ElQarar Journal for Refereed Scientific Research | Issue 8, Vol 3, Year 1 | August 2024
ISSN 3006-7294
Creative Commons Attribution 4.0 International (CC BY 4.0)

الإثبات الجنائي في جرائم الإنترنت

إعداد: الباحث / عمر عبد الكريم سويدان الدليمي

E-mail: alasafy2007@uoanbar.edu.iq

تاريخ الاستلام: 2024/8/7	تاريخ القبول: 2024/8/11	تاريخ النشر: 2024/8/15

للاقتباس: الدليمي، عمر عبد الكريم سويدان، الإثبات الجنائي في جرائم الإنترنت، مجلة القرار للبحوث العلمية المحكّمة، المجلد الثالث، العدد 8، 2024، ص-ص 829-850.

ملخص

إن ظاهرة الإجرام المعلوماتي في تصاعد مستمر، كما تخطت آثارها حدود الدول، وقد ترتب على ذلك مجموعة تحديات قانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها، نظرا لأنها لا تترك أثرًا ماديًا ملموسًا، كما هو الحال في الجرائم التقليدية، إضافة لما ينتج عن ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض الإجراءات عبر الحدود كالمعاينة والتفتيش والضبط في نطاق البيئة الافتراضية.

وذلك ما شكل دافعا لمطالبة المشرع العراقي بوضع نص واضح وصريح يكرس القوة الثبوتية لنسخ الدليل الرقمي، ويبين قيمته القانونية، إضافة إلى ضرورة العمل على تعزيز قدرات رجال الضابطة القضائية والمحققين في مجال التحقق من الأدلة الرقمية وجمعها.

الكلمات المفتاحية: جرائم الإنترنت، الإثبات الجنائي، الدليل الرقمي.

0009-0006-8488-5433

مجلة القرار للبحوث العلمية المحكّمة | العدد 8، المجلد 3، السنة 1 | آب (أغسطس) 2024 | صفر 1445
ISSN 3006-7294
مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

Criminal proof of cyber crimes

Author: Omar Abd-alkarim Swaidan Aldoulaimi

E-mail: alasafy2007@uoanbar.edu.iq

Received : 7/8/2024 **Accepted :** 11/8/2024 **Published :** 15/8/2024

Cite this article as: Aldoulaimi, Omar Abd-alkarim Swaidan, Criminal proof of cyber crimes; ElQarar Journal For Refereed Scientific Research, vol 3, issue 8, 2024, pp. 829-850.

Abstract

The phenomenon of cybercrime is constantly on the rise, and its effects have crossed the borders of countries. This has resulted in a set of legal challenges at the procedural level, embodied primarily in some of the difficulties surrounding proving these crimes and accepting evidence regarding them, given that they do not leave a tangible material trace, as is the case. The situation in traditional crimes, in addition to the resulting obstacles facing the judicial and security agencies in order to initiate some cross-border procedures such as inspection, inspection and seizure within the scope of the virtual environment.

This constituted an impetus to demand that the Iraqi legislator establish a clear and explicit text devoting the evidentiary power of copying digital evidence, and demonstrating its legal value, in addition to the necessity of working to strengthen the capabilities of judicial police officers and investigators in the field of verifying and collecting digital evidence.

Keywords: Internet crimes, criminal evidence, digital evidence.

0009-0006-8488-5433

Creative Commons Attribution 4.0 International (CC BY 4.0)

المقدمة

من المتعارف عليه على المستوى الإجرائي أن قواعد الإجراءات الجزائية التقليدية وضعت في الأصل لتطبق على الشيء أي المنقول والمادي، استنادا لمعايير ثابتة، حيث لم تكن الجرائم المعلوماتية من ضمنها، لكن ظهور هذه الجرائم المستحدثة والمتميزة بطابعها التقني خلق العديد من المصاعب والتعقيدات الإجرائية كثيرة، فقد أزاحت هذه الجرائم الستار عن أساليب حديثة ومتطورة يستخدمها المجرم المعلوماتي، وقفت الإجراءات التقليدية أمامها عاجزة، لا من حيث التحقيق فحسب، بل وصلت الى أدلة الإثبات ومبدأ حرية الاقتناع الشخصي للقاضي الجزائي.

وإذا كان هناك تلازم بين الحق والدليل عليه إلا ان الدليل في الحقيقة هو شيء مختلف عن الحق ذاته، فهو لا يعدو إلا أن يكون مجرد وسيلة لإثبات وجود الحق بشروطه وأوصافه فلو كان الدليل باطلاً مثلاً فإن ذلك لا يحول دون إثبات الحق بدليل آخر[1].

ويقصد بالإثبات في المسائل الجزائية عمومًا «إقامة الدليل لدى السلطة الجزائية المختصة على حقيقة واقعة ذات أهمية قانونية، وذلك بالطرق المنصوص عليها قانوناً»، وعليه، فإن الإثبات هو العمود الفقري للعدالة الجزائية، إذ لا يمكن أن تتحقق هذه العدالة بدون اللجوء إلى نظام إثبات يضمن تحقيقها[2].

أهمية البحث

تنبع أهمية الدراسة من انتشار المعاملات الإلكترونية، بحيث يشهد العالم اليوم ثورة كبيرة في مجال المعلوماتية، خصوصًا بعد فتح المجال أمام المعاملات المدنية والتجارية بأن أصبحت تتم بوسائل إلكترونية، الأمر الذي دفع بالقوانين المقارنة إلى عد حماية تلك المعاملات مصلحة

(1) مجيد خضر أحمد السبعاوي، الحماية الجنائية لقرينة البراءة بأبعاد دولية دستورية، الطبعة الاولى، المركز العربي للنشر والتوزيع، القاهرة، 2017، ص 435.

(2) محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الطبعة الاولى، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1977، ص 95.

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

اجتماعية تستحق التدخل لتحقيقها، وعلى أساس ذلك قامت العديد من الدول الأجنبية بإدخال واستحداث قوانين خاصة بالجرائم المعلوماتية.

