المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية

العدد الرابع والثمانين شهر (مايو) 2025

ISSN: 2617-9563

مشروعية الدليل الرقمي وحجيته في الإجراءات الجنائية

دراسة تحليلية مقارنة

اعداد: الرائد حسين محمد عساف

2025

الملخّص

تتناول هذه الدّراسة التحدّيات القانونيّة المرتبطة بمشروعيّة الدليل الرقميّ وحجّيّته في الإثبات الجنائيّ، في ظلّ التطوّر المتسارع للتكنولوجيا الرقميّة وانتشار الجرائم المعلوماتيّة. وقد أبرزت الدّراسة أهمّيّة الدليل الرقميّ كوسيلة إثبات حديثة، مع تحليل الإشكاليّات المتعلّقة بشرعيّة تحصيله، وإمكانيّة قبوله أمام القضاء. كما ناقشت مدى كفاية القواعد التقليديّة في تنظيم هذا النوع من الأدلة، والحاجة إلى تطوير معايير قانونيّة وتقنيّة خاصة لضمان مصداقيّة الدليل الرقميّ وسلامته. وتخلص الدّراسة إلى ضرورة تحقيق التوازن بين فعاليّة الدليل الرقميّ وضمانات المحاكمة العادلة، من خلال تحديث التشريعات وتعزيز التعاون بين الجهات القضائيّة والتقنيّة.

الكلمات المفتاحية: الدليل الرقميّ، الجرائم المعلوماتيّة، مشروعيّة الأدلّة، حجّيّة الإثبات، التفتيش المعلوماتيّ، الأدلّة الإلكترونيّة، قواعد الإثبات، العدالة الجنائيّة.

Abstract

This study addresses the legal challenges surrounding the admissibility and authenticity of digital evidence in criminal proceedings, amid the rapid development of digital technologies and the rise of cybercrimes. It highlights the importance of digital evidence as a modern means of proof and analyzes issues related to its lawful acquisition and judicial acceptance. The study also explores whether traditional evidentiary rules are sufficient to regulate digital evidence or if new legal and technical standards are required to ensure its reliability and integrity. It concludes with the need to strike a balance between the effectiveness of digital evidence and the guarantees of fair trial by updating legislation and strengthening collaboration between judicial and technical bodies.

Keywords: Digital evidence, Cybercrime, Legality of evidence, Evidentiary value, Digital search, Electronic evidence, Rules of evidence, Criminal justice.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

المقدمة:

يشهد العالم تطورات تقنية متسارعة أثّرت في مختلف المجالات، ومنها المجال القانوني، حيث برزت الجرائم المعلوماتية كتهديد متزايد يعتمد على وسائل تقنية تعقّد من اكتشافها وإثباتها. وفي هذا السياق، أصبح الدليل الرقمي عنصرًا محوريًا في تحقيق العدالة الجنائية، لكنه يطرح تحديات تتعلق بمشروعية الحصول عليه وحجيته أمام القضاء، ما يستدعي فهمًا دقيقًا للإطار القانوني الناظم له.

تهدف إجراءات التحقيق إلى تحصيل دليل مشروع يثبت الجريمة وينسبها إلى مرتكبيها، وقد أثرت ثورة المعلومات على وسائل التحقيق وطرق الإثبات، حيث لم تعد الطرق التقليدية كافية لمواكبة البيئة الرقمية. فقد أصبحت الأجهزة الذكية وشبكات الاتصال مستودعات رئيسية للبيانات ذات القيمة الإثباتية.

الدليل الرقمي يلعب دورًا حاسمًا في توثيق الجرائم المرتكبة في العالم الافتراضي، إلا أن استخدامه يثير تساؤلات حول مصداقيته وإمكانية التلاعب به، مما يتطلب تحليله بدقة والتأكد من سلامته. وقد انقسم الفقه بين من يرى إخضاعه لقواعد الإثبات التقليدية ومن يدعو لوضع معايير خاصة به.

ويواجه القاضي تحديًا في تقييم هذا النوع من الأدلة، إذ تتطلب معايير صارمة للتحقق من صحتها ومشروعية تحصيلها، بالتعاون بين الخبراء التقنيين والجهات القضائية. رغم قوته، فإن الدليل الرقمي يفرض تحديات تستوجب تحديثًا تشريعيًا وتطويرًا في آليات التعامل القضائي معه لضمان عدالة فعالة ومتوازنة.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية

العدد الرابع والثمانين شهر (مايو) 2025

ISSN: 2617-9563

إشكالية الدراسة

تتمحور إشكالية الدراسة حول السؤال التالي: **كيف يمكن ضمان مشروعية الدليل الرقمي المتحصل عن التفتيش المعلوماتي وحجيته في الإثبات الجنائي؟**

ويتفرع عن هذه الإشكالية تساؤلات فرعية:

1. ما هي المعايير القانونية التي تحكم مشروعية الدليل الرقمي؟
2. كيف يمكن التأكد من مصداقية الأدلة الرقمية وصحتها؟
3. ما هي التحديات التي تواجه القاضي الجنائي في التعامل مع الأدلة الرقمية؟

منهجية الدراسة

اعتمدت الدراسة على منهجية تحليلية مقارنة تشمل:

1. **التحليل القانوني:** دراسة النصوص القانونية المتعلقة بالدليل الرقمي في النظم القانونية المختلفة.
2. **المنهج المقارن:** مقارنة بين القوانين الوطنية والدولية فيما يتعلق بمشروعية الأدلة الرقمية.
3. **التحليل التطبيقي:** استعراض الحالات القضائية المرتبطة باستخدام الأدلة الرقمية.

أهمية الدراسة

تبرز أهمية الدراسة من خلال:

1. **الأهمية النظرية:** تسليط الضوء على موضوع معاصر يمس النظام القانوني والتحديات الناتجة عن الجرائم المعلوماتية.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

2. **الأهمية العملية:** تقديم مقترحات لتحسين التعامل مع الأدلة الرقمية وضمان قبولها أمام القضاء.
3. **الأهمية القانونية:** المساهمة في تطوير القوانين المحلية والدولية لمواكبة التحولات التقنية.

المبحث الأوّل: مشروعية ومصداقية الأدلة الرقمية

لا شك أن الهدف الرئيسي الذي تسعى إليه كل النظم الإجرائية هو وصول القاضي إلى الحقيقة ليصدر حكمه سواء بالبراءة أو بالإدانة. تحقيق هذا الهدف يتطلب من القاضي الجنائي الاعتماد على الأدلة المعروضة أمامه، سواء كانت مادية أو إلكترونية. للوصول إلى الاقتناع الكامل، يجب أن يكون الدليل الإلكتروني قاطعًا وحاسمًا. فإذا كان القاضي يحكم باقتناعه هو وليس باقتناع غيره فإنه يجب عليه أن يعيد فحص كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناعه بتقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاضٍ عادلٍ ومجتهد (قنديل، 2018، ص156).

في ضوء ذلك يستطيع القاضي أن يقرر قوة الدليل الرقميّ ومصداقيته وصحته ومدى نسبة الجريمة لشخص معين (Durham, 1993, p. 114). ولضمان قبول الدليل الإلكتروني أمام القضاء، هناك نوعان من الضوابط والمتطلبات التي يجب توفرها. النوع الأول هو المتطلبات القانونية، التي تتمثل في أن يكون الدليل مقبولاً وفقًا للقواعد القانونية المعمول بها. أما النوع الثاني، فهو المتطلبات المتعلقة بمشروعية الدليل، والتأكد من مصداقيته وصحته وسلامته، بحيث يمكن للقاضي الاعتماد عليه في تكوين قناعته اليقينية (Ngomane, 2010, p. 53).

أهمّيّة النوع الثاني من هذه المتطلبات تكمن في أن الأدلّة الرقميّة غالبًا ما تتعرض للتعديل أو التشويه أو

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

الإخفاء من قبل الجناة، مما يستوجب على المحاكم اعتماد معايير صارمة للتحقق من مصداقية وصحة وسلامة الدليل (Ngomane, 2010, p. 53). يتعين على المحكمة مناقشة الأدلّة الرقميّة المعروضة عليها للتأكد من صحتها وعدم تعرضها للتلاعب. هذا ما أكد عليه القضاء الأمريكي في قضية Lorraine، حيث قررت المحكمة أن مناقشة الأدلّة الرقميّة هي المعركة الأساسية لتحديد قبول أو عدم قبول الدليل الإلكتروني(Kemp, 2007, pp. 537–538).

بذلك، يصبح التحقق من الأدلّة الرقميّة ضرورة حتمية لتحقيق العدالة في الجرائم المعلوماتيّة. يجب أن تكون هذه الأدلة خاضعة لتقنيات متقدمة وأطر قانونية صارمة لضمان مشروعيتها وقبولها أمام القضاء، مما يعزز الثقة في النظام القضائي ويضمن حماية حقوق الأفراد والمجتمع.

