

Digital Proof الإثبات الرقمي

إعداد:
د. أشرف الراعي

LAW637

الماجستير في القانون الرقمي

Lecture 1



Digital Proof

Lecture 1

LAW637
Master of Digital law

Chapter

01

الإثبات الرقمي



في السياقات القانونية، يمكن أن يشير الإثبات الرقمي إلى الأدلة الإلكترونية المقدمة في الإجراءات القانونية. وقد يشمل ذلك المستندات الرقمية أو رسائل البريد الإلكتروني أو غيرها من أشكال الاتصالات الإلكترونية التي تكون بمثابة دليل في القضية المنظورة.



Chapter

01

الإثبات القانوني

يشير الإثبات إلى الأدلة أو الحجج المقدمة لإثبات حقيقة أو إقناع المحكمة بحقيقة شيء ما، وقد يشمل الدليل القانوني شهادة الشهود أو المستندات أو غيرها من أشكال الأدلة.

عادةً ما يكون الإثبات مطلوبًا بموجب المبدأ القانوني المشترك المتمثل في "مسؤولية التحقيق"، مما يعني أن الطرف الذي يقدم المطالبة يتحمل عبء إثبات ذلك.

هناك نوعان رئيسيان من الإثبات في القانون:

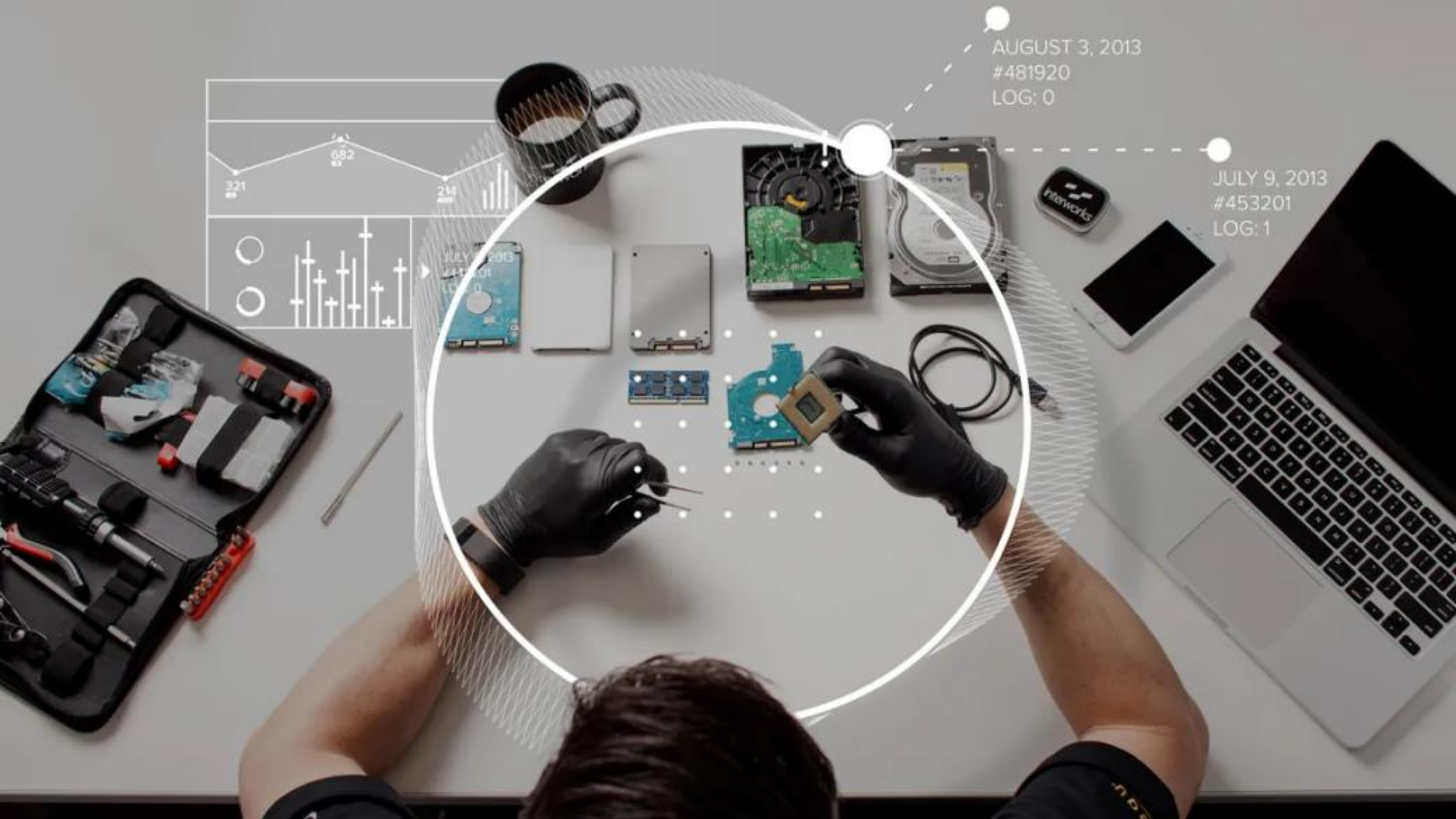
إثبات إيجابي:

