

The Evidentiary Value of Digital Evidence in Digital Violence Crimes Against Women under Omani Law(A Legal Study)

10.35781/1637-000-198-004

د. نزار حمدي قشطة *
فاطمة بنت خليفة بن حميد العبرية
بيان بنت بدر بن محمد المرجبية
لوزة بنت صالح بن سالم المشايخية

*رئيس قسم القانون العام، جامعة الشرقية، سلطنة عمان

الملخص

جرائم العنف الرقمي ضد المرأة، وبما يحقق التوازن بين فعالية استخدامه في كشف الجريمة وإثباتها، وبين ضمان مشروعية الحصول عليه وسلامته وموثوقيته وحماية الحقوق والحريات الأساسية، وللإجابة على هذه الإشكالية اعتمد البحث على المنهج الوصفي التحليلي.

وقد توصلنا في هذا البحث إلى عدة توصيات كان أبرزها الحاجة إلى إعداد دليل إجرائي وطني موحد لجمع الأدلة الرقمية وحفظها وفحصها وتقديمها أمام القضاء، مع تدريب القضاة وأعضاء الادعاء العام ومأموري الضبط القضائي والخبراء على تطبيقه.

الكلمات المفتاحية: حجية الدليل، العنف الرقمي، الجرائم الالكترونية، الوسائل التقنية

في ظل التنامي المتسارع لاستخدام الوسائل التقنية في ارتكاب صور متعددة من العنف الرقمي، تبرز تحديات قانونية وعملية تواجه سلطات التحقيق والمحاكم الجنائية في إثبات هذه الجرائم، ولا سيما فيما يتعلق بجمع الأدلة الرقمية والتحقق من سلامتها وتحديد مدى حجيتها في الإثبات الجنائي، ويهدف البحث إلى بيان ماهية الدليل الرقمي وخصائصه، وتحليل الإطار التشريعي المنظم له، وتقييم مدى كفاية القواعد القانونية النافذة في إقرار حجيته في الإثبات الجنائي، فضلاً عن دراسة دور القاضي الجنائي في تقدير قيمته الإثباتية والتحقق من مشروعيته ومدى استيفائه للضوابط القانونية اللازمة للاعتماد به في تكوين عقيدته القضائية.

وتتمثل مشكلة البحث في إلى أي مدى يكفل التشريع العماني حجية الدليل الرقمي في إثبات

The Evidentiary Value of Digital Evidence in Digital Violence Crimes Against Women under Omani Law(A Legal Study)

NIZAR QASHTA*

FATMA ALABRI

Bayan Al-Marjabi

Lawza Al-Mashaykhi

*A'Sharqiyah University

Abstract

We present to you a research paper titled "The Evidentiary Value of Digital Evidence in Crimes of Digital Violence Against Women Under Omani Law (A Legal Study)." This study was prepared by researchers Nizar Qashta ,Fatma Al-Abri, Bayan Al-Marjibi, and Lawza Al-Mashaykhi, against the backdrop of the increasing use of technology to commit various forms of digital violence, and the accompanying challenges faced by investigative and judicial authorities in proving such crimes through digital evidence. The study aims to clarify the concept and characteristics of digital evidence, analyze the legislative framework governing it, and assess the adequacy of the applicable legal rules in recognizing its evidentiary value. It also examines the role of the criminal judge in assessing the admissibility, reliability, and legality of digital evidence.

The research problem is centered on the extent to which Omani legislation guarantees the evidentiary value of

digital evidence in proving crimes of digital violence against women, while achieving a balance between its effectiveness in detecting and proving crimes and ensuring the legality of its acquisition, integrity, reliability, and the protection of fundamental rights and freedoms. To address this issue, the study adopts the descriptive and analytical approach.

The research reaches several recommendations, most notably the need to develop a unified national procedural guide for the collection, preservation, examination, and presentation of digital evidence before the courts, together with specialized training for judges, members of the Public Prosecution, judicial police officers, and experts on its proper application.

Keywords: Evidentiary Value of Digital Evidence, Digital Violence, Cybercrime, Technological Means

المقدمة:

شهد العالم في السنوات الأخيرة تطوراً ملحوظاً ومتسارعاً في مجال تقنية المعلومات، وأصبح العالم الرقمي جزءاً لا يمكن تجزئته من حياة الأفراد اليومية لما يوفره من تسهيلات في مختلف مجالات الحياة، إلا أن هذا التطور قد صاحبه ظهور تصرفات مخالفة للقانون، ومن بينها جرائم العنف الرقمي والتي أصبحت تمثل تحدياً اجتماعياً وقانونياً لا سيما عندما تستهدف هذه الجرائم المرأة من خلال جرائم التهديد والابتزاز والتشهير وغيرها من الجرائم التي يتم استخدام تقنية المعلومات في ارتكابها.

وتختلف الجرائم التي تقوم على العنف الرقمي عن الجرائم التقليدية، وذلك من حيث الأثر، حيث أن الأثر الذي تتركه الجريمة الالكترونية يختلف عن الأثر الذي تتركه الجريمة التقليدية، ويتميز أثر الجريمة الالكترونية بأنه غير مادي كالمراسلات والصور والبيانات الرقمية، كما أن هذه الطبيعة للدليل الرقمي جعلت له قابلية للنسخ أو التعديل أو الحذف. وقد أثار ذلك تساؤلات حول مدى حجيتها في الإثبات والتأكد من صحتها وسلامة الحصول عليها ليتم اعتباره دليل يمكن من خلاله نسبة الجريمة إلى مرتكبها.

إشكالية البحث:

أثار التطور السريع في التقنية وظهور وسائل التواصل الاجتماعي المختلفة إلى ظهور العديد من الإشكاليات التي تستعدي التدخل السريع من التشريعات لمواجهة هذه التحديات وما ينتج عنها من تعدي على الغير، ويشير هذا البحث إشكالية مهمة تسعى لدراستها في هذا البحث وهي إلى أي مدى يكفل التشريع العماني حجية الدليل الرقمي في إثبات جرائم العنف الرقمي ضد المرأة، وبما يحقق التوازن بين فعالية استخدامه في كشف الجريمة وإثباتها، وبين ضمان مشروعية الحصول عليه وسلامته وموثوقيته وحماية الحقوق والحريات الأساسية؟

، ويتفرع عن هذه الاشكالية عدة أسئلة:

- 1- ما المقصود بالدليل الرقمي وما هي صوره وخصائصه ؟
- 2- ما هي أبرز جرائم العنف الرقمي ضد المرأة وصورها في التشريع العماني؟
- 3- ما الأساس القانوني لإثبات الجرائم الالكترونية بالدليل الرقمي؟
- 4- ما هي ضوابط قبول الدليل الرقمي؟
- 5- ما مدى سلطة القاضي التقديرية في تقدير الدليل الرقمي؟
- 6- ما هي أبرز التحديات العملية والقانونية في تقدير الدليل الرقمي؟

أهداف الدراسة:

ونهدف في هذا البحث لتحقيق عدة أهداف أهمها:

1. تحديد مفهوم الدليل الرقمي وصوره وخصائصه.
2. بيان أبرز صور جرائم العنف الرقمي ضد المرأة في التشريع العماني.
3. تحليل الأساس القانوني لحجة الدليل الرقمي في إثبات جرائم العنف الرقمي ضد المرأة.
4. تحديد الضوابط القانونية لقبول الدليل الرقمي في الدعوى الجزائية.
5. بيان نطاق السلطة التقديرية للقاضي الجنائي في تقدير الدليل الرقمي.
6. تحديد أبرز التحديات القانونية والعملية المرتبطة بحجة الدليل الرقمي.

أهمية البحث:

تظهر أهمية البحث في سعيها لمعالجة الإشكاليات التي يثيرها موضوع الدليل الرقمي وحجته في الإثبات في جرائم العنف الرقمي ضد المرأة، والإجابة على التساؤلات التي تثيرها الإشكالية، وتبرز أهمية البحث من الناحية النظرية في كون موضوع الأدلة الرقمية لا يزال فيه متسع كبير للبحث والتطوير، وذلك في ظل التطور المتسارع والمتجدد للعالم التقني، وسيساهم هذا البحث بإذن الله في إثراء المكتبة القانونية بدراسة جديدة خاصة في ظل صدور قانون مكافحة جرائم تقنية المعلومات مؤخراً.

أما من الناحية العملية فإننا نأمل أن تساهم هذه الدراسة في رفع الوعي القانوني في المجتمع العماني بشكل عام ولدى النساء بشكل خاص، فيما يتعلق بالأدلة الرقمية التي تتعلق بجرائم العنف الرقمي التي تقع على المرأة وطرق الوقاية منها ودور المرأة في مواجهتها للحد من آثار الجريمة.

منهجية الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي والتحليلي وذلك بما يتناسب وطبيعة موضوع البحث، بحيث يتمثل المنهج الوصفي في بيان طبيعة الدليل الرقمي ومقارنته بالأدلة التقليدية الأخرى وبيان صورته وخصائصه وعموماً ما يتعلق بالجانب النظري للبحث، أما المنهج التحليلي فيبرز في تحليل النصوص القانونية المنظمة للأدلة الرقمي والنصوص الاجرائية الأخرى المتعلقة بها.