المطلب الأوّل: التقييم القانوني لموثوقية الأدلة الرقمية المستمدة من الفضاء الإلكتروني

في هذا الموضع من الدراسة نتعرض لمدى خضوع التأكد من صحة الأدلّة الرقميّة للقواعد التقليدية، وكذلك سلطة القاضي في التأكد من صحة وسلامة الأدلّة الرقميّة المعروضة عليه وذلك فيما يلي:

1. مدى خضوع مسألة التأكد من مصداقية الأدلّة الرقميّة للقواعد التقليدية :

– الرأي الأول – الغالب –: خضوع التأكد من صحة الأدلّة الرقميّة للقواعد التقليدية

يرى أغلب الفقه في الولايات المتحدة أن التأكد من صحة السجلات الإلكترونية لقبولها كدليل رقمي يخضع لنفس القواعد التي تتبعها المحكمة للتأكد من صحة أي دليل معروض عليها، دون الحاجة لوضع قواعد جديدة للتأكد من صحة الأدلّة الرقميّة. (Rubin, 2013, p. 1) (Salgado, 2001, p. 453).

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

وفي ذات الاتجاه، قررت المحكمة العليا بولاية بنسلفانيا الأمريكية أن التأكد من صحة الأدلّة الرقميّة يخضع لذات القواعد المعمول بها في مجال الأدلة التقليدية. فقد قالت المحكمة: "نحن لا نرى أي مبرر لإنشاء قواعد فريدة أو متميزة لقبول الأدلة المستمدة من الاتصالات الإلكترونية مثل الرسائل، بحيث يتم تقديمها للمحكمة على أساس كل حالة على حدة مثلها مثل أي وثيقة أخرى لتحديد ما إذا كان هناك أسس وشواهد كافية للتأكد من أصالتها وصحتها" (Rubin, 2013, p. 1).

غير أن التأكد من صحة الأدلّة الرقميّة أكثر صعوبة من التأكد من صحة الأدلة التقليدية، حيث يجب على المحكمة أن تتأكد من أن النظام الحاسوبي محل الدليل الإلكتروني يعمل بطريقة دقيقة ومنتظمة (Jarrett & Judish, n.d., p. 200).

في ذات الاتجاه، يرى الفقه الفرنسي ضرورة توافر مجموعة من الشروط لقبول واعتماد الأدلّة الرقميّة، مثل التأكد من سلامة النظام الحاسوبي المستمد منه الدليل الإلكتروني، وضرورة اتخاذ كافة الاحتياطات الفنية اللازمة لضمان سلامة الدليل وعدم تعرضه للتلف، مع تفضيل إعداد عدة نسخ احتياطية للدليل من المصدر الأصلي(Barel, 2005, p. 12) .

على المحكمة أيضًا أن تتبع مراحل عملية إنتاج الدليل الإلكتروني لتقديمه، مثل التأكد من مراحل عملية النسخ باستخدام البرامج التقنية اللازمة التي توضح ما إذا تم نسخ الملف من خلال النظام أم لا (Migayron, n.d., p. 25).

في الولايات المتحدة، تخضع مسألة التأكد من مصداقية وصحة الأدلّة الرقميّة للقواعد المقررة في القاعدة رقم 901 من قواعد الإثبات الفيدرالية، والتي يتم التركيز فيها على دور المحلفين في تحديد قيمة الأدلة

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

المقدمة من الخصوم في ضوء القواعد المطبقة على الأدلة التقليدية، مع ضرورة التدقيق بشكل أكبر في مجال الأدلّة الرقميّة (Vinhee, 2005, pp. 444–445) (Hogan, n.d., p. 75).

وفي قضايا مختلفة على مستوى الولايات، مثل قضية People v. Lenstine في نيويورك وقضية Robert Eleck في كونيتيكت، يتضح اعتماد المحاكم على المعايير المطبقة بشأن الأدلة التقليدية مع مراعاة خصوصية الأدلّة الرقميّة وتحدياتها (Clevenstine, 2009, p. 511) (Hogan, n.d., p. 76) (Eleck, 2014).

الرأي الثاني: عدم خضوع مسألة التأكد من صحة وسلامة الأدلّة الرقميّة للقواعد التقليدية

يمثل هذا الرأي محكمة الاستئناف بولاية ماريلاند، التي قررت عدم خضوع مسألة التأكد من صحة وسلامة الأدلّة الرقميّة للقواعد التقليدية. في قضيةAntone Lever Griffin ، انتهت المحكمة إلى أن وسائل ومواقع التواصل الاجتماعي تحتاج إلى معايير خاصة للتأكد من سلامة وصحة الأدلة المستمدة منها نظراً لأنها عرضة للتحريف(Hogan, n.d., p. 81).

تتلخص وقائع القضية(Hogan, n.d., p. 62) في اتهام Griffin بقتل شخص يدعى Darvell في حمام سباحة عن طريق إطلاق الرصاص عليه في وقت مبكر من يوم 24 أبريل 2005. قدم المتهم للمحاكمة وطلبت شهادة شخص يدعىGibbs ، وهو شاهد عيان تواجد في مكان وقوع الجريمة وشهد بأن Griffin لم يطلق الرصاص على المجني عليه. لاحقًا، غير Gibbs شهادته وأقر برؤية المتهم وهو يرتكب الجريمة، وذكر أن إنكاره الأول كان نتيجة تلقيه تهديدًا من السيدةBarber ، صديقة المتهم، عبر موقع.MySpace

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

قدم Gibbs مستخرجًا مطبوعًا من صفحة الموقع الخاص بصديقة المتهم، وتأكدت المحكمة من صحة المستخرج المطبوع من خلال الكشف عن البيانات الخاصة بمالك الموقع. كان المستخرج يحتوي على صورة تظهر Barber وهي تحتضنGriffin ، مما دعم رواية الشاهد.

طعن المتهم أمام محكمة الاستئناف بولاية ماريلاند، مدعياً خطأ المحكمة في قبول مستخرج مطبوع من موقع صديقته. قبلت المحكمة الطعن، مستندة إلى أن مواقع التواصل الاجتماعي قابلة للتلاعب من قبل أشخاص غير الشخص الذي أنشأ الحساب، كما يمكن لأي شخص إنشاء حساب وهمي باسم شخص آخر. كما لا بد من الإشارة، إن إنشاء حساب على الإنترنت قد يكون جزءًا من جريمة إذا كان القصد منه تسهيل ارتكاب جريمة أخرى، كما يظهر في حكم الطعن رقم 8707 لسنة 2022".

التعليق على الحكم:

يرى البعض أن محكمة استئناف ماريلاند، كغيرها من المحاكم الفيدرالية ومحاكم الولايات، لا تعتمد معايير محددة للتأكد من سلامة الأدلّة الرقميّة، وأن الأمر يخضع للقواعد العامة في مجال التأكد من سلامة الدليل. بالإضافة إلى ذلك، فإن العديد من السوابق القضائية قد قبلت سجلات مكالمات الهاتف كدليل رقمي بعد التأكد من وجود مكالمة فعلية بين الجاني والمجني عليه من سجل الاتصالات في الهاتف، كما في قضية.Carpenter

من خلال هذا الحكم، يتبين أن محكمة استئناف ماريلاند تتبع نفس المعايير المتعلقة بالأدلة التقليدية في مجال الأدلّة الرقميّة. علاوة على ذلك، فإن العيب الذي استندت إليه المحكمة في حكمها، والمتمثل في أن وسائل ومواقع التواصل الاجتماعي عرضة للتحريف وأن شخصًا ما يمكن أن ينشئ حسابًا وهميًا باسم

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

شخص آخر، لا يقتصر على الأدلة المستمدة من مواقع التواصل الاجتماعي بل ينطبق أيضًا على الأدلة التقليدية والأدلّة الرقميّة الأخرى (Carpenter, 2010) (Chaney, 2007) (Hogan, n.d., p. 73).

هذا الرأي يعكس التحديات التي تواجهها المحاكم في التأكد من صحة وسلامة الأدلّة الرقميّة، ويبرز الحاجة إلى تطوير معايير وأطر قانونية جديدة تتناسب مع طبيعة الأدلّة الرقميّة وخصوصياتها.

2. سلطة القاضي الجنائي في التأكد من مصداقية الأدلّة الرقميّة

لكي يكون الدليل الإلكتروني مقبولاً أمام المحكمة، يجب أن تستوثق المحكمة من مصداقية وصحة الدليل الإلكتروني. يمكن للمحكمة أن تعتمد على أي وسيلة للتأكد من ذلك، وفي ضوء ذلك، يحق للمحكمة الاعتماد على البرامج والتقنيات الحديثة في بحث مدى سلامة وصحة الأدلّة الرقميّة المعروضة عليها، على أن يكون ذلك بالاستعانة بالخبراء التقنيين.

من أمثلة هذه البرامج، برامج Hash values التي تعتمد على نظام البصمة الرقمية (digital fingerprints). من خلال هذه البرامج، يمكن الدخول إلى القرص الصلب للحاسوب وفحص أصل الدليل الموجود عليه للتأكد من سلامته وصحته من خلال عمليات فنية ورياضية تجريها هذه البرامج (Krotoski, n.d., pp. 67–68).