يتضمن تقديم أدلة تدعم وتثبت صحة الادعاء أو الحقيقة المزعومة. وفي هذه الحالة، يتعين على الطرف الذي يقدم المطالبة تقديم أدلة كافية لإثبات قضيته.

دليل سلبي:

يتضمن تقديم أدلة تنفي أو تثبت زيف الادعاء أو الحقيقة المزعومة. في بعض الأحيان، قد يحتاج الطرف المعارض للمطالبة أيضًا إلى تقديم أدلة لدعم تحفظاته.

يمكن أن تتخذ الأدلة أشكالاً مختلفة، بما في ذلك الشهادة الشخصية والمستندات وآراء الخبراء والأشياء الملموسة، ويتم تقديمها أمام المحكمة أو الهيئة القانونية ذات الصلة. وقد ينجح الطرف الذي يقدم أدلة قوية ومقنعة في رفع دعوى قضائية أو في الدفاع عن حقوقه.



AUGUST 3, 2013
#481920
LOG: 0

JULY 9, 2013
#453201
LOG: 1

يلعب الإثبات دورًا حاسمًا ومهمًا وأساسياً في العملية القضائية وله أهمية كبيرة في ضمان العدالة واتخاذ القرارات الصحيحة. وفيما يلي بعض الأسباب التي تسلط الضوء على أهمية الإثبات في العملية القضائية:

تحديد الحقائق:

يساعد الإثبات في التعرف على الوقائع والأحداث الحقيقية المتعلقة بالقضية؛ فهو يمكّن الأطراف المعنية والمحكمة من فهم ما حدث بدقة وتقييم الأدلة المقدمة.

تحقيق العدالة:

يشكل الدليل الأساس لاتخاذ قرارات عادلة وعادلة، وعندما يتم تقديم أدلة قوية وقانونية، يمكن للمحكمة أن تتخذ قرارات مبنية على أسس متينة.

أهمية الإثبات في العملية القضائية

تحقيق الشفافية:

يساهم الإثبات في تحقيق الشفافية في العملية القضائية؛ حيث أن وجود نظام قوي لتقديم الأدلة والمطالبات يزيد من الثقة في نظام العدالة.

تشجيع الالتزام بالقانون:

إن وجود نظام إثبات فعال يشجع الأفراد والمؤسسات على الالتزام بالقوانين، فيكون لديهم حافز لتقديم الأدلة التي تثبت امتثالهم للقوانين واللوائح.

حماية الحقوق الفردية:

يعمل الدليل على حماية الحقوق الفردية، ومن خلال نظام إثبات فعال، يمكن للأفراد الدفاع عن حقوقهم وتقديم الأدلة التي تدعم وجهة نظرهم.

تعزيز السلوك الجيد:

إن وجود نظام إثبات يشجع الأفراد والمؤسسات على التصرف بشكل قانوني ومسؤول، مع العلم أنهم قد يحتاجون إلى تقديم الأدلة في حالة حدوث نزاعات.