إشكالية البحث

يثير البحث في هذا الموضوع مجموعة متعددة من الإشكاليات التي تتنوع في مظهرها وتتحد في مضمونها، والعامل المشترك فيها هو الإشكالية التي يثيرها تطبيق القانون الجزائي (بشقيه الموضوعي والإجرائي) على الجرائم المعلوماتية التي تعد من الجرائم التقنية. وعليه، يثير هذا البحث من الناحية الإجرائية الإشكالية الرئيسية التالية:

«ما أهمية الدليل الرقمي في عملية الإثبات الجنائي لجرائم المعلوماتية؟»

منهج البحث

وللإحاطة بجوانب الموضوع يتطلب البحث اتباع المنهج التحليلي الوصفي المقارن، وذلك لتعدد الآراء التي أثيرت بشأن جرائم المعلوماتية، فضلًا عن ضرورة المقارنة بين النصوص القانونية، بالإضافة إلى اتباع المنهج التأصيلي التطبيقي.

وبناء على ما تقدم، سنتناول في هذا البحث الدليل الرقمي ودوره في إثبات جرائم المعلوماتية، من خلال المبحث الأول، ومن ثم سنوضح صعوبات الإثبات الجزائي في جرائم المعلوماتية مع بيان سبل مواجهتها والتخلص منها، من خلال المبحث الثاني.

0009-0006-8488-5433

Creative Commons Attribution 4.0 International (CC BY 4.0)

المبحث الأول: الدليل الرقمي كعنصر إثبات في جرائم المعلوماتية

نظرا لخصوصية الجرائم الإلكترونية من ناحية طبيعتها وخطورتها الإجرامية وأركانها وخصوصية مرتكبيها وأساليب كشفها، فقد أثارت العديد من الصعوبات الإجرائية التي تمثلت بتحديات من الناحية القانونية والعملية التي تثيرها عملية الاستقصاء أمام سلطات التحقيق بجميع مستوياتها وباختلاف أدوارها، سيما لناحية مسألة إثبات هذه الجرائم والآلية المناسبة لمباشرة إجراءات الاستقصاء والتحقيق عبر البيئة الافتراضية وصولًا إلى الحقيقة.

فالجهات المكلفة بهذه الإجراءات في الجريمة المعلوماتية التي يجري ارتكابها في بيئة افتراضية يختلف مسرحها كليًا عن المسرح التقليدي، ولا يخلف مرتكبها أي آثار، بسبب دقة وسرعة اقترافها، وإمكانية محو آثارها، وإخفاء الأدلة المحصلة عقب وقوعها مباشرة، ويزداد الوضع تعقيدًا بالنسبة إلى الجهات المكلفة بالاستقصاء حينما يتعلق التحقيق بجريمة معلوماتية امتد آثارها إلى خارج الإقليم الوطني، إذ تثير مسألة تتبعها مشكلة تتعلق بسيادة الدولة والولاية القضائية، والتي لا يحتاج حلها إلى تعاون دولي في هذا المجال، إضافة لطبيعة وسائل الإثبات فيها كما هو الحال فيما يتعلق بالدليل الرقمي كأحد أبرز هذه الوسائل، وذلك على خلاف الجرائم التقليدية التي يتم ارتكابها في عالم مادي وملموس يلعب فيه السلوك المادي الدور الأكبر والأهم، ويسهل الاستقصاء فيها بالنظر إلى ما تتضمنه من عناصر مادية يمكن إدراكها بالحواس، وما يمكن أن يخلفه المجرم من آثار محسوسة في مسرح الجريمة.

وبناء على ما تقدم سنخصص هذا المبحث لدراسة دور الدليل الرقمي في الثبات في جرائم المعلوماتية، حيث نبين ماهية هذا الدليل في المطلب الأول، ومن ثم نتناول هذا الدليل كأحد عناصر الإثبات الجزائي في جرائم المعلوماتية، وذلك من خلال تقسيمه على فصلين، وعلى النحو الآتي:

المطلب الأول: ماهية الدليل الرقمي

كان للثورة التكنولوجية وما ترتب عنها من ثورة معلوماتية تأثيرات كبيرة على وسائل الإثبات،

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

فالتجانس المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي ينتج عنها أفرز نوعًا جديدًا من الأدلة يتماشى مع طبيعة جرائم المعلوماتية المرتكبة عبر شبكة الإنترنت، وهو ما يعرف بالدليل الإلكتروني، ومع ذلك فإن الأدلة التقليدية كالشهادة والقرائن والاعتراف لم تتلاش أمام هذه الجريمة المستحدثة، وإن كان دورها قد تضاءل في عملية الإثبات، الأمر الذي أدى إلى ظهور ما يعرف بالدليل الرقمي الذي يتم الحصول عليه من خلال عملية البحث والتحري في حاسوب الجاني أو المجني عليه، أو في المواقع الإلكترونية، فالأدلة الرقمية التي تنتج عن هذا الفحص التقني تبقى هي رأس الخيط الذي يوصل إلى تسلسل أحداث النشاط الجرمي[1].

ولقد أسهم الفقه المقارن في رسم مفهوم الأدلة الإلكترونية وتحديد الدور الذي تلعبه في كشف معالم الجريمة المعلوماتية، وهذا ما سنحاول توضيحه في مطلبين، وعلى النحو الآتي:

الفرع الأول: تعريف الدليل الرقمي

إن الدليل الرقمي الذي تنتجه البيئة الافتراضية للجرائم الإلكترونية مرتبطاً بتكنولوجيات وسائل الاتصال وشبكات الربط الحديثة، فمن الضروري أن يكون أي تعريف لهذا النمط من الأدلة متسماً بالمرونة بما يسمح باستيعابه وتواكبه مع سائر الجرائم المرتكبة بالتقنيات المبتكرة الراهنة والمستقبلة في تكنولوجيا التعامل مع المعلومات، بيد أن التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم الدليل الإلكتروني، خشية حصر نطاقه داخل إطار تجريمي محدد قد يحد منه خاصة في ظل التطور المستمر للتقنية الإلكترونية[2].

وفيما يتعلق بتعريف الدليل الرقمي فإن فقهاء القانون الجنائي لم يتفقوا حتى الآن حول تعريف

(1) د. نبيلة هبه هروال: مرجع سابق، ص40.
(2) سيدي محمد البشير: دور الدليل الرقمي في إثبات الجرائم المعلوماتية (دراسة تحليلية تطبيقية)، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص 15.

