدليل الرقمي في أبسط معانيه هو الدليل الذي يجد له أساسا في العالم الافتراضي إلى الجريمة⁴، وهو بذلك الدليل الذي ينشأ في العالم الرقمي، والذي يكون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة⁵.

وترجع تسمية الدليل الرقمي كترجمة لمصطلح الكتروني إلى أن البيانات داخل الوسط الافتراضي سواء كانت صورا أم تسجيلات أم نصوص تأخذ شكل أرقام على هيئة الرقمين (1 أو 0) ويتم تحويل هذه الأرقام عند عرضها لتكون في شكل صورة أو مستند أو تسجيل⁶.

وإجمالا يمكن استخلاص تعريف للدليل الرقمي بأنه ذلك الدليل ذو الطبيعة التقنية الذي تكون البيئة الرقمية العنصر الجوهري والأساسي فيه، يتم استخراجه منها عن طريق الأنظمة البرمجية المعلوماتية للحاسب الآلي ووسائل تكنولوجيا

¹ _ عبد الله ذيب محمود، أسامة إسماعيل دراج، **الوجيز في الجرائم الالكترونية "القواعد الموضوعية والإجرائية"**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، سنة 2022، ص 201.

² _ Eoghan Casey، **Digital Evidence and Computer Crime**، Third Edition، Published by Elsevier Inc، London، Uk، 2011، p 07.

³ _ مروة صلاح الدين محمد، **الدليل الالكتروني ومدى حجتيه في الإثبات الجنائي**، الطبعة الأولى، المكتب العربي للمعارف، دار البحوث القانونية، القاهرة، مصر، سنة 2021، ص 61.

_ جاسم محمد جندل، **الجرائم الالكترونية**، الطبعة الأولى، دار معتر للنشر والتوزيع، عمان، الأردن، سنة 2022، ص 204.

⁵ _ بن فردية محمد، **الدليل الجنائي الرقمي وحجتيه أمام القضاء الجزائي**، دراسة مقارنة، **المجلة الأكاديمية للبحث القانوني**، جامعة عبد الرحمان ميرة بجاية، كلية الحقوق والعلوم السياسية، المجلد 05، العدد 01، الجزائر، جوان 2014، ص 278

⁶ _ طارق محمد الجملي، **الدليل الرقمي في مجال الإثبات الجنائي**، **مجلة الحقوق**، جامعة بنغازي، كلية الحقوق، المجلد 12، العدد 01، ليبيا، دون ذكر السنة، ص 44 .

الاتصال الحديثة، ويكون الحصول عليه بطرق مشروعة قانوناً، ويخضع بعد ذلك للتحليل العلمي والتفسير ليترجم في شكل نصوص مكتوبة أو صور أو رسومات وأشكال تكون قابلة للمناقشة قصد إثبات صحة واقعة الجريمة ونسبتها للمتهم.

الفرع الثاني: خصوصية الدليل الرقمي الجنائي

إن البيئة الافتراضية الحركية والمتطورة التي ينشأ فيها الدليل الرقمي، تجعل منه دليلاً يمتاز بخصائص يغلب عليها الطابع التقني والفني، وهو ما يميزه عن الدليل التقليدي، ويمكن تقسيم هذه الخصائص إلى: خصائص متعلقة بطبيعته، وأخرى متعلقة بمرونته، وهو ما سنتناوله تباعاً في هذا الفرع.

أولاً: الخصائص المتعلقة بطبيعته

ينظر إلى الدليل الرقمي من حيث طبيعته على أنه دليل علمي، فني وتقني، تحليلي وغير مرئي وذلك وفق التفصيل التالي:

— **دليل علمي:** تجدد هذه الخاصية مبررها في القاعدة الفقهية المعروفة أن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة ، ولذلك فإن التعامل مع الدليل الرقمي ينبغي أن يكون وفقاً لأسس علمية وقانونية تتماشى مع أحكام القانون، وهذا لن يكون إلا باستخدام الأساليب العلمية الحديثة والاستعانة بأجهزة ومعدات الكترونية، وبرامج ونظم خاصة تسمح بالتعامل مع مسرح الجريمة الافتراضي¹.

— **دليل فني وتقني:** وأساس هذه الميزة أن الدليل الرقمي يبنى على أساس مقومات التقنية الكاملة، وهذه الطبيعة التقنية تنتج نبضات الكترونية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه ، بمعنى آخر التقنية لا تنتج سكيناً يتم بها اكتشاف القاتل أو اعترافاً مكتوباً أو مالا قدّم كرشوة أو أصبح بصمة².

— **دليل تحليلي:** تفيد هذه الخاصية أن الدليل الرقمي بإمكانه تعقب ورصد تحركات الجاني المعلوماتي ومخططاته والأماكن التي يتواجد فيها، بشكل يمكن من تجميع كافي للمعلومات حوله³، وهو ما يساعد جهات التحقيق في تكوين فكرة شاملة عن طبيعة المجرم التي تتعامل معه، ومن ثم توقع خطواته القادمة، وذلك لن يتأتى إلا باستعمال أداة التحليل للمعلومات المجمعة من الحاسب الآلي أو أي وسيلة من وسائل تكنولوجيا الاتصال الحديثة.

¹ — عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سبق ذكره، ص 203.

² — مروة صلاح الدين محمد، مرجع سبق ذكره، ص 64.

³ — عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سبق ذكره، ص 206.

— دليل غير مرئي: أي أنه يدور في كنف الحقل المغناطيسي أو الكهربائي، حيث يحتوي على بيانات ومعلومات ذات هيئة الكترونية غير ملموسة، يتم إدراكها باستخدام أجهزة ومعدات الحاسب الآلي (Hardware) ونظم برمجيات الحاسوب (Software)¹.

ثانيا: الخصائص المتعلقة بمرونته

تتعلق هذه الخصائص بسرعة تطوره، قابليته للنسخ وسهولة استرجاعه، وستتناول بالدراسة الحديث عن هذه العناصر وفق التقسيم التالي:

— دليل متنوع ومتطور: تتسم الأدلة الجنائية الرقمية بطبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعددة بذلك الحدود الزمانية والمكانية²، وتظهر ميزة التنوع في الدليل الرقمي في أنه قد يتخذ أشكالا متعددة تحمل بيانات ومعلومات قابلة للتداول، وفي ذات الوقت فهو متطور بحكم ارتباطه ببيئة افتراضية حركية تشكل مستودعا رقميا يصعب احتواء مضامينها.

— دليل قابل للنسخ: على خلاف الأدلة التقليدية التي لا تتوافر فيها هذه الخاصية، فإن الدليل الرقمي يمكن استخراج نسخ منه مطابقة للأصل ولها نفس القيمة العلمية³، وهو ما من شأنه توفير حماية تقنية لهذا الدليل من أي استخدام غير مشروع لمحتواه بغرض محاولة الطمس أو الإخفاء أو الإتلاف أو التصرف فيه.