إذن هذا كله يحقق أهمية الإثبات في العملية القضائية، وبما يحقق:

- تحديد الحقائق
- تحقيق العدالة
- توفير الشفافية
- تشجيع الالتزام بالقانون
- حماية الحقوق الفردية
- تعزيز السلوك الجيد

مع التقدم التكنولوجي، شهدت عملية تقديم الأدلة في الإجراءات القانونية تحولات كبيرة.

وفيما يلي بعض الجوانب التي تعكس كيفية تطور عملية الأدلة مع التقدم التكنولوجي:

Chapter 01

كيف تطورت عملية الإثبات مع التطور التقني؟



الأدلة الرقمية:

ظهرت الأدلة الرقمية مع الاستخدام الواسع النطاق للتكنولوجيا في المجتمع. ويتضمن ذلك البيانات الرقمية مثل رسائل البريد الإلكتروني وسجلات المكالمات وملفات الوسائط المتعددة، وتلعب الأدلة الرقمية دورًا حاسمًا في حالات الجرائم الإلكترونية والتلاعب الرقمي.

التصوير الفوتوغرافي والفيديو:

أصبحت تقنيات التصوير والفيديو وسيلة شائعة لتوثيق الأحداث وتقديم الأدلة في المحكمة. يمكن استخدام تسجيلات الفيديو والصور لتوضيح الظروف المحيطة بحادث ما أو تقديم دليل على سلوكيات معينة.

التكنولوجيا البيومترية:

لقد تطورت تكنولوجيا القياسات الحيوية، مثل تحليل الحمض النووي والأدلة البيومترية الأخرى، لتقديم أدلة قوية في القضايا الجنائية والتحقق من الهوية.

التحقيق الرقمي:

مع التقدم في الطب الشرعي الرقمي، أصبح بإمكان المتخصصين القانونيين الآن استرداد البيانات الرقمية وتحليلها بشكل فعال، مما يسهل تحديد مصادر المعلومات والتحقق من دقتها.

تقنيات الإحصاء الحيوي:

يساعد استخدام تقنيات الإحصاء الحيوي والذكاء الاصطناعي في معالجة كميات هائلة من البيانات لاستخدامها كأدلة. يمكن لهذه التقنيات تحليل الأنماط والعلاقات المتبادلة داخل البيانات.

أدوات الاتصال الرقمي:

تتيح أدوات الاتصال المحسنة، مثل الهواتف الذكية ومنصات التواصل الاجتماعي، للأفراد توثيق الأحداث وتبادل المعلومات بسرعة وكفاءة أكبر.

تعزيز أمن البيانات:

ومع التقدم في تقنيات الأمان، تم تعزيز حماية البيانات والأدلة الرقمية، مما يساعد على منع التلاعب أو التلاعب. وقد أثرت هذه التطورات التكنولوجية بشكل كبير على كيفية تحقيق العدالة وكيفية تقديم الأدلة واستخدامها في العمليات القانونية.



Source: Rocky Mountain

Chapter
01

أنظمة الإثبات



يشير نظام الإثبات في القانون إلى القواعد والمبادئ التي تحدد كيفية تقديم الأدلة واستخدامها في الإجراءات القانونية. ويختلف نظام الإثبات بين الأنظمة القانونية المختلفة، مع وجود اختلافات في القوانين واللوائح المتعلقة بجمع الأدلة وتقديمها. فيما يلي نظرة عامة على بعض أنظمة الإثبات:

(1) نظام إثبات القانون الجنائي:

في القانون الجنائي، يُطلب من النيابة العامة أو السلطات القانونية ذات الصلة تقديم أدلة تثبت ذنب المتهم. القواعد والإجراءات المتعلقة بالإثبات محددة في القوانين الجنائية.

(2) نظام إثبات القانون المدني:

في القانون المدني، يكون الطرف الذي يرفع الدعوى مسؤولاً عن تقديم الأدلة التي تدعم ادعاءاته. قد يكون لأنظمة القانون المدني المختلفة قواعد مختلفة اعتماداً على الإطار القانوني المعمول به.

(3) نظام رجحان الأدلة:

في بعض الأنظمة القانونية، يُطلب من الطرف الذي يملك رجحان الأدلة أن يفوز بالقضية. ويهدف هذا النظام إلى زيادة الإقناع لصالح المطالبات المقدمة.