الدراسات السابقة: فيما يلي أبرز الدراسات التي تم استخدامها في الدراسة الحالية:

1- أحمد محمد العمر، الدليل الرقمي وحجتيه في الإثبات الجزائي، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، سلطنة عمان، العدد الثالث، يناير 2020

تناولت هذه الدراسة موضوع الدليل الرقمي وحجتيه في الإثبات الجزائي وتمثلت إشكالية البحث في القيمة القانونية للدليل الرقمي والحجة التي تحظى بها في مجال الإثبات الجزائي، وتكمن أهمية دراسة الباحث في أهمية موضوع الإثبات الجزائي في الجرائم الإلكترونية، واتبع الباحث المنهج الوصفي التحليلي في دراسته مع الإشارة الى بعض مواقف المشرعين الجزائريين في هذا الصدد، وتتشابه هذه الدراسة مع دراستنا في الدليل الرقمي وحجتيه في الإثبات الجزائي، وتختلف دراستنا عن الدراسة السابقة في تناول الموضوع في ظل قانون مكافحة جرائم تقنية المعلومات العماني الصادر بالمرسوم السلطاني رقم (2026/61)، كما تناولنا لموضوع الدليل الرقمي جاء مرتبطاً بجرائم العنف الرقمي الواقع على المرأة في حين جاءت الدراسة السابقة لتتناول الدليل الرقمي بشكل عام.

2- ديب أكرم، نورة بن بوعبدالله، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الإلكتروني، مجلة الحقوق والعلوم الانسانية، مجلد 16، العدد 1، 2023

جاءت الدراسة السابقة أعلاه لمعالجة إشكالية رئيسية تمثلت في أي مدى يعبر الدليل الرقمي الجنائي عن الحقيقة التي تصبو إليها الدعوى الجزائية في جريمة الابتزاز الإلكتروني، وتهدف دراسة الباحث إلى بيان خصوصية الدليل الرقمي الجنائي من الناحيتين الفنية والقانونية وإبراز دوره في إثبات جريمة الابتزاز الإلكتروني من خلال استعراض قيمته القانونية أمام القاضي الجزائي والإشكالات التي يثيرها الدليل الرقمي في جريمة الابتزاز الإلكتروني، وخلصت الدراسة إلى عدة نتائج كان أبرزها أن الأدلة الرقمية أخذت حيزاً كبيراً في الإثبات في الجرائم الجزائية، كما توصلت الدراسة إلى وجود فراغ التشريعي في التشريع الجزائري لمعالجة مسألة الدليل الرقمي وطريقة التعامل مع هذا النوع من الأدلة، وأوصت الدراسة المشرع الجزائري بضرورة مواكبة التطور التشريعي ووجود تنظيم قانوني لمسألة الدليل الرقمي في الإثبات وإصدار دليل استرشادي لكيفية التعامل مع الأدلة الرقمية، وتتشابه هذه الدراسة مع الدراسة الحالية في بعض التوصيات الأخرى التي تمثلت في ضرورة تعزيز الثقافة المعلوماتية ووجود دليل إجرائي ينظم مسألة الدليل الرقمي إلا أن هذه الدراسة السابقة تختلف عن الدراسة الحالية في كون المشرع العماني نص على مسألة الدليل الرقمي في القانون إلا أننا نأمل أن يكون هناك تنظيم إجرائي لضمان سلامة الدليل الرقمي وإثبات حجتيه في الدعوى الجزائية.

جازية جبريل شعيتير، الحماية الجنائية للمرأة من العنف الإلكتروني: دراسة تحليلية مقارنة،

مجلة دراسات قانونية، جامعة بنغازي، العدد 32، ديسمبر 2025

بحث الدراسة السابقة في موضوع الحماية الجنائية للمرأة من العنف الإلكتروني، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي لنصوص التشريع الليبي والمنهج المقارن مع الإتفاقيات الدولية وبعض التشريعات الإقليمية، وتوصلت الباحثة إلى عدة نتائج كان أبرزها وجود قصور تشريعي في القانون الليبي الحالي، وأوصت الباحثة في الدراسة السابقة إلى ضرورة تعديل القانون لتشديد العقوبات في الجرائم التي تقوم على الكراهية والتمييز، وتختلف الدراسة السابقة عن الدراسة الحالية في تركيز الدراسة الحالية على موضوع الدليل الرقمي في جرائم العنف الرقمي ضد المرأة، في حين جاءت الدراسة السابقة لتتحدث عن الحماية الجنائية للمرأة من العنف الرقمي بشكل عام وتطرقت في دراستها إلى موضوع الدليل الرقمي، في حين تتشابه الدراسات في مسألة تعلق الحماية الجنائية والدليل الرقمي بجرائم العنف الرقمي ضد المرأة.

خطة البحث:

- المبحث الأول: الدليل الرقمي وجرائم العنف الرقمي ضد المرأة: الأسس والخصوصية
- المطلب الأول: الأسس القانونية للدليل الرقمي
- المطلب الثاني: خصوصية جرائم العنف الرقمي ضد المرأة
- المبحث الثاني: الضوابط القانونية لإثبات جرائم العنف الرقمي ضد المرأة بالدليل الرقمي
- المطلب الأول: حجية الدليل الرقمي وضوابط قبوله في الإثبات الجنائي
- المطلب الثاني: تقدير الدليل الرقمي في إثبات جرائم العنف الرقمي

المبحث الأول

الدليل الرقمي وجرائم العنف الرقمي ضد المرأة: الأسس والخصوصية

يتطلب البحث في موضوع الدليل الرقمي الوقوف أولاً على الإطار المفاهيمي للدليل الرقمي وجرائم العنف الرقمي ضد المرأة، وفي المبحث الأول من هذا المبحث سنبحث فيه في الأسس والخصوصية ونبدأ في المطلب الأول في بحث الأسس القانونية للدليل الرقمي، ثم نخرج إلى المطلب الثاني من هذا المبحث لبحث موضوع خصوصية جرائم العنف الرقمي ضد المرأة.

المطلب الأول: الأسس القانونية للدليل الرقمي

يعد الدليل الرقمي من المستجدات التي فرضها التطور التقني على نظام الإثبات، وذلك لما يختلف فيه الدليل الرقمي عن الدليل التقليدي، ويقتضي تحديد الأساس القانوني للدليل الرقمي إلى التعريف بالدليل الرقمي أولاً وتمييزه عن غيره من الأدلة التقليدية وهو ما سنبحث في الفرع الأول من هذا المطلب، كما تستلزم هذه الدراسة التعرف على خصائص الدليل الرقمي ومصادره في الفرع الثاني.

الفرع الأول: مفهوم الدليل الرقمي وتمييزه عن الدليل التقليدي

بداية وقبل تعريف الدليل الرقمي لابد من تعريف الدليل بشكل عام، ويعرف الدليل في الإصطلاح القانوني على أنه "الأداة التي تؤدي إلى إظهار الحقيقة أو الحق المتنازع عليه، أو يعرف على أنه الوسيلة التي يستخدمها أطراف النزاع لإثبات صحة الوقائع التي يدعونها"¹، فالدليل القانوني عموماً هو "ما يعين القاضي على الفصل في النزاع المعروض عليه بهدف الوصول إلى الحق وإظهار الحقيقة"²، أما الدليل الرقمي فيمكن تعريفه على أنه: "الدليل الذي يجد له أساساً في العالم الافتراضي إلى الجريمة"³، أو بتعريف آخر "هو الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة ومعدات أدوات الحاسوب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"⁴. ومما سبق يمكننا تعريف الدليل الرقمي على أنه "نوع من أنواع إثبات الجريمة يكون على شكل بيانات أو صور أو أي شكل

¹ أحمد محمد العمر، الدليل الرقمي وحجتيه في الإثبات الجزائي، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، سلطنة عمان، العدد الثالث، يناير 2020، ص 131-132

² المرجع السابق، ص 131

³ المرجع نفسه، ص: 132

⁴ المرجع نفسه، ص: 132

آخر من الأشكال التي يتم استخلاصها من الأجهزة التقنية بمختلف أنواعها وذلك لتعين القاضي الجزائي للوصول إلى الحقيقة وإظهار الحق".

وفي نصوص القانون، فقد عرف المشرع العماني الأدلة الرقمية وذلك في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61) التي تختص بالتعريفات في البند (12)، والتي جاء فيها على أنها: "أي بيانات أو معلومات إلكترونية لها قيمة ثبوتية مخزنة أو منقولة أو مستخرجة من النظام المعلوماتي أو وسيلة تقنية المعلومات"¹. ونلاحظ بأن التعريف قد بدأ بالبيانات أو المعلومات الإلكترونية، والتي عرفها المشرع العماني أيضا في ذات القانون وذات المادة في البند رقم (3) على أنها: "كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو نقله بوسيلة تقنية المعلومات أيا كان شكله، كالكتابة والصور والأصوات والرموز والإشارات والأرقام والشفرات والحروف"².