— إمكانية وسهولة الاسترجاع: بالرغم من إتاحة الحاسب الآلي ووسائل الاتصال الحديثة لإمكانية حذف أو إلغاء المحتويات التي تتضمنها بمجرد النقر على خاصية "الحذف"، غير أن ذلك لا يمنع من إعادة استرجاعها باستخدام برامج تقنية حديثة، ذلك أن المعلومات والمحتويات المخزنة حتى وإن تم حذفها نهائيا من قرص التخزين، ستظل محتفظة برموز وشيفرات رقمية خاصة بتلك الملفات.

المطلب الثاني: موضوع جريمة الابتزاز الالكتروني

إن التطورات والتغيرات التي عرفها العالم في شتى المجالات اقترن بظهور أنماط جديدة من الجرائم المستحدثة اتخذت من الفضاء الافتراضي بيئة خصبة لممارسة هذه النشاطات الإجرامية، ومن أكثر الجرائم استفحالا في وقتنا الحالي، تلك الجرائم التي ترتكب بواسطة وسائل التواصل الاجتماعي كجريمة الابتزاز الالكتروني التي تعد نتاج الاستخدام السليبي للإنترنت بصفة

— بن فردية محمد، مرجع سبق ذكره، ص 278.

² — مروة صلاح الدين محمد، مرجع سبق ذكره، ص 65.

³ — بن طالب ليندا، الدليل الالكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه علوم، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، نوقشت في 2019/01/23، ص 43.

عامة، وتصنف ضمن الجرائم الإلكترونية الواقعة على الأشخاص الأكثر إضرارا بمصالح الأفراد وسمعتهم ومكانتهم الاجتماعية على اختلاف مراكزهم القانونية في المجتمع.

نتعرض في هذا المطلب إلى التعريف بجريمة الابتزاز الإلكتروني في الفرع الأول، ثم نحدد أركان جريمة الابتزاز الإلكتروني من خلال الفرع الثاني.

الفرع الأول: التعريف بجريمة الابتزاز الإلكتروني

تعتبر جريمة الابتزاز الإلكتروني من الظواهر الإجرامية المستحدثة التي أخذت في الاستفحال بشكل متسارع في البيئة الرقمية وعرفت منحنا تصاعديا خطيرا في المجتمعات، وقصد الإلزام بجوانب الموضوع يتوجب تحديد المقصود بجريمة الابتزاز الإلكتروني أولا، ومن ثم التعرف على دوافع الابتزاز الإلكتروني ثانيا.

أولا: تحديد المقصود بجريمة الابتزاز الإلكتروني

قبل الشروع في تحديد المقصود بجريمة الابتزاز الإلكتروني لابد من الوقوف على معنى الابتزاز، والذي يراد به الحصول على المال أو المنافع من شخص بالإجبار والإكراه بواسطة التهديد بفصح أسرارته التي يمتلكها¹، وانطلاقا من التعريف السابق يعدّ الابتزاز الإلكتروني صورة مستجدة للابتزاز أو التهديد التقليدي كإحدى مظاهر التطور التكنولوجي.

و الابتزاز الإلكتروني أسلوب من أساليب الضغط والإكراه، يتمثل في قيام المبتز بالضغط على شخص آخر و هو المجني عليه بالتهديد تارة و الوعيد تارة أخرى، و ذلك بنشر صور أو معلومات أو مقاطع فيديو لا يرغب المجني عليه إظهارها، و غرض الجاني من ذلك تحقيق مقاصده الإجرامية و الوصول إلى هدفه الذي قد يكون ماديا أو معنويا أو جنسيا، و في حالة عدم استجابة المجني عليه لمطالبه يقوم بنشر هذه المعلومات السرية التي بحوزته على منصات أي وسيلة من وسائل التواصل الاجتماعي، و هو ما يدفع المجني إليه إلى تلبية مطالب الجاني خوفا من المساس بسمعته أو مكانته في المجتمع².

ثانيا: دوافع جريمة الابتزاز الإلكتروني

تتنوع المحركات الداخلية والخارجية لجريمة الابتزاز الإلكتروني حسب طبيعة الجريمة وصفة المجني عليه وجنسه والغاية التي يرمي إليها المبتز من وراء ابتزازه الإلكتروني، فقد تكون دوافع مادية، دوافع غير أخلاقية أو دوافع عاطفية.

¹ _ حسين عبد الكريم يونس، خليل يوسف جندي، الابتزاز الإلكتروني والجرائم الإلكترونية المفهوم والأسباب، الطبعة الأولى، دار كفاءة المعرفة، عمان، الأردن، سنة 2021، ص49.

² _ سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي (دراسة مقارنة)، دون طبعة، دروب المعرفة للنشر والتوزيع، الإسكندرية، مصر، سنة 2022، ص111.

ـ **دوافع مادية:** فقد تكون الرغبة التي تحرك السلوك الإجرامي لدى المبتز رغبة تتعلق بالحصول على كسب مادي¹، وينصرف هذا الأخير إلى منفعة مالية أو خدماتية يطلبها المبتز من المجني عليه ويحدد مهلة معينة لتنفيذ طلباته تحت طائلة التهديد بنشر أو تسريب المعلومات السرية التي يحوزها عن الضحية.

ـ **دوافع غير أخلاقية:** وتعرف أيضا بالدوافع والرغبات الجنسية، وتجد هذه الدوافع تطبيقاتها على النساء والأطفال خصوصا في البيئة الرقمية، حيث يسعى المبتز لتلبية رغباته الجنسية من خلال ابتزاز ضحاياه من الجنسين، وقد يكون الابتزاز نتاج علاقة عاطفية أو ارتباط عبر وسائط التواصل الاجتماعي وتنتهي باستغلالها من طرف المبتز تحت التهديد والإكراه لإقامة علاقة جنسية افتراضية أو جسدية.

ـ **دوافع عاطفية:** في هذه الحالة يكون الانتقام أو الكره والحقد وكذا الضغائن الشخصية دافعا لارتكاب الجريمة، كما قد يكون حبا في التسلط وإثبات الذات، حيث يقوم المبتز باستدراج ضحيته عبر الوسائط الافتراضية التي غالبا تكون شخصا معلوما من محيطه سواء المهني، الأسري أو الاجتماعي، ويعتمد المبتز في ذلك على إنشاء حسابات وهمية لتنفيذ مخططاته.

الفرع الثاني: أركان جريمة الابتزاز الإلكتروني

بالنظر إلى جريمة الابتزاز الإلكتروني على أنها فعل إجرامي مستحدث، فإن قيامها يتطلب توافر ثلاثة أركان أساسية المتعارف عليها في الجرائم التقليدية، غير أن الأولى تتسم بخصوصية تجعلها تختلف وتباين عن الجريمة الكلاسيكية، وهو ما سيتم التفصيل فيه من خلال هذا الفرع.

أولا: الركن الشرعي

تخضع جميع الجرائم مهما كان نوعها وطبيعتها لمبدأ الشرعية الجزائية، وفحواه سيادة القانون في مجال التجريم والعقاب ، وتستقر التشريعات الجنائية الحديثة في مواجهة أنماط الإجرام المستحدث إلى إيجاد نصوص خاصة في تجريمها لتلك الأفعال الإجرامية، سواء عن طريق دمج النصوص الجزائية في قانون العقوبات أو وضعها في تشريع جزائي خاص.