(4) نظام ميزان الاحتمالات :

في بعض الأنظمة القانونية، يجب على الطرف الذي يرفع الدعوى أن يقدم أدلة ترجح كفة ميزان الاحتمالات لصالحه. ويكون تقدير الأدلة على أساس القيمة والوزن الذي يحدده المحكمون.

(5) نظام إثبات القبول:

وقد يكون الاعتراف أساس الإثبات في بعض الحالات، حيث يتم الاعتماد على إقرار الطرف المعني كدليل قوي على الوقائع.

(6) مبدأ الإثبات العام:

في بعض الأنظمة القانونية، ينص المبدأ العام للإثبات على أن الطرف الذي يقدم المطالبة يجب أن يقدم أدلة تدعم تأكيده.

Chapter

01

عيوب عملية الإثبات الرقمي



لخص آرثر ميللر السلبيات الناتجة عن ظهور أجهزة الكمبيوتر بقوله: "إن الكمبيوتر جهاز نهم في جمع المعلومات الدقيقة، والتي لا يمكن فقدانها إلا عند تعرضها للفيروسات أو البرامج الضارة.

وهذا يمكن أن يقلب الحياة رأساً على عقب عن طريق تحويل العالم إلى عالم شفاف، حيث تكون حياة الناس ومعاملاتهم المالية وحالتهم العقلية ورفاههم الجسدي مكشوفة ليراها الجميع".

تحتوي أنظمة الكمبيوتر بشكل عام على خوادم خاصة يمكن من خلالها تحميل البيانات أو ترحيلها أو توصيلها بمئات الخوادم ومحركات الأقراص الثابتة المتعددة في جميع أنحاء العالم، بالإضافة إلى تركيب أقراص ثابتة متعددة. ولذلك، فإن الوصول إلى هذه البيانات ليس بالضرورة أن يتم من خلال جهاز واحد، أو قرص ثابت واحد، أو هاتف واحد.

يمكن إنشاء اتصال إلكتروني بين مجموعة من الخوادم والأجهزة للوصول إلى معلومات حول فرد تم انتهاك خصوصيته، ويمكن أن يتم ذلك من خلال عدة أفراد وليس شخص واحد فقط أو عدة مؤسسات وليس مؤسسة واحدة فقط، مما يدل على خطورة مثل هذه الإجراءات.

هناك نوعان من أنظمة شبكات نقل البيانات في هذا السياق: شبكات المناطق المحلية (LAN)، والمعروفة أيضًا باسم "الشبكات المحلية"، والشبكات واسعة النطاق (WAN)، وهي "شبكات عالمية أو دولية تمتد لتشمل عددًا كبيرًا من البلدان وربط مجموعة من الشبكات المحلية الموجودة في مختلف أنحاء العالم." تشمل الشبكات الداخلية نوعين من الشبكات الداخلية (الإنترنت): أحدهما يتضمن شبكة معلومات داخل مؤسسة واحدة والآخر (إكسترنال) الذي توسع وامتد ليشمل المستخدمين الخارجيين المصرح لهم من خارج المؤسسة بالوصول إلى استخداماتها.

أعتقد أن عملية جمع الأدلة في شبكات نقل البيانات، وخاصة داخليا في عصرنا الحالي، أصعب مما هي عليه في الشبكات الدولية التي تستخدم الإنترنت، حيث تعمل العصابات الدولية المنظمة. وهذا يثير مسائل قانونية متعددة عند الحصول على البيانات أو المعلومات أو الاتصال من خلالها.

هناك عدة عيوب تتعلق بعملية الأدلة الرقمية:

- (1) التلاعب بالتزوير الرقمي: قد يكون التحقق من صحة البيانات الرقمية أمرًا صعبًا في ظل وجود التزوير الرقمي أو التلاعب. يمكن للأفراد المهرة التعامل مع المعلومات الرقمية لخدمة أهدافهم الشخصية.
- (2) حماية البيانات الشخصية: في بعض الحالات، قد تؤدي عمليات الأدلة الرقمية إلى تسرب البيانات الشخصية أو استخدامها بشكل غير مصرح به، مما يثير مشكلات تتعلق بالخصوصية والأمن.
- (3) تقنيات التشفير: على الرغم من أن تقنيات التشفير قد تكون قوية، إلا أن إثبات البيانات المشفرة قد يكون أمرًا صعبًا، خاصة في حالة فقدان مفاتيح التشفير أو في حالة عدم توفر تقنيات فك التشفير الفعالة.