هذا ما أقره القضاء الأمريكي في العديد من القضايا التي عرضت عليه، مثل قضية Finley (Finley, 2010, p. 1000)، التي اتهم فيها المتهم بحيازة صور إباحية للأطفال وتوزيعها. اكتُشفت الواقعة من خلال قاعدة بيانات للصور الإباحية للأطفال المنشورة على الإنترنت، حيث استخدمت السلطات برنامج

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

Hash value (SHA)لإثبات أن الملفات الموجودة على جهاز المتهم هي نفس الصور الإباحية المضبوطة.

في قضيةRichardson ، اتهم المتهم بحيازة وتوزيع صور إباحية للأطفال، وتأكدت المحكمة من أن الصور الإباحية المضبوطة صدرت من البريد الإلكتروني الخاص بالمتهم (Richardson, 2010, p. 363).

وفي قضيةMinish (Miknevich, 2011, p. 181)، اتهم المتهم بحيازة وتوزيع صور إباحية للأطفال، وعند تفتيش حاسوبه، ضُبط عدد كبير من صور دعارة الأطفال واعترف المتهم بجريمته شفويًا للضابط. دفع المتهم بأن أمر التفتيش صدر دون سبب أو مبرر، ورفضت المحكمة دفعه بناءً على نتائج برنامج SHA وشبكات تبادل الملفات(P2P) .

على ذات النهج، يرى الفقه الفرنسي(Migayron, n.d., p. 25) ضرورة قبول المحكمة لأي وسيلة للتأكد من نسبة الدليل الإلكتروني إلى المتهم، بما في ذلك استخدام برامج البصمة الرقمية مثلVIS ، التي تظهر الوضع التاريخي للنظام الذي تم الحصول على الدليل منه للتأكد من وجود الدليل بنفس المحتوى في حاسوب المتهم.

ومع ذلك، إذا تشككت المحكمة في صحة الدليل الإلكتروني المعروض عليها، فإنها ترفضه (Krotoski, n.d., p. 66). هذا ما قرره القضاء الأمريكي في قضيةJackson، (Jackson, 2007, p. 871) (Frieden & Murray, 2011, p. 8)

حيث رفضت المحكمة دليلًا تم تقديمه في صورة ملف Word نُقل إليه محتوى الدردشة عبر الإنترنت

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

باستخدام خاصية القص واللصق، مشيرة إلى أن هذا النوع من الأدلة يقبل التلاعب.

يجب على المحكمة التأكد من صحة الدليل الإلكتروني المأخوذ من شبكة الإنترنت، مع التركيز على التفرقة بين المواد المنشورة بموافقة صاحب الموقع والمواد التي نُشرت بدون رضاه (قرصنة الإنترنت). يجب على القاضي بذل كل المساعي للتأكد من صحة الدليل من خلال الظروف المحيطة بتقديمه، لضمان تحقيق العدالة وعدم رفض الأدلّة الرقميّة دون مبرر.

- **المطلب الثّاني: المعايير الفنية والقانونية للتحقق من سلامة الدليل الرقمي**

يتناول هذا الفرع موضوعًا حيويًا في مجال الجرائم الإلكترونية والأدلة الرقمية، حيث يركز على أسس التأكد من مصداقية الأدلة الرقمية المستمدة من المواقع والشبكات الإلكترونية. في العصر الرقمي الحالي، تزايد الاعتماد على الأدلة الرقمية في التحقيقات الجنائية والمحاكمات القضائية، وهذا يستدعي ضرورة التأكد من صحة ومصداقية هذه الأدلة لضمان تحقيق العدالة.

أولًا، يشير الفرع إلى التحديات المرتبطة بالأدلة الرقمية المستمدة من المواقع غير الحكومية وشبكات التواصل الاجتماعي. في هذه الحالة، تصبح مسألة الثقة في المصدر والدليل أكثر تعقيدًا، نظرًا لإمكانية تعديل أو تزوير المعلومات بسهولة عبر الإنترنت. لذلك، تعتمد المحاكم على قواعد صارمة لتوثيق الأدلة الرقمية، بما في ذلك التحقق من عنوان الموقع وتاريخ إنشاء الدليل ومصداقية المصدر.

ثم ينتقل الفرع إلى الحديث عن أهمّيّة شهادات الخبراء التقنيين في تقييم الأدلة الرقمية. هؤلاء الخبراء يلعبون دورًا محوريًا في تفسير وتحليل البيانات الرقمية المقدمة للمحكمة، وهو ما يظهر في قضايا متعددة

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

مثل قضيةSalcido ، حيث تم استخدام الخبرة التقنية لتحديد الأدلة التي تدعم إدانة المتهم.

كما يتناول الفرع أهمّيّة التوقيعات الإلكترونية والمصادقة على الأدلة الرقمية. التوقيعات الإلكترونية تعتبر أداة فعالة لضمان أن المحتوى الرقمي لم يتم تعديله أو تزويره، وهذا ما تم تأكيده في قضيةSafavian ، حيث تم الاعتماد على التوقيعات الإلكترونية لإثبات صحة البريد الإلكتروني.

ويختم الفرع بالتركيز على مصداقية الأدلة المستمدة من المواقع الإلكترونية الحكومية والرسمية، حيث تتمتع هذه الأدلة بحجية ذاتية وقبول واسع في المحاكم، نظرًا للثقة الكبيرة في الجهات الحكومية التي تنشر هذه البيانات.

باختصار، هذا الفرع يعكس التعقيدات التي تواجه المحاكم في التعامل مع الأدلة الرقمية ويبرز أهمّيّة وضع أسس واضحة وموثوقة لضمان مصداقية الأدلة الرقمية في تحقيق العدالة.

في هذا الموضع من الدراسة نعرض لأسس التأكد من مصداقية وصحة وسلامة الأدلّة الرقميّة المستمدة من المواقع والشبكات الإلكترونية سواء الحكومية أو غير الحكومية (Blackstone & Fox, n.d., p. 7)

1. أسس التأكد من صحة الأدلّة الرقميّة المستمدة من المواقع غير الحكومية وشبكات التواصل الإجتماعي :

يمكن لأي شخص أن يضع معلومات على المواقع غير الحكومية ومواقع التواصل الإجتماعى من خلال أي موقع وفي أي وقت، ولذلك فإن الأدلّة الرقميّة المستمدة من هذه المواقع لا يمكن اعتبارها دليلاً كافيًا، حث تظل المشكلة التي تواجه المحاكم الأمريكية في هذه الحالة أن شخصا ما هو الذي أدخل أو عدل

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

المعلومات الموجودة على هذا الموقع بخلاف المسئول عن الموقع وبدون علمه، ولذا فإن المحاكم تحتاج لقبول واعتماد الدليل الإلكتروني المستمد من هذه المواقع أن يثبت الخصم مقدم الدليل نسبة الدليل إلى المتهم(Blackstone & Fox, n.d., p. 7).

وهذا ما قررته محكمة ولاية Ohio في أحد الأحكام غير المنشورة لها، حيث قررت أن " الدليل المستمد من مواقع الويب Websites يكون مقبولاً حينما يثبت مقدم الدليل عنوان الموقع ومكان وجود الدليل وتاريخ وعنوان إنشائه وتاريخ عمل Download للدليل، كما يقدم للمحكمة ما يفيد

أن المحتوى المقدم للمحكمة هو المحتوى الموجود فعليًا على الموقع دون تغير .

وتعد من أهم القضايا التي أثيرت في هذا الصدد قضية Grifien والتي سبق وعرضنا لها، كما سبق وأشرنا أيضا إلى أن مسألة التأكد من صحة الأدلّة الرقميّة يخضع للقواعد المعمول بها في مجال الأدلة التقليدية، ففي القانون الأمريكي يلتزم الخصم بأن يقدم الأدلة الكافية ليؤكد ويدعم صحة ومصداقية أي عنصر من عناصر الإثبات وهذا ما قررته القاعدة رقم ٩٠١ من قواعد الإثبات الفدرالية، والتي تنص على أنه " يجب على المدعى أن يقدم الأدلة الكافية ليؤكد ويدعم صحة ومصداقية عنصر من عناصر الإثبات، ومن أمثلة هذه الأدلة : شهادة أحد الشهود الذي لديه معرفة بالواقعة محل الإثبات، أو شهادة شخص من غير الخبراء عن مدى صحة الكتابة المقدمة من المدعى بناءًا على معرفته بهذا الخط محل الإثبات، أو شهادة الخبراء، أو الخصائص المميزة للدليل مثل شكله الخارجي ومحتوياته وغير ذلك، أو رأى شخص في تحديد صوت شخص ما في أي آلة ميكانيكية أو إلكترونية أو أي وسيلة صوت، أو بشأن المحادثات التليفونية إثبات أن مكالمة صدرت من رقم معين في وقت ما، أو أي دليل يصف

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

العملية أو النظام الذي أنتج الدليل، أو أي طريق آخر للتوثيق يسمح به القانون الاتحادي أو المحكمة العليا (Federal Rules of Evidence, 2014, p. 23).