ومن بين التشريعات العربية التي عנית بتجريم الأفعال المادية المكونة لجريمة الابتزاز الإلكتروني التشريع السعودي، حيث أشار إلى تجريم الابتزاز الإلكتروني ضمن المادة 03 من نظام مكافحة الجرائم المعلوماتية السعودي²، ويندرج تحت شمول

¹ Hassan Obaid Alkaabi, **Extortion and fraud crimes through electronic media at the UAE legislation**, an analytical study, E- Journal on integration of knowledge, 7th Edition , 2009, p 160, Published by <https://worldconferences.net>.

² المادة 03 من نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ الموافق لسنة 2007، مرسوم ملكي رقم م/17 بتاريخ 08 ربيع الأول سنة 1428هـ الموافق لـ 27 مارس/آذار سنة 2007، قرار مجلس الوزراء رقم 79 الصادر بتاريخ 07 ربيع الأول سنة 1428هـ الموافق لـ 28 مارس/آذار سنة 2007، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية، متوفر على الموقع الإلكتروني لهيئة الخبراء عبر الرابط: <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1>، تم

الاطلاع بتاريخ 01 أوت 2022، على الساعة 11:40.

النص كل ما شأنه المساس بالحياة الخاصة باستخدام وسائل التكنولوجيا والاتصال الحديثة كالهواتف النقالة المزودة بتقنية الكاميرا أو ما في حكمها.

كما جرمّ المشرع الإماراتي الابتزاز الإلكتروني قانونا بموجب المادة 16 من قانون مكافحة جرائم تقنية المعلومات الصادر سنة 2012¹، مشيرا إلى الوسيلة المستعملة في ارتكاب الجريمة سواء باستخدام الشبكة المعلوماتية أو أي وسيلة من وسائل تقنية المعلومات، وشدد العقوبة إذا نتج عن الجريمة مساسا بالشرف والاعتبار.

المشرع الجزائري على غرار باقي التشريعات تبني الشمولية في تجريمه للأفعال التي يكون مسرحها الكتروني، وذلك من خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها²، وهو ما يستشف من نص المادة 02 منه التي جرمت كل الأفعال الإجرامية التي ترتكب باستخدام تكنولوجيا الإعلام والاتصال، فتكون جريمة الابتزاز الإلكتروني بذلك من ضمنها استنادا إلى عمومية النص الذي يحيلنا بدوره إلى القواعد التقليدية المطبقة على جريمة التهديد في صورتها الكلاسيكية.

فجريمة التهديد التقليدية التي تقتزن غالبا بالتشهير لم تتغير من حيث الأركان في ظل التحولات الرقمية والمعلوماتية، إذ لا يأبه المشرع بالوسيلة التي ترتكب بها الجريمة مدام أنها تنصرف إلى ذات النتيجة الإجرامية أي المساس بالحياة الخاصة³، وما الابتزاز الإلكتروني إلا صورة مستجدة للتهديد والابتزاز التقليدي المنصوص عليه في المادة 371 من قانون العقوبات الجزائري⁴، وإن كانت العديد من التشريعات تعتبر الابتزاز و التهديد مصطلحين لهما نفس المدلول، بيد أنه من وجهتنا نكون أمام جريمة ابتزاز إذا حصل تهديد مصحوبا بحمل الضحية للقيام بعمل أو الامتناع عنه، أما جريمة التهديد فتتنصرف إلى الوعيد دون مطالبة المبتز للمجني عليه و إرغامه على القيام بعمل معين.

ثانيا: الركن المادي

¹ _ مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ 25 رمضان سنة 1433 الموافق لـ 13 أغسطس سنة 2012، **الجريدة الرسمية**، العدد خمسمائة وأربعون 540 (ملحق)، السنة الثانية والأربعون، الصادرة في شوال 1433هـ الموافق أغسطس 2012.

² _ قانون رقم 04-09 مؤرخ في 14 شعبان عام 1430هـ الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، العدد 47، الصادرة بتاريخ 25 شعبان عام 1430هـ الموافق 16 غشت سنة 2009.

³ _ عكوش سيهام، الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري، **مجلة السياسة العالمية**، الصادرة عن مخبر الدراسات السياسية والدولية بجامعة احمد بوقرة يومرداس المجلد (6)، العدد (1)، الجزائر، سنة 2022، ص1300.

⁴ _ قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427هـ الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، **الجريدة الرسمية**، العدد 87، الصادرة بتاريخ 4 ذي الحجة عام 1427هـ الموافق 24 ديسمبر سنة 2006.

يتمثل الركن المادي لجريمة الابتزاز الالكتروني في السلوك الصادر عن الجاني، والذي يتحقق بقيام المبتز (المستخدم) بتهديد المجني عليه سواء كتابة أو قولاً أو أي فعل آخر يتجسد في القيام بفعل التهديد بنشر بيانات أو صور أو مقاطع مرئية للضحية المقترن بالضغط والإكراه لإرغام المجني عليه للقيام بذلك الفعل أو الامتناع عنه، مهما كانت الوسيلة التي حصل بواسطتها الجاني على تلك المعلومات، ولا يشترط أن يتم التهديد بطريقة معينة، إذ يمكن أن يتم عن طريق غرف الدردشة أو عن طريق البريد الالكتروني أو بتسجيل صوتي¹.

ومن ثم متى بث المبتز الرعب والخوف والرغبة في نفسية الشخص المجني عليه بالتهديد والوعيد بإفشاء أسرار أو جانب من حياته الخاصة مقابل الحصول على منفعة مادية أو معنوية أو جنسية، ترتب على ذلك قيام المسؤولية الجزائية للجاني بتوافر الركن المادي للجريمة، حتى وإن لم تتحقق النتيجة الإجرامية المتمثلة بتنفيذ الجاني لوعيده ونشر وعرض تلك المعلومات والصور والمقاطع المرئية وجعلها معلنة ومتاحة للجمهور.

فجريمة التهديد قائمة بذاتها ويكفي أن يكون التهديد جدياً كأن يباشر الجاني التنفيذ بإنشاء موقع أو صفحة عبر وسائل التواصل الاجتماعي للتشهير بشخص معين دون البدء في طرح وإفشاء المحتويات السرية التي بحوزته، فالركن المادي لجريمة الابتزاز الالكتروني يقوم على ثلاثة عناصر: نشاط إجرامي يأتيه الجاني و نتيجة إجرامية سواء تحققت أو لم تتحقق و اقتصر على التهديد فقط ، إضافة إلى العلاقة السببية بتنفيذ الجاني لتهديده بالنشر و العلانية لتلك المعلومات التي تتعلق بالشخص المجني عليه على المنصات الالكترونية و وسائل التواصل الاجتماعي².

ويمكن أن يحصل الابتزاز الالكتروني عن طريق الاختراق كقيام أحد الجناة بالدخول غير المشروع إلى حاسوب شخصي أو صفحة شخصية لأحد الأفراد مستخدماً برمجيات الاختراق، ومن التطبيقات القضائية على ذلك، ما اهتمت إليه الهيئة الجزائية لمحكمة التمييز الاتحادية بالعراق في قرارها الصادر بتاريخ 2019/03/17 بإدانة متهم قام باختراق صفحة شخصية لأحد الأشخاص، والاستيلاء على صور شخصية له والتهديد بنشرها والإساءة إليه ومساومته بإعطائه أرصدة بطاقات تعبئة ومبالغ مالية³.