- (4) التوقيعات الرقمية: على الرغم من فعالية التوقيعات الرقمية في التحقق من هوية الشخص الذي أنشأ الوثيقة الرقمية، إلا أن الإدارة السليمة لمفاتيح التشفير والتوقيع يمكن أن تكون معقدة في بعض الحالات.
- (5) التغيرات التكنولوجية: مع التقدم التكنولوجي، قد تصبح بعض التقنيات الرقمية قديمة أو غير فعالة، مما يفتح الباب أمام تحديات جديدة في عمليات الأدلة الرقمية.
- (6) الفروق القانونية: قد تنشأ تحديات قانونية فيما يتعلق بقبول الأدلة الرقمية في بعض الأنظمة القانونية، حيث قد لا يتم الاعتراف بها بشكل كافٍ أو قد تواجه تحديات في المقبولية القانونية.
- (7) التكلفة والتعقيد: يمكن أن تكون بعض عمليات الأدلة الرقمية مكلفة ومعقدة، خاصة عند استخدام التقنيات المتقدمة والمكلفة، مما قد يقلل من موثوقيتها واعتمادها على نطاق واسع.

Chapter

01

الوسائل الرقمية في التحقيق وجمع الأدلة في جرائم الوسائط الرقمية



وبما أن معظم الجرائم التي ترتكب عبر الأنظمة التكنولوجية والإنترنت والذكاء الاصطناعي يصعب إثباتها، فإنها تتطلب تدخلاً تقنياً عبر مجموعة من الوسائل.

أولاً، تقنيات الذكاء الاصطناعي: يندرج الذكاء الاصطناعي ضمن أحد فروع علوم الحاسوب، ويعتبر ركيزة أساسية في تكنولوجيا العصر الحديث. يمكن تعريف الذكاء الاصطناعي بأنه "قدرة الآلات الرقمية وأجهزة الكمبيوتر على أداء مهام محددة تحاكي وتشبه تلك التي تؤديها كائنات ذكية، مثل القدرة على التفكير أو التعلم من التجارب السابقة أو العمليات العقلية الأخرى. ويهدف الذكاء الاصطناعي إلى تحقيق أنظمة تتمتع بالذكاء، وتتصرف بطريقة تشبه البشر من حيث التعلم والفهم".

وقد استخدمت العديد من الدول مثل هذه الأنظمة والروبوتات لحل المشكلات القانونية المعقدة. وقد قامت وكالات إنفاذ القانون، مثل تلك الموجودة في المملكة المتحدة على المستوى العالمي، والإمارات العربية المتحدة على المستوى العربي، باستخدام هذه الأنظمة بشكل احترافي في عمليات التحقيق والكشف عن الجرائم.

ومن أبرز مميزات أنظمة الذكاء الاصطناعي قدرتها على الوصول إلى نتائج التحقيق وكشف الجرائم دون تدخل بشري، وبالتالي تحقيق نتائج دقيقة في كشف الجرائم والتحقيق فيها وتحديد المجرمين وإحالتهم إلى الجهات القضائية. وتستخدم هذه الأنظمة أيضًا في تنفيذ العقوبات التي يستحقونها. إلا أن هذا المفهوم قد يحتاج إلى سنوات عديدة وتعديلات تشريعية لتتماشى مع التطورات السريعة في أنظمة الذكاء الاصطناعي على مستوى العالم.

ثانياً: برامج التتبع: تلعب برامج التتبع دوراً حاسماً في جريمة انتهاك الخصوصية، نظراً لقدرتها الهائلة على كشف محاولات الاختراق وتعقب المسؤولين عنها. وهذا أمر ضروري في جرائم الإعلام بشكل عام وفي الجرائم التي تشكل انتهاكاً للخصوصية بشكل خاص.