ويختلف الدليل الرقمي عن الدليل التقليدي في طبيعته ومفهومه وطريقة جمعه وحفظه وقابليته للتغيير وغيرها من الجوانب، إلا أنه وباختصار فإن الدليل التقليدي يرتبط بجوانب مادية يمكن فحصها بشكل مباشر، أي أنه ذو طبيعة مادية محسوسة مثل الدم والشعر والمستندات الورقية وتشمل وسائل الإثبات التقليدية شهادة الشهود واليمين والإثبات بالكتابة، كما أن طريقة حفظ الدليل الرقمي تختلف عن طريقة حفظ الدليل التقليدي، وتتضح هذه الفروقات بشكل أكبر في الفرع الثاني من هذا المبحث.

الفرع الثاني: خصائص الدليل الرقمي

يتميز الدليل الرقمي بعدة خصائص تميزه عن الدليل التقليدي، ومنها ما يلي:

أولا: الدليل الرقمي دليل غير ملموس: وذلك بسبب الطبيعة الغير مادية للدليل الرقمي، فهو غير ملموس كالسلاح وبصمات القاتل عليه في جريمة القتل، أو المال المسروق والآثار التي يتركها السارق في جريمة السرقة، أما في الجريمة الإلكترونية فإن الدليل الرقمي عبارة عن بيانات أو موجات على شكل رموز أو أشكال أو حتى شفرات، ولا تغير عملية التحليل أو النقل لهذه البيانات لتقديمها كدليل ملموس من طبيعتها الرقمية، لأن عملية نقلها من بيانات غير ملموسة إلى دليل مادي ملموس يمكن الاستدلال به ولا يغير من طبيعته الرقمية، وبسبب هذه الطبيعة فإن الدليل الرقمي يصعب التخلص منه بعكس الدليل التقليدي سهل الاتلاف³.

¹ (قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61) - المنشور في الجريدة الرسمية بالعدد 1651 - المنشور بتاريخ 7 / يونيو / 2026م.

(2) المرجع السابق

(3) أحمد محمد العمر، الدليل الرقمي وحجتيه في الإثبات الجزائي، مجلة الدراسات الفقهية والقانونية، مرجع سابق، ص134

ثانياً: الدليل الرقمي دليل علمي تقني: تعود هذه الخاصية للدليل الرقمي لكون البيانات التي يتم تحويلها إلى دليل ملموس هي في الحقيقة عبارة عن بيانات وأرقام ذات طبيعة إلكترونية تنشأ في عالم تقني وافتراضي يتم معالجتها بواسطة المختصين والفنيين عن طريق أجهزة تقنية وأسس علمية لاستخلاص الدليل الذي يستعين فيه القاضي في إثبات الجريمة للوصول إلى مرتكبها، أي أن هذه البيانات يتم معالجتها تقنياً حتى تصبح قابلة للاستناد عليها كدليل إدانة أو براءة، ويعد الدليل الرقمي دليل علمي لأن التقنية في حد ذاتها علم من العلوم التي يستعين بها المختصون للوصول إلى نتائج علمية تقنية¹.

ثالثاً: الدليل الرقمي متطور ومتنوع وعابر للحدود: ينشأ الدليل الرقمي في بيئة تقنية افتراضية، وهو ما يجعل وجوده لا يرتبط بمساحة معينة، فيسهل وجود الدليل الرقمي بين الدول بسرعه وسهولة، ويعود ذلك إلى الطبيعة الديناميكية للدليل الرقمي الذي يتخطى الحدود الزمانية والمكانية، إضافة إلى أن الدليل الرقمي بطبيعته هو دليل متطور لما يشهده العالم التقني بشكل عام من تطور مستمر².

ومما تقدم، نستنتج إن الدليل الرقمي يتميز عن الدليل التقليدي بخصائصه التي تفرضها طبيعته غير المادية، واعتماده على الوسائل التقنية في استخراج وإثباته، فضلاً عن سرعة تطوره وتجاوزه للحدود الإقليمية للدولة. ففي حين يرتبط الدليل التقليدي غالباً بمادة محسوسة يمكن معاينتها وإدراكها بصورة مباشرة، فإن الدليل الرقمي لا يستمد قيمته من وجوده المادي، وإنما من سلامة الوسائل الفنية التي تكشف عن محتواه وتثبت مصدره وسلامة تداوله، ومن ثم فإن هذه الخصائص تفرض تحديات خاصة أمام حجية الدليل الرقمي، لاسيما في جرائم العنف الرقمي ضد المرأة، بما يستلزم إحاطته بضمانات فنية وقانونية تكفل موثوقيته وتحول دون العبث به أو إنكار مصدره.

المطلب الثاني: خصوصية جرائم العنف الرقمي ضد المرأة

تُعد جرائم العنف الرقمي ضد المرأة من أخطر الجرائم التي تواجهها النساء في الوقت المعاصر، لما تخلفه من آثار نفسية واجتماعية ومهنية جسيمة تمتد إلى سمعتهن ومكانتهن وأمنهن الشخصي، وإزاء ذلك، اتجهت غالبية التشريعات إلى مواجهة هذه الجرائم باستحداث نصوص وقوانين خاصة، تستجيب للتحديات التي أفرزتها البيئة الرقمية، وتعالج قصور القواعد التقليدية عن الإحاطة بصور

¹ (بدور خالد الكربي، سليمان بن محمد المعلم، تأثير التقنية على وسائل الإثبات الرقمية في النظام السعودي، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، العدد 46، يوليو 2024، ص3268

² (ديب أكرم، نورة بن بوعبدالله، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الإلكتروني، مجلة الحقوق والعلوم الانسانية، مجلد 16، العدد1، 2023، ص403

الاعتداء المستجدة، وسنبحث في هذا المطلب صور العنف الرقمي الواقع على المرأة في الفرع الأول منه، وفي الفرع الثاني سنخرج إلى خصوصية إثبات جرائم العنف الرقمي ضد المرأة.

الفرع الأول: صور العنف الرقمي الواقع على المرأة

تتعدد صور العنف الرقمي الواقع على المرأة، وتتخذ أشكالاً متفاوتة في خطورتها ودرجتها، وعادة ما يتم ارتكاب جرائم العنف الرقمي دون مواجهة مباشرة بين الجاني والضحية، ويستغل الجناة الطبيعة المختلفة للجرائم الرقمية الغير ملموسة والسرية التي يتيحها المجال الرقمي ويصعب معها تعقب الجناة ومحاسبتهم، ومن صور العنف الرقمي الواقع على المرأة، الجرائم التي تمثل إعتداء على حرمة الحياة الخاصة مثل جريمة التحرش الإلكتروني، والتحرّض والاغواء لارتكاب الفجور أو البغاء، السب والقذف، والمطاردة الإلكترونية، التمرر الإلكتروني وجرائم التزييف العميق وغيرها من الجرائم الإلكترونية التي تمثل عنفاً رقمياً على المرأة، وفي هذا الفرع من هذا المطلب سنركز على أكثر الصور انتشاراً من جرائم العنف الرقمي ضد المرأة وهي:

1- الابتزاز الإلكتروني: وهي وسيلة ضغط أو تهديد يمارسها الجاني على الضحية للحصول على مكاسب مادية أو معنوية، وعندما يكون الابتزاز الإلكتروني موجهاً ضد المرأة فإن الجاني عادة ما يهدف إلى استغلال الضحية والسيطرة عليها لتلبية مطالبه، وتتوعد أهداف الجاني في جريمة الابتزاز بين أهداف مالية وأهداف جنسية أو قد يكون الهدف منها الإذلال والتحقير، ويستغل الجاني المرأة في جريمة الابتزاز الإلكتروني لضعف المرأة النفسي ومكانتها الاجتماعية¹، وقد نص المشرع العماني في قانون مكافحة جرائم تقنية المعلومات العماني الصادر بالمرسوم السلطاني رقم (2026/61) في المادة (40) منه والتي نصت على: "يعاقب بالسجن مدة لا تقل عن سنة، ولا تزيد على (3) ثلاث سنوات، وبغرامة لا تقل عن (1000) ألف ريال عماني، ولا تزيد على (3000) ثلاثة آلاف ريال عماني، كل من استخدم موقعاً إلكترونياً أو نظاماً معلوماتياً أو وسيلة تقنية المعلومات في تهديد شخص، أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، حتى ولو كان مشروعاً، وتكون العقوبة السجن مدة لا تقل عن (3) ثلاث سنوات، ولا تزيد على (10) عشر سنوات، وبغرامة لا تقل عن (3000) ثلاثة آلاف ريال عماني، ولا تزيد على (10,000) عشرة آلاف ريال عماني، إذا كان التهديد أو الابتزاز بارتكاب جنائية، أو بإتيان أمور مخلة بالشرف أو الكرامة"².

¹ (إيمان محمد عادل السعيد، الحماية الجنائية للمرأة من العنف الإلكتروني، مجلة روح القوانين، جامعة طنطا، المجلد 37، العدد 111، أغسطس 2025، ص 676)

² (قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61)، مرجع سابق)

2- التشهير الإلكتروني: التشهير يتمثل في "إطلاق شائعات أو معلومات سواء كانت كاذبة أم حقيقية تتضمن انتهاك لحرمة الحياة الخاصة، أو التلميح بما يضر بسمعة الشخص الطبيعي أو الاعتباري وينتج عن هذا التشهير ضرراً على المشهور يسبب له المعاناة"، وفي تعريف التشهير الإلكتروني لا يختلف في معناه عن التشهير بمفهومه السابق، إلا أنه وفي هذه الحالة يكون باستخدام وسائل التواصل الاجتماعي أو الوسائل الإلكترونية الأخرى بقصد الإضرار بسمعة الشخص والمساس بكرامته¹، ويجرم فعل التشهير الإلكتروني من خلال المادة القانونية الواردة في قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61)، وهي المادة (36) في الفقرة 3 منها والتي نصت على: "نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مقطع صوتي أو مرئي أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية بقصد الإضرار بالشخص"².