ثالثاً: الركن المعنوي

تتطلب جريمة الابتزاز الالكتروني قيامها ركناً معنوياً إلى جانب الركن المادي و الشرعي لها، فهي تعد من الجرائم العمدية تأخذ صورة القصد الجنائي الذي يقوم بتوافر عنصري العلم الإرادة، أي لا بد أن يعلم الجاني بنتيجة السلوك الذي اقترفه و أن ينصب علمه على أن ما يقوم به من حصول على صور فاضحة و بيانات سرية لأحد الأشخاص و تهديده بها مقابل

¹ _ عراب مريم، جريمة التهديد والابتزاز الالكتروني، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، الجزائر، سنة 2021، ص1208.

² _ عكوش سيهام، مرجع سبق ذكره، ص1301.

³ _ قرار لمحكمة التمييز الاتحادية العراقية، رقم 3758، الهيئة الجزائية، الصادر بتاريخ 2019/03/17، قرار غير منشور، ينظر: سيف مجيد العاني ، مرجع سبق ذكره، ص115 وما بعدها.

الحصول على منفعة جريمة يعاقب عليها القانون¹، أما العنصر الثاني المتمثل في الإرادة المنصرفة إلى السلوك الإجرامي و توقع النتيجة الإجرامية في الوقت نفسه²، أي أن يكون الجاني مدركا إدراكا تاما لما سيقدم عليه من نشاط إجرامي و أن هذا الأخير من شأنه إلحاق ضررا و أذى بالغير سواء في نفسه أو ماله أو شرفه و سمعته.

المبحث الثاني: القيمة القانونية للدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني

يحرص مرتكبي جريمة الابتزاز الإلكتروني على طمس أفعالهم الإجرامية و إخفاء هوياتهم حتى لا تطالهم يد العدالة و يتملصوا من العقاب، و هذا يعدّ أكبر تحدي تواجهه الأجهزة المكلفة بالتحقيقات الجنائية و القاضي على حد سواء ، حيث تنصب القوة الإثباتية الدامغة للدليل الرقمي الجنائي على صلاحيته و مكانته أمام القضاء الجزائي، فالأدلة جوهر الحكم التي لا يمكن إدراكها إلا بتوافر عناصر هامة و ممارسة القاضي لسلطته في تقديرها، و بالتالي فإن هذا المبحث سيتعرض بالدراسة إلى الأحكام الخاصة بالدليل الرقمي في الإثبات الجنائي في **المطلب الأول**، و تقييم الدليل الرقمي الجنائي في جريمة الابتزاز الإلكتروني **كمطلب ثان**.

المطلب الأول: الأحكام الخاصة للدليل الرقمي في الإثبات الجنائي

يرتكز الإثبات الجنائي بالأدلة الرقمية على مراعاة أسس ومعايير، فمجرد وجود دليل على وقوع جريمة ما ليس معناه إدانة مرتكبها، وإنما يتوقف ذلك على مراعاة ضوابط إجرائية يشترك في احترامها المكلفين بالتحقيقات الجنائية والقاضي الجزائي وفقا لسلطته التي يتمتع بها، وهو ما سنحاول التفصيل فيه من خلال هذا المطلب، بالتطرق إلى المتطلبات الإجرائية الواجب توفرها لقبول الدليل الرقمي في **الفرع الأول**، ثم تناول سلطة القاضي الجزائي في تقدير الدليل الرقمي في **الفرع الثاني**.

الفرع الأول: المتطلبات الإجرائية الواجب توفرها لقبول الدليل الرقمي

إن الحديث عن مقبولية الدليل الرقمي أمام القضاء الجزائي مرهون بتوافر عدّة ضوابط تعد بمثابة حجر الأساس في صحة الإجراءات المتخذة لاستخلاص الدليل الرقمي الجنائي من رحم النظم المعلوماتية والحاسب الآلي، أو مختلف تقنيات التكنولوجيا والاتصال الحديثة، و يسبق توافر هذه الضوابط الإجرائية حتمية الخوض في الأساس الذي يستند إليه هذا الدليل حسب نظام الإثبات السائد في الدولة، و هو ما يفرض علينا تحديد أساس قبول الدليل الرقمي الجنائي في الإثبات الجنائي **أولا**، انطلاقا من تبين موقف التشريعات المقارنة و المشرع الجزائري من الدليل الرقمي الجنائي، لنتطرق بعدها إلى شروط قبول الدليل الرقمي أمام القضاء الجزائي **ثانيا**.

أولا: أساس قبول الدليل الرقمي الجنائي في الإثبات الجنائي

¹ _ عراب مريم، مرجع سبق ذكره، ص1208.

² _ سيف مجيد العاني، مرجع سبق ذكره، ص117.

يعتبر الإثبات الجنائي العصب الرئيسي للحكم الجزائي الذي يهتدي من خلاله القاضي إما للبراءة أو الإدانة، و قد عرفت التشريعات الجنائية ثلاثة أنظمة للإثبات، و لا يثار الإشكال بشأن الأدلة الرقمية للتشريعات التي تأخذ بنظام الإثبات الحر طالما أن القاضي يملك الحرية في تقدير الأدلة المعروضة أمامه، و بالمقابل يكتنف قبول الأدلة الرقمية في الأنظمة التي تعتنق نظام الإثبات القانوني أو المقيد عدّة إشكالات قانونية نظرا لطبيعة هذا النظام و تفويضه لقناعة القاضي و حريته في تقدير قيمة الدليل المعروض عليه وفق ما يمليه عليه ضميره المهني.

و خروجاً عن الأصل العام الذي تتبناه التشريعات التي أخذت بنظام الإثبات القانوني أو المقيد، نجد البعض منها يجيز الأخذ بالدليل الرقمي على أساس أصالته، وهو ما سلكه المشرع الأمريكي في قانون الإثبات الأمريكي من خلال المادة 1001 في فقرتها الثالثة التي أجازت للقضاء الاستناد إلى المخرجات الرقمية كدليل إثبات متى تبين لها أن تلك المخرجات تتسم بالدقة وبوصفها أصلية، شريطة أن يتم طباعتها في شكل نسخ يمكن قراءتها بالعين المجردة¹، و هو نفس ما أخذ به المشرع الإنجليزي في المادة 69 من قانون الشرطة و الإثبات الجنائي لسنة 1984 المعدل و المتمم، حيث اعتبر أن مقبولية مخرجات الحاسب الآلي كدليل إثبات مرتبط بتوافر الشروط المحددة قانوناً لهذا الدليل².

و فيما يخص التشريعات الجنائية ذات الصياغة اللاتينية، فإن إثبات الجرائم يكون بجميع طرق الإثبات المشروعة، و يخضع ذلك لمبدأ اقتناع القاضي كأصل عام ما لم ينص القانون على خلاف ذلك، و قد تبنى مبدأ الإثبات الحر المشرع الفرنسي في المادة 427 من قانون الإجراءات الجزائية الفرنسي³، و كذا المشرع الجزائري في المادة 212 من قانون الإجراءات الجزائية الجزائري⁴، و جاءت المادة 06 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، لتؤكد مقبولية الدليل الإلكتروني أمام القضاء كدليل إثبات و الذي يخضع للقواعد العامة المقررة في قانون الإجراءات الجزائية.