يتكون برنامج التتبع من شاشة رئيسية توفر للمستخدم معلومات محددة وشاملة عن كافة محاولات الاختراق التي يتعرض لها جهازه. ويتضمن اسم الحادثة، ومرتكب الجريمة، والتوقيت، والجهاز موضوع محاولة الاختراق، والرقم التعريفي للجهاز (IP)، وكافة التفاصيل التي تؤدي إلى محاولة الجاني محاولة الاختراق.

وتستخدم برامج التتبع هذه في العديد من المؤسسات الهامة، وخاصة المؤسسات المالية والمصرفية، لأنها تحتوي على معلومات مالية مهمة عن العملاء. يشكل الوصول غير المصرح به إلى هذه المعلومات انتهاكاً لخصوصيتهم ويمكن استخدامه للتشهير من خلال وسائل الإعلام. وقد تستغل المنظمات الإجرامية الدولية أيضاً هذه البرامج.

ثالثاً: برامج البريد الإلكتروني والدردشة: يعد البريد الإلكتروني أداة رقمية مهمة في التحقيق وجمع الأدلة في جرائم انتهاك الخصوصية عبر الوسائل التكنولوجية الحديثة.

فهو يحتوي على معلومات حول المرسل والمستقبل، مما يجعله مكاناً لجرائم القرصنة. تم إنشاء البنية التحتية للبريد الإلكتروني في أوائل الثمانينيات من خلال توجيه الرسائل ومعالجتها. الأمر نفسه ينطبق على برامج الدردشة.

رابعاً، أنظمة كشف التسلل "الوكلاء": يعمل الوكلاء كوسطاء بين الشبكة والمستخدم، ويتم التحقق منها بواسطة نظام التخزين المؤقت مما يضمن تنزيل الصفحة من قبل المستخدم. لذلك، يلعب الوكلاء دوراً مهماً في الأدلة من خلال فحص العمليات المخزنة.

أما أنظمة كشف التسلل فتقوم بمراقبة بعض العمليات التي يتم تنفيذها عبر الإنترنت أو على أجهزة الكمبيوتر من خلال تحليل حزم البيانات. تعتبر أنظمة كشف التسلل حاسمة في التحقيق وجمع الأدلة حول كيفية إدخال الأنظمة واختراقها في عمليات تهدف إلى الحصول على المعلومات والبيانات الشخصية، مما يشكل انتهاكاً للخصوصية.

خامساً: نظام Honeypot: يعتبر نظام Honeypot (نظام جرة العسل) من أهم الأنظمة التكنولوجية في التحقيق وجمع الأدلة في الجرائم التكنولوجية بشكل عام.

يقوم هذا النظام باعتراض الهجمات عبر شبكة الويب العالمية وتحليل بيانات الهجوم نفسه، والأنظمة التكنولوجية المستخدمة في عملية الاختراق، مما يؤدي في النهاية إلى تحديد الجريمة.

سادسا، أدوات التحكم وأدوات فحص ومراقبة الشبكة: تعمل برامج التحكم على تنظيم عملية الاختراق، مما يجعلها مهمة ليس فقط في التحقيق وجمع الأدلة ولكن أيضا في التحقيق الأولي.

وفيما يتعلق بأدوات فحص ومراقبة الشبكة، فإنها تقوم بفحص ما إذا كانت الشبكة نفسها قد تعرضت لعمليات اختراق وتحديد المشكلات الفنية التي تؤثر على الشبكات.



نظام الأدلة الرقمية هو نهج يستخدم التكنولوجيا الرقمية لتأكيد وثيقة أو حقيقة. ويُشار إلى هذا النوع من الأدلة أيضًا باسم "الأدلة الإلكترونية" أو "الأدلة الرقمية". وفي سياق الإثبات، يعتبر الدليل الرقمي وسيلة فعالة لتأكيد صحة أو حقيقة شيء ما.

ويمكن أن تشمل الأدلة الرقمية عناصر مختلفة، بما في ذلك:

1- التوقيع الرقمي: تتيح التوقيعات الرقمية للأفراد أو المؤسسات التوقيع على المستندات الإلكترونية بطريقة تؤكد هوية الموقع وسلامة الوثيقة.