0009-0006-8488-5433

Creative Commons Attribution 4.0 International (CC BY 4.0)

موحد بشأنه، ويعود ذلك إلى التطور المستمر في البيئة الإلكترونية.

وقد عرفه البعض بأنه دليل ذو طابع رقمي مأخوذ بواسطة برمجيات تكنولوجية معينة من الأجهزة التي تعمل بنظم تشغيل حاسوبية سواء تمثل في شكل نصوص مكتوبة أو مرسومة أو صور أو أصوات أو مواد فيلمية بغرض إثبات جريمة معينة وتقرير الإدانة أو البراءة فيها»[1].

واستنادا لهذا المعنى فإنه الدليل الرقمي لا يعدو كونه سوى وسيلة للتوصل إلى الحقيقة القضائية، وعليه، فإنه من الممكن أن يكون هذا الدليل ناشئ أو مستمد من أنظمة الحاسبات أو أنظمة المعالجة الآلية للبيانات، طالما يمكن الوصول من خلاله إلى ذات الهدف وهو الحقيقة القضائية [2].

وعلى الصعيد الدولي وعرفته المنظمة العالمية لدليل الكمبيوتر (IOCE)[3] بأنه: «كل معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو متنقلة عبرها بواسطة شبكة الاتصالات في شكل مجالات إلكترونية أو ذبذبات كهربائية أو نبضات مغناطيسية، يتم استخلاصها وجمعها وتحليلها وفق إجراءات قانونية وعلمية، وترجمتها لتظهر في شكل مخرجات يقبلها العقل والمنطق ويعتمدها العلم ويمكن استخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات الجريمة وتقرير البراءة أو الإدانة»[4].

وبناء على ما تقدم يمكننا تعريف الدليل الرقمي بأنه الدليل المأخوذ من أي جهاز يعتمد في تشغليه على التقنية، ويتخذ شكل مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية

(1) د. محمود عبدالغني جاد المولى: دور الدليل الإلكتروني في الإثبات الجنائي (دراسة مقارنة)، ط1، دار الفكر الجامعي، الإسكندرية، 2019، ص28.

(2) د. محمد كمال شاهين: مرجع سابق، ص363.

(3) (IOCE) اختصار «international organization of computer Evidence» وهى تنظيم دولي مقره الولايات المتحدة الأمريكية وتم اعتماده عام ١٩٩٥، وتسعى هذه المنظمة إلى إقامة منتدى دولي لوكالات وهيئات إنفاذ القانون لتبادل المعلومات بشأن التحقيق في جرائم الحاسوب، وتتكون من وكالات إنفاذ القانون والأجهزة الحكومية المعنية بالتحقيق الرقمي وتحقيقات الطب الشرعي. للمزيد من التفاصيل عن المنظمة يراجع الرابط الالكتروني الآتي:

http//:www.ioce.org/index?phpid.

(4) مصطفى محمد مرسي: مرجع سابق، ص213.

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

الفرع الثاني: خصائص الدليل الرقمي

يمتاز الدليل الإلكتروني بكونه برهانًا علميًا، باعتبار أنه مؤلف من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي، وأن ما يسري على الدليل العلمي يسري على الدليل الإلكتروني فإن الدليل الإلكتروني له الطبيعة ذاتها، لذلك يجب ألا يخرج عمّا توصل إليه العلم الإلكتروني الرقمي وإلا فقد معناه[1].

كما أن الدليل الرقمي قد يتخذ أشكالاً متعددة، فقد يكون واضحاً ومقروءا ومفهوماً للبشر كما لو كان وثيقة مكتوبة ومعدة بنظام المعالجة الآلية للبيانات أو صورة ثابتة أو متحركة، وعلى العكس من ذلك قد يتخذ أشكالاً غير واضحة مثل الأدلة المتمثلة في إشارات رقمية يتم الحصول عليها من خلال المراقبة عبر الشبكات، وهذه الصورة هي التي تعبر عن التطور المستمر للأدلة الرقمية بسبب تطور علم المعالجة الآلية للبيانات [2].

بالإضافة إلى أن الدليل الرقمي يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد أو التلف أو التغيير من خلال عمل نسخ طبق الأصل من الدليل[3].

المطلب الثاني: الدليل الرقمي كأحد عناصر الإثبات

إن الدليل الرقمي يخضع لنفس القواعد المطبقة على الأدلة الاخرى، سواء لناحية القواعد

(1) يقصد بالدليل العلمي الدليل المتحصل عليه من الأجهزة والوسائل العلمية التي أقرها العلم الحديث والخبرات الإنسانية المتمثلة في الطب الشرعي والعلم النفسي التجريبي، فهو ثمرة توظيف معطيات العلوم الحديثة في مجال الاثبات الجنائي مقربا بين نظرية العلم والقانون، ولذلك فإنه يمكن إضافة الأدلة المستمدة من أجهزة الحاسب الآلي وشبكة الإنترنت إلى التعريف بالدليل العلمي بوصفها من الأجهزة والوسائل التي أفرزها العلم الحديث. للمزيد ينظر: د. السيد محمد سعيد عتيق: النظرية العامة للدليل العلمي في الإثبات الجنائي اطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 1992، ص98.

(2) د. فتحي محمد أنور عزت: الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2010، ص 652.

(3) قحطان عدنان عويد العطار: مرجع سابق، ص299.

0009-0006-8488-5433

Creative Commons Attribution 4.0 International (CC BY 4.0)

المنظمة لسلطة القاضي في قبول الدليل الرقمي، أم تتعلق بسلطته في تقدير هذا النوع من الدليل، ذلك أن القاضي لا يقدر إلا الدليل المقبول، ولا يكون الدليل مقبولًا إلا بعد التأكد من مراعاته للضوابط والشروط المحددة قانونًا والتي لا يمكن من دونها أن يترتب على الدليل الرقمي أية آثار قانونية[1].

لذلك سوف نبين في هذا المطلب سلطة القاضي الجزائي في قبول الدليل الرقمي وذلك في الفرع الأول، ومن ثم سنتطرق إلى الشروط التي يقتضي توفرها في الدليل الرقمي، وذلك في الفرع الثاني، وعلى النحو الآتي:

الفرع الأول: مدى صلاحية القاضي الجزائي في قبول الدليل الرقمي

إن قبول الأدلة من قبل القاضي الجنائي تمثل الخطوة الإجرائية الأولى التي يمارسها تجاه الأدلة الجنائية بصفة عامة بما فيها الأدلة الرقمية، وذلك قبل البدء في تقديرها للتأكد من مدى صلاحيتها لتحقيق ما قدمت من أجله.