الفرع الثاني: خصوصية إثبات جرائم العنف الرقمي ضد المرأة

تقع جريمة العنف الرقمي ضد المرأة بوسائل مختلفة، فقد لا يكون الدليل موجوداً في مكان واحد ليسهل ضبطه واستخراجه وحفظه، وإنما قد يكون في هاتف المجني عليه أو هاتف المتهم، ويعتبر الهاتف الأداة الأهم في إثبات جريمة العنف الرقمي التي قد تقع على المرأة، كون الهاتف يجمع أغلب البرامج ووسائل التواصل الاجتماعي التي يتم استخدامها في الوقت الحالي، والتي قد يتم ارتكاب جريمة العنف الرقمي من خلالها، مثل تطبيق الواتساب والانسجرام أو مكالمات تهديد أو تحرش أو إنشاء حسابات مزيفة أو نشر الشائعات والإبتزاز والتهديد، كما يمكن العثور على تطبيقات التتبع في هاتف المتهم أو المجني عليها، وقد يتواجد الدليل الرقمي في البريد الإلكتروني للمتهم أو المجني عليه على شكل روابط خبيثة لاخترق حسابات المجني عليها وتهديدها وابتزازها بما يحصل عليه الجاني من بيانات، لذا فإنه ومع تعدد الوسائل التي يتم فيها ارتكاب جرائم العنف الرقمي ضد المرأة يتعدد معها الأدلة الرقمية لإثبات هذا النوع من الجرائم³.

وتتردد العديد من النساء في الإبلاغ عن جرائم العنف الرقمي التي تتعرض لها، وذلك خوفاً من الجاني في حال قامت بالإبلاغ عنه في أن ينفذ تهديده بكشف بياناتها أو صورها أو نشر الشائعات عنها، بالإضافة إلى خوف المرأة من نظرة المجتمع، لذا فقد أحاط المشرع مسألة الإثبات في جرائم العنف

¹ (منى أحمد عبدالفتاح أحمد السيد، مفهوم التشهير الإلكتروني والحماية القانونية الممنوحة للشخص، مجلة البحوث القانونية والاقتصادية، المجلد 15، العدد 92، ص4

² (قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61)، مرجع سابق

³ (جازية جبريل شعيتير، الحماية الجنائية للمرأة من العنف الإلكتروني: دراسة تحليلية مقارنة، مجلة دراسات قانونية، جامعة بنغازي، العدد 32، ديسمبر 2025، ص67

الرقمي بخصوصية عالية، فمن حيث إثبات جرائم العنف الرقمي فيمكن إثباتها ابتداءً بطرق الإثبات التقليدية وهي الاعتراف وشهادة الشهود والمعاينة والقرائن، إلا أنه وبسبب طبيعتها التقنية والفنية فإن إثبات الجرائم الرقمية يتم عن طريق الاستعانة بخبراء مختصين للحصول على الدليل الرقمي الذي يعين القاضي في الوصول إلى الحقيقة كمتتبع عناوين الIP للمتهمين أو تحليل بيانات الدخول أو غيرها وذلك عن طريق فحص الأجهزة المستخدمة في ارتكاب الجريمة، إلا أن مسألة الإثبات في الجرائم الرقمية تعد من الصعوبة بمكان وذلك لأن أغلب الجناة يكون لديهم القدرة على إخفاء آثار الجريمة أو ارتكابها باستخدام حسابات مزيفة مؤقتة¹.

وفي هذا الصدد فإن حماية خصوصية الإثبات في جرائم العنف الرقمي نظمها المشرع في قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61) فقد نصت المادة (5) منه على: "يعاقب بالسجن مدة لا تقل عن شهر، ولا تزيد على (5) ستة أشهر، وبغرامة لا تقل عن (100) مائة ريال عماني، ولا تزيد على (1000) ألف ريال عماني، أو بإحدى هاتين العقوبتين، كل من دخل عمداً - ودون وجه حق - موقعا إلكترونيا أو نظاما معلوماتيا أو وسيلة تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك.

فإذا ترتب على ذلك إلغاء أو تغيير أو تعديل أو إضافة أو تشويه أو إتلاف أو نسخ أو تدمير أو إبطاء أو نشر أو إعادة نشر أو إفشاء أو حجب أو تشفير بيانات أو معلومات إلكترونية مخزنة في الموقع الإلكتروني أو النظام المعلوماتي أو وسيلة تقنية المعلومات أو تدمير ذلك الموقع أو النظام أو وسيلة تقنية المعلومات أو إلحاق ضرر بالمستخدمين أو المستفيدين أو شغل عنوان أو اسم نطاق الموقع الإلكتروني، تكون العقوبة السجن لمدة لا تقل عن (6) ستة أشهر، ولا تزيد على سنة، وبغرامة لا تقل عن (1000) ألف ريال عماني، ولا تزيد على (3000) ثلاثة آلاف ريال عماني، أو بإحدى هاتين العقوبتين. وإذا كانت البيانات أو المعلومات الإلكترونية المنصوص عليها في الفقرة الثانية من هذه المادة شخصية تكون العقوبة السجن لمدة لا تقل عن سنة، ولا تزيد على (3) ثلاث سنوات، وبغرامة لا تقل عن (2000) ألفي ريال عماني، ولا تزيد على (5000) خمسة آلاف ريال عماني، أو بإحدى هاتين العقوبتين.

ويعفى من العقاب إذا كان الفاعل وليا أو وصيا أو قима أو متوليا الرعاية، أقدم على الفعل حفاظا على مصلحة فاقد الأهلية أو ناقصها."

كما نصت المادة (7) من ذات القانون على: "يعاقب بالسجن مدة لا تقل عن سنة، ولا تزيد على (3) ثلاث سنوات، وبغرامة لا تقل عن (3000) ثلاثة آلاف ريال عماني، ولا تزيد على (7000) سبعة آلاف ريال عماني، أو بإحدى هاتين العقوبتين، كل من ارتكب إحدى الجرائم المنصوص عليها في المادة

¹ (جازية جبريل شعيتير، الحماية الجنائية للمرأة من العنف الإلكتروني: دراسة تحليلية مقارنة، مرجع سابق، ص75

(5) من هذا القانون في أثناء أو بمناسبة تأدية عمله، ولا يحول انتهاء الخدمة أو زوال الصفة دون تطبيق حكم هذه المادة¹.

ومما سبق، فإن مسألة خصوصية الإثبات في جرائم العنف الرقمي ضد المرأة لا تعني استبعاد الأدلة اللازمة للإثبات، بل أن يتمتع هذا الإثبات بما يضمن حماية خصوصية المرأة، ويتمثل ذلك في عدة أوجه منها مشروعية الحصول على الدليل واقتصاره على الجمع والفحص في الأدلة على ما يتصل بالجريمة مع المحافظة على سرية وسلامته وعدم العبث به لضمان أن لا تؤدي إجراءات استخراج الدليل في الإعتداء على خصوصية المرأة من جانب آخر بإعادة نشر الصور أو الأخبار أو المعلومات التي بسببها قد تعرضت المرأة للعنف الرقمي وإنما يجب أن تقتصر إجراءات استخراج الدليل على القدر اللازم لإثبات الجريمة ونسبتها لمرتكبها.

¹ (قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61)،.

المبحث الثاني

الضوابط القانونية لأبواب جرائم العنف الرقمي ضد المرأة بالدليل الإلكتروني

يعد الدليل الرقمي من أهم الوسائل التي يتم الاستناد عليها في مسألة الإثبات في جرائم العنف الرقمي، إلا أن الإعتداد بهذا الدليل لا يكون على إطلاقه، وإنما يجب أن تتوافر عدة شروط وضوابط تضمن مشروعيتها، بما يكفل حجتيه أمام القاضي الجنائي، لذا فإننا نتناول في هذا البحث الضوابط القانونية التي تحكم مسألة الإثبات في جرائم العنف الرقمي ضد المرأة، ويتطلب ذلك بيان مدى حجية الدليل الرقمي والضوابط اللازمة لقبوله في الإثبات الجنائي وذلك في المطلب الأول، وفي المطلب الثاني سنبحث في تقدير الدليل الرقمي في إثبات جرائم العنف الرقمي وذلك في فرعين نصلها لاحقاً.

المطلب الأول: حجية الدليل الرقمي وضوابط قبوله في الإثبات الجنائي

تتضح أهمية الدليل الإلكتروني في مشروعيتها ومدى الإعتراف بقيمته القانونية وقدرته على إقناع القاضي الجنائي كما هو الحال في الأدلة التقليدية التي يتم قبولها والاحتذاء بها متى توافرت فيها الشروط والضمانات اللازمة¹، ومن ثم تبرز أهمية تحديد الأساس القانوني الذي تستند إليه حجية الدليل الرقمي والإعتراف به كدليل إثبات في حال توافر الضوابط والشروط اللازم توافرها في الدليل، وفي هذا الصدد فإننا سنبحث في هذا المطلب موضوع حجية الدليل الرقمي وضوابط قبوله في الإثبات الجنائي، وسيتم تناول هذا المطلب في فرعين، الفرع الأول حول الأساس القانوني لحجية الدليل الرقمي في التشريع العماني، أما الفرع الثاني نخصصه لموضوع تقدير الدليل الرقمي في إثبات جرائم العنف الرقمي.