ثانياً: شروط قبول الدليل الرقمي أمام القضاء الجزائي

بعد الحديث عن الأساس القانوني الذي يستند عليه الدليل الرقمي الجنائي ومدى مقبوليته أمام القضاء الجزائي، فإن ذلك غير كاف لتقدميه كدليل ما لم تتوفر الضوابط الإجرائية الكفيلة باعتباره دليل إثبات أمام الجهات القضائية المختصة، فلا بد أن يتم الحصول عليه بطرق مشروعة قانوناً و يخضع للمناقشة، إضافة إلى عدم قابليته للشك و هو ما يعبر عنه بيقينية الدليل الرقمي الجنائي.

¹ _ Federeal rules of evidence, 116th congress 1st session No.5, december 1.2019, printed for the use of the committee on the judiciary house of representatives, U.S government publishing office. Washington 2020, Published by : <https://www.uscourts.gov>

² _ police and Criminal Evidence act 194 c.60, UK public general acts, published by : www.legislation.gov.uk

³ _ Article 427, code de procédure pénale république France, publiée par : <https://www.legifrance.gouv.fr>

⁴ _ الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية، المعدل بالقانون رقم 19-10 مؤرخ في 11 ديسمبر سنة 2019، طبعة محينة، دار بلقيس للنشر، الدار البيضاء، الجزائر، سنة 2020، ص124.

فمن حيث مشروعيته يتوجب أن يتم استخلاص الدليل الرقمي الجنائي بطرق صحيحة و مشروعة قانونا، في إطار أحكام القانون و احترام قيم العدالة و أخلاقياتها بما فيها احترام و صون حقوق الأفراد و عدم المساس بها، و هذه المسؤولية ملقاة على كاهل المكلفين بالتحقيقات و التفتيش الجنائي، و يناط بمؤلاء الحصول على الدليل وفق ما يقضي به القانون و بما لا يتعارض مع القواعد الجوهرية للإجراءات الجزائية و القواعد العامة¹، و إلا ترتب على ذلك بطلان الإجراءات و عدم صحتها و فقدان الدليل لقيمته أمام القضاء، و من قبيل ذلك الحصول على الدليل الرقمي عن طريق التدليس و الغش أو الضغط أو إكراه المشتبه فيه أو التحريض دون مسوغ قانوني، فكل ذلك يقع تحت طائلة البطلان و العقوبات الجزائية المنصوص عليها في المادة 107 من قانون العقوبات الجزائري² و المادة 85 من قانون الإجراءات الجزائية.

هذا و تعد مشروعية الدليل الرقمي شرطا أساسيا وجوهريا تضمنته التوصية 18 للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في مجال إصلاح الإجراءات الجزائية و حماية حقوق الإنسان التي انعقدت بربو دي جانيرو عاصمة البرازيل بشأن جرائم الكمبيوتر في الفترة ما بين 04 و 10 سبتمبر سنة 1994، حيث اعتبرت الأدلة المتحصل عليها بطرق غير مشروعة باطلة ولا يمكن أن يعتد بها أمام القضاء³.

و لا يصوغ للقاضي أن يبني حكمه بأي حال من الأحوال بناء على أهوائه الشخصية، ما لم يعرض الأدلة الموجودة في ملف الدعوى مهما كانت طبيعتها إلى المناقشة من طرف الأطراف، حيث يشكل هذا المبدأ ضمانة هامة من ضمانات المحاكمة العادلة ، و تم التنصيص عليه في المادة 212 في فقرتها الثانية من قانون الإجراءات الجزائية، و ينطبق ذلك على الأدلة الرقمية المستخرجة من البيئة الالكترونية، فمبدأ المناقشة موجب للقاضي حتى يكون حكمه مبني على أساس و مستساغ ، و ذلك بمنحه للخصوم حق مناقشة الدليل و الرد عليه و من ثم يكون للدليل أصل في أوراق الدعوى.

و يضاف إلى الشروط السابقة عدم قابلية الدليل الرقمي للشك، أي أن يكون مبني على الجزم و اليقين حتى يصلح دليلا للإدانة، فلا مجال لجحد قرينة البراءة و افتراض عكسها إلا عندما يتحقق اقتناع القاضي المبني على الجزم و اليقين⁴، غير أن اليقين بالدليل الالكتروني يختلف عن اليقين بالدليل التقليدي الذي يكون محلا للتحليل و التمحيص من طرف القاضي و من ثم ينطبع في ذهن هذا الأخير التصور الصحيح لصحة الدليل من عدمه، في حين يتوجب أن يخضع الدليل الالكتروني للخبرة الالكترونية للتأكد من عدم العبث به أو التغيير فيه، و هذه المهمة منوطة بالخبراء الذين لهم دراية بالمعارف التقنية

¹ _ بن طالب ليندا، مرجع سبق ذكره، ص 138.

² _ الأمر رقم 66-156 مؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، ج ر 49 المؤرخة في 11 جوان 1966 المعدل بالقانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016، ج ر 37، المؤرخة في 22 يونيو سنة 2016، دار بلقيس للنشر، الجزائر، سنة 2019، ص 54.

³ _ 15ème congrès international de droit pénal, 3 ème section : **les mouvements de réforme de la procédure et la protection des droits de l'homme**, rio de Janeiro, Brésil, 4-10 septembre 1994, association internationale de droit pénal, édition érès , N°20, année 2009 ,Toulouse, France, p178.

⁴ _ مروة صلاح الدين محمد، مرجع سبق ذكره، ص 120.

و الفنية و هي الخبرة التي تعبر عن أصالة الدليل الالكتروني و سلامته، و بناء على ذلك تبنى اليقينية التي تقود القاضي للبيئة القانونية و الحقيقة وفق استخلاص سليم سائع.

الفرع الثاني: سلطة القاضي الجزائي في تقدير الدليل الرقمي الجنائي

اتجهت العديد من التشريعات الجنائية الحديثة إلى تكريس مبدأ الاقتناع الشخصي للقاضي الجنائي بفعل تبنيها لنظام الاقتناع الحر أو ما يعرف بنظام الأدلة المعنوية، حيث أضحى للقاضي الجزائي دورا إيجابيا في عملية الإثبات وتقدير الأدلة وقوتها الإثباتية التي يبنى على أساسها حكمه ، دون أن يكون مقيدا بتطبيق النصوص القانونية تطبيقا آليا، والغرض من ذلك تمكين القاضي الجزائي من تحري الحقيقة حسب طبيعة و ملاسبات كل واقعة لاسيما أن القاضي الجزائي أضحى يتعامل مع أصناف جديدة من الإجرام المستحدث مسرحها الكتروني، و سنحاول في هذا الفرع تحديد مضمون هذا المبدأ (أولا)، ثم نطاق تطبيقه في التشريع الجزائري (ثانيا).