2- الطابع الزمني الرقمي: يثبت الطابع الزمني الرقمي الوقت الذي تم فيه إنشاء الملف أو المستند أو تعديله، مما يعزز التصديق الزمني له.

3- التشفير: يمكن استخدام التشفير لتأمين المعلومات والتأكد من سريتها وسلامتها أثناء نقلها أو تخزينها.

4- سجلات الأنشطة الرقمية: تسجل سجلات الأنشطة الرقمية المختلفة، مثل تسجيل الدخول والمعاملات، ويمكن استخدامها كدليل لمتابعة تسلسل الأحداث.

5- الشهادات الرقمية: تستخدم للتحقق من هوية الكيان الرقمي ودقة المعلومات المرتبطة به.

6- الصور الرقمية وملفات الوسائط المتعددة: يمكن استخدام الصور الرقمية ومقاطع الفيديو كدليل وتحليلها للتحقق من صحة الحدث المسجل.

7- قواعد البيانات الرقمية وسجلات النظام: يمكن أن توفر سجلات النظام وقواعد البيانات دليلاً قوياً على الأنشطة والتغيرات في النظام.

8 - التجزئة الرقمية: يمكن استخدام التجزئة الرقمية للتحقق من سلامة الملفات والتأكد من عدم التلاعب بها.

Chapter
01

الأدلة العلمية الرقمية



تشير الأدلة العلمية الرقمية إلى الأدلة التي تعتمد على التقنيات الرقمية وتكنولوجيا المعلومات لتقديم الدعم للحجج العلمية أو القانونية. تشمل هذه الأنواع من الأدلة مجموعة واسعة من العناصر التي يمكن استخدامها لإثبات الحقائق أو الظواهر بطريقة علمية أو قانونية.

وتتضمن بعض الأمثلة على الأدلة العلمية الرقمية ما يلي:

- 1- تحليل البيانات الرقمية: ويتضمن ذلك فحص البيانات الرقمية لفهم الأنماط والاتجاهات والعلاقات داخل البيانات.
- 2- نتائج التجارب الرقمية: استخدام التكنولوجيا لإجراء التجارب وتحليل النتائج رقمياً.
- 3- النماذج الرياضية والمحاكاة: استخدام النماذج الرياضية وبرامج المحاكاة لتحليل سلوك الظواهر.
- 4- تحليل الصور الرقمية: توظيف تقنيات تحليل الصور لاستخلاص المعلومات من الصور الرقمية.

5- التقارير الرقمية والوثائق الإلكترونية: استخدام الوثائق الرقمية والتقارير الإلكترونية كأدلة علمية.

6- تحليل بيانات الاستشعار الرقمي: استخدام بيانات الاستشعار الرقمي لفحص وفهم الظواهر البيئية.

7- النماذج الإحصائية: استخدام الإحصائيات الرقمية لتحليل وتفسير البيانات.

8- البحث الرقمي: إجراء البحوث باستخدام الوسائل الرقمية وتحليل النتائج رقمياً.

الإثبات هو نشاط إجرائي يهدف مباشرة إلى الوصول إلى اليقين القضائي وفق معيار الحقيقة الموضوعية، فيما يتعلق باتهام أو أي تأكيد أو نفي لفعل معين يخضع لإجراء قضائي.

الأدلة الرقمية هي جزء من الإثبات الجنائي والمدني، ويعني إثبات الفعل الذي ارتكبه الفاعل أو الفاعل أو من ارتكب الفعل، بغض النظر عن وصف الفاعل.

الهدف العام من الإثبات، والهدف الخاص من الإثبات الرقمي، هو بيان مدى التوافق بين النموذج القانوني للجريمة والحادث المزعوم. يستخدم القاضي وسائل رقمية محددة في عملية إثبات الحقيقة.

نكون قد وصلنا إلى نهاية هذه المحاضرة التي أتمنى أن تكونوا قد استفدتم منها. ناقشنا العديد من المواضيع المهمة، حيث تعرفنا على مفهوم الإثبات والإثبات الرقمي وأهميته، والدليل الرقمي، والدليل الرقمي العلمي، والعديد من التفاصيل الأخرى المرتبطة بشكل مباشر أو غير مباشر بعملية الإثبات

شكراً لكم