وهنا يقتضي الإشارة إلى أن الطبيعة الفنية الخاصة للدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث الحصول على الدليل الرقمي، وينجم عن ذلك أن تقديمه للقضاء لا يكفي بحد ذاته لاعتباره كدليل للإدانة، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة، فإذا كانت الأدلة المتحصلة عن الوسائل الإلكترونية قد توجّسَ منها كلٌ من رجال القضاء والفقه خشية عدم تعبيرها عن الحقيقة، نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتحريف أو التغيير والأخطاء المتعددة، فإن ذلك قد تطلب وجوب توافر مجموعة من الشروط والضوابط التي قد تضفي عليها المصداقية، ومن ثم اقترابها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجزائية[2].

(1) د. سميرة بيطام: حجية الدليل البيولوجي أمام القاضي الجنائي، أمواج للنشر والتوزيع، عمان، الأردن، 2015، ص 153.

(2) يمكن أن يشكك في سلامة الدليل الرقمي من ناحيتين، الناحية الأولى إمكانية خضوعه للعبث والخروج به على نحو يخالف الحقيقة، إذ يقدم هذا الدليل معبراً عن واقعة معينة صنع أساساً لأجل التعبير عنها خلافا للحقيقة ودون أن يكون في استطاعة غير المتخصص إدراك ذلك العبث، أما الناحية الثانية فتتمثل بوجود نسبة خطأ في الحصول على الدليل الرقمي وهذا الخطأ قد يكون بسبب الآلة المستخدمة في الحصول عليه، أو الخطأ في

0009-0006-8488-5433

الفرع الثاني: الشروط التي يقتضي توفرها في الدليل الرقمي كأحد عناصر الإثبات

لكي يتم قبول الدليل الرقمي في الإثبات الجزائي، يقتضي توفر مجموعة من الشروط أهمها:

مشروعية الوسائل المستخدمة في الحصول على الدليل الرقمي، حيث يقتضي التقيد بأحكام القانون والعمل في إطاره، بهدف تقرير ضمانة أساسية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة بالتعدي عليها في غير الحالات المسموح فيها بذلك [1]. إضافة إلى إتاحة إمكانية مناقشة هذا الدليل أسوة بسائر الأدلة. وهو ما كرسه القانون العراقي[2].

كما يقتضي أن يتصف هذا الدليل باليقين، فالاقتناع هو ثمرة اليقين، وحتى يتحقق اليقين للأدلة الرقمية أكثر ينبغي إخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل، بحيث تسمح بالتحقق من مدى سلامة الدليل الرقمي المقصود في عدم وقوع تعديل أو تغيير في نظام الحاسوب[3].

والجدير بالذكر أن مناقشة الأدلة الرقمية تثير تساؤلات عديدة، منها كونها أدلة غير مرئية بالعين المجردة، وتسجل على وسائل إلكترونية، ولا يمكن قراءتها أو استخراجها إلا باستعمال أجهزة إلكترونية، فضلاً عن إمكانية التلاعب في المعلومات المسجلة بمسحها أو استبدال مضمونها دون علم أحد، وهو ما يثير التساؤل عن إمكانية المناقشة العلنية لهذه الأدلة في أصالتها، ومدى تأثير ذلك على مبدأ قبولها من قبل القضاء.

علما أنه وفقا للقانون العراقي، فإننا نجد أنه يخلو من وجود نص يوضح القيمة القانونية والقوة الثبوتية للنسخ المستخرجة من الدليل الرقمي الأصلي، وهذا بتقديرنا يعد نقصًا تشريعيًا من شأنه ان يربك العمل القضائي.

استخلاص الدليل نفسه.

(1) هلالي عبد اللاه أحمد: حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1997، ص10.

(2) – وهو ما سار عليه المشرع العراقي أيضًا، من خلال المادة (212) من قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل في قانون أصول المحاكمات الجزائية أكد فيه على أنه «لا يجوز للمحكمة أن تستند في حكمها إلى دليل لم يطرح للمناقشة، أو لم يشر إليه في الجلسة، ولا إلى ورقة قدمها أحد الخصوم، دون أن يمكن باقي الخصوم من الاطلاع عليها، وليس للقاضي أن يحكم في الدعوى بناء على علمه الشخصي.

(3) خالد حسن احمد لطفي الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية، 2020، ص 204.

0009-0006-8488-5433

المبحث الثاني: صعوبات الإثبات الجزائي في جرائم المعلوماتية

بالإضافة للآثار السلبية لجرائم المعلوماتية، نتج عنها أيضا العديد من الصعوبات المتعلقة بالقانون الجزائي الموضوعي، وأيضا أثارت الكثير من الإشكاليات الخاصة بالجوانب الإجرائية، سيما وأن نصوص قانون الإجراءات الجزائية أقرت لتحكم الإجراءات الخاصة بالجرائم التقليدية، والتي لا توجد صعوبات في إثباتها أو التحقيق فيها أو جمع الأدلة المتعلقة بها، وهذه الأخيرة تعد من الضروريات التي تظهر كفاءة الأنظمة القانونية المختلفة في التعامل مع المعلومات ومدى تواصلها مع التطور التقني، فلا يكفي مجرد التجريم الموضوعي للأفعال الخطرة أو غير المشروعة الناتجة عن استخدام الإنترنت، وإنما يجب أن يتسع الأمر ليشمل أيضا تنظيم الجوانب الإجرائية لهذه الجرائم، إذ أن الناحية الإجرائية للقانون الجزائي تعمل على تحريك الناحية الموضوعية ونقلها من حالة الجمود إلى حالة التنفيذ.

خاصة في ظل خضوع الدليل الرقمي للمبدأ العام في الإثبات الجزائي والمتمثل بحرية القاضي الجزائي في الاقتناع، فهو وحده الذي يقرر قيمة الدليل الرقمي بحسب الأثر الذي يحدثه في وجدانه من ارتياح واطمئنان.