أولا: مضمون مبدأ حرية اقتناع القاضي الجزائي

تقوم نظرية الإثبات على عدة أسس و مبادئ و يعتبر مبدأ الاقتناع القضائي من أهمها، و وصول القاضي لحالة الاقتناع تكون نتاج الإمام بكافة عناصر الواقعة المعروضة أمامه، فالأقتناع الشخصي للقاضي الجزائي مؤداه الإيمان العميق و الركون إلى صحة الوقائع التي يقدمها أطراف الدعوى، و التي اعتمدها القاضي، و يتمخض عنها أثرا عميقا في نفسيته تجعله يصدر حكمه عن قناعة تامة¹، و عليه متى ساور القاضي شك بخصوص الأدلة المعروضة عليه و لم يطمئن إليها لا يمكنه الأخذ بها في بناء حكمه، و إنما وجب عليه استبعادها تطبيقا لقاعدة الشك يفسر لصالح المتهم، و إن كان مبدأ حرية اقتناع القاضي لا يطرح أي إشكال من ناحية الأدلة التقليدية التي يلعب فيها القاضي دورا إيجابيا فإن الأمر مغاير بالنسبة للأدلة الالكترونية، حيث يثار التساؤل عن مدى إمكانية تفعيل مبدأ الاقتناع الشخصي للقاضي الجزائي في تقديره للدليل الالكتروني المعروض عليه؟ وبعبارة أخرى هل يلعب القاضي الجزائي دورا أساسيا في تقدير الدليل الالكتروني تبعا لأقتناعه الشخصي؟ ذلك أن البعض يسلّم بأن تقدير القاضي من تقدير الخبر وأن هذا الأخير حسبهم يمثل حجز الزاوية في الإثبات القضائي.

الواقع أن الطبيعة العلمية للدليل الالكتروني تفرض الاستعانة بأهل الاختصاص، أي إخضاع هذا الدليل للخبرة الالكترونية من طرف مختص ملم بالجوانب الفنية والتقنية للنظم المعلوماتية وتحليل البرمجيات، فالقاضي لا يملك هذه الثقافة الفنية والتقنية بقدر ما يملكها الخبير، وهذا الأخير من خلال معالجته الالكترونية للبيانات يستطيع أن يؤكد أصالة الدليل وسلامته من أي عبث أو تغيير في محتوياته بشكل يمكنه أن يؤثر في ملاسبات الواقعة.

¹ _ عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سبق ذكره، ص249.

ومن ثم يتوقف عمل الخبير الإلكتروني على إعطاء القيمة العلمية القاطعة للدليل فحسب، و ليس للقاضي حرية في مناقشة الحقائق العلمية الثابتة و تقديره لا يتناول هذا الجانب، أما الظروف و الملابسات التي وجد فيها الدليل الإلكتروني فهي تدخل في نطاق التقدير الذاتي للقاضي و من صميم وظيفته القضائية¹، و مهما بلغ إلمام الخبير بالجوانب الفنية و التقنية لهذه الأدلة الرقمية، يبقى التقدير الأخير للقاضي الجزائي كونه يتمتع بالخبرة العلمية و القضائية معا و تأهيلا كافيا يمكنه من رسم صورة متكاملة العناصر و الملامح للواقعة المعروضة أمامه، و من ثم فالخبرة الإلكترونية و وسائل التكنولوجيا الحديثة المسخرة في استخلاص الأدلة الإلكترونية مساعدة للقاضي الجزائي في تكوين اقتناعه و الركون إلى الحقيقة التي تصبو إليها العدالة و لا تحل محل الاقتناع القضائي.

يستنتج أن مبدأ الاقتناع الشخصي للقاضي الجزائي ملازم لليقينية التي يتوجب أن يدركها القاضي الجزائي في بناء حكمه من خلال الموازنة بين الأدلة و تقديرها تقديرا صحيحا وسليما، وهذا المبدأ لا يتأثر بتغير طبيعة الأدلة مثلما هو الشأن في الدليل الرقمي موضوع الدراسة، فيجوز للقاضي أن يأخذ به متى اطمئن له، كما يمكنه استبعاده إذا سايره الشك حياله أو تبين له من خلال ملاحظات الواقعة أنه لا يصلح دليلا وأساسا.

ثانيا: نطاق تطبيق مبدأ حرية اقتناع القاضي الجزائي في التشريع الجزائري

أخذ المشرع الجزائري بمبدأ الاقتناع الشخصي للقاضي الجزائي صراحة ضمن نصوص قانون الإجراءات الجزائية، و كرس هذا المبدأ أمام جميع المحاكم الجزائية بمختلف درجاتها، و هو ما يستفاد من نصي المادتين 212 و 307 من قانون الإجراءات الجزائية، و بما لا يدع مجالا للشك فإن تكريس المشرع الجزائري لهذا المبدأ يجد مبرره في الدور الإيجابي الذي يلعبه القاضي الجزائي في مضامياته و موازنته للأدلة وفق بما يمليه عليه ضميره المهني و بما يتوافق مع المنطق و العقل سعيا للوصول إلى الحقيقة دون أن يخضع لأي رقابة تقوض قناعته أو تأثر عليها، ناهيك عن مبدأ حرية اقتناع القاضي الجزائي ينسجم مع التطورات و التغيرات الحاصلة في الوسائل الحديثة للإثبات الجنائي و ما قد يسفر عنها من أخطاء عند التسليم بها، فهي في نهاية المطاف غير ملزمة للقاضي و تخضع لتقديره و اقتناعه.

المطلب الثاني: تقييم الدليل الرقمي الجنائي في جريمة الابتزاز الإلكتروني

إن المواجهة التشريعية لجريمة الابتزاز الإلكتروني من خلال وضع قواعد موضوعية وإجرائية لم تكن كافية لاحتواء هذه الظاهرة الإجرامية والحد منها، ويرجع ذلك إلى الصعوبات التي تعترض الدليل الإلكتروني في هذه الجريمة والمرتبطة أساسا بطبيعة جريمة الابتزاز الإلكتروني وسرعة ارتكابها و القدرة على طمسها بإيعاز من المجني عليه حفاظا على سمعته، و هو ما

¹ _ خالد أبو بكر محمد أبو دبوس، حرية القاضي الجنائي في الاقتناع بالدليل الإلكتروني، *المجلة القانونية*، مجلة متخصصة في الدراسات والبحوث القانونية، المجلد 9، العدد 9، مصر، سنة 2021، ص 3134.

سنحاول التعرض له بالدراسة في هذا المطلب، حيث نتطرق إلى الصعوبات التي يثيرها الدليل الرقمي في جريمة الابتزاز الإلكتروني من خلال الفرع الأول، و من ثم نتناول معالجة هذه الإشكالات في الفرع الثاني.

الفرع الأول: الصعوبات التي يثيرها الدليل الرقمي في جريمة الابتزاز الإلكتروني

يكتنف الدليل الرقمي في جريمة الابتزاز الإلكتروني صعوبات تحول دون إمكانية الوصول إلى هذا الدليل أو إهداره ، وتتعلق أساسا هذه المشكلات فيمايلي:

أولا: امتناع المجني عليه عن الإبلاغ عن الجريمة

غالبا ما ترتكب جريمة الابتزاز الإلكتروني دون أن يتم الإبلاغ عنها من طرف المجني عليه أو يتماطل في إعلام الجهات المختصة بالانتهاك الواقع على خصوصيته وما تعرض له من تهديد وابتزاز، وذلك خشية من المجني عليه على سمعته مثلما هو الشأن في جرائم الابتزاز الإلكتروني التي تكون الفتاة ضحية فيها، فتتصرف هذه الأخيرة إلى الاستجابة لمطالب المبتز تحت طائلة الإكراه والخوف من نشر أسرارها.