وفي ضوء الفقرة العاشرة من القاعدة رقم ٩٠١ السابقة فإن هذه الوسائل التي وردت على سبيل المثال حيث قررت هذه الفقرة قبول أي وسيلة للتوثيق وتأكيد الأدلة طالما أنها لا تخالف القانون الاتحادي أو أحكام المحكمة العليا.

وبالإضافة إلى ذلك فإن الأدلّة الرقميّة تساند بعضها البعض، فقد يتم الحصول على دليل رقمي ولكنه قد يكون غير كاف لإثبات الجريمة محل التحقيق، وبعد ذلك يتم الحصول على دليل اخر يساند الدليل السابق في الإثبات(Krotoski, n.d., pp. 58–59) .

- **التأكد من مصداقية وصحة الدليل الرقميّ بالاستعانة بشهادة الخبراء التقنيين :**

وهذا ما طبقه القضاء الأمريكي في قضيةSalcido (Salcido, 2007, p. 729)، وتتلخص وقائع هذه القضية أنه في فبراير ٢٠٠٥ تم العثور على مجموعة من الصور الإباحية للأطفال على أحد المواقع، وبالفعل قام المحقق بتحديد موقع هذه الصور وكذلك بروتوكول الإنترنت الخاص بصاحب الموقع وهو السيدSalcido .

وبالفعل تم استصدار إذن تفتيش لحاسوب المتهم، وبالفعل ضبط الخبير التقني على حاسوب المتهم مجموعة من الصور لدعارة الأطفال وتم ذلك من خلال قيام الخبير باستخدام خاصية البحث عن ملفات يكون امتدادهاJ baby ، وكذلك تم ضبط فيديوهات جنسية للأطفال.

وعلى ذلك اتهمت المحكمة المتهم بحيازة وتوزيع مواد إباحية تشتمل على استغلال جنسي للقاصرين، وتم

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

عرض الصور والفيديوهات على المحلفين واستوثقوا منها وحكمت المحكمة بالإدانة وقررت أن الصور والفيديوهات التي تم تحصيلها بإجراءات سليمة تم التأكد من صحتها ونسبتها للمتهم في ضوء القاعدة رقم ٩٠١ من قواعد الإثبات الفيدرالية، ومن خلال شهادة الخبير التقني.

وفي ذات الاتجاه تجد قضيةShear،(Shea, 2007, p. 1110) (Krotoski, n.d., p. 59) والتي أتهم فيها السيدShea بالتلاعب في قاعد البيانات الخاصة بالشركة التي يعمل بها، وأثبتت السجلات الإلكترونية التي تم الحصول عليها من حاسوب المتهم ذلك.غير أن الدفاع شكك في نزاهة هذه السجلات حيث قام المتهم بإحداث تغيير في تاريخ المعاملات التي قام بها من خلال حاسوبه، فقررت المحكمة فحص شبكة الشركة نفسها بمعرفة الخبراء الفنيين، وأكدوا صحة التهم الموجهة إلى المتهم وأن التغير الذي أحدثه Shea في تاريخ المعاملات التي تمت من حاسوبه كان تغيرا ماديًا فحسب كما يجوز للقاضي أصلاً قبول الأدلّة الرقميّة المقدمة إليه من الخبير باعتباره شخصا عاديا طالما أنه اعتمد في حصوله على الدليل على برامج حاسوبية متاحة للمستخدمين العاديين(Krotoski, n.d., p. 61)، وهذا ما طبقه القضاءالأمريكي في قضيةGanier. (Krotoski, n.d., p. 61) حيث رفضت المحكمة دفع المتهم باستبعاد تقرير أو شهادة الخبير لأنه لم تلتزم المحكمة بإخباره بتقرير رسمي يبين شهادة الخبير وأسبابها ومن ثم تكون قد خالفت المادة رقم ١٦ A/1/Gمن قواعد الإثبات الفيدرالية في الإجراءات الجنائية، وأخذت برأي وشهادة السيد Drueck بصفته شاهدا عاديا وليس خبيرًا لأنه استخدم برامج البحث العادية المتاحة تجاريًا لكل المستخدمين.

التأكد من مصداقية وصحة الدليل الرقمي من خلال التوقيعات الإلكترونية المرفقة بالدليل :

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

وهذا ما طبقه القضاء الأمريكي في قضية Safavian (Safavian, 2006, p. 36) (Newman & Ellis, 2011)، وتتلخص وقائع القضية في أن المتهم Safavian يعمل موظفا حكوميا وضبطت لدية مجموعة من رسائل البريد الإلكتروني E-mails والتي تثبت صلته بإحدى جماعات الضغط ضد الحكومة وتم تقديم هذه الرسائل للمحكمة واقتنعت المحكمة بصحة هذه الرسائل من خلال مضمونها والتوقيعات المرفقة بها وكذلك أنه تم ضبطها في حالة توضح مرسلها ومستلمها.

التأكد من مصداقية الدليل الرقميّ بالاستعانة بشهادة الشهود:

وهذا ما طبقه لقضاء الأمريكي في قضيةBarlow ، حيث أدانت هيئة المحلفين المتهم بأنه انتهك القانون وحاول إقناع وإغراء فتاة في الانخراط معه في علاقة جنسية، وكذلك أرسل صورا مخلة بالآداب لقاصر(Barlow, 2009, p. 220) (Frieden & Murray, 2011, p. 10).

وتتلخص وقائع القضية أنه في أغسطس عام ٢٠٠٦ قام بارلو البالغ من العمر ٣٩ عاما بإجراء محادثات عبر البريد الإلكتروني مع فتاة تدعى Rebecca. وكان عمرها حوالي ١٤ عامًا واستمرت هذه المحادثات بشكل متقطع، وبدأ المتهم في إرسال صور جنسية لها محاولاً إقناعها بإقامة علاقة جنسية معها وطلب منها إرسال صورة جنسية لها. وافقت المجني عليها بالفعل على الاجتماع مع المتهم، وبالفعل تم تحديد الموعد في الحدائق البعيدة، ووصل المتهم قبل الميعاد فوجد شخصا بالغا فقرر الانسحاب حتى لا يتم ضبطه. إلا أن السلطات ضبطت جهاز الحاسوب الخاص بالمتهم ووجدت به الدردشة والرسائل والصور التي تربط بينه وبين Rebecca .

دافع المتهم عن نفسه بأن السلطات لم تستطع إثبات أنه حاول إقناع الضحية بإقامة علاقة جنسية معه

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

وهو يعلم أنها قاصرة، كما دفع بأنه يجب على السلطات أن تثبت أنه استخدم إحدى الوسائل التي تستخدم في الاتصال والتجارة بين الولايات.

رفضت المحكمة دفع المتهم على أساس أن استخدام البريد الإلكتروني يعد إحدى وسائل التواصل والتجارة بين الولايات، كما أن محتوى الرسائل التي جرت بين المتهم والمجني عليها تؤكد رغبة المتهم في إقامة علاقة جنسية معها، كما أنه أرسل إليها صورا جنسية بالمخالفة للقانون.

وعلاوة على ذلك تأكدت المحكمة من صحة هذا الدليل من خلال شاهد إنجليزي كان يجرى محادثات عبر البريد الإلكتروني معRebecca واستطاع أن يطلع على مضمون رسائل Barlow من خلال البريد الخاص بصديقته. وعلى ذلك فإن المحكمة قبلت البريد الإلكتروني بعد أن استوثقت منه من خلال شهادة صديق المجني عليها، كما أن ضبط الرسائل كان عن طريق عمل نسخة طبق الأصل منها وليس من خلال خاصية القص واللصق.

وفي ذات الاتجاه نجد قضيةSiddiqui (Siddiqui, 2000, pp. 1321–1323)، وتتلخص وقائع القضية في أن المتهم مواطن هندي يعمل في جامعة Alabama تقدم من خلال ال E–mail للحصول على منحة علمية من الولايات المتحدة الأمريكية مدعما طلبه بتوصيات أو ترشيحا من علماء في اليابان وسويسرا، واكتشفت السلطات في الولايات المتحدة أنها مزورة.

ولذا تم توجيه الاتهام إليه بالاحتيال على إحدى المؤسسات الفيدرالية وأدانته المحكمة استنادًا إلى الـ Emailالمزيف الذي قدمه المتهم، وقد دعمت المحكمة قبولها لهذا الدليل الرقميّ طبقا للقاعدة الفيدرالية رقم ٩٠١ من قواعد الإثبات الفيدرالية بدليل آخر، وهذا الدليل هو شهادة العالم Yamada من اليابان

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

والعالم Gunten من سويسرا بعدم الموافقة على إصدار تزكيات للباحثSiddiqui .