الفرع الأول: الأساس القانوني لحجية الدليل الرقمي في التشريع العماني

أولى المشرع العماني الدليل الرقمي عناية بالغة في قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61)، فبدأ بتحديد مفهومه في المادة الأولى من القانون، ثم أحاطه بحماية جزائية في أكثر من موضع، تشمل حمايته من الإخفاء والامتناع عن تقديمه والعبث به، فضلاً عن تنظيم سبل الحصول عليه.

فقد جرمت المادة (12) من الفصل الثالث إساءة استخدام التقنية في إخفاء الآثار والأدلة الرقمية، إذ نصت على أنه: «يعاقب بالسجن ... كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة

¹ (د. نزار حمدي إبراهيم. قشقة الأحكام العامة لمراقبة وتسجيل المكالمات في التشريع العماني: دراسة تحليلية نقدية. الأمانة، مج. 2020، ع. 34، 2020، ص. 227-257).

أو مطورة أو محورة أو كلمات مرور أو شيفرات أو رموزاً أو أي بيانات مماثلة، وذلك بقصد استخدام أي منها في ارتكاب أو تسهيل ارتكاب أي من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها الرقمية.»

وفي الفصل الرابع جرم القانون الامتناع عن تقديم الأدلة والعبث بها، فنصت المادة (١٤) على أنه: «يعاقب بالسجن ...، كل من أخفى أو امتنع عن تقديم الرموز السرية لوسيلة تقنية المعلومات المستخدمة في ارتكاب أو تسهيل ارتكاب أي من الجرائم المنصوص عليها في هذا القانون إلى مأموري الضبط القضائي». كما شددت المادة (15) على المسؤول عن الأدلة الرقمية، فنصت على أنه: «يعاقب بالسجن مدة لا تقل عن (6) ستة أشهر، ولا تزيد على (3) ثلاث سنوات، وبغرامة لا تقل عن (1000) ألف ريال عماني، ولا تزيد على (3000) ثلاثة آلاف ريال عماني، أو بإحدى هاتين العقوبتين، كل مسؤول عن الأدلة الرقمية أخفى أو امتنع عن تقديمها لمأموري الضبط القضائي، أو عبث بها.»

ولم يقتصر المشرع على التجريم، بل نظم كذلك الجانب الإجرائي للحصول على الدليل الرقمي، إذ نصت المادة (4) على أنه: "مع عدم الإخلال باختصاصات مركز الدفاع الإلكتروني، يجوز للوزارة بالتنسيق مع الجهات المختصة - في حال وجود أسباب كافية بوقوع جريمة تقنية المعلومات - الحصول على البيانات أو المعلومات الإلكترونية من الجهات النظرية، وغيرها من الجهات الحكومية وغير الحكومية في سلطنة عمان وخارجها، بناء على أمر قضائي صادر عن الادعاء العام، أو المحكمة المختصة بحسب الأحوال"

ويستفاد من مجموع هذه النصوص أن المشرع العماني قد اعترف بالدليل الرقمي كوسيلة يمكن الاستناد إليها في كشف الجرائم وإثباتها، ولم يتعامل معه باعتباره مجرد بيانات تقنية عديمة الأثر القانوني، وإنما أحاطه بمجموعة من الضمانات التشريعية التي تستهدف المحافظة على وجوده وسلامته وإمكانية الحصول عليه وتقديمه إلى الجهات المختصة. ومن ثم، فإن هذه الأحكام تمثل أساساً تشريعياً للاعتماد بالدليل الرقمي في المجال الجنائي، وإن كانت الحجية القضائية لهذا الدليل لا تستند إلى مجرد وجوده، وإنما ترتبط كذلك بمدى مشروعية الحصول عليه، وسلامته، وإمكان التحقق من مصدره ونسبته إلى مرتكب الجريمة. ويتضح من استقراء أحكام قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم (2026/61) بأن المشرع العماني لم ينظر إلى الدليل الرقمي كوسيلة فنية لأثبات الجريمة فقط وإنما أحاطه بحماية قانونية تتعلق بطريقة الحصول عليه والمحافظة عليه من الإخفاء والعبث بما تم إيرادها من نصوص تجرم هذه الأفعال، كما تظهر في المادة (4) التي سبق ذكرها تنظيم المشرع العماني للحصول على البيانات الإلكترونية وتكامل الجهات فيما يتعلق بذلك، أما المادة (12) فقد جاءت لحماية الدليل من الوسائل التي تهدف إلى إخفاء الأدلة أو العبث بها، أما المادة (14) و (15) فقد جرمت مسألة إخفاء الدليل أو الامتناع عن تقديمه أو العبث به، وتتضح أهمية

هذه الحماية التي أحاطها المشرع للدليل الإلكتروني في جرائم العنف الرقمي ضد المرأة ومسألة اثباتها بالأدلة الرقمية، ومع الأهمية الكبيرة للدليل الرقمي في مثل هذه الجرائم فإن حماية هذه الأدلة أيضا يمثل ضمانا أساسية للمجني عليه في إثبات الجريمة بالدليل الرقمي دون عبث أو تغيير.

الفرع الثاني: ضوابط وشروط قبول الدليل الرقمي

لقبول أي دليل سواء كان تقليدي أو رقمي يجب أن تتوافر فيه شروط معينة، ولقبول الدليل الرقمي أمام القضاء الجزائي ينبغي أن تتوافر فيه جملة من الاشتراطات يمكن أن نوجزها فيما يلي:

أولا: ضمان عدم تعرض الدليل الرقمي للعبث أو التلف وحفظه بصورته الأصلية: إن إثبات الوقائع الجرمية بالدليل الرقمي يستلزم أن يكون أصل الدليل الرقمي موجوداً بصورته الأصلية وأن يتم تقديمه للمحكمة، ولا يشترط أن يكون ما يتم تقديمه للمحكمة هو عبارة عن بيانات رقمية بحتة، بل يمكن أن يكون ذلك الأصل على شكل ملفات مخزنة في أقراص ممغنطة أو مطبوعة على أوراق، فما يستخرج من الطابعات من الأجهزة الإلكترونية المستخرج منها الدليل تعد أدلة أصلية، وقد جاء ذلك أيضا في قانون الأمم المتحدة النموذجي للتجارة الإلكترونية والذي أقرت بالدليل الكتابي الرقمي. إضافة إلى ما سبق فإنه ينبغي التأكد من أن الملفات الإلكترونية التي يتم استخراج الأدلة الرقمية منها لم يتم العبث بها أو إتلافها أو التغيير في محتوياتها، وأن ما يتم تقديمه من أدلة للمحكمة هي الأدلة ذاتها التي تم جمعها وحفظها، ولم تتعرض لأي تغيير أو تعديل، ولتأمين سلامة الأدلة الرقمية من العبث والتلف فإنه ينبغي أن يتم مراعاة عدة أمور أهمها أن يتم تحديد الأجهزة الإلكترونية الموجودة في مكان المعاينة وتحديد مواقعها وتصويرها بالحالة التي كانت عليها وعزل أجهزة الكمبيوتر عن الشبكات لضمان عدم اختراقها، كما ينبغي مراعاة التأكد من خلو موقع المعاينة من أي قوى مغناطيسية يمكن أن تؤثر على سلامة الدليل وصحته وذلك عند نقل المواد المعلوماتية خارج مسرح المعاينة، وأن تقتصر المعاينة والجمع على المختصين ممن تتوفر لديهم الكفاءة العلمية والعملية والفنية في مجال الحاسب الآلي والشبكات¹.

ثانيا: ينبغي أن تكون الأدلة التي يتم تقديمها أمام القضاء هي أدلة يقينية، ويعني ذلك أن تكون أقرب للواقع والحقيقة قدر المستطاع، وذلك بابتعادها عن الظن والتخمين والشك والاحتمال حتى يمكن الإستناد عليها في القضاء، كما أنه من المهم أن تكون هذه المخرجات من الأدلة قابلة للعرض والنقاش في جلسات المحكمة تحقيقاً لمبدأ شفوية المرافعة، أي أن تكون محلاً للنقاش، حتى يستطيع القاضي من خلال مناقشة هذه الأدلة مع المختصين ومع غيرهم من تكوين القناعة التي توصله للحكم في الدعوى، وذلك لأنه من المهم أن يفهم القاضي الجنائي الدليل الرقمي، ولا يتصور أن يكون هذا الفهم

¹ (أحمد محمد العمر، الدليل الرقمي وحجتيه في الإثبات الجزائي، مرجع سابق، ص 157-159

إلا من خلال نقاش الدليل نفسه واقتناع القاضي فيه، ومن الشروط التي يجب أن تستوفيها الأدلة الرقمية أيضاً أن تكون متسقة مع مبدأ شرعية الجرائم والعقوبات، ويتمثل ذلك في بطلان أي دليل يتم الحصول عليه بطرق غير مشروعة، أو خالف القواعد الإجرائية في الحصول على الدليل، وفي هذه الحالة يكون الدليل غير صالح للاستناد عليه، لذا، فإن القاضي يجب أن يكون أكثر حرصاً ودقة لتجنب الوقوع في الخطأ عن الحكم في الدعوى والاقترب أكثر من الحقيقة¹.