كما يمكن أن تكون ضحايا هذه الجريمة من الشركات أو المؤسسات التي تمتنع هي الأخرى عن الإبلاغ عنها، خشية من اهتزاز سمعتها بين المتعاملين معها الذي ينجر عنه الإضرار بمصالحها الاقتصادية¹.

وبالتالي فإن ذلك يصعب من مأمورية الحصول على الدليل الرقمي، لاسيما إذا ما مضى وقت من الزمن قبل أن يتم اكتشاف الجريمة أو الإبلاغ عنها، ذلك أن الطبيعة الديناميكية التي يتسم بها الدليل الرقمي في مثل هاته الجرائم وسرعته وسلاسة عملية حذفه والتلاعب أو التغيير في مضمونه قد يؤدي إلى إهدار قيمته وإسقاط حجتيه ومن ثم الإفلات من العقاب.

ثانيا: استخدام برامج إخفاء الهوية وتطبيقاتها

يستخدم مرتكبي جرائم الابتزاز الإلكتروني في الكثير من الحالات برامج إخفاء الهوية التي توفرها تكنولوجيا المعلومات والاتصالات للمستخدمين، ومن أكثر هذه البرامج شيوعا برنامج "TOR" الذي تم تطويره من طرف مختبر أمريكي ك تقنية تعتمد على التشفير أي حظر الوصول وحركة المرور وإخفاء عنوان بروتوكول الإنترنت²، ويتيح مشاركة المعلومات دون الكشف عن أنشطة الجناة.

¹ _ عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سبق ذكره، ص228.

² _ Obstacles to Cyber crime investigations, United office on drugs and crime, published by : www.unodc.org

ومما لا شك فيه أن اعتماد الجناة على مثل هاته التقنيات والأدوات الفنية في إخفاء الهوية أو استعمال الهوية المستعارة يضع المكلفين بالتحقيقات الجنائية أمام عقبة أخرى تتعلق بالإسناد، أي تحديد المسؤول عن نشر معلومات أو بيانات سرية عن المجني عليه، وصعوبة تحديد الموقع الجغرافي للجاني.

الفرع الثاني: معالجة الإشكالات التي يثيرها الدليل الرقمي في جريمة الابتزاز الإلكتروني

على الرغم من الصعوبات التي سبق الحديث عنها إلا أن هذا لا ينفي وجود تقنيات وأدوات فنية تتلاءم وطبيعة الدليل الرقمي في جريمة الابتزاز الإلكتروني لاسيما مع النمو الرقمي في مجال تكنولوجيا المعلومات والاتصالات التي تشهده العديد من الدول وتبادل الخبرات فيما بينها.

أولاً: الاستعانة بالخبرة التقنية والفنية

إن عمق التغير و التحول الرقمي و التقني الذي شهده العالم تمخض عنه فكر بشري يمتلك قدرات و مهارات تقنية و دراية فنية بنظم تكنولوجيا المعلومات يسهل توظيفها في ارتكاب الجرائم و جريمة الابتزاز الإلكتروني من ضمنها لسهولة تنفيذها و صعوبة استخلاص الدليل الرقمي ، و من ثم يتوجب الاعتماد على خبراء معلوماتيين يجوزون على قدرات في التحليل الرقمي و الإعدادات البرمجية و الخوارزميات الرقمية لفك شيفرات و طلاسمة البيئة الافتراضية، و المساعدة في جمع الآثار الرقمية و تحديد مدى أصالة الدليل الرقمي أو إعادة تجميع مكوناته في حالة محاولة إتلافه، و كذا اقتفاء الأثر من خلال استخدام أدوات فنية و برامج للتتبع و أنظمة كشف الاختراق.

ثانياً: تسخير التكنولوجيا الحديثة في استخلاص الأدلة الرقمية

لتحافظ أجهزة الضبط القضائي و الجهات المكلفة بالتحقيقات الجنائية على نقطة تفوق دائمة في الكشف عن مرتكبي جريمة الابتزاز الإلكتروني يتوجب اتباع منهج مبتكر لاستخلاص الأدلة الرقمية ومعالجتها وتحليلها، وذلك من خلال تطوير التكنولوجيا وتطوير برامج مضادة لاقتفاء أثر الجناة والوصول إليهم¹، واستخلاص الأدلة من برمجيات إلكترونية متطورة تخضع للتحديث الدائم حسب التغيرات و التحولات التي تشهدها البيئة الرقمية، و إدراج الذكاء الاصطناعي في هذه العملية والذي يتيح إمكانية الكشف عن الوجه و التعرف التلقائي على الصوت.

¹ _ عبد الله ذيب محمود، أسامة إسماعيل دراج، مرجع سبق ذكره، ص232.

خاتمة:

سعت الدراسة إلى استيضاح الموضوعات المحيطة بالدليل الرقمي الجنائي ودوره في إثبات جريمة الابتزاز الإلكتروني من الناحيتين التقنية والقانونية، وقد توصلت الدراسة إلى جملة من النتائج تعد بمثابة حجر الأساس للتوصيات القابلة للنظر والتجسيد.

_ النتائج:

_ أخذت الأدلة الرقمية حيزا كبيرا في النظرية العامة للإثبات خصوصا في المسائل الجزائية، ودفع ذلك العديد من التشريعات إلى تطوير قواعدها القانونية بما يتماشى وطبيعة هذه الأدلة غير المادية وبما يستجيب للتحولات التقنية والمعلوماتية التي يشهدها العالم.

_ غياب تنظيم قانوني خاص بالأدلة الرقمية في التشريع الجزائري رغم ما تشهده البيئة الافتراضية من سلوكيات إجرامية استفحلت بشكل غير مسبوق، ووجود فراغ تشريعي يعتري الدليل الرقمي وكيفية التعامل مع هذا النوع من الأدلة.

_ قصور نصوص التجريم في المنظومة القانونية الجزائية في مجابهة واحتواء جريمة الابتزاز الإلكتروني في ظل غياب نص تشريعي واضح من منطلق مبدأ الشرعية الجزائية لتجريم مثل هاته النشاطات الإجرامية، وإحالة تجريمها إلى جريمة التهديد في صورتها التقليدية.

_ إحجام المجني عليه عن التبليغ واستخدام الجناة لرامج إخفاء الهوية في جريمة الابتزاز الإلكتروني يعد من أهم التحديات التي تواجه الدليل الرقمي، وهو ما يساعد على ضياع هذا الأخير وإهداره.

_ التوصيات:

_ ضرورة تعزيز الثقافة المعلوماتية والبرمجية من خلال إدراج مقررات دراسية تعنى بالأمن المعلوماتي التي تساعد في الحفاظ وتوفير الحماية للمعلومات والبيانات الشخصية من الاستخدام غير الآمن للإنترنت.