دفع المتهم طاعنا في قبول رسائل الـ E-mail كدليل رقمي ضـده دون أن يكون هناك ما يؤكد صحة التهم الموجهة إليه، رفضت المحكمة الدفع المقدم منه استنادًا إلى أنه تم التأكد من أن البريد الإلكتروني الذي أرسله المتهم إلى " المؤسسة الوطنية للعلوم NSF للحصول على منحة بحثية تؤهل للحصول على جائزة قيمتها 500000 دولار أمريكي قد صدر من المتهم Siddiqui ومن خلال جامعة Alabama التي يعمل بها المتهم بالإضافة إلى شهادة Gunten-Yamada بعدم صحة التزكيات التي قدمها المتهم بأسمائهم.

التأكد من مصداقية وصحة الدليل الرقمي من خلال شهادة أو أقوال المجني عليه:

وهذا ما تم تطبيقه في قضية Williams (Williams, 2008, p. 254) ، وتتلخص وقائع القضية في أن المجني عليها Jennie التقت بالمتهم لأول مرة في صيف عام 2005 في كنيسة Baptist وكان يعمل بوزارة رعاية الطفولةChildren's ministry وكان عمره فى هذا الوقت 27 عامًا وكان عمر المجني عليها 13عاما، وبدأ التواصل بينهما عبر وسائل البريد الإلكتروني والهاتف النقال.

2. التأكد من صحة ومصداقية الأدلّة الرقميّة المستمدة من المواقع الالكترونية الحكومية والرسمية

من الملاحظ أن المحاكم في الولايات المتحدة الأمريكية لديها استعداد أكبر القبول الأدلّة الرقميّة المستمدة من المواقع الحكومية والرسمية، ومرد ذلك إلى أن الفقرة الخامسة من القاعدة رقم ٩٠٢ من قواعد الاثبات الفيدرالية تقرر أن الأدلة المستمدة من السجلات والوثائق الحكومية مقبولة بذاتها وتتمتع بحجية كاملة أمام القضاء دون الحاجة لأدلة أخرى تصدق عليها أو تؤكدها فهي أدلة مؤكدة بنفسها self

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

authentication، طالما أنها استوفت الشروط الواردة في القاعدة الفيدرالية رقم 803/8.

(Joseph, 2012, p. 19) (Frieden & Murray, 2011) (Federal Rules of Evidence, 2014, p. 24) (Scurmont LLC, 2011)

وفي ظل هذه القاعدة فإن الأدلّة الرقميّة المستمدة من المواقع الالكترونية الحكومية تعد مقبولة بذاتها، وهذا ما أكد عليه القضاء الأمريكي في العديد من أحكامه.

ففي قضية Scurmont LLC v. Firehouse Restaurant Grp قررت المحكمة أن "السجلات المأخوذة من مواقع حكومية تعتبر مقبولـة بشكل عام، حيث أنها مؤكدة بذاتها (Blackstone & Fox, n.d., p. 5) (Shea, 2005, pp. 104–105) وكذلك ما قررته المحكمة في قضيةWeingartner Lumber & Supply Co. v. Kadant Composites, LLCحيث قررت المحكمة أن المستخرج المطبوع من السجلات الرسمية من موقع هيئة البورصة والأوراق المالية يعتبر مؤكد بذاته (Weingartner Lumber, 2010) ، وفي قضية أخرى Williams. Long قررت المحكمة أن " المنشورات المأخوذة من مواقع الويب الحكومية لها حجية بطبيعتها ومؤكدة بذلك (Williams, 2008, pp. 686–688).

ويندرج ضمن هذه الطائفة من الأدلّة الرقميّة المستمدة من المواقع الرسمية للصحف والمقالات المنشورة عليها، وهذا ما قررته الفقرة السادسة من القاعدة الفيدرالية 902/6 من قواعد الإثبات الفيدرالية وهذا ما قرره القضاء الأمريكي في أحد القضايا بأن "الموقع الالكتروني لوزير الدولة يعتبر من الأدلة التي تتمتع بحجية بذاتها باعتبارها من السجلات الحكومية الرسمية، كما أن نسخ المواد التي تعتبر من قبيل المقالات

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية

العدد الرابع والثمانين شهر (مايو) 2025

ISSN: 2617-9563

الصحفية تعتبر كذلك.(Tippie, 2008)

ونشير إلى أن القاعدة رقم ٩٠٢/٦ من قواعد الإثبات الفيدرالية والتي قررت تمتع مقالات الصحف المنشورة على المواقع الرسمية للصحف.

المبحث الثّاني: العلاقة بين الدليل الرقمي ونظام الإثبات في القانون الجنائي

يواجه الفقه والقضاء الجنائيين تحديات كبيرة في التعامل مع الأدلة الرقمية نظراً لإمكانية تعرضها للتزييف والتحريف، مما يثير الشكوك حول مشروعيتها وصحتها. يهدف نظام الإثبات الجنائي إلى حماية حقوق الأفراد وضمان عدم تعسف السلطة في جمع الأدلة، مما يتطلب وضع معايير دقيقة لقبول الأدلة الرقمية. تختلف طريقة الاعتراف بالدليل الرقمي في الإثبات من دولة لأخرى، حيث يتبع بعضها نظام الأدلة القانونية المقيدة، بينما يتبع البعض الآخر نظام حرية الإثبات.

في الدول التي تتبع نظام الأدلة القانونية، يحدد المشرع الأدلة المقبولة وشروط قبولها، مما يحد من دور القاضي في تقدير الدليل. في المقابل، يعتمد نظام حرية الإثبات على قناعة القاضي الذاتية، حيث يمكنه قبول أي دليل طالما توافرت الشروط القانونية المطلوبة. يعتبر الدليل الرقمي في هذا النظام جزءًا من الأدلة المقبولة، شريطة أن يكون قد تم الحصول عليه بطرق مشروعة ووفق الأصول القانونية.

تكمن أهمّيّة الدليل الرقمي في قدرته على تقديم معلومات دقيقة وموثوقة حول الجرائم المعلوماتيّة، مثل تاريخ استخدام الأجهزة وتحديد المواقع. يعتمد القاضي في تقدير حجية الدليل الرقمي على مدى يقينيته وعدم قابليته للشك، مع التركيز على التحقق من سلامة الدليل وصحته من خلال الخبراء التقنيين.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

إذًا يعد الدليل الرقمي المتحصل عن التفتيش المعلوماتيّ أداة فعالة في النظام القضائي الحديث، بشرط أن يتم جمعه وتحليله وفقًا للمعايير القانونية والتقنية الدقيقة. يتطلب ذلك تضافر الجهود بين القانونيين والتقنيين لضمان تحقيق العدالة وحماية حقوق الأفراد في البيئة الرقمية المتزايدة التعقيد. وهذا ما سنناقشه في هذا المبحث.

المطلب الأوّل: الدليل الرقمي واتصاله بنظام الإثبات الجنائي

يبدي الفقه والقضاء الجنائيين عادة قلقا كبيرًا حيال الإثبات واستخدام الأدلة الرقمية خشية عدم تعبيرها من الحقيقة بالنظر لكم التزييف والتحريف الذي يمكن أن يقع على هذا النوع من الأدلة الأمر الذي يطعن في مشروعية الدليل كشرط أساسي المقبوليته في الإثبات وفق الأصول العامة (مهدي، 2020، ص 1671 وما بعدها).

ولا تتفلت الأدلة الرقمية من غطاء المشروعية كباقي الأدلة، بغية تقرير ضمانة أساسية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة (هلالي، 1997، ص 104). وتتسع وتضيق سلطة القاضي في قبول الدليل في الإثبات بحسب النظام الذي ينتمي إليه القاضي، هل يتبع نظام الأدلة القانونية، أم نظام حرية الإثبات(Merle & Vitu, 1979, no. 925) .

وعليه تختلف طريقة الاعتراف بالدليل الرقمي في الإثبات من دولة لأخرى بحسب طبيعة نظام الإثبات السائد فيها (رياض، 1997، ص 85) (حسين، 2011، ص 81)، ففي نظام الإثبات المقيد يحدد المشرع الأدلة المقبولة ويحدد شروط قبولها وقوتها الإقناعية، فليس للقاضي من دور في تقدير الدليل سوى مجرد التحقق من الشروط التي تطلبها المشرع(هلالي، 1997، ص 91)، وهو الأمر الذي يفقد

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

القاضي عمله الرئيس وهو الحكم بناءً على الاقتناع وفقا لضميره، وهو ما تسبب في تراجع العمل به حتى في دولته المؤسسة له – أي بريطانيا – واصبح للقاضي أي يستخلص الحقيقة من أي دليل ولو لم يكن منصوصا عليه قانونا وفق قاعدة الإدانة دون أدنى شك، وهو ما اتبعه كذلك القضاء الأمريكي وفق قاعدة الدليل الأفضل(Stephen et al., 1992, p. 33) التي تعطي للقاضي سلطة تقديرية في قبول نسخ أو صور الدليل الأصلي في حالة عدم توافر هذا الأخير (أي الدليل الأصلي) أو فقدانه.