واستنادا لما سبق سوف نخصص هذا المبحث لتناول الصعوبات الفنية والقانونية التي برزت في إطار جرائم الإنترنت من خلال المطلب الأول، على أن نتطرق لأبرز الآليات التشريعية والقضائية التي هدفت لتذليل هذه الصعوبات في المطلب الثاني.

المطلب الأول: الصعوبات الفنية والقانونية في الإثبات

إن مسألة الإثبات في نظم الحاسوب والإنترنت خلقت العديد من الإشكاليات، سيما في جمع الأدلة الرقمية التي تمتاز بكونها غير مرئية، وهذه الخاصية تمثل عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة إلكترونيًا أو المنقولة عبر الإنترنت صعوبة أمام إثباتها، كما أن سهولة محو الدليل تعد من أهم الصعوبات التي تعترض طرق الوصول إلى أدلة الإثبات الجزائي في مجال الجرائم المعلوماتية، ولا شك أن الطبيعة العالمية التي تتميز بها

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

هذه الجرائم قد تثير مشكلات عدة تتعلق بتحديد الاختصاص المكاني وقواعد سريان القانون الوطني، مما يزيد عقبة الإثبات الجزائي لهذه الجرائم، خاصة في حالات ارتكابها خارج النطاق المكاني للإقليم، وعلى هذا الأساس فإن الاستقصاء والتحري في هذا النوع من الجرائم يحتاج إلى طرق إلكترونية فنية وتقنية تتناسب مع طبيعتها بشكل يمكنها من فك كلمات المرور السرية وترجمة النبضات الإلكترونية إلى بيانات مقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ونسبتها إلى مرتكبيها.

ونتيجة لما سبق، سنتناول في هذا المطلب أهم الصعوبات التي تعترض الإثبات الجزائي في جرائم المعلوماتية، وذلك من خلال تقسيمه على فرعين، وكما يأتي:

الفرع الأول: صعوبات الإثبات الفنية

تتنوع صعوبات الإثبات الجزائي لجرائم المعلوماتية ذات الصلة بطبيعة الجريمة وأدلتها الرقمية، حيث توجد صعوبة في فهم الدليل الرقمي، ومثل هذا الأمر يتطلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا الاحتيال، وقد يستعصي هذا الأمر فهماً على عضو الضابطة القضائية لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة، والتي من خلالها يمكن الوصول إلى الدليل الرقمي.

كما أن ذكاء مرتكبي هذه الجرائم يعد من الأسباب المنتجة للصعوبات، حيث أن هؤلاء يقومون بإخفاء جرائمهم وإزالة آثارها من خلال التلاعب بقواعد البيانات والقوائم في جهاز الكمبيوتر وبرامجه، من دون ترك أثر، ولا سيما أن التخزين الإلكتروني غير مرئي والبيانات مكتوبة بلغة رقمية لا يفهمها إلا الآلة ما لم تستعاد على شاشة الكمبيوتر ليتمكن الإنسان من قراءتها وفهمها، وهذا يشكل عقبة أمام إقامة الدليل على الجريمة المعلوماتية وإثباتها[1].

الفرع الثاني: صعوبات الإثبات القانونية

تتجلى الصعوبات القانونية في مجال إثبات جرائم المعلوماتية في شقين: الشق الموضوعي

(1) عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص65.

0009-0006-8488-5433

Creative Commons Attribution 4.0 International (CC BY 4.0)

للقانون الجزائي، والشق الإجرائي للقانون الجزائي، إذ وجدت العديد من الثغرات القانونية التي اعتبرت قصور تشريعي لمواجهة الجرائم المستحدثة، ومن ثم عدم إمكانية احتضان القانون الجزائي لهذه الطائفة من الجرائم، وهنا سوف نقوم على إجمال أوجه القصور التشريعي في القانون الجزائي لمواجهة الجرائم المعلوماتية، والتي تحول دون إمكانية ملاحقة مرتكبي هذه الجرائم.

ومن ناحية أخرى فإن النصوص الواردة في قانون العقوبات عاجزة عن مواكبة هذه الصور والأشكال المستحدثة من الإجرام المعلوماتي[1]. وذلك يعتبر بديهيا على اعتبار أن القانون الجزائي لا يتميز بالقدرة على التطور السريع، بالتوازي مع سرعة تطور الحياة أو التكنولوجيا أو مهارة الذهن البشري والذي سخر المعلوماتية المستحدثة للاستخدام السيئ وكذلك الأشكال المستحدثة للجريمة.

من دون ان ننسى عدم إمكانية تطبيق بعض مبادئ القانون الجزائي، كمبدأ الإقليمية الذي يقوم على أساس أن القانون الجزائي للدولة يحكم جميع ما يقع على إقليمها من جرائم، بصرف النظر عن جنسية مرتكبها سواء كان وطنيا أم أجنبياً، وبالمقابل لا سلطان للقانون الجنائي للدولة إلا أن هذا المبدأ يفقد صلاحيته ويصبح غير قابل للتطبيق فيما يتعلق بالجرائم المعلوماتية التي تتجاوز حدود المكان، فهي جرائم عابرة للحدود[2].

وبناء على ما سبق يتأكد لنا ضرورة التخلي عن الدعوة لتطويع نصوص قوانين العقوبات التقليدية لمواجهة الجديد في عالم الإجرام، وندعو المشرع لتوفير الحماية الجزائية للمعلومات، وكفالة استخدام الحاسوب ومعطياته، ومواجهة كافة صور الاعتداء على معطيات الحاسوب من بيانات ومعلومات وبرامج، والتدخل الذي نأمل من مشرعنا تحقيقه يستوجب مراعاة مرتكزات حماية الحق في المعلومات، والحق في الحياة الخاصة، وغيرها من الحقوق المقدسة.

(1) نهلا عبد القادر المومني: مرجع سابق، ص 72 وما بعدها.
(2) شيماء عبد الغني، الحماية الجزائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2007، ص 378.