_ دعوة المشرع الجزائري إلى مواكبة فعلية وواقعية لما يعيشه العالم من تطور تقني وتكنولوجي واتساع النشاطات الإجرامية في البيئة الافتراضية، من خلال استحداث تنظيم قانوني خاص بالأدلة الرقمية وإصدار دليل ارشادي حول

كيفية التعامل مع الأدلة الرقمية وإتاحة الحصول عليه للعاملين في سلك القضاء وأجهزة الضبط القضائي والفنيين والمتخصصين.

__ الاعتماد على الخبرة الفنية والتقنية باستحداث مركز قانوني " الخبير المعلوماتي أو الإلكتروني " من ذوي الكفاءات ومن يملكون مهارات في علم نظم المعلومات والتحليل البرمجي، وتقييمهم في جدول الخبراء المعتمدين لدى الجهات القضائية المختصة.

__ الاستفادة من خبرات الدول الأجنبية في التعامل مع الأدلة الرقمية والأحكام والضوابط المتعلقة بها، كإجراء اختبارات الثقة الذي تعتمد عليه بعض الدول للتأكد من أصالة الدليل الرقمي وسلامته.

قائمة المراجع:

- 1_ بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتوراه علوم، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، نوقشت في 2019/01/23.
- 2_ بن فردية محمد، الدليل الجنائي الرقمي وحجتيه أمام القضاء الجزائري، دراسة مقارنة، المجلة الأكاديمية للبحث القانوني ، جامعة عبد الرحمان ميرة بجاية، كلية الحقوق والعلوم السياسية، المجلد 05، العدد 01، الجزائر، جوان 2014.
- 3_ جاسم محمد جندل، الجرائم الإلكترونية، الطبعة الأولى، دار معتز للنشر والتوزيع، عمان، الأردن، سنة 2022.
- 4_ حسين عبد الكريم يونس، خليل يوسف جندي، الابتزاز الإلكتروني والجرائم الإلكترونية المفهوم والأسباب، الطبعة الأولى، دار كفاءة المعرفة، عمان، الأردن، سنة 2021.
- 5_ خالد أبو بكر محمد أبو دبوس، حرية القاضي الجنائي في الاقتناع بالدليل الإلكتروني، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، المجلد 9، العدد 9، مصر، سنة 2021.
- 6_ سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي (دراسة مقارنة)، دون طبعة ، دروب المعرفة للنشر والتوزيع، الإسكندرية، مصر، سنة 2022.
- 7_ طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، جامعة بنغازي، كلية الحقوق، المجلد 12 ، العدد 01، ليبيا، دون ذكر السنة.
- 8_ عبد الرحمان خلفي، الإجراءات الجزائية في القانون الجزائري والمقارن، الطبعة السادسة، دار بلقيس، الجزائر، سنة 2022.
- 9_ عبد الله ذيب محمود، أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية "القواعد الموضوعية والإجرائية"، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، سنة 2022.
- 10_ عراب مريم، جريمة التهديد والابتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، الجزائر ، سنة 2021.

- 11_ عكوش سيهام، الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري، *مجلة السياسة العالمية*، الصادرة عن مخبر الدراسات السياسية والدولية بجامعة محمد بوقرة بومرداس، المجلد (6) ، العدد (1)، الجزائر، سنة 2022.
- 12_ عمر زودة، *الإثبات في المواد الجزائية*، دون طبعة، دار هومة، الجزائر، سنة 2021.
- 13_ مروة صلاح الدين محمد، *الدليل الالكتروني ومدى حجتيه في الإثبات الجنائي*، الطبعة الأولى، المكتب العربي للمعارف، دار البحوث القانونية ، القاهرة، مصر، سنة 2021.
- 14_ الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية، المعدل بالقانون رقم 19-10 مؤرخ في 11 ديسمبر سنة 2019، طبعة مخينة، دار بلقيس للنشر، الدار البيضاء، الجزائر، سنة 2020.
- 15_ الأمر رقم 66-156 مؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، ج ر 49 المؤرخة في 11 جوان 1966 المعدل بالقانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016، ج ر 37، المؤرخة في 22 يونيو سنة 2016، دار بلقيس للنشر، الجزائر، سنة 2019، ص 54.
- 16_ قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427هـ الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، *الجريدة الرسمية* ، العدد 87، الصادرة بتاريخ 4 ذي الحجة عام 1427هـ الموافق 24 ديسمبر سنة 2006.
- 17_ قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430هـ الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، *الجريدة الرسمية*، العدد 47، الصادرة بتاريخ 25 شعبان عام 1430هـ الموافق 16 غشت سنة 2009.
- 18_ نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428هـ الموافق لسنة 2007، مرسوم ملكي رقم م/17 بتاريخ 08 ربيع الأول سنة 1428هـ الموافق لـ 27 مارس/آذار سنة 2007، قرار مجلس الوزراء رقم 79 الصادر بتاريخ 07 ربيع الأول سنة 1428هـ الموافق لـ 28 مارس/آذار سنة 2007، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية، متوفر على الموقع الإلكتروني لهيئة الخبراء عبر الرابط: <https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1>، تم الاطلاع بتاريخ 01 أوت 2022، على الساعة 11:40.
- 19_ مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ 25 رمضان سنة 1433 الموافق لـ 13 أغسطس سنة 2012، *الجريدة الرسمية*، العدد خمسمائة وأربعون 540 (ملحق)، السنة الثانية والأربعون، الصادرة في شوال 1433هـ الموافق أغسطس 2012.
- 20_ قرار لمحكمة التمييز الاتحادية العراقية، رقم 3758، الهيئة الجزائية، الصادر بتاريخ 2019/03/17، قرار غير منشور.

21_charles R. swanson, Neil C. Chamelin, Leonard Territo, Robert W. Taylor, **Criminal investigation**, 11th edition. McGraw-Hill. United Kingdom, London, a business Unit of the McGraw-Hill Companies, New York, United States, 2011.

22_Eoghan Casey, **Digital Evidence and Computer Crime**, Third Edition, Published by Elsevier Inc, London, Uk, 2011.

23_ Hassan Obaid Alkaabi, **Extortion and fraud crimes through electronic media at the UAE legislation**, an analytical study, E- Journal on integration of knowledge, 7th Edition , 2009, Published by <https://worldconferences.net>

24_ Federal rules of evidence, 116th congress 1st session No.5, december 1.2019, printed for the use of the committee on the judiciary house of representatives, U.S government publishing office. Washington 2020, Published by : <https://www.uscourts.gov>

25_ police and Criminal Evidence act 194 c.60, UK public general acts, published by : www.legislation.gov.uk

26_ Article 427, code de procédure pénale république France, publiée par : <https://www.legifrance.gouv.fr>

27_ 15ème congrès international de droit pénal, 3 ème section: **les mouvements de réforme de la procédure et la protection des droits de l'homme**, rio de Janeiro, Brésil, 4-10 septembre 1994, association internationale de droit pénal, édition érés , N°20, année 2009 ,Toulouse, France.

28_ **Obstacles to Cyber crime investigations**, United office on drugs and crime, published by: www.unodc.org