وهكذا ساد وتوسع – لاسيما في جل التشريعات الأوروبية والعربية – نظام الاثبات الحر، القائم على ألا يحدد المشرع طرقاً معينة للإثبات ولا حجيتها أمام القضاء، إنما يترك ذلك للقاضي الجنائي، صاحب الدور الإيجابي في البحث عن الأدلة المناسبة وتقدير قيمتها الثبوتية حسب قناعته الذاتية (عفيفي، 2003، ص ص 373–379)، ويقتصر دور المشرع على بيان الشروط القانونية المتطلبة في الدليل، منعا للشطط في قبول الأدلة (الطحطاوي، 2015، ص 93)، مع الأخذ أحيانًا وفي نطاق محدود بنظام الأدلة القانونية، ليصير النظام نظامًا مختلطاً في الإثبات الجنائي، وهو وضع القانون المصري والياباني والشيلي (براهيمي، 2018، ص 143 وما بعدها).

وهكذا لم يعد يقيد قبول الأدلة الرقمية في الإثبات الجنائي سوى أن تكون حصلت بطرق مشروعة وفق الأصول القانونية(Demarchi, 2007, p. 2012) ، مع خضوع الدليل لمبدأ الاقتناع الذاتي للقاضي الجنائي.

وعليه، لا يجوز للقاضي قبول دليل رقمي دون مراعاة الشروط الشكلية والموضوعية للإذن بالتفتيش المعلوماتيّ مثلاً، أو كان قد تحصل بإكراه المتهم المعلوماتيّ على فك شفرة أو الإفصاح عن كلمة السر

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

اللازمة للدخول إلى الملفات المخزنة داخل النظم المعلوماتيّة، أو القيام بإجراء التصنت أو المراقبة الإلكترونية عن بعد دون مسوغ قانوني (الطوالبة، 2009، ص 4).

المطلب الثّاني: سلطة القاضي في تقدير الأدلة الرقمية وحدود قبولها القضائي

يثار التساؤل حول القوة التدليلية للدليل الرقمي في الدعاوى الجنائية، أي ما قوته في كشف الحقيقة، ومدى صدقيته على نسبة الفعل للمتهم (أبو حطب، 2014، ص 303).

مسألة موضوعية محضة تدخل في صميم سلطة القاضي التقديرية ومسألة تقييم الدليل هي بحثا عن الحقيقة والسائد بالنسبة للأدلة التقليدية من اعتراف أو شهادة شهود أو قرائن...الخ أن سلطة القاضي الجنائي في تقدير الدليل يحكمها مبدأ حرية القاضي في تكوين عقيدته، فهل ينطبق ذلك على الدليل الرقمي؟ (الصغير، 2001، ص13).

من المؤكد والمشاهد هو ضعف القاضي الجنائي من حيث الكفاءة الفنية والمعرفة في المجال المعلوماتيّ، لاسيما وأنه مجال تتطور فيه التقنية بشكل متسارع، وأمام ذلك يتعذر على القاضي الجنائي إدراك الحقائق المتعلقة بأصالة الدليل الرقميّ، فضلا عن تمتع هذا الدليل في قوته التدليلية بقيمة في الإثبات قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، إلى جانب الطبيعة الفنية الخاصة بالدليل الرقمي والتي تمكن من العبث بمضمونه بسهولة على نحو يقبل تغيير حقيقته، دون أن يدرك ذلك سوى ذوي الخبرة الفنية. فالدليل الرقمي يخضع لذات القواعد التي تطبق على الأدلة العلمية بشأن الفحص والدراسة والتوصل إلى مدى مشروعيته، وذلك بالشكل الذي لا يتعارض مع القواعد الأساسية في الإثبات العلمي (الشاهد وعبد الحميد، 2022، ص 24).

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

وهنا يطرح التساؤل، ما سلطة القاضي الجنائي تجاه الدليل الرقمي؟، وهل له من دور في تقدير صدقيته وقياس قوته التدليلية؟، وهل له حق رفضه بحكم عدم قناعته به ؟ (هلالي، 1997، ص 135 وما بعدها).

إن الإجابة على هذا التساؤل يوجب على القاضي في البدء التيقن من توافر الشروط التي تمنح باجتماعها الدليل الرقمي حجية في الإثبات الجنائي، وأهمها على الإطلاق شرط اليقينية.

إذ يلزم أن يتحقق القاضي المطروح أمامه الدليل الرقمي من أنه غير قابل للشك وليس دليلا مرجوحا عندما يتجه إلى هدم مبدأ أصل البراءة، فهذا الأخير لا يهدمه إلا إدانة جازمة مبنية على أدلة لا يتسرب إليها الظن والاحتمال.

والمبدأ إذا هو افتراض أصالة الدليل الرقمي ومن ثم القناعة اليقينية به، تلك القناعة المدركة بالحواس وفق التصورات الإنسانية والخبرة التي تتشكل في وجدان وعقل القاضي عبر سنوات عمله بالمحاكم المختلفة، وهو الأمر المعتمد في القضاء الأمريكي وفقا لقانون الحاسب الآلى لولاية أيوا الصادر في عام 1984 وقانون الإثبات لولاية كاليفورنيا لعام في 1983، حيث تعتبر النسخ المستخرجة من البيانات التي يحتويها الحاسب من أفضل الأدلة المتاحة للإثبات وأكثرها يقينية (أبو حطب، 2014، ص 305). وعليه أكدت المحكمة العليا الأمريكية في قضية United States v. Russo في عام 1974 حينما قضت أنه مع افتراض استخدام حاسب يؤدي وظائفه بشكل سليم، ومع توافر الثقة فيه وإمكانية التعويل عليه، فان مخرجاته يجب أن تكون مقبولة كدليل على المعاملات التي أدخلت فيه (رستم، 1994، ص 182).

كذلك نص قانون الإثبات الأمريكي في المادة 1001/3 على أنه إذا كانت البيانات مخزنة في حاسب أو

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

آلة مشابهة فان أية مخرجات طابعة منها أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية. وتضيف المادة 1500/5 من قانون الإثبات لولاية كاليفورنيا لعام 1983 بأن المعلومات المسجلة بواسطة الحاسب أو برامج الحاسب، أو نسخ أيهما، يجب ألا توصف أو تعامل على أنها غير مقبولة بمقتضى قاعدة فضل دليل (حسن، 1999، ص 1).

وعلى ذات المنوال سار المشرع ين الإنجليزي والياباني بقبولهما ضمن أدلة الإثبات مخرجات الحاسب الآلي التي تم تحويلها إلى صور مرئية، سواء أكانت هي الأصل أم كانت نسخا مستخرجة عن هذا الأصل(Amory & Pouliet, 1985, p. 339) . أما المشرع الألماني فقد جعل من خلال المادة (224) فقرة ثانية من قانون الإجراءات الجنائية مخرجات الحاسب الآلي بأنواعها المختلفة من بيانات أو مطبوعات أو نسخ من قبيل المصادر التي يجب على المحكمة تقبلها في الإثبات وهو الشيء نفسه الذي تبناه المشرع اليوناني في المادة 364 من قانون الإجراءات الجنائية.

ولا يعود هذا القبول للدليل الرقمي والإقرار بحجيته إلا للتسليم بمنطق افتراض الأصالة في الدليل الرقمي، والناشئة عن الطابع العلمي لهذا النوع من الأدلة، والذي يبقيه في مكانه الذي تم استخلاصه منه رغم حذفه من النظام المعلوماتيّ بالحاسب الآلي أو شبكة المعلومات.

وللقاضي المزود ببعض المعارف التقنية أن يلجأ إلى استخدام عدة وسائل للتحقق من سلامة الدليل الرقمي وعدم تغييره أو تحريف، ومن ثم النيل من أصالته ويقينيته، منها(Ammar, 1993, p. 499):

- تقنية التحليل التناظري الرقمي وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم الحكم على النسخ المستخرجة.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

- استخدام عمليات حسابية خاصة تسمى بالخوارزميات ويتم اللجوء إلى هذه العملية عادة في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي أو في حالة ما إذا كان هناك شك في أن العبث قد من النسخة الأصلية.
- – استخدام الدليل المحايد: وهو نوع من الأدلة الرقمية المخزنة في البيئة الافتراضية ولا علاقة له بموضوع الجريمة، ولكنه يساهم في التحقق من مدى سلامة الدليل وعدم تحريفه.
- – إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لعدة تجارب بغية التأكد من أنها عرضت كل المعطيات المتعلقة بالدليل الرقمي وأنها لم تضف إليه نتائج جديدة.

على أنه من المهم التأكيد على أن يقينية الدليل الرقمي وخضوعه لما يخضع له الدليل العلمي لا تعني عدم قابلية سلامته عند التحصل عليه للخطأ، ومثال ذلك الخطأ في استخدام الأداة المناسبة لاستخلاص الدليل، كالخلل في الشفرة المستخدمة، أو استعمال معلومات ومواصفات خاطئة. وإما بسبب الخطأ في استخدام أداة تقل نسبة صوابها 100%، مثل ما يحدث غالبا في وسائل اختزال المعطيات أو معالجتها بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها بها.