0009-0006-8488-5433

المطلب الثاني: الآليات التشريعية والقضائية الآيلة لمواجهة صعوبات الإثبات

إن عملية الإثبات الجزائي في جرائم المعلوماتية كما سبق وذكرنا تعترضها معوقات وعقبات إجرائية عديدة، منها ما يتعلق بالطبيعة المتميزة للجريمة المعلوماتية، أو بالجهات المتضررة، ومنها ما يتعلق بجهات الاستقصاء والتحقيق، وأخرى تتعلق بإجراءات الحصول على الدليل الرقمي لارتباطها ببيانات معالجة إلكترونياً وكيانات منطقية غير مادية، وأن كثرة وتشعب هذه العقبات قد انعكس سلباً على مردود سلطات الضابطة القضائية والتحقيق الجزائي في ملاحقة مرتكبي هذه الجريمة، بل وتسبب بارتفاع معدل الجريمة المعلوماتية في العالم بسبب إدراك المجرم المعلوماتي أن وجود تلك العقبات من شأنه أن يعيق الجهات الأمنية عن اكتشاف أمره أو ملاحقته، ما يعطيه ثقة أكبر في ارتكابه المزيد من هذه الجرائم[1].

مما تقدم نلاحظ أن آليات مواجهة صعوبات الإثبات الجزائي في جرائم المعلوماتية تكون إما آليات تشريعية أو آليات قضائية، وهذا ما سنبحثه في الفرعين الآتيين:

الفرع الأول: الآليات التشريعية الرامية إلى مواجهة صعوبات الإثبات الجنائي

يرى جانب من الفقهاء أن مواجهة الصعوبات الإجرائية الناجمة عن جرائم المعلوماتية تتم عبر ترشيد النصوص الجزائية التقليدية بحيث تصبح ممكنة التطبيق والسريان على الجرائم المعلوماتية، خاصة تلك الجرائم التقليدية التي ترتكب عبر شبكة الإنترنت، والتي لا تعدو هذه الشبكة أن تكون سوى مجرد وسيلة حديثة لارتكابها، على أن يتم ذلك في حدود ما يفرضه مبدأ الشرعية الجزائية من الالتزام بالتفسير الضيق للنصوص الجزائية، وحظر القياس[2].

ومن ناحية أخرى يعتبر جانب آخر من الفقهاء بعدم ضرورة التعويل كثيراً على القواعد التقليدية لمواجهة هذه التحديات، إنما لا بد من التوجه إلى مراجعة هذه النصوص بصفة

(1) عمر فاروق الحسيني: المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وآثارها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنًا بالتشريع الفرنسي، الطبعة الثانية، بلا دار ومكان نشر، 1995، ص 146.

(2) د. هدى حامد قشقوش: السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012، ص72.

0009-0006-8488-5433

دورية ومستمرة بما يضمن مواكبة متغيرات وتطورات الجريمة المعلوماتية، وإلى إرساء قواعد قانونية جديدة خاصة تواجه المشكلات المعاصرة الناجمة عن هذا النوع من الإجرام المستحدث وتطوراته اللامتناهية[1].

ويعتبر كلا من التضامن والتعاون بين التشريعات الدولية من أبرز هذه الآليات نظرا لقدرتها على التقليل من فرص هروب الجناة من العدالة، ويضمن تطبيق العدالة الجنائية على مرتكب الجريمة في أي مكان في العالم[2].

إضافة إلى تنظيم ورشات العمل الدولية الخاصة بمنع الجريمة ومعاملة المجرمين وإشرافها على عقد مؤتمرات دولية في هذا المجال[3]. حيث نجم عنها على سبيل المثال اعتماد منظمة الأمم المتحدة في عام 1996 قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية. إضافة إلى إصدار منظمة الأمم المتحدة القانون النموذجي بشأن التوقيعات الإلكترونية في عام 2001 بعده صكاً قانونياً جديداً مستمدًا من قانون الأونسيترال النموذجي بشأن التجارة الالكترونية، ومتسقاً مع أحكامه وبشكل مفصل[4].

وأيضا على المستوى الإقليمي فيمكن تجسيد الآليات التشريعية على المستوى الأوروبي بالدور الذي يؤديه المجلس الأوروبي في تحقيق الانسجام بين التشريعات الوطنية للدول الأطراف بشأن مكافحة جرائم المعلوماتية، وقد تجسدت أولى جهوده في توقيع دول المجلس الأوربي عام 1981 اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات الشخصية والتي شكلت الإطار القانوني المشترك لضمان حرية تنقل البيانات الشخصية المعالجة آليًا وحمايتها من أي شكل من أشكال الاعتداء عليها[5].

(1) د. يوسف حسن يوسف: مرجع سابق، ص126.
(2) د. مصطفى محمد موسى: مرجع سابق، ص205.
(3) محمود احمد عبد الله: جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2009، ص155.
(4) سيناء عبد الله محسن: المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، بحث مقدم إلى الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، المنعقدة بالرباط للفترة من 19 – 20/7/2007، ص54.
(5) من المهم التمييز بين المجلس الاوربي والاتحاد الاوربي، فالمجلس الاوربي هو منظمة دولية تم انشائها عام

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

الفرع الثاني: الآليات القضائية

تلعب الآليات القضائية دورًا مهمًا إلى جانب الآليات التشريعية، لأنها تهتم بتجسيد الآليات التشريعية في أرض الواقع ونقلها من دائرة التجريد القانوني إلى التطبيق العملي.

حيث تتجلى الآليات القضائية الآيلة لمواجهة صعوبات الإثبات الجزائي في جرائم المعلوماتية من خلال تعزيز التعاون الدولي القضائي بمختلف صوره، باعتباره أبرز التدابير التي تكرس المساعدة المتبادلة والتنسيق المشترك بين سلطات العدالة الجنائية التابعة لدول مختلفة في مواجهة الجريمة المعلوماتية، فمن الصعوبات الشائعة التي تواجه عمليتي التحقيق والإثبات في جرائم المعلوماتية، احترام سيادة الدول وإشكاليات الحدود والولايات القضائية، وذلك راجع إلى الطابع العابر للحدود الذي تتميز به هذه الجرائم، ولعل من أبرز الآليات التي وجدتها الدول لتجاوز هذه الصعوبات وتحقيق التوافق بين حرية كل دولة في ممارسة اختصاصها الجزائي على كافة حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، هو تعزيز التعاون والمساعدة القضائية المتبادلة فيما بينها[1].