وتعد مسألة نسبة الدليل الرقمي إلى المتهم من أهم المسائل التي تحدد مدى قوة هذا الدليل في الإثبات، حيث لا يكفي أن يتم إثبات وجود بيانات أو صور رقمية تتصل بالجريمة، بل يجب أن يتم التحقق من صدور هذه البيانات عنه وإنها كانت تحت سيطرته وقت ارتكاب الجرم، وتزداد أهمية ذلك في مسألة جرائم العنف الرقمي ضد المرأة²، وذلك لإمكانية أن يتم إنشاء حسابات بأسماء مستعارة أو وهمية أو انتحال هوية الغير أو أن يتم استخدام جهاز الغير في ارتكاب هذا النوع من الجرائم، الأمر الذي يجعل مسألة ارتباط الدليل الرقمي بحساب معين أمر غير كافٍ لإسناد الجريمة إلى صاحب الحساب. وتتحقق واقعية اسناد الدليل الرقمي إلى مرتكب الجريمة من خلال عدة قرائن فنية وموضوعية تساند بعضها البعض، من بين هذه القرائن بيانات الحساب ووسيلة الدخول إليه، وعنوان بروتوكول الانترنت (IP)، وبيانات الجهاز المستخدم وسجلات الدخول والخروج فضلاً عن محتوى المراسلة محل الجريمة وما قد يتوافر من بيانات أخرى تربط المتهم بشكل مباشر بالوسيلة الرقمية الذي صدر منها الدليل، وتمثل مسألة الوصول إلى هوية مرتكب الجريمة أحد أبرز الصعاب لذا يقتضي التعامل مع الدليل الرقمي بوسائل فنية تضمن الحفاظ على الأدلة الرقمية وتحويل البيانات التي يتم استخراجها إلى دليل يمكن الاستناد إليه³.

المطلب الثاني: تقدير الدليل الرقمي في إثبات جرائم العنف الرقمي

لقد أصبح الدليل الرقمي من أهم وسائل الإثبات في جرائم العنف الرقمي، وذلك بسبب الطبيعة الرقمية لهذا النوع من الجرائم، لما تساهم فيه هذه الأدلة الرقمية من الكشف عن تفاصيل الجريمة وملاساتها ومرتكبها، غير أن تقدير هذا الدليل يثير إشكالات قانونية وفنية، وعليه فإن دراسة تقدير الدليل الرقمي تقتضي الوقوف على سلطة القاضي الجنائي في تقدير الدليل الرقمي في

¹ (د. وليد سعد الدين محمد سعيد، أهمية الدليل الجنائي الرقمي في الإثبات الجنائي، مجلة القانون والاقتصاد، العدد 98، أبريل 2025، ص 293-294)

² (د. نزار حمدي قشقة مركز الضحية في السياسة الجنائية الفلسطينية. مجلة جامعة الخليل للبحوث (ب): العلوم الإنسانية، مج. 11، ع. 1، 2016، ص. 136-158.

³ (د. مسعود بن حميد المعمر، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد 3، الجزء الثاني، أكتوبر 2018، ص 244-246)

الفرع الأول، كما تستلزم الوقوف على الاشكالات العملية والقانونية في تقدير الدليل الرقمي في الفرع الثاني من هذا المطلب.

الفرع الأول: سلطة القاضي الجنائي في تقدير الدليل الرقمي

إن مبدأ شرعية الجرائم والعقوبات ينعكس على قواعد الإثبات الجنائي، التي تستلزم عدم قبول أي دليل قد تم بطرق غير مشروعة، فالسلطة التقديرية للقاضي عند البحث عن الأدلة لا يعني أن يتم قبول الدليل بأي طريقة، بل يترتب البحث عن الدليل الجنائي احترام حق الدفاع ومبدأ العدالة، وينعكس ذلك على الأدلة الرقمية وإجراءات الحصول عليها، ويعني ذلك أن استخراج الدليل إذا لم يتم وفق القواعد الاجرائية فإنها تكون باطلة، ولا يمكن أن تبنى عليها الاحكام الجزائية، ومن غير المتصور أن يقوم المشرع بتجريم الافعال التي تقوم على العالم الرقمي في قانون مكافحة تقنية المعلومات ولا يقبل الدليل عليها لإثباتها، وبالتالي فإن الأدلة الرقمية تتمتع بالحجية ذاتها التي تتمتع بها الأدلة التقليدية في الإثبات متى توافرت فيها الشروط اللازمة لقبولها وضوابطها وظروفها وآليات الحصول على الدليل الرقمي¹.

وهنا يثار تساؤل مهم في ما يتعلق بالسلطة التقديرية للقاضي في الأخذ بالدليل الرقمي، فهل مجرد الحصول على الدليل الرقمي يعني إلزامية قبوله والاخذ به في الاثبات الجنائي وذلك لطبيعته الفنية؟ الإجابة عن هذا السؤال تعود إلى طبيعة الدليل الرقمي، الذي يسهل العبث فيه وتحريفه، فضلا عن ارتفاع نسبة الخطأ في طريقة استخراجه، لذا فإن قرينة البراءة تستلزم أن يتم استبعاد أي دليل يكون في موضع شك في صحته وذلك لأن الشك يفسر لمصلحة المتهم، ولذا فإن القاضي الجنائي يملك السلطة التقديرية، إلا أن القاضي لا يملك البت في امور فنية تستوجب تدخل خبير، لذا فإن السلطة التقديرية للقاضي تطبق في العوامل المتعلقة باستخراج الدليل الرقمي وليس الدليل نفسه،

حيث أن القاضي الجنائي يملك السلطة التقديرية في التأكد من سلامة الدليل الرقمي ومصداقيته وامكانية الأخذ به والاعتماد عليه في بناء الحكم الجنائي في الدعوى، وعليه يمكن القول بأن تقدير القاضي الجنائي للدليل الرقمي يكون من عدة جوانب وهي تقييم الدليل والتأكد من سلامته من العبث، وتقييم الدليل الرقمي من حيث السلامة الفنية لاستخراج الدليل الرقمي والاجراءات المتبعة في ذلك ويتم ذلك عن طريق الاجهزة المتقدمة والخبرة الفنية التي لا يملكها القاضي، لذلك فإن مسألة سلطة القاضي التقديرية في تقدير الدليل الرقمي لا تكون في الدليل الرقمي نفسه وإنما ما قد يشوبه من عبث في مضمونه او في طريقة استخراجه، فإذا ثبت بالخبرة الفنية بما لا يدع مجالاً للشك بأن الدليل الرقمي صحيح ومرتبط بالجريمة وقد سلم من العبث والخطأ فإن القاضي الجنائي لا يكون

¹ (د.إيمان محمد عادل السعيد، الحماية الجنائية للمرأة من العنف الإلكتروني، مجلة روح القوانين، مرجع سابق، ص 698)

أمامه إلا الأخذ به في الدعوى كون موضوع الدليل الرقمي مسألة فنية يخرج من اختصاص القاضي، ما لم يكن الدليل الرقمي غير متصل بالدعوى¹.

وقد نصت المادة (215) من قانون الاجراءات الجزائية العماني على الأساس التشريعي لمبدأ الاقتناع القضائي وحرية القاضي في تقدير الأدلة والتي جاء فيها: "يحكم القاضي في الدعوى حسب القناعة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبنّي حكمه على أي دليل لم يطرح على الخصوم أمامه في الجلسة أو على معلوماته الشخصية"². وجاء في الطعن رقم 2019/520 ما يدل على أن الدليل الرقمي يساند غيره من الأدلة الأخرى ليصل القاضي الى تكوين قناعته، ونص على: "إن الأدلة في المواد الجزائية ضمايم متساندة يكمل بعضها بعضا ومنها مجتمعة تتكون عقيدة المحكمة فلا ينظر إلى دليل بعينه لمناقشته على حدة دون باقي الأدلة، بل يكفي أن تكون الأدلة في مجموعها وحدة واحدة تؤدي إلى ما قصده الحكم منها ومنتجة في اقتناع المحكمة واطمئنانها إلى ما انتهت إليه ولو عن طريق الاستنتاج طالما أن القانون لم يحدد وسيلة معينة لإثبات الجريمة"³.

وجاء في المبدأ رقم (53) في الطعن رقم 2020/15 ما يتعلق بتقدير القاضي للخبرة الفنية ليظل أحد عناصر الاثبات التي يملك القاضي تقدير قوتها الدليلية وقد نص على: "إن تقدير آراء الخبراء والفصل فيما يوجه إلى تقاريرهم من مطاعن مرجعه إلى محكمة الموضوع التي لها كامل الحرية في تقدير القوة الدليلية لتقرير الخبر شأنه في ذلك شأن سائر الأدلة فلها مطلق الحرية في الأخذ بما تطمئن إليه منها والالتفات عما عداها، ولا تقبل مصادرة سلطة المحكمة في هذا التقدير، ولا تجوز مجادلة المحكمة في هذا الشأن، ولا مصادرة عقيدتها فيه أمام المحكمة العليا، ما دام تسببها لما انتهت إليه سائغاً وذا صدق في الأوراق"⁴.