ولهذا تنص المادة 69 من قانون الشرطة والإثبات الجنائي البريطاني على أنه لا يكون البيان المتضمن في مستند صادر عن طريق الحاسب مقبولا كدليل على أية واقعة واردة فيه إلا إذا تبين:

1– عدم وجود أسس معقولة الاعتقاد بأن البيان يفتقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسب؛

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

2- أن الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فأي جزء لم يكن يعمل فيه بصورة سليمة أو كان معطلا عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته .(Ammar, 1993, p. 500) (Casile, 2004, p. 76)

أما عن القانون المصري بشأن مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 فقد مال إلى هذا التوجه حين نص في المادة الحادية عشرة من القانون المعنونة "في الأدلة الرقمية هذه الحجية حين أكدت على أنه يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإليكترونية، أو النظام المعلوماتيّ أو من برامج الحاسب أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الاثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية.

ولكن لم يجب على المشرع المصري على تساؤلنا حول سلطة القاضي الجنائي تجاه الأدلة الرقمية، هل تخضع لما تخضع له الأدلة الجنائية المادية من حيث مبدأ حرية القاضي الجنائي في تكوين عقيديته؟

إن الإجابة على هذا التساؤل نراها ترتبط بالطابع العلمي للدليل الرقمي ؛ فهذا الطابع يجب أن يلعب دورا حاسما في الحد من حرية القاضي الجنائي في تكوين عقيدته، فقد أصبح هذا النوع من الأدلة جزءاً من نتاج العلم الموثوق في نظرياته ونتائجه، وهو ما يحتم على القاضي الجنائي قبوله والإقرار بحجته في الإثبات رغم عدم إلمامه بمعارف تقنية المعلومات، دون إعمال للمفاهيم التقليدية لنظامي حرية الإثبات والإثبات المختلط، وهو ما استقر في التطبيق القضائي في أغلب الدولة العملاقة في مجال تقنية المعلومات كأمريكا وبريطانيا وكندا (هلالي، 1997، ص 93)، وليصبح المعتمد بشأن الدليل الرقمي هو مبدأ الإثبات القانوني المقيد، كحالة جديدة من الحالات المقرة في التشريح المصري، بمقتضاها لا يجب

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية
العدد الرابع والثمانين شهر (مايو) 2025
ISSN: 2617-9563

أن ينازع القاضي في قيمة ما يتمتع به الدليل الرقمي من قوة تدليلية تأكدت بقوة العلم طالعة توافرت في الدليل الشروط التي يتطلبها القانون لتحصيله وكان مشروعا (بوكر، 2012، ص 507).

الخاتمة

أدى التطور التكنولوجي المتسارع إلى بروز الدليل الرقمي كأحد الركائز الجوهرية في مجال الإثبات الجنائي، لا سيما في الجرائم التي تُرتكب عبر الفضاء السيبراني أو من خلال الأدوات التقنية الحديثة. وقد كشفت هذه الدراسة عن أن التعامل مع هذا النوع من الأدلة لا يقتصر على البُعد الفني أو التقني فحسب، بل يتطلب كذلك معالجة قانونية دقيقة توازن بين حماية الحقوق والحريات وضمان فعالية العدالة الجنائية.

لقد تبين أن مشروعية الدليل الرقمي تُعدّ أساسًا لقبوله، إذ لا يمكن الاعتماد عليه في بناء الحكم القضائي ما لم يكن قد تم تحصيله وفقًا للإجراءات القانونية المشروعة، سواء من حيث الترخيص بالتفتيش المعلوماتي أو من حيث احترام المبادئ الدستورية كحرمة الحياة الخاصة. كما أن حجية هذا الدليل ترتبط ارتباطًا وثيقًا بمدى التأكد من سلامته التقنية ومصداقيته وعدم تعرضه للتزوير أو التحريف، وهو ما يستدعي تفعيل دور الخبراء الرقميين وتدريب القضاة والضباط على قراءة وتحليل هذه الأدلة.

كذلك كشفت الدراسة عن تباين مواقف النظم القانونية في التعامل مع الأدلة الرقمية، بين من يُخضعها للقواعد التقليدية في الإثبات، ومن يرى ضرورة تطوير قواعد خاصة بها نظرًا لخصوصيتها وتعقيداتها. ويبدو أن الخيار الأنسب هو اعتماد نهج وسط يجمع بين المبادئ القانونية الراسخة والمعايير التقنية

الحديثة.

بناءً عليه، توصي الدراسة بضرورة:

1. تحديث التشريعات الوطنية لمواكبة تحديات الإثبات الرقمي.
2. اعتماد معايير فنية وقضائية موحدة لضمان سلامة الدليل الرقمي ومصداقيته.
3. تعزيز التعاون بين الجهات القضائية والتقنية لضمان تكامل الجهود في إثبات الجرائم المعلوماتية.
4. تدريب القضاة وأعضاء النيابة العامة على فهم خصائص الأدلة الرقمية وتقييمها علميًا وقانونيًا.

إن المستقبل العدلي لا يمكن أن يتجاهل الواقع الرقمي، وبالتالي فإن العدالة الجنائية مطالبة بالانفتاح على التكنولوجيا الحديثة دون التفريط في الضمانات الأساسية التي يقوم عليها نظام العدالة.

المجلة الالكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية

العدد الرابع والثمانين شهر (مايو) 2025

ISSN: 2617-9563

المصادر والمراجع

أولًا: الكتب

أبو حطب، ي. م. الكومي .(2014) .*الحماية الجنائية و الأمنية للتوقيع الإلكتروني: دراسة مقارنة* . الإسكندرية: منشأة المعارف.

بلال، أ. ع .(1994–1993) .*قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة* .القاهرة: دار النهضة العربية.

بوكر، ر .(2012) .*جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن* .بيروت: منشورات الحلبي الحقوقية.

حسن، س. ع .(1999) .*إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت: الجرائم الواقعة في جمال تكنولوجيا المعلومات* (ط.1). دار النهضة العربية.

حسين، س. ج. ف .(2011) .*الأدلة المتحصلة من الحاسب وحُجيتها في الإثبات* .القاهرة: دار الكتب القانونية.

حسين، س. ج. ف .(2011) .*التفتيش في الجرائم المعلوماتية* .القاهرة: دار الكتب القانونية.

رستم، هـ. م. ف .(1994) .*الجوانب الإجرائية للجرائم المعلوماتية* .القاهرة: مكتبة الآلات الحديثة.

رياض، ر. ع .(1997) .*مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها: دراسة تحليلية تأصيلية مقارنة* .القاهرة: دار النهضة العربية.

رياض، ر. ع .(2004) .*سلطة القاضي الجنائي في تقدير الأدلة* .القاهرة: دار النهضة العربية.

الشاهد، أ. ج. م.، &عبد الحميد، م. ج .(2022) .*حجية الدليل الإلكتروني في الإثبات الجنائي* . القاهرة: دار النهضة العربية.

الصغير، ج. ع .(2001) .*أدلة الإثبات الجنائي والتكنولوجيا الحديثة* .القاهرة: دار النهضة العربية.

الطحطاوي، أ. ي .(2015) .*الأدلة الإلكترونية ودورها في الإثبات الجنائي: دراسة مقارنة* .القاهرة: دار النهضة العربية.

عفيفي، ع. ك .(2003) .*جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون* . بيروت: منشورات الحلبي الحقوقية.

فرج، أ. ي .(2008) .*الجرائم المعلوماتيّة على شبكة الإنترنت* (ط.1). دار المطبوعات الجامعية.

قنديل، أ. ع .(2018) .*الوسائل الإلكترونية ودورها في الإثبات الجنائي: دراسة مقارنة* .الإسكندرية: دار الجامعة الجديدة.

مهدي، ع. ر .(2020) .*شرح القواعد العامة لقانون العقوبات* .القاهرة: دار النهضة العربية.

هلالي، ع. أ .(1997) .*حجية المخرجات الكمبيوترية في المواد الجنائية: دراسة مقارنة* .القاهرة: دار النهضة العربية.

ثانيًا: رسائل جامعية

براهيمي، ج .(2018) .*التحقيق الجنائي في الجرائم الإلكترونية* (رسالة دكتوراه، جامعة مولود معمري، تيزي وزو).

خليل، أ. ض .(1982) .*مشروعية الدليل في المواد الجنائية* (رسالة دكتوراه، جامعة عين شمس).

ثالثًا: مقالات في دوريات ومجلات علمية

المنشاوي، م. أ .(2012) .*سلطة القاضي الجنائي في تقديم الدليل الإلكتروني* .*مجلة الحقوق*، الكويت، عدد 2، ص 552 وما بعدها.

رابعًا: أبحاث مؤتمرات وأوراق علمية

إسماعيل، ع. ش .(2000) .*أمن المعلومات في الإنترنت* [بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت]. كلية الشريعة والقانون، الإمارات.