ويأخذ هذا التعاون على المستوى القضائي أشكالا متعددة، كالمساعدة الأمنية والفنية بين الدول، التي تسهم في تخطي الصعوبات التي يثيرها الطابع العالمي الخاص بهذا النوع من الجرائم، فضلًا عن إنشاء وتطوير كل النظم القادرة على المساهمة بفعالية في الوقاية من هذه الجرائم ومواجهتها[2].

1994 ويضم (46) دولة، ومقره في مدينة ستراسبورغ في فرنسا، ويمارس نشاطه في مكافحة الجريمة من خلال اللجنة الاوربية الخاصة بمكافحة الجرائم، اما الاتحاد الاوربي فهو جمعية دولية للدول الاوربية تضم (28) دولة، تم تأسيسها بناءً على معاهدة (ماستريخت) عام 1992، ويمار الاتحاد نشاطات تجارية كنقل الاموال والسلع والخدمات بين دول الاعضاء، للمزيد ينظر: د. مخلد عبيد: الاتحاد الاوربي كظاهرة اقليمية متميزة، ط1، الاكاديميون للنشر والتوزيع، عمان، 2010، ص102.

(1) جمال براهيمي: مرجع سابق، ص294.

(2) أنشئت هذه الهيئة في عام 1923 تحت اسم «اللجنة الدولية للشرطة الجنائية» بمناسبة المؤتمر الدولي للشرطة القضائية المنعقد بمدينة فيينا، ثم تحولت في عام 1956 إلى «المنظمة الدولية للشرطة الجنائية»، وذلك بعد إصدار الجمعية العامة لمنظمة الأمم المتحدة في دورتها الخامسة والعشرون قرار اعتماد نظامها الأساسي، وجعلت مقرها في مدينة ليبون (Lyon) الفرنسية، وتظم حالياً أكثر من 189 دولة عضو، للمزيد من التفاصيل حول نشأة الإنتربول: ينظر الرابط الالكتروني الآتي:

0009-0006-8488-5433

وتعد المنظمة الدولية للشرطة الجنائية (الانتربول) من أبرز الأمثلة التي تعد أفضل نموذج للتعاون الأمني، فهي تمثل أكبر شبكة اتصالات لتبادل المعلومات الأمنية على المستوى العالمي، بالإضافة إلى تأسيسها شراكات استراتيجية في هذا المجال مع منظمات دولية حكومية وغير حكومية ومع هيئات من القطاع الخاص[1].

إضافة إلى المساعدة القضائية التي ترمي إلى تبادل المعلومات ونقل الإجراءات، والإنابة القضائية والدولية، وفيما يتعلق بهذا التعاون تعتبر الاتفاقية الأوروبية حول الجريمة المعلوماتية (اتفاقية بودابست) لعام 2001 أنموذجا لذلك، لإقرارها عدة إجراءات تعاون مستحدثة، بالإضافة إلى تعزيزها لصور التعاون القضائي الدولي المتعارف عليها، فقد أوصت هذه الاتفاقية من خلال المادة 23 منها الدول الأطراف بتطبيق الاتفاقات الدولية حول التعاون الدولي في المسائل الخاصة بالجريمة ذات الصلة[2].

، تاريخ الزيارة http://www.interpol.int/public/icpo/default.asp.22/8/2023

(1) وتجدر الإشارة هنا إلى أن منظمة الانتربول أسهمت بالمشاركة مع سلطات أمن وطنية في إحباط عدة عمليات إجرامية خطيرة عبر العالم، والكشف عنها وتوقيف مرتكبيها أشهرها قضية النصب والاحتيال الاستثماري التي شملت أكثر من (2000) ضحية من (60) دولة وبمبلغ مسروقات قدر ب (166) مليون يورو، فقد باشر الانتربول التحقيق فيها بالتنسيق مع سلطات الأمن في الدول المعنية، وتوصل إلى الكشف عن المجرمين وتوقيفهم في اسبانيا عام 2004، وكذلك عملية فالكون (FALCON) عام 2005، التي تمت بين كل من الإنتربول والشرطة الفيدرالية الأمريكية (FBI) والشرطة الفرنسية، والتي انتهت إلى تفكيك شبكة إجرامية تنشط في العديد من الدول الأوروبية، للمزيد ينظر: فهد عبدالله العازمي: مرجع سابق، ص522.

(2)() نصت المادة (٢٣) من اتفاقية بودابست لعام ٢٠٠١، على انه «... سوف يتعاون الأطراف فيما بينهم طبقًا للأحكام الواردة في هذا الفصل ومن خلال تطبيق الأدوات الدولية اللازمة في شأن التعاون الدولي في المسائل الجنائية والترتيبات المتفق عليها وذلك على أساس التشريعات الموحدة او النظيرة والقوانين المحلية إلى أبعد حد ممكن في مجال التحريات والإجراءات الخاصة بالأفعال الجنائية المتعلقة بنظم الحاسبات والمعلومات او بجمع الأدلة في شكلها الإلكتروني في شأن الجرائم الجنائية».

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

الخاتمة

بعد أن انجزنا البحث في موضوع الدراسة الموسوم بـ(الإثبات الجنائي في جرائم الإنترنت)، ظهر لنا أن تنامي ظاهرة الإجرام المعلوماتي وتخطي آثاره حدود الدول، أفرز جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض الصعوبات التي تكتنف إثبات هذه الجرائم وقبول الدليل بشأنها، نظرا لأنها لا تترك أثرًا ماديًا ملموسًا، كما هو الحال في الجرائم التقليدية، إضافة لما ينتج عن ذلك من عقبات تواجه الأجهزة القضائية والأمنية في سبيل مباشرة بعض الإجراءات عبر الحدود كالمعاينة والتفتيش والضبط في نطاق البيئة الافتراضية، بالإضافة الى إشكالية تنازع الاختصاص بصدد هذه الجرائم التي تتجاوز آثارها حدود

وبناءً على ما تقدم، فقد أنهينا بحثنا بمجموعة من الاستنتاجات والمقترحات، والتي سنحاول عرضها على النحو الآتي:

الاستنتاجات

– يعاب على القانون العراقي خلوه من وجود نص يوضح القيمة القانونية والقوة الثبوتية للنسخ المستخرجة من الدليل الرقمي الأصلي، وهذا بتقديرنا يعد نقصًا تشريعيًا من شأنه ان يربك العمل القضائي.