¹ طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، مجلة الحقوق، المجلد 12، العدد 1، يونيو 2015، ص 69-70
² قانون الاجراءات الجزائية العماني الصادر بالمرسوم السلطاني رقم 99/97 والمنشور في الجريدة الرسمية رقم (661) بتاريخ 1999/12/15م

³ مجموعة الاحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة من 2019/10/1 إلى 2020/9/30 السنة القضائية عشرون، المكتب الفني

⁴ مجموعة الاحكام الصادرة عن الدائرة الجزائية بالمحكمة العليا والمبادئ المستخلصة منها في الفترة من 2019/10/1 إلى 2020/9/30 السنة القضائية عشرون، المكتب الفني، مرجع سابق

الفرع الثاني: الإشكالات العملية والقانونية في تقدير الدليل الرقمي

يثار التساؤل في الصعوبات التي تواجه الدول في التعامل مع جرائم العنف الرقمي الواقعة على المرأة والتي تتعلق بالدليل الرقمي، ويمكن الإجابة على هذا السؤال من خلال العودة إلى طبيعة الأدلة الرقمية نفسها، فمن الصعوبات التي تواجه الجهات المختصة والقضاء في مسألة عدم وضوح الدليل الرقمي، وذلك كون الدليل الرقمي يتم استخراجه من عالم افتراضي وغير واقعي، وبالتالي فإن مسألة العبث فيه أو التغيير في حقيقته تكون سهلة للمجرمين المتخصصين في الجرائم الالكترونية، كما أن عدم الإبلاغ بشكل مباشر عن الجريمة الالكترونية وخاصة التي تتعرض لها المرأة يتسبب بصعوبة استخراج الدليل بعد مضي فترة من الزمن عليه، وبالتالي صعوبة الوصول الى مرتكب الجريمة، ويضاف إلى ما سبق من إشكالات هو عدم ما يواجه المختصين من صعوبة في معاينة الأدلة الرقمية واستخراجها ونقص الخبرات اللازمة في ظل التطور المستمر للجريمة الرقمية والذي يتطلب خبرة فنية وتقنية عالية وتدريب مستمر للعاملين في هذا المجال للتعرف على أحدث الأجهزة التي تمكنهم من الوصول الى الأدلة الرقمية¹.

ومن الإشكالات العملية والقانونية التي تظهر في مسألة الدليل الرقمي أيضا هي قيام بعض مرتكبي الجرائم باستخدام برامج إخفاء الهوية، والتي توفرها تكنولوجيا المعلومات والاتصالات للمستخدمين، ومن بين هذه البرامج، الذي تم تطويره في مختبر أمريكي (TOR) والذي يتم استخدامه كتقنية تعتمد على التشفير وإخفاء عنوان الوصول إلى المستخدم ويتيح للمستخدم مشاركة المعلومات دون الوصول إلى أنشطة المستخدم أو عنوانه، وبالتالي صعوبة معرفة الجاني، وبلا شك فإن استخدام المجرمين في جرائم العنف الرقمي لمثل هذه البرامج التي تعتمد على إخفاء الهوية والموقع يمثل صعوبة على المختصين في الوصول إلى الجاني وتحديد موقعه الجغرافي وهويته وبالتالي صعوبة إثبات الجريمة ونسبتها إلى مرتكبها².

ومع تعدد الإشكالات التي تواجه الإثبات بالدليل الرقمي في جرائم العنف الرقمي على وجه الخصوص فإن الحل يتمثل في بناء منظومة من الحلول القانونية والاجرائية والفنية تتكامل مع بعضها البعض للاستفادة من الأدلة الرقمية في مسألة الإثبات الجنائي، على أن تبدأ من لحظة الإبلاغ عن الجريمة نظراً لما تحتاجه الأدلة الرقمية من سرعة في الحفظ تجنباً لحذفها أو تعرضها للتعديل ولتمكين المختصين من استخراج الدليل بصورته الأصلية، كما ينبغي أن يتم اعتماد إجراءات فنية موحدة لتحريز الأدلة من الأجهزة المرتبطة بالجريمة بما يضمن سلامة الدليل الرقمي، وفي ذات الوقت فإنه ينبغي أن

¹ د. إيمان محمد عادل السعيد، الحماية الجنائية للمرأة من العنف الالكتروني، ص 679

² (ديب أكرم، نورة بن بوعبدالله، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مرجع سابق، ص 413.

يتم تحقيق التوازن بين سرعة الحصول على الاثباتات الرقمية وبين حماية خصوصية المرأة المجني عليها حيث تتضمن الأدلة في الغالب صوراً شخصية للمجني عليها أو محادثات أو بيانات شخصية جديرة بالحماية، لذا ينبغي أن يقتصر الفحص والضبط على البيانات التي تتصل بالجريمة وعدم تداولها الا بالقدر اللازم الذي تتطلبه إجراءات التحقيق والمحاكمة، وعدم التوسع في التفتيش أو التوسع في الاطلاع على البيانات بما يجاوز الغرض منها¹.

إضافة إلى ذلك يتطلب أن يتم معالجة إشكالية نسبة الدليل الرقمي الى المتهم، وقد تكون هذه الاشكالية من أهم الاشكاليات التي ينبغي مواجهتها نظرا لكون العديد من مرتكبي جرائم العنف الرقمي ضد المرأة يستخدمون أسماء مستعارة أو ينتحلون شخصيات غير حقيقية او يقومون بالاستيلاء على حساب شخص آخر للقيام بجريمتهم، لذا فإن من المهم أن يتم تحديد المتهم في جريمة العنف الرقمي وذلك بالاستعانة بالأدلة الرقمية من خلال التحقق من هوية مستخدم الحساب والقرائن الفنية المساندة كبيانات الجهاز وعنوان بروتوكول الانترنت ورقم الهاتف المرتبط بالحساب ومعلومات مزود الخدمة وغيرها من الوسائل التي تتيح للمختصين التوصل الى حقيقة مرتكب الجريمة، لذا فإن تعزيز الخبرة الفنية لدى جهات الضبط والتحقيق والاستعانة بالخبراء والمختصين في الأدلة الرقمية يمثل ضرورة عملية لضمان عملية إسناد التهمة للمتهم الحقيقي مرتكب الجريمة².

تم تمويل المشروع البحثي الذي أدى الى هذه النتائج من قبل هيئة البحث العلمي والابتكار
بسلطنة عمان ضمن برنامج التمويل المؤسسي المني على الكفاءة بموجب العقد رقم

MoHERI/BFP/ASU/2025

¹ (أحمد محمد العمر، الدليل الرقمي وحجبه في الاثبات الجزائي، مرجع سابق، ص152.

² (أمانى بنت علي بن سيف المقابلية، حجية الأدلة الرقمية في الاثبات الجزائي وموقف المشرع العماني منها، رسالة ماجستير، كلية القانون، جامعة صحر، سلطنة عمان، 2024، ص70-72

الخاتمة

الحمد لله رب العالمين والصلاة والسلام على النبي الهادي الأمين وعلى من تبعه ووالاه بإحسان إلى يوم الدين وسلم تسليما كثيرا .

فأننا بحمد الله وتوفيقه انتهينا من إعداد هذا البحث الذي يدور حول موضوع حجية الدليل الرقمي في إثبات جرائم العنف الرقمي ضد المرأة في القانون العماني، وذلك لما للموضوع من أهمية فرضها التطور المتسارع في التقنيات الحديثة، وما ترتب على ذلك من ظهور جرائم مستحدثة تمثلت أحداها في جرائم العنف الرقمي ضد المرأة، ومع زيادة هذه الأنواع من الجرائم الالكترونية أصبحت مسألة إثباتها متعلقة بأدلة رقمية لما تمثله هذه الأدلة من بيانات ومعلومات تساهم في الكشف عن الجريمة والوصول الى مرتكبها.

وقد سعى البحث الذي تضمن في طياته جملة من الأفكار لمعالجة إشكالية البحث والتي تمثلت في مدى قدرة المشرع العماني في تحقيق التوازن بين الاستفادة من الدليل الالكتروني في كشف الجرائم وبين ضمان سلامة الدليل وعدم مساسه بالحقوق والحريات ، وذلك في مبحثين من خلال دراسة الأسس والنظرية للدليل الرقمي ثم الوقوف على الضوابط القانونية لأثبات جرائم العنف الرقمي ضد المرأة بالدليل الرقمي، وقد أظهر البحث بأن مسألة مواجهة جرائم العنف الرقمي ضد المرأة لا تقتصر على النص على تجريم الفعل الجرمي وحسب وإنما تتطلب حماية بمنظومة متكاملة، ومما لا شك فيه فإن الدليل الرقمي والحاجة الى استخدامه أصبحت تمثل أهمية كبيرة في مجال الاثبات الجنائي.