عبد المطلب، م. ع.، جاسم، ز. م.، &عبد العزيز، ع .(2003) .*نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم غير الكمبيوتر* .مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، دبي، 10–12 مايو، ص 2246–2247.

الطوالبة، ع. ح .(2009) .*مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي* .منشور على الرابط:...www.policemc.gov.bh/reports/2009/

المصادر الأجنبية والإنترنت:

Ammar, D. (1993). *Preuve et vraisemblance: Contribution à l'étude de la preuve technologique*. Revue Trimestrielle de Droit Civil (RTD Civ.),

juillet–septembre, 499–500.

Amory, B., & Pouliet, Y. (1985). *Le droit de la preuve face à l'informatique et la télématique*. Revue Internationale de Droit Comparé (RIDC), (Avril), 339.

Antoine Levar Griffin v. State of Maryland, No. 74 (Md. 2010). Retrieved from http://www.courts.state.md.us/opinions/coa/2011/74a10.pdf

Barel, M. (2005). *Fraude informatique et preuve*. Actes du Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC). Retrieved from http://sondage.sstic.org/SSTIC05/Delits_informatiques_et_preuve/SSTIC05-article-Barel

Blackstone, R., & Fox, S. E. (n.d.). *Hearsay Rule* (op. cit., p. 5).

Blackstone, R., Fox, S. E., et al. (2008). *ESI meets the hearsay rule*. In Workplace Data Law (BNA), Employment Rights and Responsibilities, Mid-Winter Meeting.

Blackstone, R., Fox, S. E., et al. (2008). *ESI meets the hearsay rule*. Draft of Chapter 14, Workplace Data Law, American Bar Association, Employment Rights and Responsibilities.

Carpenter v. State, 196 Md. App. 212, 9 A.3d 99 (2010).

Casile, J.-F. (2004). *Plaidoyer en faveur d'aménagement de la preuve de l'infraction informatique*. Revue de Science Criminelle (RSC), 76.

Chaney v. Family Dollar Store of Maryland, No. 24-C-06-11462, 2007 WL 5997994 (Md. Cir. Ct. Dec. 26, 2007).

Cole, D. (1993). *The emerging structures of criminal information law: Tracing the contour of a new paradigm*. Report presented to Association internationale de droit pénale, Revue internationale de droit pénale, 1993, 114.

Demarchi, J.-R. (2007). *La loyauté de la preuve en procédure pénale, outil transnational de protection du justiciable*. Recueil Dalloz, p. 2012.

Erman, S. (1993). *Les crimes informatiques et autres crimes dans le domaine de la technologie informatique en Turquie*. Revue internationale de droit pénale, 624.

Federal Rules of Evidence. (2014). *Federal Rules of Evidence (as amended to December 1, 2014)*. U.S. Government Printing Office. Retrieved from https://www.uscourts.gov/file/rules-evidence

Federal Rules of Evidence. (2014). *Rules of evidence as amended to December 1, 2014*. U.S. Government Printing Office. Retrieved from

https://www.uscourts.gov/file/rules-evidence

Frieden, J. D., & Murray, L. M. (2011). *The admissibility of electronic evidence under the Federal Rules of Evidence*. Richmond Journal of Law and Technology, 17(2), 8. Retrieved from https://jolt.richmond.edu/v1712/article5.pdf

Frieden, J. D., & Murray, L. M. (2011). *The admissibility of electronic evidence under the Federal Rules of Evidence*. Richmond Journal of Law and Technology, 17(2), 10. Retrieved from https://jolt.richmond.edu/v17i2/article5.pdf

Hogan, B. W. (2010). *Griffin v. State: Setting the bar too high for authenticating social media evidence*. (Multiple citations: pp. 62, 73, 75, 76, 78, 81).

Jarrett, H. M., & Judish, N. (n.d.). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*.

Joseph, G. P. (2012, February). *Internet and email evidence (Part 1): The facts may be new, but the rules are familiar*. The Practical Lawyer, 19. Retrieved from http://files.alicle.org/thumbs/datastorage/lacidoirep/articles/TPL1112_Joseph_thumb.pdf

Kemp, L. (2007). *An authoritative opinion sets the bar for admissibility of electronic evidence*. North Carolina Journal of Law & Technology. Retrieved from http://www.ncjolt.org/sites/default/files/lindsay_kemp.pdf

Krotoski, M. L. (n.d.). *Effectively using electronic evidence before and at trial* (pp. 67–68).

Krotoski, M. L. (n.d.). *Effectively using electronic evidence before and at trial*. (Multiple citations: pp. 58–61, 66).

Lorraine v. Markel American Insurance Co., 241 F.R.D. 534, 537-38 (D. Md. 2007).

Merle, R., & Vitu, A. (1979). *Traité de droit criminel, Tome II: Procédure pénale* (No. 925).

Migayron, S. (n.d.). *Critères d'appréciation technique, vraies et fausses preuves numériques*. Expert de justice près la Cour d'appel de Paris.

Migayron, S. (n.d.). *Critères d'appréciation technique, vraies et fausses preuves numériques*. Expert de justice près la Cour d'appel de Paris.

Newman, Z. G., & Ellis, A. (2011, January 25). *The reliability, admissibility, and power of electronic evidence*. American Bar Association. Retrieved from https://apps.americanbar.org/litigation/committees/trialevidence/articles/01

2511-electronic-evidence.html

Ngomane, A. R. (2010). *The use of electronic evidence in forensic investigation* (Master's dissertation, University of South Africa). Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/4200/dissertation_ngomane_a.pdf?sequence=1

People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009).

Rubin, J. (2013). *Admissibility of electronic writings: Some questions and answers*. UNC School of Government. Retrieved from http://nccriminallaw.sog.unc.edu/wp-content/uploads/2011/05/Admissibility-of-Electronic-Writings-4-16-13.pdf

Scurmont LLC v. Firehouse Restaurant Group, 2011 U.S. Dist. LEXIS 75715 (D.S.C. July 8, 2011).

Shea v. State of Texas, 167 S.W.3d 98 (Tex. App.–Waco 2005, pet. ref'd). Retrieved from https://casetext.com/case/shea-v-state-1

State ex rel. Leslie v. Ohio Housing Finance Agency, No. 02AP-1147, 2003 Ohio App. LEXIS 5856, at *23 n.1 (Ohio Ct. App. Dec. 9, 2003).

State of Connecticut v. Robert Eleck, SC 18876 (Conn. 2014). Retrieved from http://www.jud.ct.gov/external/supapp/Cases/AROCR/CR314/314CR82.pdf

State v. Williams, 191 N.C. App. 254 (2008). Retrieved from https://casetext.com/case/state-v-williams-2480

Stephen, et al. (1992). *La preuve en procédure pénale comparée: Rapport de synthèse pour les pays de Common Law*. AIDP.

Tippie v. Patník, 2008 Ohio 1653, 2008 Ohio App. LEXIS 1429 (Ohio Ct. App. Apr. 4, 2008).

U.S. v. Siddiqui, 235 F.3d 1318, 1321–1323 (11th Cir. 2000). Retrieved from http://www.americanbar.org/content/dam/aba/publications/litigation_news/united-states-siddiqui.authcheckdam.pdf

United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009). Retrieved from https://www.courtlistener.com/opinion/65821/united-states-v-barlow/

United States v. Finley, 612 F.3d 998, 1000 (8th Cir. 2010). Retrieved from https://casetext.com/case/us-v-finley-10

United States v. Ganier, 468 F.3d 920, 925 (6th Cir. 2006). Retrieved from https://casetext.com/case/us-v-ganier-2

United States v. Jackson, 488 F. Supp. 2d 866, 871 (D. Neb. 2007). Retrieved from https://www.quimbee.com/cases/united-states-v-jackson--4

United States v. Miknevich, 638 F.3d 178, 181 (3d Cir. 2011). Retrieved from

https://casetext.com/case/us-v-miknevich

United States v. Richardson, 607 F.3d 357, 363 (4th Cir. 2010). Retrieved from https://casetext.com/case/us-v-richardson-51

United States v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006). Retrieved from https://casetext.com/case/us-v-safavian-4

United States v. Salcido, 506 F.3d 729 (9th Cir. 2007). Retrieved from https://casetext.com/case/us-v-salcido-5

United States v. Salgado, 250 F.3d 438, 453 (6th Cir. 2001). Retrieved from https://casetext.com/case/us-v-salgado-2

United States v. William Carl Shea, 493 F.3d 1110 (9th Cir. 2007). Retrieved from https://casetext.com/case/us-v-shea-10

Vee Vinhee, 336 B.R. 437, 444-445 (9th Cir. B.A.P. 2005).

Weingartner Lumber & Supply Co. v. Kadant Composites, LLC, No. 2008-225-DCR, 2010 U.S. Dist. LEXIS 24918 (E.D. Ky. Mar. 10, 2010).

Williams v. Long, 585 F. Supp. 2d 679 (D. Md. 2008).