– تتميز جرائم المعلوماتية بصعوبة إثباتها، نظرا لصعوبة الاحتفاظ الفني بآثارها إن وجدت، والحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها، وهذا ما يسهم بعرقلة عمل سلطات التحقيق وأعضاء الضابطة القضائية الذين اعتادوا على التعامل مع الجرائم التقليدية.

– أن عملية استخلاص الدليل الرقمي سواء بالطرق الإجرائية التقليدية أم المستحدثة فيها من الصعوبة الكثير، إذ تعوقها في معظم الأحيان صعوبات تتصل إما بالطبيعة التكوينية للدليل الرقمي أو بالعامل البشري.

0009-0006-8488-5433

ISSN 3006-7294
Creative Commons Attribution 4.0 International (CC BY 4.0)

التوصيات

– نوصي المشرع العراقي بوضع نص واضح وصريح يكرس القوة الثبوتية لنسخ الدليل الرقمي، ويبين قيمته القانونية.

– ضرورة العمل على تعزيز قدرات رجال الضابطة القضائية والمحققين في مجال التحقق من الأدلة الرقمية وجمعها، وذلك من خلال توفير التدريب المكثف والدورات التعليمية اللازمة في تحليل البيانات الرقمية.

– تعزيز التعاون والشراكة بين القطاع العام والخاص، وبين الجهات الوطنية والدولية المختصة بمكافحة جرائم المعلوماتية، وذلك من أجل تعزيز القدرات والموارد الأساسية، فضلًا عن تبادل المعلومات والتجارب الناجحة في هذا المجال.

– الانضمام إلى الاتفاقيات الدولية المعقودة بهذا الشأن ومنها اتفاقية مجلس اوروبا بشأن الإجرام المعلوماتي (اتفاقية بودابست)، والإفادة من خبرات الدول والمنظمات في مجال مكافحة جرائم المعلوماتية سواء على المستوى الموضوعي أم الإجرائي

0009-0006-8488-5433

المراجع

الكتب

1. خالد حسن احمد لطفي الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، الطبعة الاولى، دار الفكر الجامعي، الإسكندرية، 2020.

2. سميرة بيطام: حجية الدليل البيولوجي أمام القاضي الجنائي، أمواج للنشر والتوزيع، عمان، الأردن، ٢٠١٥.

3. شيماء عبد الغني، الحماية الجزائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الاسكندرية، 2007.

4. فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون للنشر والتوزيع، المنصورة، ٢٠١٠.

5. عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكومبيوتر والإنترنت (دراسة متعمقة في جرائم الحاسب الآلي والإنترنت)، دار الكتب القانونية، القاهرة، ٢٠٠٩.

6. عمر فاروق الحسيني: المشكلات العامة في الجرائم المتصلة بالحاسب الآلي وآثارها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنًا بالتشريع الفرنسي، الطبعة الثانية، بلا دار ومكان نشر، 1995.

7. قحطان عدنان عويد العطار، الحماية الجزائية للمحررات الإلكترونية الشخصية (البطاقة الوطنية والجواز السفر أنموذجا)، ط1، مكتبة القانون المقارن، بغداد، 2022.

8. مجيد خضر أحمد السبعاوي، الحماية الجنائية لقرينة البراءة بأبعاد دولية دستورية، الطبعة الاولى، المركز العربي للنشر والتوزيع، القاهرة، ٢٠١٧.

9. مخلد عبيد، الاتحاد الاوربي كظاهرة إقليمية متميزة، ط1، الأكاديميون للنشر والتوزيع، عمان، 2010.

10. محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الطبعة الاولى، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، ١٩٧٧.

11. محمود عبد الغني جاد المولى، دور الدليل الإلكتروني في الإثبات الجنائي (دراسة مقارنة)، ط1، دار الفكر الجامعي، الإسكندرية، 2019.

12. محمد كمال شاهين، الجوانب الاجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي (دراسة مقارنة)، دار الجامعة الجديدة، الاسكندرية، 2018.

13. محمود احمد عبد الله: جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع،

0009-0006-8488-5433

عمان، 2009.

14. مصطفى محمد مرسي، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009.

15. نبيلة هبه هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2007.

16. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 1997.

17. هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012.

18. يوسف حسن يوسف، الجرائم الدولية للإنترنت، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2011.

المعاهدات الدولية

- اتفاقية بودابست لعام 2001،

القوانين

- قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

الرسائل والأطروحات

1. سيدي محمد البشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية (دراسة تحليلية تطبيقية)، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

2. السيد محمد سعيد عتيق: النظرية العامة للدليل العلمي في الإثبات الجنائي أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 1992.

الأبحاث

سيناء عبد الله محسن: المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية، بحث مقدم إلى الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، المنعقدة بالرباط للفترة من 19 - 20/7/2007.

0009-0006-8488-5433

مرخصة بموجب المشاع الإبداعي Attribution 4.0 International

الفهرس

المقدمة

المبحث الأول: الدليل الرقمي كعنصر إثبات في جرائم المعلوماتية

المطلب الأول: ماهية الدليل الرقمي

الفرع الأول: تعريف الدليل الرقمي

الفرع الثاني: خصائص الدليل الرقمي

المطلب الثاني: الدليل الرقمي كأحد عناصر الاثبات

الفرع الأول: مدى صلاحية القاضي الجزائي في قبول الدليل الرقمي

الفرع الثاني: الشروط التي يقتضي توفرها في الدليل الرقمي كأحد عناصر الاثبات

المبحث الثاني: صعوبات الاثبات الجزائي في جرائم المعلوماتية

المطلب الأول: الصعوبات الفنية والقانونية في الاثبات

الفرع الأول: صعوبات الإثبات الفنية

الفرع الثاني: صعوبات الإثبات القانونية

المطلب الثاني: الآليات التشريعية والقضائية الآيلة لمواجهة صعوبات الاثبات

الفرع الأول: الآليات التشريعية الرامية لمواجهة صعوبات الاثبات الجنائي

الفرع الثاني: الآليات القضائية

الخاتمة

المراجع

الفهرس

0009-0006-8488-5433