وفي الختام، فإن إثبات جرائم العنف الرقمي لا تقتصر على العقوبة الجزائية فقط، بل تتطلب حماية إجرائية لإثبات هذه الجرائم عن طريق الدليل الرقمي، وما يصاحب هذا الدليل من تحديات، الأمر الذي يتطلب استمرار التشريعات ومن بينها المشرع العماني في تطوير منظومة الاثبات بما يتلاءم مع التطور التقني المتسارع وطبيعة الجرائم التقنية المستحدثة، وقد توصلت في بحثي هذا الى نتائج وتوصيات عرضها للقارئ الكريم.

النتائج:

- لقد أحاط المشرع العماني مسألة الدليل الرقمي بأهمية تمثلت في وضع مفهوم للأدلة الرقمية في قانون مكافحة جرائم تقنية المعلومات العماني الصادر بالمرسوم السلطاني رقم (2026/61) وعاقب الأفعال التي تؤدي إلى ضياع الدليل أو العبث فيه أو إخفاؤه.
- ان الدليل التقليدي يختلف عن الدليل الرقمي في طريقة حفظه والحصول عليه وجمعه وذلك كون الدليل التقليدي هو دليل مادي ملموس يمكن فحصه بشكل مباشر وهو بذلك يختلف بطبيعته عن الدليل الرقمي.

- الدليل الرقمي قد أصبح من أهم وسائل الإثبات في جرائم العنف الرقمي ضد المرأة، وذلك لما تتمتع به الجريمة الرقمية من خصوصية في كون ارتكابها يكون في الغالب عن طريق الأجهزة الرقمية مثل أجهزة الهاتف وأجهزة الحاسب الآلي مما يعني أن اثبات هذه الجرائم يكون عن طريق أدلة رقمية.
- إن حجية الدليل الرقمي لا تقوم بمجرد وجود الدليل الرقمي بل يتطلب أن يتم التأكد من سلامة مصدر هذا الدليل وإن طريقة الحصول عليه كانت مشروعة وطريقة حفظه كانت صحيحة، ويمثل قانون مكافحة تقنية المعلومات أساس الاعتراف بحجية الدليل الرقمي، وتلعب الخبرة الفنية دوراً كبيراً في مسألة الحصول على الدليل الرقمي نظراً للطبيعة الفنية لهذا النوع من الأدلة.
- للدليل الرقمي أهمية كبيرة في إثبات جرائم العنف الرقمي لذا فإن من المهم تحقيق التوازن بين مسألة تجريم جرائم العنف الرقمي والطريقة الصحيحة في الحصول على الدليل الرقمي بما يضمن معه اثبات الجريمة والوصول الى مرتكبها.

التوصيات:

- نوصي المشرع العماني بالنص صراحةً على حجية الدليل الرقمي في الإثبات الجنائي، ووضع تنظيم تشريعي أكثر تفصيلاً يحدد شروط قبوله أمام القضاء، بما يزيل أي لبس بشأن مدى الاعتداد به كوسيلة من وسائل الإثبات.
- وضع تعريف تشريعي موحد للدليل الرقمي في التشريعات العمانية ذات الصلة، بما يحقق الاتساق بين قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية وقانون حماية البيانات الشخصية وقانون الإجراءات الجزائية.
- نوصي المشرع العماني باستحداث نصوص أكثر تحديداً بشأن شروط قبول الدليل الرقمي، وبصفة خاصة مشروعية الحصول عليه، وسلامته، وإمكان التحقق من مصدره، ونسبته إلى المتهم، وعدم تعرضه للتعديل أو العبث.
- نوصي الجهات المختصة والتي تتعامل مع الدليل الرقمي في لحظة ضبطه والمتمثلة في شرطة عمان السلطانية والنيابة العامة والمختصين الفنيين بتنظيم إجراءات جمع وضبط وحفظ وفحص الأدلة الرقمية بصورة تفصيلية، بما يضمن سلامة الدليل منذ لحظة ضبطه وحتى تقديمه أمام المحكمة، مع تحديد المسؤوليات القانونية للقائمين على هذه الإجراءات.
- تعزيز الحماية الإجرائية للمرأة ضحية العنف الرقمي، بما ييسر الإبلاغ عن الجرائم الرقمية والمحافظة السريعة على الأدلة الإلكترونية التي يكون احتمال حذفها أو تغييرها مرتفعاً.

- وضع آليات سريعة لحفظ المحتوى الرقمي محل الجريمة بناءً على طلب المجني عليها أو الجهات المختصة، خصوصاً في جرائم الابتزاز والتشهير ونشر الصور أو البيانات الخاصة.
- إعداد دليل إجرائي وطني موحد لجمع الأدلة الرقمية وحفظها وفحصها وتقديمها أمام القضاء، مع تدريب القضاة وأعضاء الادعاء العام ومأموري الضبط القضائي والخبراء على تطبيقه.

المراجع:

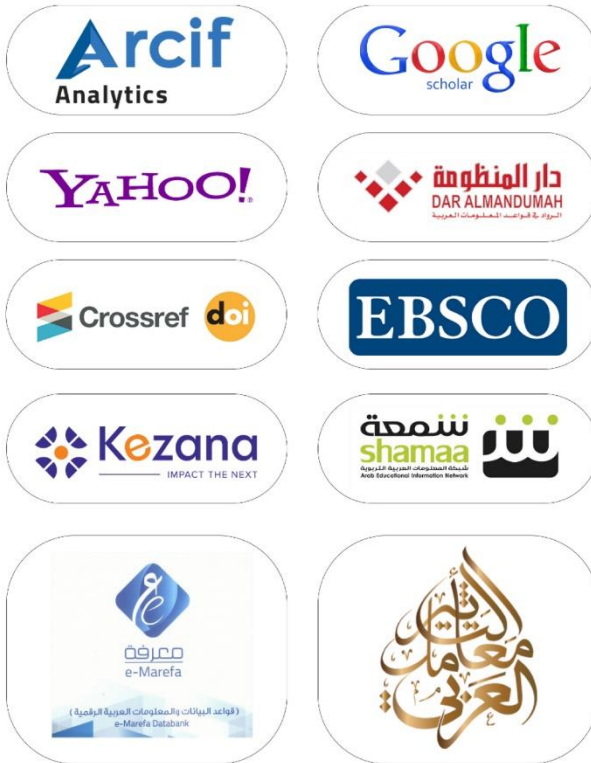
الكتب والدراسات:

- أحمد محمد العمر، الدليل الرقمي وحجتيه في الاثبات الجزائي، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، سلطنة عمان، العدد الثالث، يناير 2020
- أماني بنت علي بن سيف المقابلية، حجية الأدلة الرقمية في الاثبات الجزائي وموقف المشرع العماني منها، رسالة ماجستير، كلية القانون، جامعة صحار، سلطنة عمان، 2024
- بدور خالد الكري، سليمان بن محمد المعلم، تأثير التقنية على وسائل الاثبات الرقمية في النظام السعودي، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، العدد 46، يوليو 2024
- ديب أكرم، نورة بن بوعبد الله، دور الدليل الرقمي الجنائي في اثبات جريمة الابتزاز الالكتروني، مجلة الحقوق والعلوم الانسانية، مجلد 16، العدد 1، 2023
- إيمان محمد عادل السعيد، الحماية الجنائية للمرأة من العنف الالكتروني، مجلة روح القوانين، جامعة طنطا، المجلد 37، العدد 111، اغسطس 2025
- منى أحمد عبدالفتاح أحمد السيد، مفهوم التشهير الالكتروني والحماية القانونية الممنوحة للشخص، مجلة البحوث القانونية والاقتصادية، المجلد 15، العدد 92
- جازية جبريل شعيتير، الحماية الجنائية للمرأة من العنف الالكتروني، دراسة تحليلية مقارنة، مجلة دراسات قانونية، جامعة بنغازي، العدد 32، ديسمبر 2025
- دكتور وليد سعد الدين محمد سعيد، أهمية الدليل الجنائي الرقمي في الاثبات الجنائي، مجلة القانون والاقتصاد، العدد 98، ابريل 2025
- طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، مجلة الحقوق، المجلد 12، العدد 1، يونيو 2015
- د. مسعود بن حميد المعمرى، الدليل الالكتروني لأثبات الجريمة الالكترونية، مجلة كلية القانون الكويتية العالمية، العدد 3، الجزء الثاني، اكتوبر 2018
- نزار حمدي إبراهيم. قششة الأحكام العامة لمراقبة وتسجيل المكالمات في التشريع العماني: دراسة تحليلية نقدية. الأمانة، مج. 2020، ع. 34، 2020.
- د. نزار حمدي قششة مركز الضحية في السياسة الجنائية الفلسطينية. مجلة جامعة الخليل للبحوث (ب): العلوم الإنسانية، مج. 11، ع. 1، 2016.



مجلة الأندلس للعلوم الإنسانية والاجتماعية
مجلة دولية شهرية علمية محكمة
الترقيم الدولي الإلكتروني: ISSN:2410- 521X
الترقيم الدولي الورقي: ISSN:2410- 1818
البريد الإلكتروني: journal@andalusuniv.net

المجلة مفهومة في المواقع الآتية :



2025	2024	2023	2022	2021	العام
0.5978	0.3068	0.3759	0.1954	0.2692	معامل أرسيف
1.59	1.55	1.25	1.73	1.60	معامل التأثير العربي